PMATH 145 - Introduction to Number Theory

1 Greatest Common Divisor

Lecture 1 Wed 09/06

Number theory is in some sense about the interplay between addition and multiplication. The theorems tend to be very innocent looking but the proofs tend to involve every branch of pure mathematics. For example, Fermat's Last Theorem states that the equation $x^n + y^n = z^n$ has no nonzero integers solutions when $n \geq 3$. The proof by Wiles and Taylor almost 30 years ago uses techniques from geometry, topology, analysis and algebraic number theory. Some examples of innocent looking but unsolved conjectures include Landau's four problems about primes:

- (Goldbach) Every even integer at least 4 is a sum of two primes.
- (Twin prime) There are infinitely many primes p such that $p + 2$ is prime.
- (Legendre) For any positive integer n, there is a prime between n^2 and $(n + 1)^2$.
- (Bunyakovsky) There are infinitely many integers n such that $n^2 + 1$ is prime.

The motivating problem for the first three quarters of this course will be the following result of Dirichlet.

Theorem 1.1 *Suppose a and m are coprime integers. Then there are infinitely many integers k such that $mk + a$ is a prime.*

We will give proofs of this result for various values of a and m and in the process discuss many abstract ideas in mathematics. You will encounter these ideas again in PMATH 347, 348, 440, 441.

In the beginning, there was nothing. Then god said, let there be 1. There is not much one can do with just 1, so addition was added. We can then **define** 2 as $1 + 1$ and then $3 = 1 + 2$. We now have two choices for the next number, as $1 + 3$ or as $2 + 2$. Note that

$$1 + 3 = 1 + (1 + 2), \qquad 2 + 2 = (1 + 1) + 2.$$

By requiring that addition is associative, we have that these two numbers are equal and we call it 4. Continuing forever gives the set of natural numbers

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

We may view the addition $n + m$ as adding 1 to n a total of m times.

In order to reverse the process of addition, we need a number that adds 1 to give 1. This number is called 0. Continuing lowering the numbers gives the usual subtraction and expands our set of numbers to the set of integers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Another familiar operation now appears. We can define multiplication $n \times m$ as adding n to 0 a total of m times if $m \geq 0$ and as adding $-n$ to 0 a total of $-m$ times if $m < 0$. The set $\mathbb{Z}$ along with $+, -, \times, 0, 1$ with the usual laws of arithmetic is a **commutative ring**.

In order to reverse the process of multiplication, namely division, the set of rational numbers

$$\mathbb{Q} = \{\frac{a}{b} \colon a, b \in \mathbb{Z}, b \neq 0\}$$

naturally appears. This process in general is called taking the **field of fractions**. The next set up is the set $\mathbb{R}$ of real numbers, which is the **completion** of $\mathbb{Q}$. In other words, one can think of real numbers as limits of sequences of rational numbers that should converge. For example, the sequence $3, 3.1, 3.14, 3.141, 3.1415, \ldots$ should converge and its limit is π. The sequence $1, -1, 1, -1, \ldots$ shouldn't converge because it keeps fluctuating. "Should converge" roughly means that if you go far out enough, any two terms are close enough. The precise terminology is **Cauchy sequence**, which you will learn in MATH 147. Note here we say two numbers a, b are close if the absolute value $|a - b|$ is small. There are other absolute values that people consider in number theory using prime factorizations, leading to other completions $\mathbb{Q}_p$ of $\mathbb{Q}$.

Finally the set $\mathbb{R}$ is not "complete" in the algebraic sense. There are polynomial equations with coefficients in $\mathbb{R}$ that don't have solutions. For example $x^2 + 1 = 0$ has no solutions in $\mathbb{R}$. Adding, or more precisely adjoining, $\sqrt{-1}$ to $\mathbb{R}$, gives the set $\mathbb{C}$ of complex numbers. The quadratic formula then allows us to solve quadratic equations in $\mathbb{C}$. It is only until the 16th century when people wanted to solve cubic equations that we finally sat down to understand how complex numbers work. Around 1800, the Fundamental theorem of Algebra was proved, which states that every non-constant polynomial equation with coefficients in $\mathbb{C}$ has a solution in $\mathbb{C}$. We say $\mathbb{C}$ is **algebraically closed**.

At this point, our number system is complete in both analytic and algebraic senses. This is also the reason why you don't hear "breaking news: mathematicians discovered new numbers". If we start relaxing the laws of arithmetic, we get the Quarternions where multiplication isn't commutative, or Octonions where multiplication also isn't associative.

Proposition 1.2 *The set $\mathbb{N}$ is well-ordered. In other words, every non-empty subset has a smallest element.*

Proof: Let S be a non-empty subset of $\mathbb{N}$. Let $n \in S$ be an element. Let $T = \{x \in S \colon x \leq n\}$. Then T is a non-empty finite set and thus has a smallest element n_0. For any $x \in S$, if $x > n$, then $x > n \geq n_0$; if $x \leq n$, then $x \in T$ and so $x \geq n_0$. Therefore, n_0 is the smallest element of S. □

Corollary 1.3 *The set $\mathbb{N} \cup \{0\}$ is well-ordered.*

Corollary 1.4 *(Induction) For any $n \in \mathbb{N}$, let $P(n)$ be a statement such that the following are true:*

1. *$P(1)$ is true,*
2. *$(P(1) \wedge \cdots \wedge P(n-1)) \Rightarrow P(n)$ is true for all integers $n \geq 2$.*

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof: Let S be the set of natural numbers n such that $P(n)$ is false. If S is empty, then we are done. Suppose for a contradiction that S is non-empty. Let $m \in S$ be its smallest element. Since $P(1)$ is true, we know that $m \neq 1$ and so $m \geq 2$. Since m is the smallest element of S, we know that $P(1), \ldots, P(m-1)$ are all true, but then by property 2, we have $P(m)$ is true. Contradiction. □

Remark: There are variant forms where multiple base cases are needed or where the starting point is > 1.

Proposition 1.5 *(Division algorithm) Let a, b be integers such that $a > 0$. Then there exists integers q, r such that*

$$b = aq + r, \qquad 0 \leq r < a.$$

Proof: Consider the set $S = \{b - ak \colon k \in \mathbb{Z}, b - ak \geq 0\}$. By taking $k = -|b|$, we have since $a \geq 1$,

$$b - ka = b + |b|a \geq b + |b| \geq 0.$$

Hence $S \subseteq \mathbb{N} \cup \{0\}$ is non-empty. Let $r \in S$ be its smallest element. Then $r = b - ak$ for some $k \in \mathbb{Z}$ and $r \geq 0$. Let $q = k$ so that $b = aq + r$. It remains to prove that $r < a$. Suppose for a contradiction that $r \geq a$. Then $r - a \geq 0$ and $r - a = b - ak - a = b - a(k+1) \in S$. However, $r - a < r$ contradicting the minimality of r. $\square$

Remark: The integers q, r are unique and are called the quotient and remainder when b is divided by a. We also have the division algorithm for negative a. In general, we have

$$\exists q, r \in \mathbb{Z}, \quad b = aq + r \text{ and } 0 \leq r < |a|.$$

Suppose we are given two integers a, b not both 0. Suppose WLOG that $a \neq 0$. Consider

$$S = \{ax + by \colon x, y \in \mathbb{Z}, ax + by > 0\}.$$

If $a > 0$, then $a = a(1) \in S$. If $a < 0$, then $-a = a(-1) \in S$. Hence S is non-empty. Let d be the smallest element of S. Write $d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$.

Lemma 1.6 *The number d divides every element of the form $ax + by$ where $x, y \in \mathbb{Z}$. In particular, $d \mid a$ and $d \mid b$.*

Proof: Let $c = ax_1 + by_1$ be an arbitrary element with $x_1, y_1 \in \mathbb{Z}$. Suppose for a contradiction that $d \nmid c$. Applying the division algorithm gives $q, r \in \mathbb{Z}$ such that $c = dq + r$ with $0 \leq r < d$. The assumption that $d \nmid c$ implies that $r \neq 0$. So $r > 0$. Now

$$r = c - dq = ax_1 + by_1 - (ax_0 + by_0)q = a(x_1 - x_0 q) + b(y_1 - y_0 q).$$

Since $r > 0$, we have $r \in S$, but this contradicts the minimality of d. $\square$

Lemma 1.7 *Any common divisor of a, b divides d. In other words, $d = \gcd(a, b)$ is the **greatest common divisor** of a and b.*

Proof: If $e \mid a$ and $e \mid b$, then $e \mid ax_0 + by_0$. So $e \mid d$. $\square$

We define $\gcd(0, 0) = 0$ so that $\gcd(0, a) = |a|$ for any $a \in \mathbb{Z}$.

Corollary 1.8 *(Bezout's Lemma) Let a, b be integers. Then there exist integers x, y such that $\gcd(a, b) = ax + by$.*

Corollary 1.9 *Let a, b be integers. Then there exist integers x, y such that $ax + by = 1$ if and only if $\gcd(a, b) = 1$. We say a and b are **coprime**.*

Proof: ($\Leftarrow$) follows immediately from Bezout's lemma. For ($\Rightarrow$), we have $1 \in S$ and so is its smallest element, implying that $\gcd(a, b) = 1$. $\square$

Example: (Easiest IMO problem 1959P1) Prove that for any integer n,

$$\gcd(14n + 3, 21n + 4) = 1.$$

Follows immediately from

$$3(14n + 3) + (-2)(21n + 4) = 1.$$

Lecture 2 Fri 09/08

Proposition 1.10 *Let a, b, c be integers such that $\gcd(a, c) = 1$. Then $\gcd(c, ab) = \gcd(c, b)$. In particular,*

$$c \mid ab \iff \gcd(c, ab) = c \iff \gcd(c, b) = c \iff c \mid b.$$

Proof: We note that it suffices to prove that

(a) $\gcd(c, b) = cx + aby$ for some $x, y \in \mathbb{Z}$,

(b) $\gcd(c, ab) = cx + by$ for some $x, y \in \mathbb{Z}$.

Indeed, they would imply that $\gcd(c, ab) \mid \gcd(c, b)$, and $\gcd(c, b) \mid \gcd(c, ab)$, and so $\gcd(c, ab) = \gcd(c, b)$ because they are both non-negative.

Statement (b) is obvious. We know $\gcd(c, ab) = cx_0 + aby_0$ for some $x_0, y_0 \in \mathbb{Z}$. So $x = x_0$ and $y = by_0$ do the job. For statement (a), we have

$$\begin{aligned} \gcd(c, b) &= cx_1 + by_1 \\ 1 &= cx_2 + ay_2 \end{aligned}$$

for some integers x_1, y_1, x_2, y_2. Multiply them to get

$$\gcd(c, b) = c(cx_1x_2 + ax_1y_2 + bx_2y_1) + ab(y_1y_2).$$

We take $x = cx_1x_2 + ax_1y_2 + bx_2y_1$ and $y = y_1y_2$. □

We can similarly prove that the greatest common divisor $\gcd(a, b, c)$ of three integers a, b, c (that are not all 0) is the smallest positive integer of the form $ax + by + cz$. Exercise: prove that

$$\gcd(a, b, c) = \gcd(a, \gcd(b, c)).$$

Last time, we give an interpretation of $\gcd(a, b)$ as the smallest positive integer that can be written as an integer combination of a and b. For computational purposes, this is pretty useless.

Proposition 1.11 *Let a, b, q be integers. Then* $\gcd(a, b) = \gcd(a, b - aq)$.

Proof: As we saw last time, to prove $\gcd(a, b) = \gcd(c, d)$, it suffices to prove $\gcd(a, b) = cx + dy$ for some $x, y \in \mathbb{Z}$ and $\gcd(c, d) = ax + by$ for some $x, y \in \mathbb{Z}$. This is obvious in this case. □

Euclidean algorithm: By swapping a and b, we may assume $|b| \geq |a|$. If $|b| = |a|$ or if $|a| = 0$, then $\gcd(a, b) = |b|$. Suppose $|b| > |a| > 0$. Then there is a very natural choice of q, namely the quotient when b is divided by a, in which case $b - aq$ equals the remainder, which is less than $|a|$. We then repeat this process.

Note that the above formula holds without requiring q to be the remainder when b is divided by a. For example,

$$\gcd(14n + 3, 21n + 4) = \gcd(14n + 3, 21n + 4 - (14n + 3)) = \gcd(14n + 3, 7n + 1)$$

and

$$\gcd(14n + 3, 7n + 1) = \gcd(14n + 3 - (7n + 1)2, 7n + 1) = \gcd(1, 7n + 1) = 1.$$

Example: How many elements does the following set have?

$$S = \{\gcd(506 - n^2, 506 - (n + 1)^2) \colon n \in \mathbb{Z}\}.$$

We have

$$\gcd(506 - n^2, 506 - (n + 1)^2) = \gcd(506 - n^2, 506 - n^2 - 2n - 1) = \gcd(506 - n^2, 2n + 1).$$

Note that $\gcd(2, 2n + 1) = 1$ since $2n + 1$ is not divisible by 2. Hence, we have

$$\begin{aligned} \gcd(506 - n^2, 2n + 1) &= \gcd(2(506 - n^2), 2n + 1) \\ &= \gcd(1012 - 2n^2 + (2n + 1)n, 2n + 1) \\ &= \gcd(1012 + n, 2n + 1) \\ &= \gcd(1012 + n, (2n + 1) - 2(1012 + n)) \\ &= \gcd(1012 + n, 2023). \end{aligned}$$

Now $\gcd(1012+n, 2023)$ is a non-negative divisor of 2023. Conversely, given any non-negative divisor d of 2023, by taking $n = d - 1012$, we have $\gcd(1012+n, 2023) = \gcd(d, 2023) = d$. In other words, S is the set of positive divisors of 2023. The prime factorization of 2023 is 7×17^2. Hence 2023 has 6 positive divisors:

$$1, \quad 17, \quad 17^2, \quad 7, \quad 7 \times 17, \quad 7 \times 17^2.$$

Exercises

1.1 Prove that the set $\mathbb{Z}$ with the usual order is not well-ordered.

1.2 Prove that the set $\mathbb{Q}^{\geq 0}$ of non-negative rational numbers with the usual order is not well-ordered.

1.3 Prove that that any finite subset of $\mathbb{R}$ with the usual order is well-ordered.

1.4 (Uniqueness of division algorithm) Given integers a, b such that $a \neq 0$, prove that the integers q, r such that $b = aq + r$ and $0 \leq r < |a|$ are unique.

1.5 Prove that if $a, b, c \in \mathbb{Z}$ such that $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.

1.6 Given $a, b, c \in \mathbb{Z}$ that not all 0, let $\gcd(a, b, c)$ be the smallest positive integer of the form $ax + by + cz$. Prove that $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$.

1.7 Let a, b, c, d be nonzero integers such that $ad - bc = \pm \gcd(a, c)$. Prove that $\gcd(an + b, cn + d) = 1$ for every integer n.

1.8 Find an example for $a, b, c, d \in \mathbb{Z}$ such that $\gcd(an + b, cn + d) = 1$ for every integer n but $ad - bc \neq \pm \gcd(a, c)$.

2 Prime factorization

A **prime** is an integer $p > 1$ such that its only positive divisors of 1 and p. For any integer a,

$$\gcd(p, a) = \begin{cases} 1 & \text{if } p \nmid a, \\ p & \text{if } p \mid a. \end{cases}$$

Proposition 2.1 *(Euclid's Lemma) Let p be a prime. Then for any integers a, b, if $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof: Suppose $p \nmid a$. Then $\gcd(p, a) = 1$. Then from $p \mid ab$, we get $p \mid b$. □

The converse of Euclid's Lemma is also true:

Proposition 2.2 *Let $n > 1$ be an integer such that whenever n divides a product of integers, n must divide one of the factors. Then n is a prime.*

Proof: Let $d \mid n$ be a positive divisor of n. Then $n = de$ for some $e \in \mathbb{Z}$. Since $d, n > 0$, we have $e > 0$ and $e \mid n$. From $n \mid de$, we get $n \mid d$ or $n \mid e$. If $n \mid d$, then along with $d \mid n$, we get $d = n$. If $n \mid e$, then along with $e \mid n$, we get $e = n$ and so $d = 1$. □

Remark: The proof of EL⇒prime uses only division, whereas the proof of prime⇒EL requires the theory of gcd. There are number systems in general where the notion of gcd doesn't exist, or worse where unique factorization doesn't hold.

Theorem 2.3 *(Fundamental Theorem of Arithmetic) Every positive integer can be written as a product of primes, unique up to reordering.*

For any prime p and any integer $n \neq 0$, we define $\nu_p(n)$ to be the largest integer k such that $p^k \mid n$. A commonly used notation is

$$p^{\nu_p(n)} \,||\, n.$$

Alternatively, $\nu_p(n)$ is the unique non-negative integer k such that

$$p^k \mid n \qquad \text{and} \qquad p \nmid \frac{n}{p^k}.$$

We use the convention $\nu_p(0) = \infty$.

Proposition 2.4 *Let p be any prime and let n, m nonzero integers. Then*

$$\nu_p(nm) = \nu_p(n) + \nu_p(m), \qquad \nu_p(n+m) \geq \min\{\nu_p(n), \nu_p(m)\}.$$

If $\nu_p(n) \neq \nu_p(m)$, then

$$\nu_p(n+m) = \min\{\nu_p(n), \nu_p(m)\}.$$

Proof: Let $k = \nu_p(n)$ and $\ell = \nu_p(m)$. From $p^k \mid n$ and $p^\ell \mid m$, we have $p^{k+\ell} \mid nm$. From $p \nmid n/p^k$ and $p \nmid m/p^\ell$, we have $p \nmid nm/p^{k+\ell}$ by the contrapositive of EL. Therefore, $\nu_p(nm) = k + \ell$.

Suppose WLOG that $k \leq \ell$. Then $p^k \mid p^\ell$ and so $p^k \mid m$. Since $p^k \mid n$, we have $p^k \mid n + m$. Thus $\nu_p(n+m) \geq k$. Suppose $k < \ell$. Then $p \mid m/p^k$ but $p \nmid n/p^k$. Hence $p \nmid (n+m)/p^k$. So $\nu_p(n+m) = k$. □

Lecture 3 Mon 09/11

It then follows by induction on ℓ that for any $\ell \in \mathbb{N}$ and nonzero integers $n_1, \ldots, n_\ell$, we have

$$\nu_p(n_1 \cdots n_\ell) = \nu_p(n_1) + \cdots + \nu_p(n_\ell).$$

Note that for primes p, q we have $\nu_p(q) = 0$ for $p \neq q$ and $\nu_p(p) = 1$. Hence, we have the following result.

Corollary 2.5 *Let n_q be non-negative integers for primes q such that all but finitely many of them are 0. Then for any prime p,*

$$\nu_p\left(\prod_q q^{n_q}\right) = n_p.$$

In particular, prime factorizations are unique. (Unless otherwise specified, a sum or product over an index p or q is running only over primes p.)

We prove next the existence of prime factorization.

Theorem 2.6 *Let $n \in \mathbb{N}$. Then $\nu_p(n) = 0$ for all but finitely many primes p and*

$$n = \prod_p p^{\nu_p(n)}.$$

In particular, prime factorizations exist.

Proof: If $p > n$, then clearly $p \nmid n$ and so $\nu_p(n) = 0$. We prove the second statement by induction on n. Suppose first that $n = 1$. Then $\nu_p(1) = 0$ for all primes p and $\prod_p p^0 = 1$.

Suppose now $n \geq 2$ and $n = q$ is a prime. In this case,

$$\prod_p p^{\nu_p(q)} = q^1 \prod_{p \neq q} p^0 = q.$$

Suppose now $n \geq 2$ and n is not a prime. Let d be a positive divisor of n with $1 < d < n$. Let $e = n/d$. Then $1 < e < n$. By induction, we have

$$d = \prod_p p^{\nu_p(d)}, \qquad e = \prod_p p^{\nu_p(e)}.$$

Multiplying them gives

$$n = de = \prod_p p^{\nu_p(d)+\nu_p(e)} = \prod_p p^{\nu_p(n)}$$

since $\nu_p(d) + \nu_p(e) = \nu_p(de) = \nu_p(n)$. □

We can extend ν_p to all rational numbers by defining $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$. The multiplicative property of ν_p implies that if $a/b = c/d$, then $ad = bc$ and so $\nu_p(a) + \nu_p(d) = \nu_p(b) + \nu_p(c)$. In other words,

$$\nu_p(a) - \nu_p(b) = \nu_p(c) - \nu_p(d).$$

Hence $\nu_p(a/b)$ is independent on the choices of a and b.

Corollary 2.7 *Let $r \in \mathbb{Q}$ be nonzero. Then $r = \pm \prod_p p^{\nu_p(r)}$. Moreover,*

1. *$r \in \mathbb{Z}$ if and only if $\nu_p(r) \geq 0$ for all primes p;*
2. *$r = \pm 1$ if and only if $\nu_p(r) = 0$ for all primes p.*

Corollary 2.8 *Let d, n be nonzero integers. Then $d \mid n$ if and only if $\nu_p(d) \leq \nu_p(n)$ for all primes p.*

Proof: We have $d \mid n$ if and only if $n/d \in \mathbb{Z}$ if and only if $\nu_p(n/d) = \nu_p(n) - \nu_p(d) \geq 0$ for all primes p. □

Corollary 2.9 *Let n be a nonzero integer. Then the number of positive divisors of n is*

$$\prod_p (1 + \nu_p(n)).$$

Proof: Any positive divisor d is uniquely determined by $\nu_p(d)$ for all primes p. There are $1 + \nu_p(n)$ possible values for $\nu_p(d)$ in order for $\nu_p(d) \leq \nu_p(n)$. □

Corollary 2.10 *Let n, m be nonzero integers. Then for any prime p,*

$$\nu_p(\gcd(n, m)) = \min\{\nu_p(n), \nu_p(m)\}.$$

Proof: Since $\gcd(n, m)$ divides n and m, we see that for any prime p, $\nu_p(\gcd(n, m)) \leq \nu_p(n)$ and also $\leq \nu_p(m)$. Hence $\nu_p(\gcd(n, m)) \leq \min\{\nu_p(n), \nu_p(m)\}$. For the other inequality, let $d_p = \min\{\nu_p(n), \nu_p(m)\}$. Note that $d_p = 0$ for $p > \max\{n, m\}$. We let $d = \prod_p p^{d_p}$. From $d_p \leq \nu_p(n)$ for all p, we get $d \mid n$ and similarly $d \mid m$. Hence $d \mid \gcd(n, m)$ and so $d_p \leq \nu_p(\gcd(n, m))$ for all primes p. □

Similarly for nonzero integers x, y, z, we have

$$\nu_p(\gcd(x, y, z)) = \min\{\nu_p(x), \nu_p(y), \nu_p(z)\}.$$

A related concept is the least common multiple $\mathrm{lcm}(m, n)$ of two integers m, n, or of multiple integers. One easily checks that

$$\nu_p(\mathrm{lcm}(n, m)) = \max\{\nu_p(n), \nu_p(m)\}.$$

Since

$$\min\{a, b\} + \max\{a, b\} = a + b,$$

we get

$$\gcd(n, m)\mathrm{lcm}(n, m) = nm.$$

Exercises

2.1 Prove Proposition 1.10 using ν_p: Let a, b, c be integers such that $\gcd(a, c) = 1$. Then $\gcd(c, ab) = \gcd(c, b)$

2.2 Prove Exercise 1.5 using ν_p: If $a, b, c \in \mathbb{Z}$ such that $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.

2.3 Let $k \in \mathbb{N}$. Prove that $n \in \mathbb{N}$ is a perfect k-th power (that is, $n = m^k$ for some $m \in \mathbb{N}$) if and only if $k \mid \nu_p(n)$ for any prime p.

2.4 Prove that if $x, y \in \mathbb{N}$ are coprime and $k \in \mathbb{N}$ such that xy is a perfect k-th power, then x and y are both perfect k-th powers.

2.5 Prove that the equation $x^2 = 2y^2$ has no non-zero integer solutions. This implies that $\sqrt{2}$ is irrational.

2.6 Prove that the equation $2^x = 3^y$ has no positive integer solutions. This implies that $\log_2 3$ is irrational.

2.7 Let p be a prime. Define $|r|_p$ for any nonzero $r \in \mathbb{Q}$ by $|r|_p = p^{-\nu_p(r)}$ and define $|0|_p = 0$. Then for any $r, s \in \mathbb{Q}$, prove that

(a) $|rs|_p = |r|_p |s|_p$,

(b) $|r + s|_p \leq \max\{|r|_p, |s|_p\} \leq |r|_p + |s|_p$.

In other words, $|.|_p$ behaves similar to the usual absolute value, and is called the p-adic absolute value.

2.8 Prove that the equation $x^3 = 2y^3 + 4z^3$ has no non-zero integer solutions.

3 Prime counting function

The number

$$L_n = \operatorname{lcm}(1, 2, \ldots, n)$$

is closely related to the prime counting function. Let p be any prime. Let k be a nonnegative integer such that $p^k \leq n < p^{k+1}$. Then no integer from 1 to n is divisible by p^{k+1} and $p^k \leq n$ with $\nu_p(p^k) = k$. In other words

$$\nu_p(L_n) = \max\{\nu_p(1), \ldots, \nu_p(n)\} = k = \left\lfloor \frac{\log n}{\log p} \right\rfloor,$$

which is also the number of integers from 1 to n that are powers of p. We define the von Mangoldt function

$$\Lambda(m) = \begin{cases} \log p & \text{if } m \text{ is a positive power of a prime } p \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\log L_n = \sum_{p \leq n} \left\lfloor \frac{\log n}{\log p} \right\rfloor \log p = \sum_{m \leq n} \Lambda(m) =: \psi(n),$$

is the Chebyshev's ψ-function.

Theorem 3.1 *(Prime number theorem) We have*

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1.$$

As a consequence, we have $L_n \sim e^n$.

Lecture 4 Wed 09/13

You might be more familiar with the Prime number theorem stated in terms of the prime counting function $\pi(x)$ which counts the number of primes less than or equal to x. From the trivial bound

$$\left\lfloor \frac{\log n}{\log p} \right\rfloor \leq \frac{\log n}{\log p},$$

we see that $\psi(n) \leq \pi(n) \log n$.

Theorem 3.2 *The Prime number theorem is equivalent to*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

The other inequality needs a bit of estimate. See below for a proof of the equivalence of Theorems 3.1 and 3.2.

You will also prove in HW2 a lower bound for L_n of the form

$$L_n \geq 2^n$$

for $n \geq 7$, which will then give a lower bound for $\pi(x)$ of the form $C_1 x/\log x$ for some constant $C_1 > 0$. We will prove next that

$$L_n \leq 4^{n-1}$$

which gives an upper bound of $\pi(x)$ of the form $C_2 x/\log x$ for some constant $C_2 > 0$.

Exercises

3.1 For any $n \in \mathbb{N}$, we use the notation $\sum_{d|n}$ to denote a sum over the positive divisors of n. Prove that

$$\sum_{d|n} \Lambda(d) = \log n.$$

3.2 Compute L_{126}/L_{120} and L_{145}/L_{135}.

This following subsection is only for personal entertainment and will not be covered in class or the exam.

A very sketchy sketch of the proof of the prime number theorem

We prove first the following comparison between $\psi(x)$ and $\pi(x)$:

$$\frac{\pi(x)}{x/\log x}\left(1 - \frac{\log\log x + \log\log\log x}{\log x}\right) - \frac{1}{\log\log x} \leq \frac{\psi(x)}{x} \leq \frac{\pi(x)}{x/\log x}.$$

Then by taking limit as $x \to \infty$, we have the equivalence of Theorems 3.1 and 3.2 by the Squeeze Theorem. The upper bound was already proved. For the lower bound, let

$$\theta_1(x) = \sum_{x/(\log x \cdot \log\log x) \leq p \leq x} \log p \leq \psi(x).$$

We can now bound $\theta_1(x)$ from below by

$$\begin{aligned}
\theta_1(x) &\geq \sum_{x/(\log x \cdot \log\log x) \leq p \leq x} \log\left(\frac{x}{\log x \log\log x}\right) \\
&= \sum_{p \leq x} \log\left(\frac{x}{\log x \log\log x}\right) - \sum_{p < x/(\log x \cdot \log\log x)} \log\left(\frac{x}{\log x \log\log x}\right) \\
&\geq \pi(x)(\log x - \log\log x - \log\log\log x) - \frac{x}{\log x \log\log x} \log x \\
&= \pi(x) \log x \left(1 - \frac{\log\log x + \log\log\log x}{\log x}\right) - \frac{x}{\log\log x}.
\end{aligned}$$

Dividing by x gives the desired lower bound.

We now give a sketch for the proof of Theorem 3.1. We define the Riemann-zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

which a priori is only defined for $s > 1$. For example,

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \qquad \zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}.$$

The value of ζ at an even positive integer n is some rational multiple of π^n. It is known that $\zeta(3)$ is irrational and that infinitely many of the $\zeta(2k+1)$ are irrational. They are of course all conjectured to be transcendental.

Using prime factorization, we have the factorization

$$\zeta(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_p \frac{1}{1 - p^{-s}}.$$

Note that if there were only finitely many primes, then this product is a finite product and thus always exist. However, $\zeta(1)$ is the harmonic series which diverges. This is Euler's proof of the infinitude of primes.

We take the logarithmic derivative of $\zeta(s)$ to get

$$\frac{d}{ds} \log \zeta(s) = -\sum_p \frac{d}{ds} \log(1 - p^{-s}) = -\sum_p \frac{p^{-s} \log p}{1 - p^{-s}} = -\sum_p \log p \left(\frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right).$$

In other words, we see the von Mangoldt function popping up:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_n \frac{\Lambda(n)}{n^s}.$$

There is a somewhat reasonable way to define $\zeta(s)$ for $0 < s < 1$. We note that

$$2^{-s}\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{(2n)^s} = \sum_{n \text{ even}} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{1 + (-1)^n}{2} \frac{1}{n^s} = \frac{1}{2}\left(\sum_{n=1}^{\infty} \frac{1}{n^s} + \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}\right).$$

So

$$\zeta(s) = \frac{1}{1 - 2^{1-s}} \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}$$

and the alternating series converges for $s > 0$. To connect the two regions $s > 1$ and $0 < s < 1$, we go to the complex world! The exponential n^s is defined as

$$n^s = e^{s \ln n} = e^{\mathrm{Re}(s) \ln n + i \mathrm{Im}(s) \ln n} = n^{\mathrm{Re}(s)}(\cos(\mathrm{Im}(s) \ln n) + i \sin(\mathrm{Im}(s) \ln n).$$

Theorem 3.3 *The function $\zeta(s)$ is analytic for $Re(s) > 1$. It has a simple pole at $s = 1$ with residue 1 and admits a (unique) analytic continuation to all $s \in \mathbb{C}\backslash\{1\}$. Moreover,*

$$\psi(x) = x - \log(2\pi) - \sum_{\zeta(\rho)=0} \frac{x^\rho}{\rho}.$$

Here:

1. **analytic** means differentiable in the complex world. It turns out that being differentiable implies being infinitely differentiable.

2. **simple pole** at $s = 1$ **with residue** 1 means that for s near 1, $\zeta(s) \sim \frac{1}{s-1}$.

3. **analytic continuation** means that there is a function L that is analytic on $\mathbb{C}\backslash\{1\}$ such that $L(s) = \zeta(s)$ for $\mathrm{Re}(s) > 1$. (The meme where $1 + 2 + \cdots = -1/12$ is the statement that $L(-1) = -1/12$. Another notable value is $L(0) = -1/2$.)

4. ζ has **trivial zeroes** at the negative even integers and the contribution from them is

$$\sum_{n=1}^{\infty} \frac{1}{2nx^{2n}} = \frac{1}{2}\log(1 - x^{-2}).$$

All other zeroes of ζ, called **nontrivial zeroes**, lie in the **critical strip** where $0 \le \mathrm{Re}(s) \le 1$ and are symmetric under $s \mapsto 1 - s$.

Theorem 3.1 then follows from the following result on the zeroes of the zeta function.

Theorem 3.4 *If $\zeta(\beta + it) = 0$ where $1/2 \le \beta \le 1$, then*

$$\beta \le 1 - \frac{1}{71\log(|t| + 2)}.$$

These results are enough to conclude that $\psi(x) \sim x$. Theorem 3.4 has been improved to

$$\beta \le 1 - \frac{1}{57.54(\log|t|)^{2/3}(\log\log|t|)^{1/3}}.$$

The **Riemann hypothesis** predicts that $\beta = 1/2$.

4 Binomial coefficients

Our goal now is to prove that

$$L_n = \mathrm{lcm}(1, 2, \ldots, n) \le 4^{n-1}$$

without using the prime number theorem. This implies Erdös' bound

$$\prod_{p \le n} p \le 4^{n-1}.$$

Recall the binomial coefficients

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}$$

for $0 \le r \le n$. We define it to be 0 if $r < 0$ or if $r > n$. They have combinatoric interpretations as the number of ways to pick r objects from a collect of n objects. Some well-known identities include:

1. Binomial Theorem: $(a + b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$.

2. Hypergeometric Identity: $\binom{n}{m} = \sum_{r=0}^{n} \binom{a}{r}\binom{n-a}{m-r}$. When $a = 1$, we have Pascal's Identity $\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$.

Pascal's identity (or the above combinatorial interpretation) can be used to prove that the binomial coefficients are all integers. Alternatively, we can use Legendre's formula:

Proposition 4.1 *For any prime p and any positive integer n,*

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Proof: For any $k \in \mathbb{N}$, let $u(k)$ denote the number of integers from 1 to n that are multiplies of p^k. Then $u(k) - u(k+1)$ is the number of integers from 1 to n with $\nu_p = k$. Then

$$\nu_p(n!) = (u(1) - u(2)) + 2(u(2) - u(3)) + 3(u(3) - u(4)) + \cdots = u(1) + u(2) + u(3) + \cdots .$$

We are done because $u(k) = \lfloor n/p^k \rfloor$. □

Lemma 4.2 *Let $a, m, n \in \mathbb{N}$ with $m < n$. Let n_a, m_a be the remainders when n, m are divided by a. Then*

$$\left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor - \left\lfloor \frac{n-m}{a} \right\rfloor = \begin{cases} 1 & \text{if } n_a < m_a, \\ 0 & \text{if } n_a \geq m_a. \end{cases}$$

Proof: We have

$$\left\lfloor \frac{n}{a} \right\rfloor = \frac{n - n_a}{a}, \qquad \left\lfloor \frac{m}{a} \right\rfloor = \frac{m - m_a}{a}$$

and

$$\frac{n-m}{a} = \frac{n-n_a}{a} - \frac{m-m_a}{a} + \frac{n_a - m_a}{a} = \left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor + \frac{n_a - m_a}{a}.$$

Since n_a, m_a are remainders, we know that $-1 < (n_a - m_a)/a < 1$. If $n_a \geq m_a$, then $(n_a - m_a)/a \in [0, 1)$ and so

$$\left\lfloor \frac{n-m}{a} \right\rfloor = \left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor .$$

If $n_a < m_a$, then $(n_a - m_a)/a \in (-1, 0)$ and so

$$\left\lfloor \frac{n-m}{a} \right\rfloor = \left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor - 1.$$

Hence we are done. □

Corollary 4.3 *Suppose p is a prime and n is a positive integer. Let k be an integer such that $p^k \leq n < p^{k+1}$. Then for any integer $m = 0, \ldots, n$, we have*

$$0 \leq \nu_p\left(\binom{n}{m}\right) \leq k \qquad \text{and} \qquad p \nmid \binom{n}{p^k}.$$

Proof: By Legendre's formula, we have

$$\nu_p\left(\binom{n}{m}\right) = \sum_{j=1}^{k} \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{m}{p^j} \right\rfloor - \left\lfloor \frac{n-m}{p^j} \right\rfloor \right).$$

By Lemma 4.2, every term in the above sum is at most 1. Moreover, if $m = p^k$, then the remainder of m when divided by p^j for any $j = 1, \ldots, k$ is 0, and so each term is 0. □

Corollary 4.4 *Suppose p is a prime and $m < n$ are positive integers. Suppose $n = p^k$ for some positive integer k. Then*

$$\nu_p\left(\binom{n}{m}\right) = k - \nu_p(m) > 0.$$

Proof: The remainder when n is divided by a power p^a of p is 0 for all $a = 1, \ldots, k$. So $\nu_p\left(\binom{n}{m}\right)$ is the number of these a such that $p^a \nmid m$. □

Lecture 5 Fri 09/15

The aim of this section is to prove $L_n \leq 4^{n-1}$ giving an upper bound for the product of primes, which will then allow us to prove Bertrand's postulate that there is always a prime in $(n, 2n]$. We begin with some basic bounds on the binomial coefficients $\binom{2n+1}{n}$ and $\binom{2n}{n}$: for $n \in \mathbb{N}$, we have

$$\frac{4^n}{n+1} < \binom{2n+1}{n} < 4^n, \qquad \frac{4^n}{2n+1} < \binom{2n}{n} < 4^n.$$

They follow from

$$2^{2n+1} = \sum_{r=0}^{2n+1} \binom{2n+1}{r}, \qquad 2^{2n} = \sum_{r=0}^{2n} \binom{2n}{r}$$

and that $\binom{2n+1}{n} = \binom{2n+1}{n+1}$ is the largest binomial coefficient of the form $\binom{2n+1}{r}$, and $\binom{2n}{n}$ is the largest binomial coefficient of the form $\binom{2n}{r}$. From the Stirling's approximation

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n,$$

we can get the more precise estimate

$$\binom{2n}{n} \sim \frac{4^n}{\sqrt{\pi n}}.$$

One may view the above as an "archimedean" estimate for these binomial coefficients. In our applications below, we will be making "p-adic" estimates for them. Fun fact: 10! seconds is exactly 6 weeks.

Theorem 4.5 *For any $n \in \mathbb{N}$, we have $L_n \leq 4^{n-1}$.*

Proof: We prove it by induction on n. When $n = 1$, we have $L_1 = 1 = 4^{1-1}$. Suppose now $n \geq 2$. Suppose first $n = 2k$ is even. Then $k \leq n - 1$ so $k \mid L_{n-1}$ and we have $L_n \leq 2L_{n-1} \leq 2 \cdot 4^{n-2} < 4^{n-1}$. Hence, it remains to consider the case where $n = 2k + 1$ is odd, where $k \geq 1$. We prove that

$$L_{2k+1} \mid L_{k+1}\binom{2k+1}{k}$$

which then implies

$$L_{2k+1} \leq L_{k+1}\binom{2k+1}{k} \leq 4^k \cdot 4^k \leq 4^{2k}.$$

by induction.

Let p be any prime. It suffices to prove that

$$\nu_p(L_{2k+1}) - \nu_p(L_{k+1}) \leq \nu_p\left(\binom{2k+1}{k}\right).$$

Let r be the unique non-negative integer such that $p^r \leq k + 1 < p^{r+1}$. Then $\nu_p(L_{k+1}) = r$. If $p^r \leq 2k + 1 < p^{r+1}$, then we also have $\nu_p(L_{2k+1}) = r$ and there is nothing to prove. Suppose now $p^{r+1} \leq 2k + 1 < p^{r+2}$. Then $\nu_p(L_{2k+1}) = r + 1$ so we need to prove that $\nu_p(\binom{2k+1}{k}) \geq 1$. Note that

$$\left\lfloor \frac{k}{p^{r+1}} \right\rfloor = 0, \quad \left\lfloor \frac{k+1}{p^{r+1}} \right\rfloor = 0, \quad \left\lfloor \frac{2k+1}{p^{r+1}} \right\rfloor = 1.$$

Hence

$$\nu_p\Big(\binom{2k+1}{k}\Big) \geq \left\lfloor \frac{2k+1}{p^{r+1}} \right\rfloor - \left\lfloor \frac{k+1}{p^{r+1}} \right\rfloor - \left\lfloor \frac{k}{p^{r+1}} \right\rfloor \geq 1.$$

Finally we note that

$$2k+1 < 2(k+1) < 2p^{r+1} \leq p^{r+2}.$$

Hence, it is not possible for $2k+1 \geq p^{r+2}$. $\square$

Let's now consider the binomial coefficient $\binom{2n}{n}$. For any positive integer a, write $(2n)_a$ and n_a for the remainders as last time. We note that if $n_a < a/2$, then $(2n)_a = 2(n_a) \geq n_a$; and if $n_a \geq a/2$, then $(2n)_a = 2(n_a) - a < n_a$. Hence

$$\left\lfloor \frac{2n}{a} \right\rfloor - 2\left\lfloor \frac{n}{a} \right\rfloor = \begin{cases} 1 & \text{if } n_a \geq a/2, \\ 0 & \text{if } n_a < a/2. \end{cases}$$

Corollary 4.6 *For any positive integer n, we have $n+1 \mid \binom{2n}{n}$. The quotients $\frac{1}{n+1}\binom{2n}{n}$ are the Catalan numbers.*

Proof: One can prove this directly by checking that

$$\frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1} \in \mathbb{Z}.$$

Alternatively, suppose $\nu_p(n+1) = k$. Then for any $a = p, p^2, \ldots, p^k$, we have $n_a = a - 1 \geq a/2$. So $\nu_p(\binom{2n}{n}) \geq k$. $\square$

Corollary 4.7 *Let $n \geq 3$ and let p be a prime such that $2n/3 < p \leq 2n$. Then*

$$\nu_p\left(\binom{2n}{n}\right) = \begin{cases} 1 & \text{if } n < p \leq 2n \\ 0 & \text{if } 2n/3 < p \leq n \end{cases}$$

Proof: The statement for $n < p \leq 2n$ is obvious because $\lfloor 2n/p \rfloor = 1$ and $\lfloor n/p \rfloor = 0$. Suppose now $2n/3 < p \leq n$. Then $n - p < 3p/2 - p = p/2$. So $\lfloor \frac{2n}{p} \rfloor - 2\lfloor \frac{n}{p} \rfloor = 0$. Now $p^2 > 4n^2/9 \geq 2n$ for $n \geq 5$. When $n = 4$, we have $8/3 < p \leq 4$ and so $p = 3$ and $p^2 > 2n$. When $n = 3$, we have $2 < p \leq 3$ and so $p = 3$ and $p^2 > 2n$. $\square$

For primes $p \leq 2n/3$, we have the "trivial" bound

$$\nu_p\left(\binom{2n}{n}\right) \leq \frac{\log 2n}{\log p}.$$

Note for $\sqrt{2n} < p \leq 2n/3$, we have

$$\nu_p\left(\binom{2n}{n}\right) \leq \frac{\log 2n}{\log p} < 2 \qquad \Longrightarrow \qquad \nu_p\left(\binom{2n}{n}\right) = 1.$$

Combining these, we find that

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} p^{\log 2n/\log p} \cdot \prod_{\sqrt{2n} < p \leq 2n/3} p \cdot \prod_{n < p \leq 2n} p \leq (2n)^{\sqrt{2n}} \cdot 4^{2n/3-1} \cdot (2n)^{\pi(n,2n)}$$

where $\pi(n, 2n)$ denotes the number of primes in $(n, 2n]$. Taking log, we get

$$\pi(n, 2n) \geq \frac{(n/3+1)\log 4 - \log(2n+1)}{\log 2n} - \sqrt{2n} \geq C\frac{n}{\log n}$$

for some positive constant $C > 0$ when n is sufficiently large.

Theorem 4.8 *(Bertrand's postulate) For any positive integer n, there is a prime $p \in (n, 2n]$.*

Proof: The above lower bound is positive for $n \geq 459$. We can verify the result directly for small n using the primes $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$. □

Exercises

4.1 Prove that for any non-negative integers r, n,

$$\sum_{r=0}^{k} \binom{n+r}{r} = \binom{n+k+1}{k}.$$

4.2 Prove that for every prime p, there exists a positive integer n, an integer $a = 0, 1$ and an integer $b = 0, 1, \ldots, n-1$ such that $p = n^2 + an + b$.

4.3 How many 0's does the number 40! ends in?

Can you figure out what the last nonzero digit of 40! is?

4.4 Prove that for any $n \in \mathbb{N}$, we have that $\nu_2(n!) = n - \#1$'s in the binary representation of n.

4.5 Prove that for any $n \in \mathbb{N}$ and any prime p, we have $\nu_p(n!) < n/(p-1)$.

4.6 Prove that for any $n \in \mathbb{N}$, if $n \mid \binom{n}{m}$ for all $m = 1, \ldots, n-1$, then n is a prime.

4.7 According to the Prime number theorem, we know that $L_n \sim e^n$. Prove (without using the PNT) that for any $\alpha > 0$, we have $L_n \geq 4^{n-\alpha}$ for n sufficiently large (depending on α).

4.8 Use Exercise 4.5 to conclude that

$$\sum_{p} \frac{\log p}{p-1} \to \infty.$$

With a little bit more effort, one can prove that

$$\sum_{p \leq n} \frac{\log p}{p} = \log n + O(1).$$

In other words, there exists an absolute constant $C > 0$ such that for any $n \in \mathbb{N}$,

$$\left| \sum_{p \leq n} \frac{\log p}{p} - \log n \right| \leq C.$$

Lecture 6 Mon 09/18

5 Euclid's proof of the infinitude of primes

Before all of these fancy results on the prime counting function, the very first proof of the infinitude of primes was due to Euclid. Here is another way to think about the proof. The key ideas are as follows:

(a) Every integer $n \geq 2$ has a prime divisor.

(b) Construct an infinite sequence of pairwise coprime integers at least 2.

The sequence constructed from Euclid's proof is $a_1 = 2$ and

$$a_{n+1} = a_1 a_2 \cdots a_n + 1, \qquad \text{for } n \geq 1.$$

Then for $i < j$, we have $a_i \mid a_1 a_2 \cdots a_{j-1}$ and so $\gcd(a_i, a_j) = \gcd(a_i, 1) = 1$.

Alternatively, if we take a_1 odd and use $a_{n+1} = a_1 \cdots a_n + 2$, we also have $\gcd(a_i, a_j) = \gcd(a_i, 2) = 1$ since each a_i is odd.

Proposition 5.1 *The sequence defined by $F_0 = 3$ and*

$$F_{n+1} = F_0 F_1 \cdots F_n + 2, \qquad \textit{for } n \geq 0$$

is the sequence of Fermat numbers $F_n = 2^{2^n} + 1$.

Proof: It suffices to prove that $F_n = 2^{2^n} + 1$ satisfies the recursion formula. This follows easily from induction along with $F_{n+1} - 1 = (F_n - 1)^2$. $\square$

There is a more general result on the infinitude of primes satisfying congruence conditions. Recall that $a \equiv b \pmod{m}$ means that $m \mid a - b$, or equivalently that a and b have the same remainder when divided by m. Since numbers congruent to a mod m form an arithmetic progression, this result is also referred to as the infinitude of primes in arithmetic progressions. It marks the beginning of modern analytic number theory.

Theorem 5.2 *(Dirichlet) Let a, m be coprime positive integers. Then there are infinitely many primes $p \equiv a \pmod{m}$.*

We now know (Siegel-Walfisz) that there are an equal number of them, asymptotically, over all possible congruence classes. More precisely, if $p \equiv a \pmod{m}$, then $\gcd(p, m) = \gcd(a, m)$. If p is prime large enough to not divide m, then $\gcd(p, m) = 1$. The number of integers $a = 1, \ldots, m$ such that $\gcd(a, m) = 1$ is $\phi(m)$, the Euler-ϕ (or the Euler-Totient) function of m. Then

$$\lim_{x \to \infty} \frac{\#\text{ primes } p \leq x, p \equiv a \pmod{m}}{x/\log x} = \frac{1}{\phi(m)}.$$

We can give an Euclid's type proof for this result in some special cases.

Primes of the form $4k + 3$

We modify the key idea of Euclid's proof to:

(a) Every integer $n \geq 2$ of the form $4k + 3$ has a prime divisor of the form $4k + 3$.

(b) Construct an infinite sequence of pairwise coprime integers at least 2 that are of the form $4k + 3$.

Property (a) follows because products of numbers of the form $4k + 1$ are still of the form $4k + 1$. In terms of congruences, we can say that if $a \equiv 1 \pmod{4}$ and $b \equiv 1 \pmod{4}$, then $ab \equiv 1 \pmod{4}$. Hence a number of the form $4k + 3$ has a prime divisor that is not of the form $4k + 1$. Since it can't be divisible by 2, primes of the form $4k + 3$ are the only possibilities left. For the sequence in (b), we take $a_1 = 7$ and

$$a_{n+1} = 4(a_1 \cdots a_n) + 3.$$

Then similar to before, for $i < j$,

$$\gcd(a_i, a_j) = \gcd(a_i, 3) = \gcd(a_1 \cdots a_{i-1}, 3) = 1$$

by induction.

The same idea also works for primes of the form $3k + 2$ and primes of the form $6k + 5$ because $\phi(3) = \phi(6) = 2$ so that if not all the prime divisors are of the form $3k + 1$ (resp. $6k + 1$), and it is not divisible by 3 (resp. 2 or 3), then it has a prime divisor of the form $3k + 2$ (resp. $6k + 5$).

Primes of the form $4k+1$

This is a bit trickier. Let p be an odd prime. We consider the congruence equation

$$x^2 \equiv -1 \pmod{p}.$$

Suppose it has a solution $x = a$. Then clearly $p \nmid a$ for if otherwise, we would have $a^2 \equiv 0$. So by Fermat's little Theorem,

$$a^{p-1} \equiv 1 \pmod{p}.$$

On the other hand,

$$a^{p-1} = (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Since p is an odd prime, we see that

$$1 \equiv (-1)^{(p-1)/2} \pmod{p} \qquad \Rightarrow \qquad 1 = (-1)^{(p-1)/2} \qquad \Rightarrow \qquad p \equiv 1 \pmod{4}.$$

In other words, if p is an odd prime divisor of an integer of the form n^2+1, then p is of the form $4k+1$. By taking $4n^2+1$ instead, we remove the possibility of $p = 2$. So we have:

(a) Every integer $n \geq 2$ of the form $4n^2+1$ has a prime divisor of the form $4k+1$.

(b) Construct an infinite sequence of pairwise coprime integers at least 2 that are of the form $4k^2+1$.

To construct our sequence, we take $a_1 = 5$ and

$$a_{n+1} = 4(a_1 \cdots a_n)^2 + 1.$$

The crucial idea here is that if $a^2 \equiv -1 \pmod{p}$, then

$$a^4 \equiv 1 \pmod{p}$$

but

$$a^3 \equiv -a \not\equiv 1 \pmod{p}, \qquad a^2 \equiv -1 \not\equiv 1 \pmod{p}, \qquad a \not\equiv 1 \pmod{p}.$$

We define the **order** of an integer n mod m, where $\gcd(n,m) = 1$, denoted $o_m(n)$, to be the smallest positive integer d such that $n^d \equiv 1 \pmod{m}$. Note that it is not obvious a priori that there exists a positive integer d such that $n^d \equiv 1 \pmod{m}$, but one can prove using the Pigeonhole principle that such a $d \leq \phi(m)$ exists by considering $n, n^2, \ldots, n^{\phi(m)} \pmod{m}$. Here we have $o_p(a) = 4$. Then from Fermat's little theorem, we know that $p-1$ is an exponent that gives 1 mod p when p is a prime. It is then natural to expect that the smallest exponent $o_p(a)$ to divide $p-1$, which would give us $p \equiv 1 \pmod{4}$.

Proposition 5.3 *Let a, m be coprime integers. Suppose $n \in \mathbb{N}$ with $a^n \equiv 1 \pmod{m}$. Then $o_m(a) \mid n$. In particular, when $m = p$ is a prime, by Fermat's little theorem, $o_p(a) \mid p-1$.*

Proof: Note that $o_m(a) \leq n$. Apply the division algorithm to get integers s, t such that $n = o_m(a)s + t$ where $0 \leq t < o_m(a)$ and $s \geq 0$. Then

$$a^t \equiv a^t (a^{o_m(a)})^s = a^{t + o_m(a)s} = a^n \equiv 1 \pmod{m}.$$

Hence it follows from the minimality of $o_m(a)$ that $t = 0$. Therefore, $o_m(a) \mid n$. □

Remark: The generalization of Fermat's little theorem to arbitrary positive integers is

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

for any integer a coprime to m. So we have in general, $o_m(a) \mid \phi(m)$. Note that $\phi(m) \leq m-1$ with equality if and only if m is a prime.

Lecture 7 Wed 09/20

Primes of the form $qk+1$ where q is a prime

Suppose now a is an integer such that $a^q \equiv 1 \pmod{p}$ and $a \not\equiv 1 \pmod{p}$. Then $o_p(a) \mid q$ and $o_p(a) \neq 1$. So $o_p(a) = q$ and $q \mid p-1$. In terms of division, we have

$$p \mid a^q - 1, \qquad p \nmid a - 1.$$

So p divides the quotient $a^{q-1} + a^{q-2} + \cdots + 1$. We define the q-th **cyclotomic polynomial** to be

$$\Phi_q(x) = \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \cdots + 1.$$

Proposition 5.4 *Let q be an odd prime. If p is a prime divisor of $\Phi_q(n)$ for some integer n, then $p \equiv 1 \pmod{q}$ or $p = q$.*

Proof: Since $\Phi_q(n) \mid n^q - 1$, we have $p \mid n^q - 1$. So $o_p(n) \mid q$. If $o_p(n) = 1$, then $n \equiv 1 \pmod{p}$ and

$$\Phi_q(n) \equiv 1^{q-1} + \cdots + 1 \equiv q \pmod{p},$$

which implies that $p \mid q$ and so $p = q$. If $o_p(n) = q$, then we have $p \equiv 1 \pmod{q}$. □

We can remove the possibility of $p = q$ by taking $\Phi_q(qn) = 1 + q(\ldots)$. Then we take the sequence $a_1 = \Phi_q(q)$ and

$$a_{n+1} = \Phi_q(qa_1a_2 \cdots a_n).$$

This gives infinitely many primes of the form $qk + 1$.

Exercises

5.1 Use the polynomial $n^2 + 4$, and a small modification, to prove that there are infinitely many primes of the form $8k + 5$.

5.2 Let $h(x)$ is a polynomial with integer coefficients with $h(0) = 1$. Prove that the sequence defined by $a_1 = 1$ and $a_{i+1} = h(a_1a_2 \cdots a_i)$ for $i \geq 1$, consists of pairwise coprime integers.

5.3 Let $h(x) = ax + b$ where a, b are coprime integers. Prove that the sequence defined by $a_1 = 1$ and $a_{i+1} = h(a_1a_2 \cdots a_i)$ for $i \geq 1$, consists of pairwise coprime integers.

5.4 Prove that there does not exist a non-constant polynomial $h(x)$ with integer coefficients such that $h(n)$ is a prime for all integers n.

5.5 Prove that $2^{2^n} - 1$ has at least $n + 1$ distinct prime divisors.

5.6 Prove that $\phi(m)$ is even for any integer $m \geq 3$. (Note that $\phi(1) = \phi(2) = 1$.)

5.7 Let m be a positive integer. Prove that there exists some real number $C > 0$ such that $\phi(m) \geq \dfrac{Cm}{\log m}$.

5.8 Let q be a prime and n be an integer. Prove that if $q \mid n^q - 1$, then $q^2 \mid n^q - 1$.

5.9 Prove that for any $k \in \mathbb{N}$, we have $o_{7^k}(2) = 3 \cdot 7^{k-1}$.

5.10 Let $q > 3$ be a prime. Prove that there does not exist integers x, y such that $x^{q-1} + \cdots + x + 1 = y^{q-2} - 1$.

6 Primes of the form $mk+1$ and Cyclotomic polynomials

Suppose now m is a positive integer, that is not necessarily a prime. It is still true that if $o_p(a) = m$, then $p \equiv 1 \pmod{m}$. The difficulty lies in finding the polynomial $\Phi_m(x)$ whose roots mod p have orders exactly m, and not proper divisors of m. Let's try some small values to see what they should be. When $m = 6$, we should remove solutions to $x^2 - 1$, as they have order dividing 2, and $x^3 - 1$, as they have order dividing 3, but

$$\frac{x^6-1}{(x^2-1)(x^3-1)} = \frac{x^6-1}{x^5-x^3-x^2+1}$$

isn't a polynomial. The problem is that when we remove the solutions to $x^2 - 1$, we have already removed the solution to $x - 1$, so we shouldn't remove it again from $x^3 - 1$. In other words, we should take

$$\Phi_6(x) = \frac{x^6-1}{(x^2-1)\big((x^3-1)/(x-1)\big)} = \frac{x^3+1}{x+1} = x^2 - x + 1.$$

What about something more complicated like $\Phi_{105}(x)$? Using the same "inclusion-exclusion sieve", we should take

$$\Phi_{105}(x) = \frac{(x^{105}-1)(x^3-1)(x^5-1)(x^7-1)}{(x^{15}-1)(x^{21}-1)(x^{35}-1)(x-1)} = x^{48} + \cdots - 2x^{41} + \cdots + 1.$$

It seems quite random that it is actually a polynomial. We need a better definition that is easier to work with. One thing to note is that we seem to have forgotten about the prime p. So let's forget it completely and think in $\mathbb{C}$.

What are the solutions to $x^m = 1$ in $\mathbb{C}$? They are given by ζ_m^k for $k = 1, 2, \ldots, q$ where $\zeta_m = e^{2\pi i/m}$ is the **primitive** m-th root of unity, as the smallest positive integer d such that $\zeta_m^d = 1$ is m. We have the factorization

$$x^m - 1 = \prod_{k=1}^{m} (x - \zeta_m^k).$$

Since we want the roots of our polynomial $\Phi_m(x)$ to have order m, we define the **m-th cyclotomic polynomial** as

$$\Phi_m(x) = \prod_{\substack{1 \le k \le m \\ o(\zeta_m^k) = m}} (x - \zeta_m^k)$$

where $o(\zeta_m^k)$ is the smallest positive integer d such that $(\zeta_m^k)^d = 1$. We know

$$\zeta_m^{kd} = 1 \Leftrightarrow m \mid kd \Leftrightarrow \frac{m}{\gcd(m,k)} \mid \frac{k}{\gcd(m,k)} d \Leftrightarrow \frac{m}{\gcd(m,k)} \mid d.$$

So $o(\zeta_m^k) = m/\gcd(m,k)$. Hence, it is m if and only if $\gcd(m,k) = 1$. In other words, we have

$$\Phi_m(x) = \prod_{\substack{1 \le k \le m \\ \gcd(k,m) = 1}} (x - \zeta_m^k).$$

The polynomial $\Phi_q(x)$ is monic with coefficients in $\mathbb{C}$ and has degree $\phi(q)$. Our next goal is to show that all the coefficients of $\Phi_m(x)$ are integers, and that $\Phi_m(x)$ can be used to prove the infinitude of primes of the form $mk + 1$.

Lecture 8 Fri 09/22

Proposition 6.1 *Let $m \in \mathbb{N}$. We have the factorization*

$$x^m - 1 = \prod_{d \mid m} \Phi_d(x).$$

Proof: In the factorization of $x^m - 1$, we can group the factors $x - \zeta_m^k$ by the order $o(\zeta_m^k)$. Since $o(\zeta_m^k) = m/\gcd(m,k)$ is a positive divisor of m, we have

$$x^m - 1 = \prod_{d|m} \prod_{\substack{1 \le k \le m \\ o(\zeta_m^k) = d}} (x - \zeta_m^k).$$

Note that $o(\zeta_m^k) = d$ if and only if $\gcd(m,k) = m/d$ if and only if $k = (m/d)j$ for some integer j with $\gcd(m,(m/d)j) = m/d$. Now

$$\gcd(m,(m/d)j) = \gcd((m/d)d,(m/d)j) = (m/d)\gcd(d,j).$$

Hence $o(\zeta_m^k) = d$ if and only if $k = (m/d)j$ for some integer j with $\gcd(d,j) = 1$. The condition $1 \le k \le m$ becomes $1 \le j \le d$. Moreover, the complex number

$$\zeta_m^k = e^{\frac{2\pi i}{m}\frac{m}{d}j} = e^{\frac{2\pi i}{d}j} = \zeta_j^d.$$

Therefore, the product

$$\prod_{\substack{1 \le k \le m \\ o(\zeta_m^k) = d}} (x - \zeta_m^k) = \prod_{\substack{1 \le j \le d \\ \gcd(j,d) = 1}} (x - \zeta_d^j) = \Phi_d(x).$$

We are now done. □

Corollary 6.2 *Let $m \in \mathbb{N}$. Then $m = \sum_{d|m} \phi(d)$.*

Corollary 6.3 *Let $m \in \mathbb{N}$. Then $\Phi_m(x)$ is a polynomial with integer coefficients. Moreover, $\Phi_1(0) = -1$ and $\Phi_m(0) = 1$ for $m \ge 2$.*

Proof: We prove by induction on m. We have $\Phi_1(x) = x - 1$. Suppose now $m \ge 2$. We know that

$$x^m - 1 = \Phi_m(x) \cdot \Phi_1(x) \prod_{\substack{d|m \\ 1<d<m}} \Phi_d(x) = \Phi_m(x) \cdot (x-1) \prod_{\substack{d|m \\ 1<d<m}} \Phi_d(x).$$

By induction, each of the $\Phi_d(x)$ for $d < m$ is a monic polynomial with integer coefficient and so is their product. Therefore, so is the quotient of $x^m - 1$ by it. Also by induction, we have $\Phi_d(0) = 1$ for $1 < d < m$. So setting $x = 0$ gives $\Phi_m(0) = 1$. □

Remark: There is a more direct proof of $\Phi_m(0) = 1$ for $m > 2$. Let S be the set of integers $1 \le j < m/2$ that are coprime to m. Then the set of integers $m/2 < k \le m$ coprime to m are all of the form $m - j$ for some $j \in S$. If $m/2$ is an integer, then it is at least 2 and divides m, so it is not coprime to m. Now

$$\Phi_m(0) = \prod_{j \in S} (-\zeta_m^j)(-\zeta_m^{m-j}) = 1.$$

Proposition 6.4 *Let $n \in \mathbb{N}$ and let $n > 1$ be an integer coprime to m. Let $a \in \mathbb{Z}$ with $n \mid \Phi_m(a)$. Then $o_n(a) = m$.*

Proof: We write $x^m - 1$ as $F(x)\Phi_m(x)$ where $F(x) \in \mathbb{Z}[x]$ is the product of $\Phi_d(x)$ over all positive integers $d \mid m$ with $d < m$. Then $\Phi_m(a) \mid a^m - 1$ and we have $n \mid a^m - 1$. Hence $o_n(a) \mid m$. Suppose for a contradiction that $\ell := o_n(a) < m$. Then we have $n \mid a^\ell - 1$. Since $\ell \mid q$ and $\ell < q$, we know that any divisor of ℓ is a divisor of q and is less than q. In other words,

$$F(x) = \prod_{d|\ell} \Phi_d(x) \cdot \prod_{\substack{d|m \\ d<m \\ d \nmid \ell}} \Phi_d(x) = (x^\ell - 1)G(x)$$

for some $G(x) \in \mathbb{Z}[x]$. We thus have the factorization

$$a^q - 1 = (a^\ell - 1)\Phi_q(a)G(a).$$

Fix some prime p dividing n, which exists since $n > 1$. From $p \mid n$ and $n \mid \Phi_m(a)$, we have $p \mid \Phi_m(a)$ and so

$$\nu_p(a^m - 1) = \nu_p(a^\ell - 1) + \nu_p(\Phi_m(a)) + \nu_p(G(a)) > \nu_p(a^\ell - 1).$$

Since $\ell \mid q$, we write $q = \ell k$ for some positive integer k. Then

$$a^q - 1 = (a^\ell - 1)((a^\ell)^{k-1} + (a^\ell)^{k-2} + \cdots + 1).$$

Since $n \mid a^\ell - 1$ and $p \mid n$, we have $a^\ell \equiv 1 \pmod{p}$ and so

$$(a^\ell)^{k-1} + (a^\ell)^{k-2} + \cdots + 1 \equiv 1 + 1 + \cdots + 1 = k \pmod{p}.$$

Since $\gcd(n, m) = 1$ and $k \mid m$ and $p \mid n$, we have $p \nmid k$. This implies that $\nu_p(a^q - 1) = \nu_p(a^d - 1)$. Contradiction. □

Corollary 6.5 *Let $n \in \mathbb{N}$. Suppose there exists $a \in \mathbb{Z}$ such that $n \mid \Phi_{n-1}(a)$, then n is a prime.*

Proof: Since n is coprime to $n - 1$, we have $o_n(a) = n - 1$ but $o_n(a) \leq \phi(n) \leq n - 1$. So $\phi(n) = n - 1$. Hence n is a prime. □

Corollary 6.6 *Let $m \in \mathbb{N}$. Let $a \in \mathbb{Z}$. Then any prime divisor of $\Phi_m(ma)$ is of the form $mk + 1$.*

Proof: Let p be prime divisor of $\Phi_m(ma)$. Since the constant term of $\Phi_m(x)$ is ± 1, we see that $\gcd(m, \Phi_m(ma)) = 1$ and so $p \nmid m$. Hence $o_p(ma) = q$ which implies that $q \mid p - 1$. □

Theorem 6.7 *Let $m \in \mathbb{N}$. There are infinitely many primes of the form $mk + 1$.*

Proof: Since $\Phi_m(x)$ is monic, we know that $\Phi_m(x) \to \infty$ as x goes to infinity. Let N be a large integer such that $\Phi_m(x) > 1$ for all $x \geq N$. We now construct the sequence by taking $a_1 = N$ and

$$a_{n+1} = \Phi_m(Nma_1a_2 \cdots a_n).$$

Then we have a sequence of pairwise coprime (because the constant term of $\Phi_m(x)$ is ± 1) integers at least 2, each having only prime divisors of the form $mk + 1$. □

Lecture 9 Mon 09/25

It makes one wonder for which coprime positive integers a and m does there exist a Euclid type proof for the infinitude of primes congruent to a mod m. All of these proofs lead to the construction of an **Euclidean polynomial** for a mod m, which is a polynomial $h(x)$ with integer coefficients such that the prime divisors of $h(n)$ for integers n (either belong to a fixed finite set, or) are 1 mod m, or are a mod m; and that infinitely many primes that are a mod m arise this way.

Theorem 6.8 *A Euclidean polynomial for a mod m exists if and only if $a^2 \equiv 1 \pmod{m}$.*

Schur (1912) proved the backwards direction and Murty (1988) proved the forwards direction. For example, this implies that there are no Euclid type argument for the infinitude of primes of the form $5k + 2$.

Here are some Euclidean polynomials in small moduli:

(a) Primes dividing $5(2n)^2 - 1$ are congruent to 1 or 4 mod 5.

(b) Primes dividing $2n^2+1$ are congruent to 1 or 3 mod 8.

(c) Primes dividing $2n^2-1$ are congruent to 1 or 7 mod 8.

(d) Primes dividing $(7n)^3+(7n)^2-2(7n)-1$ are congruent to 1 or 6 mod 7.

(e) Primes dividing $(3n)^3-3(3n)-1$ are congruent to 1 or 8 mod 9.

Statements (a) - (c) are results in Quadratic Reciprocity. Statement (d) and (e) use the theory of finite fields. Schur's result uses a bit more of the theory of fields and Galois theory. We will spend the remainder of this semester working towards these theories. Murty's result is about the splitting of primes and uses Chebotarev's density theorem, which is ironic because it is actually a generalization of Dirichlet's result on primes in arithmetic progression!

Exercises

6.1 Compute $\Phi_9(x)$ and find a polynomial $f(x)$ such that $x^3 f(x+x^{-1}) = \Phi_9(x)$.

6.2 Prove that for any $k \in \mathbb{N}$, we have $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$.

6.3 Prove that for any $k \in \mathbb{N}$, we have $\Phi_{3^k}(x) = x^{2\cdot 3^{k-1}} + x^{3^{k-1}} + 1$.

6.4 Prove that for any $h, k \in \mathbb{N}$, we have $\Phi_{2^h 3^k}(x) = x^{2^h 3^{k-1}} - x^{2^{h-1} 3^{k-1}} + 1$.

6.5 Suppose $q \in \mathbb{N}$ such that $\Phi_q(x) = x^{2s} + cx^s + 1$ for some nonzero integer c, where $s = \phi(q)/2$. Prove that $c = \pm 1$.

6.6 Prove that if p is a prime at least 5, then there exists a polynomial $h(x)$ with integer coefficients such that $x^{2p} + x^p + 1 = (x^2 + x + 1)h(x)$.

6.7 We will see later that the cyclotomic polynomials $\Phi_q(x)$ are all irreducible in the sense that they do not admit a factorization into a product of polynomials with integer coefficients with smaller degrees. You will prove in HW 3 that $\Phi_q(x)$ is reciprocal in the sense that $\Phi_q(x^{-1}) = x^{-\phi(q)}\Phi_q(x)$. Prove that if $\Phi_q(x)$ is a trinomial, that is of the form $x^{\phi(q)} + cx^s + 1$ for some nonzero integers c, s, then $q = 2^h 3^k$ for some non-negative integer h and positive integer k.

6.8 Using the fact that primes dividing $2n^2+1$ are congruent to 1 or 3 mod 8, prove that there are infinitely many primes of the form $8k+3$.

7 Abstract Algebra

We have seen so many beautiful results about the integers and if you think about it, everything really just boils down to addition and multiplication, and a notion of size. The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or the sets of polynomials with coefficients in them also have addition and multiplication and a notion of size. Can we try defining primes and gcd and do all of the above? For example, what should a prime in $\mathbb{R}$ mean, what should a prime in $\mathbb{R}[x]$ mean?

The key in defining a prime is the notion of divisibility. We say $a \mid b$ in $\mathbb{Z}$ if $b = ka$ for some $k \in \mathbb{Z}$. The natural extension to $\mathbb{R}$ would be that $a \mid b$ in $\mathbb{R}$ if $b = ka$ for some $k \in \mathbb{R}$. This is a little silly because we can divide in $\mathbb{R}$ so if $a \neq 0$, then by taking $k = b/a$, we have $b = ka$. This is more meaningful in $\mathbb{R}[x]$ where we say $a \mid b$ in $\mathbb{R}[x]$ if $b = ka$ for some $k \in \mathbb{R}[x]$. Then we have non-divisions like $x+1 \nmid x^2+1$. Note that the definition of division only uses multiplication.

In abstract algebra, we step away from numbers and consider any set for which arithmetic operations like addition and multiplication can be defined.

Definition: A **commutative ring** R is a set equipped with two binary operations:

$$(a,b) \mapsto a+b : R \times R \to R, \qquad (a,b) \mapsto ab : R \times R \to R,$$

one unary operation:

$$a \mapsto -a : R \to R$$

and two nullary operations:

$$0 \in R, \qquad 1 \in R$$

such that the usual laws of arithmetic hold:

(1) (Commutative) $a + b = b + a$ and $ab = ba$;

(2) (Associative) $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$;

(3) (Distributive) $a(b + c) = ab + ac$;

(4) (Additive identity) $a + 0 = a$ and $a + (-a) = 0$;

(5) (Multiplicative identity) $a \cdot 1 = a$.

Remark: More generally, we do not assume multiplication to be commutative (for example matrix multiplication is not commutative) in which case we will add $(b + c)a = ba + ca$ to (3) and $1 \cdot a = a$ to (5). All rings are assumed to be commutative in this class.

We do not assume that a multiplicative inverse a^{-1} always exist. We say $a \mid b$ in R if there exists $k \in R$ such that $b = ka$. If $a \mid 1$, that is if $ab = 1$ for some $b \in R$, then we say a is a **unit** and write $b = a^{-1}$. We define the **group of units** as

$$R^\times = \{a \in R \colon \exists b \in R, ab = 1\}.$$

Examples:

1. The set $\mathbb{Z}$ of integers with the usual $0, 1, +, \times, -$ is a commutative ring. An integer $a \in \mathbb{Z}$ is a unit if and only if $a \mid 1$ if and only if $a = \pm 1$. So $\mathbb{Z}^\times = \{1, -1\}$.

2. The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with the usual operations are all commutative rings. Every nonzero element is a unit.

   A commutative ring R is **field** if $R^\times = R \backslash \{0\}$.

3. If R is a commutative ring, then the set $R[x]$ of polynomials with coefficients in R is a commutative ring. When $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, we know that $\deg(fg) = \deg(f)\deg(g)$; so if $fg = 1$, then $\deg(f) = 0$ and $\deg(g) = 0$. So they are constants in R. Hence when $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $R[x]^\times = R^\times$.

   In general, we can still define the degree $\deg(f)$ of a polynomial $f \in R[x]$ as the largest integer n such that the coefficient of x^n in f is nonzero. An essential step in proving $\deg(fg) = \deg(f)\deg(g)$ requires knowing that if $a, b \neq 0$, then $ab \neq 0$.

   A commutative ring is an **integral domain** if $a \neq 0 \wedge b \neq 0 \Rightarrow ab \neq 0$.

   Lemma 7.1 *If R is an integral domain, then $R[x]$ is also an integral domain and $R[x]^\times = R^\times$. Moreover, for any $f, g \in R[x]$ that are nonzero,* $\deg(fg) = \deg(f) + \deg(g)$.

   Lemma 7.2 *If R is a field, then R is an integral domain.*

4. Can we make $R = \{0\}$ into a ring? Take $1 = 0$ and $0 + 0 = 0 \times 0 = -0 = 0$. This is the trivial ring. We will henceforth assume $0 \neq 1$ for rings.

5. Can we make $R = \{0, 1\}$ (where $0 \neq 1$) into a ring? We must have

   $$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 \times 1 = 1, \quad -0 = 0.$$

   The next two lemmas force

   $$0 \times 1 = 0, \quad 0 \times 0 = 0, \quad 1 + 1 = 0, \quad -1 = 1.$$

   Since $1 \times 1 = 1$, we see that $\{0, 1\}$ is a field (and an integral domain). We denote this ring suggestively by $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{F}_2$. It is then a boring exercise to prove that $\times$ and $+$ satisfy associativity and distributivity. We will see a better way to check this next time.

Lemma 7.3 *Let R be a commutative ring. Then $a \cdot 0 = 0$, $a \cdot (-1) = -a$ and $-(-a) = a$ for any $a \in R$.*

Lemma 7.4 *Let R be a commutative ring. Let $a \in R$. The map $x \mapsto x + a$ defines a bijection $R \to R$. The map $x \mapsto xa$ is a bijection $R \to R$ if and only if $a \in R^\times$.*

Proof: The map $x \mapsto x + (-a)$ is the inverse of $x \mapsto x + a$. If $a \in R^\times$, then $x \mapsto xa^{-1}$ is the inverse of $x \mapsto xa$. Conversely, if $x \mapsto xa$ is surjective, then $ba = 1$ for some $b \in R$ and so $a \in R^\times$. □

Corollary 7.5 *Let R be an integral domain. Suppose R is finite. Then R is a field.*

Proof: Let a be a nonzero element. Then for any $x \neq y$, we have $x - y \neq 0$ and so $(x - y)a \neq 0$, implying that $xa \neq ya$. So the map $x \mapsto xa : R \to R$ is injective. An injective map between two finite sets of the same size is surjective (by the Pigeonhole principle). □

Lecture 10 Wed 09/27

The above arithmetic on $\{0, 1\}$ looks just like the addition and multiplication property of even and odd numbers. More precisely, consider a map $f : \mathbb{Z} \to \{0, 1\}$ sending all even numbers to 0 and all odd numbers to 1. Then for any $a, b \in \mathbb{Z}$, we have

$$f(a + b) = f(a) + f(b), \qquad f(ab) = f(a)f(b), \qquad f(-a) = -f(a), \qquad f(0) = 0, \qquad f(1) = 1.$$

In other words, f respects the ring operations on $\mathbb{Z}$ and on $\{0, 1\}$. Since f is surjective and we know the usual addition and multiplication on $\mathbb{Z}$ are associative and distributive, we can also use it to prove that $+, \times$ on $\{0, 1\}$ satisfy associativity and distributivity.

In general, a **ring homomorphism** is a map $f : R_1 \to R_2$ between two rings R_1, R_2 such that for any $a, b \in R_1$,

$$f(a + b) = f(a) + f(b), \qquad f(ab) = f(a)f(b), \qquad f(1) = 1.$$

Take $a = b = 0$, we get $f(0) = f(0) + f(0)$ and so $f(0) = 0$. Then take $b = -a$ to get $f(-a) = -f(a)$. The assumption $f(1) = 1$ is required to rule-out the 0 map.

6. What about a ring with 3 elements?

   Suppose R is a ring with 3 elements, namely 0, 1, α. Let's write down its addition and multiplication table. Each row and column of the addition table should be a permutation of $0, 1, \alpha$ by Lemma 7.4. To find α^2, we use $\alpha\alpha = \alpha(1 + 1) = \alpha + \alpha = 1$.

$+$	0	1	α
0	0	1	α
1	1	α	0
α	α	0	1

$\times$	0	1	α
0	0	0	0
1	0	1	α
α	0	α	1

   Since there is only one way to fill out the addition and multiplication tables, we know there is at most "one" ring with 3 elements. More precisely, suppose R' is another ring with 3 elements, namely 0, 1, β. We can define a map $f : R \to R'$ by

$$f(0) = 0, \qquad f(1) = 1, \qquad f(\alpha) = \beta.$$

   Then f is a ring homomorphism that is also a bijection. An **isomorphism** is a ring homomorphism that is a bijection. We say the two rings R and R' are **isomorphic** if there is an isomorphism between

them and we write $R \cong R'$. Isomorphic rings are really the "same thing" but just with different labels. Any two rings with 3 elements are isomorphic and they are fields.

Finally to prove that a ring with 3 elements exists, we can take the above addition and multiplication and verify distributivity and associativity. Alternatively, we can use the surjective map $f : \mathbb{Z} \to \{0, 1, \alpha\}$ sending integers of the form $3k$ to 0, $3k+1$ to 1, and $3k+2$ to α. We denote this ring suggestively by $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{F}_3$.

7. When we go to 4 elements, we encounter the first ring that is not an integral domain (and so not a field). We can use the surjective map $f : \mathbb{Z} \to \{0, 1, \alpha, \beta\}$ sending integers of the form $4k$ to 0, $4k+1$ to 1, $4k+2$ to α, and $4k+3$ to β, to define a ring structure on $\{0, 1, \alpha, \beta\}$. The addition and multiplication table look like

$+$	0	1	α	β
0	0	1	α	β
1	1	α	β	0
α	α	β	0	1
β	β	0	1	α

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	0	α
β	0	β	α	1

Note that we have $\alpha^2 = 0$ in this ring. So it is not an integral domain. We denote this ring suggestively by $\mathbb{Z}/4\mathbb{Z}$.

In the above addition table, the key is that $1+1 \notin \{0, 1\}$. We may assume, by renaming, that $1+1 = \alpha$, which then forces $1 + \alpha = \beta$ and $1 + \beta = 0$ and then the rest of the addition table will be identical to the above. Note that since every element here is a sum of 1's, the multiplication is also determined because by distributivity,

$$\underbrace{(1 + \cdots + 1)}_{n} \cdot \underbrace{(1 + \cdots + 1)}_{m} = \underbrace{(1 + \cdots + 1)}_{nm}.$$

This also implies that there is a unique ring structure on $\mathbb{Z}$ if $+$ is the usual addition.

There are three other (non-isomorphic) rings with 4 elements where $1 + 1 \in \{0, 1\}$, that is $1 + 1 = 0$. Note that we must have $\alpha + \alpha = \alpha(1 + 1) = 0$. The addition table is now uniquely determined.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times_1$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	0	α
β	0	β	α	1

$\times_2$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	α	0
β	0	β	0	β

$\times_3$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

There are now multiple options for the multiplication table. We note that it is determined by α^2 as

$$\alpha\beta = \alpha(\alpha + 1) = \alpha^2 + \alpha, \qquad \beta^2 = (\alpha + 1)^2 = \alpha^2 + 1.$$

There are now three isomorphism classes. If $\alpha^2 \in \{0, 1\}$, then either $\alpha^2 = 0$ or $\beta^2 = 0$ and so by renaming, we may assume $\alpha^2 = 0$ and we get the ring $\mathbb{F}_2[x]/(x^2)$. If $\alpha^2 = \alpha$, then we get the ring $\mathbb{F}_2[x]/(x^2 - x)$. If $\alpha^2 = \beta$, then we get the ring $\mathbb{F}_4$. We list the special property that they each have to show that they are all non-isomorphic.

(a) $\mathbb{Z}/4\mathbb{Z}$ has an element a such that $a + a \neq 0$.

(b) $\mathbb{F}_2[x]/(x^2)$ has a nonzero element a such that $a^2 = 0$.

(c) $\mathbb{F}_2[x]/(x^2 - x)$ has the property that every element a is idempotent, that is $a^2 = a$.

(d) $\mathbb{F}_4$ is an integral domain (and also a field).

Lemma 7.6 *Let R be a commutative ring. There is a unique ring homomorphism $f : \mathbb{Z} \to R$ (called the canonical homomorphism).*

If this map f is injective, then we say that the **characteristic** of R is 0. If f is not injective, then there is some nonzero integer a such that $f(a) = 0$. Now $f(-a) = -f(a) = 0$, so we may assume a is positive. The smallest positive integer d such that $f(d) = 0$ is the **characteristic** of R.

Lemma 7.7 *If R is an integral domain, then its characteristic is either 0 or a prime.*

Proof: Suppose the characteristic d of R is positive. Let q be a positive divisor of d so $d = qk$ for some $k \in \mathbb{N}$. Then $f(q)f(k) = f(d) = 0$. Since R is an integral domain, either $f(q) = 0$ or $f(k) = 0$. By minimality of d, we have $q = d$ in the first case, and $k = d$ so $q = 1$ in the second case. Hence we have shown that the only positive divisors of d are 1 and d. In other words, d is a prime. □

The ring $\mathbb{Z}/4\mathbb{Z}$ has characteristic 4 while the other 3 has characteristic 2. In (b), (c), (d), the subset $\{0, 1\}$ with addition and multiplication in the respective rings forms a ring, isomorphic to $\mathbb{F}_2$. A **subring** of a ring R is a subset R' that is closed under all the operations of R: namely it contains 0 and 1, contains $a + b$, ab and $-a$ for any $a, b \in R'$.

8. If R_1, R_2 are two rings, then $R_1 \times R_2 = \{(a, b) : a \in R_1, b \in R_2\}$ has a ring structure by coordinate-wise operations. It is the unique ring structure on $R_1 \times R_2$ so that the projection maps $(a, b) \mapsto a$ and $(a, b) \mapsto b$ are ring homomorphisms. The ring $\mathbb{F}_2 \times \mathbb{F}_2$ has 4 elements $(0, 0), (0, 1), (1, 0), (1, 1)$ and every element is idempotent. Hence $\mathbb{F}_2 \times \mathbb{F}_2 \cong \mathbb{F}_2[x]/(x^2 - x)$.

   Note that if R is a ring and $f_1 : R \to R_1$ and $f_2 : R \to R_2$ are ring homomorphisms, then the map $f : R \to R_1 \times R_2$ defined by $f(r) = (f_1(r), f_2(r))$ is a ring homomorphism.

Exercises

7.1 Let R be a commutative ring with $a, b, c \in R$. Prove that if $ab = 1 = ac$, then $b = c$.

7.2 Prove Lemmas 7.1, 7.2, 7.3, 7.6.

7.3 Let R be a commutative ring and let S be a set with $+, \times, -, 0, 1$. Let $f : R \to S$ be a surjective map such that for any $a, b \in R$, we have

$$f(a + b) = f(a) + f(b), \qquad f(ab) = f(a)f(b), \qquad f(-a) = -f(a), \qquad f(0) = 0, \qquad f(1) = 1.$$

Prove that S with $+, \times, -, 0, 1$ is a commutative ring.

7.4 Let R_1, R_2, R_3 be commutative rings and let $f : R_1 \to R_2$ and $g : R_2 \to R_3$ be ring homomorphisms. Prove that $g \circ f : R_1 \to R_3$ defined by $(g \circ f)(a) = g(f(a))$ is a ring homomorphism.

7.5 Let $f : R \to R'$ be an isomorphism between two commutative rings. Prove that its inverse $f^{-1} : R' \to R$ is a ring homomorphism, and so is also an isomorphism. (Recall that f^{-1} is defined so that for any $b \in R'$, $f^{-1}(b)$ is the unique $a \in R$ such that $f(a) = b$.)

7.6 Let R be a commutative ring with characteristic d. Let $f : \mathbb{Z} \to R$ be the unique ring homomorphism. Prove that if $f(n) = 0$ for some integer n, then $d \mid n$.

7.7 Let R be a commutative ring with characteristic d and let R' be a commutative ring with characteristic e. Let $f : R \to R'$ be a ring homomorphism. Prove that $e \mid d$.

7.8 Prove that a subring of a field is an integral domain.

7.9 Prove that $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic.

7.10 Let $R = \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$. Let $r = (0, 1)$. Prove that:

(a) whenever $r \mid ab$ for some $a, b \in R$, we have $r \mid a$ and $r \mid b$;

(b) there exist $a, b \in R \backslash R^\times$ such that $r = ab$.

7.11 Let $R = \mathbb{Q} + x\mathbb{R}[x] = \{f(x) \in \mathbb{R}[x] \colon f(0) \in \mathbb{Q}\}$. Verify that R is a subring of $\mathbb{R}[x]$. Prove that:

(a) there exist $a, b \in R$ such that $x \mid ab$ but $x \nmid a$ and $x \nmid b$;

(b) there do not exist $a, b \in R \backslash R^\times$ such that $x = ab$.

Lecture 11 Fri 09/29

8 Quotients

It is time to stop beating around the bush and talk about what / means. Let R ba a commutative ring. An **ideal** is a subset $I \subseteq R$ such that

(a) for any $a, b \in I$, we have $a + b \in I$;

(b) for any $a \in I$ and any $r \in R$, we have $ra \in I$.

Suppose $f : R \to R'$ is a ring homomorphism between two rings R and R'. We define the **kernel** of f to be

$$\ker(f) = \{a \in R \colon f(a) = 0\}.$$

Then for any $a, b \in \ker(f)$, we have $a + b \in \ker(f)$ since

$$f(a + b) = f(a) + f(b) = 0 + 0 = 0$$

and for any $r \in R$, we have $ra \in \ker(f)$ since

$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0.$$

In other words, the kernel of a ring homomorphism is a **proper** ideal, that is an ideal not equal to R. The punchline is that conversely, every proper ideal arises as the kernel of some ring homomorphism from R.

Examples:

1. Let R be a commutative ring. Let $a \in R$ be any element. The set

   $$aR = (a) = \{ra \colon r \in R\}$$

   is the smallest ideal containing a. It is easy to check that $r_1a + r_2a = (r_1 + r_2)a$ and $r(r_0a) = (rr_0)a$. For example, this gives the ideals $(d) = d\mathbb{Z}$ of $\mathbb{Z}$ for any integer d, and the ideals $(f(x))$ of $R[x]$ for any polynomial $f(x) \in R[x]$. When $a = 0$, we have the zero ideal $(0) = \{0\}$ and when $a = 1$, we have the full ring $(1) = R$.

   Ideals of the form (a) are called **principal** ideals. Note that $b \in (a)$ if and only if $a \mid b$. Then $(a) = (b)$ if and only if $a \mid b$ and $b \mid a$. When R is an integral domain, the latter is equivalent to $b = au$ for some unit $u \in R^\times$.

2. If an ideal I contains a unit $u \in R^\times$, then I contains $uu^{-1} = 1$ and so $I = R$. If R is a field, then any nonzero ideal contains a nonzero element, which we know is a unit. So then a field (e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$) has only the zero ideal and the full ring as ideals.

3. If I_1 and I_2 are ideals, then so are $I_1 \cap I_2$ and $I_1 + I_2 = \{a+b\colon a \in I_1, b \in I_2\}$. An arbitrary intersection of ideals is also an ideal. Given any set S, we can define the ideal generated by S, denoted (S), as the intersection of all the ideals containing S.

   Suppose $a, b \in \mathbb{Z}$. Then

$$\begin{aligned} a\mathbb{Z} + b\mathbb{Z} &= \{ax + by\colon x, y \in \mathbb{Z}\} &&= \gcd(a,b)\mathbb{Z} \\ a\mathbb{Z} \cap b\mathbb{Z} &= \{n \in \mathbb{Z}\colon a \mid n, b \mid n\} &&= \operatorname{lcm}(a,b)\mathbb{Z}. \end{aligned}$$

   The set $\{ab\colon a \in I_1, b \in I_2\}$ is generally not an ideal since it may not be closed under addition. The ideal generated by it is denoted $I_1 I_2 = \{a_1 b_1 + \cdots + a_n b_n\colon a_i \in I_1, b_i \in I_2\}$. Note each $a_i b_i \in I_1 \cap I_2$. So $I_1 I_2 \subseteq I_1 \cap I_2$. In $\mathbb{Z}$, we have $(a\mathbb{Z})(b\mathbb{Z}) = (ab)\mathbb{Z}$.

We now construct the quotient ring given a commutative ring R and a proper ideal I. A **coset** of I is a subset of R of the form

$$a + I = \{a + b\colon b \in I\} = \{c \in R\colon c - a \in I\}.$$

Such a coset is called the coset of I containing a, since it literally contains a as a set. We see that two cosets $a_1 + I$ and $a_2 + I$ are equal if and only if $a_1 - a_2 \in I$. Let R/I be the set of all cosets of I. So

$$R/I = \{a + I\colon a \in R\}.$$

The assumption that I is a proper ideal instead of just an ideal ensures that R/I contains at least 2 elements. When $R = \mathbb{Z}$ and $I = m\mathbb{Z}$, a coset $a + m\mathbb{Z}$ is the set of integers congruent to a mod m, i.e. is what we know to be a congruence class. The set $\mathbb{Z}/m\mathbb{Z}$ is then the set of all congruence classes mod m.

There is now an obvious way to define arithmetic on R/I:

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I)(b + I) = (ab) + I, \qquad -(a + I) = (-a) + I$$

with $0 + I$ as 0 and $1 + I$ as 1. In other words, to add (resp. multiply, negate) two cosets, we simply pick any element from them and add (resp. multiply, negate) them in R, and then take the coset containing them. We need to check that this definition does not depend on the choice of the elements picked. Suppose $a + I = a' + I$ and $b + I = b' + I$. Then $a - a' \in I$ and $b - b' \in I$. Now

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I, \qquad (-a') - (-a) = a - a' \in I,$$

and

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I.$$

When $R = \mathbb{Z}$ and $I = m\mathbb{Z}$, these are just the usual laws on adding and multiplying numbers mod m.

There is natural surjective map $\pi : R \to R/I$ defined by $a \mapsto a + I$. It is a ring homomorphism by construction of R/I and its kernel

$$\ker(\pi) = \{a \in R\colon a + I = I\} = \{a \in R\colon a \in I\} = I.$$

This proves that every proper ideal arises as the kernel of some ring homomorphism. In fact, every ring homomorphism is "basically" a quotient map.

Theorem 8.1 *(First isomorphism theorem) Let $f : R_1 \to R_2$ be a homomorphism of rings. Then the image $im(f) = \{f(r)\colon r \in R_1\}$ is a subring of R_2 and the map $R_1/\ker(f) \to im(f)$ sending $r + \ker(f)$ to $f(r)$ is an isomorphism.*

Proof: Exercise. Just check definitions. □

Corollary 8.2 *If R has characteristic m, then R has a subring isomorphic to $\mathbb{Z}/m\mathbb{Z}$. This subring is called the prime subring of R, or prime subfield if m is prime.*

Proof: The unique homomorphism $\mathbb{Z} \to R$ has kernel $m\mathbb{Z}$ (by Section 7 Exercise 6). Hence, its image is a subring of R isomorphic to $\mathbb{Z}/m\mathbb{Z}$. $\square$

We may also view R/I as the set of equivalence classes. Recall that a relation $\sim$ is an **equivalence relation** if:

(a) (Reflexive) $a \sim a$;

(b) (Symmetric) $a \sim b \Rightarrow b \sim a$;

(c) (Transitive) $a \sim b \wedge b \sim c \Rightarrow a \sim c$

An equivalence class containing a is the set $[a] = \{b \in R\colon b \sim a\}$. Two distinct equivalence classes are disjoint so that R is a disjoint union of equivalence classes. We then define the set $R/\sim$ of equivalence classes as $\{[a]\colon a \in R\}$. Now given an ideal I, we define $a \sim b$ by $b - a \in I$.

Lecture 12 Mon 10/02

We remark that the definition of cosets and R/I only uses the addition of R and the fact that I is closed under addition. So if J is a subset of R that is closed under addition and subtraction, then we can still define the set R/J of cosets of J and we can still define $+$ on it. One example where this may be useful is when J is the image of a ring homomorphism $f : R_1 \to R_2$. The quotient $R_2/\mathrm{im}(f)$ is called the **cokernel** of f, denoted $\mathrm{coker}(f)$. It is not a ring.

Theorem 8.3 *(Chinese remainder theorem) Let R be a commutative ring. Let I and J be two ideals of R such that $I + J = R$. Then the natural map*

$$\varphi : r \mapsto (r + I, r + J)\colon R \to R/I \times R/J$$

is a surjective homomorphism with kernel IJ. In other words,

$$R/(IJ) \cong R/I \times R/J.$$

Remark: When $R = \mathbb{Z}$ and $I = m_1\mathbb{Z}$, $J = m_2\mathbb{Z}$, we saw before that $I+J = \gcd(m_1, m_2)\mathbb{Z}$ and $IJ = m_1m_2\mathbb{Z}$. So the condition that $I + J = R$ is the same as $\gcd(m_1, m_2) = 1$. The conclusion gives

$$\mathbb{Z}/m_1m_2\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}.$$

An integer mod m_1m_2 is uniquely determined by what it is mod m_1 and mod m_2 and all combinations occur.

Proof: The assumption $I + J = R$ means that there exist $a \in I$ and $b \in J$ such that $a + b = 1$. We prove φ is surjective. Take any $s, t \in R$. We need to find an $r \in R$ such that $r - s \in I$ and $r - t \in J$. Let $r = ta + sb$. Then

$$\begin{aligned} r - s &= ta + s(b - 1) = ta - sa \in I, \\ r - t &= t(a - 1) + sb = -tb + sb \in J. \end{aligned}$$

The kernel of φ is clearly $I \cap J$. We already know that $IJ \subseteq I \cap J$, so it remains to prove $I \cap J \subseteq IJ$. Let $r \in I \cap J$. Then $r = r(a + b) = ra + rb \in IJ$. $\square$

We consider the application to modular arithmetic. Suppose $m \geq 2$ with prime factorization

$$m = p_1^{k_1} \cdots p_r^{k_r}.$$

Then

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z} \\ \left(\mathbb{Z}/m\mathbb{Z}\right)^\times &\cong \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{k_r}\mathbb{Z}\right)^\times \end{aligned}$$

Lemma 8.4 *Let $m \geq 2$. Then $(\mathbb{Z}/m\mathbb{Z})^\times = \{a + m\mathbb{Z} \colon \gcd(a, m) = 1\}$. Its size is $\phi(m)$.*

Proof: The coset $a + m\mathbb{Z}$ is a unit if and only if there exists $b + m\mathbb{Z}$ such that $(a + m\mathbb{Z})(b + m\mathbb{Z}) = 1 + m\mathbb{Z}$. In other words, $ab \equiv 1 \pmod{m}$. This is the same requiring $ax + my = 1$ to have an integer solution, which is the same as $\gcd(a, m) = 1$. □

Corollary 8.5 *Let $m \geq 2$. Then $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if $m = p$ is a prime. We write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$.*

Corollary 8.6 *Let $m \in \mathbb{N}$. Then*

$$\phi(m) = \prod_{i=1}^{r} \left(p_i^{k_i} - p_i^{k_i - 1} \right) = m \prod_{p \mid m} \left(1 - \frac{1}{p} \right).$$

Proof: We have $\phi(m) = \prod_{i=1}^{r} \phi(p_i^{k_i})$. It is easy to see that for any prime p and positive integer k, $\phi(p^k) = p^k - p^{k-1}$ since there are p^{k-1} numbers in $1, 2, \ldots, p^k$ that are divisible by p. □

Theorem 8.7 *Let R be a finite commutative ring. Then for any $a \in R$, we have $|R| \cdot a = 0$. For any $a \in R^\times$, we have $a^{|R^\times|} = 1$.*

Proof: We prove the statement for $R^\times$. The statement for R follows by a similar argument. We note that if $b \in R^\times$, then so it ab since $ab(b^{-1}a^{-1}) = 1$. Hence the map $x \mapsto xa$ defines a permutation on $R^\times$. Let $a_1, \ldots, a_n$ denote all the elements of $R^\times$. Then $aa_1, \ldots, aa_n$ also are all the elements of $R^\times$. Multiplying them together gives

$$a_1 \cdots a_n = (aa_1) \cdots (aa_n) = a^{|R^\times|}(a_1 \cdots a_n).$$

Multiplying both sides by $a_n^{-1} \cdots a_1^{-1}$ gives $a^{|R^\times|} = 1$. □

Corollary 8.8 *(Euler's Theorem, Fermat's little Theorem) Let $m \in \mathbb{N}$. Let a be an integer coprime to m. Then $a^{\phi(m)} \equiv 1 \pmod{m}$. If $m = p$ is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

We write $o_+(a)$, the additive order of a in R, for the smallest positive integer d such that $da = 0$. Then by a standard division algorithm argument (see for example the proof of Proposition 5.3, we have $o_+(a) \mid |R|$. We write $o(a)$, the order of a in $R^\times$, for the smallest positive integer d such that $a^d = 1$ if $a \in R^\times$. Then $o(a) \mid |R^\times|$.

Example: Let's find the last 2 digits of $3^{3^{3^3}} = 3^{3^{27}}$. This is the same finding what it is mod 100, which is the same as finding what it is mod 25 and mod 4.

Lemma 8.9 *Suppose $n \in \mathbb{N}$ and $n \equiv 7 \pmod{20}$. Then $3^n \equiv 87 \pmod{100}$.*

Proof: Since n is odd, we see that $3^n \equiv (-1)^n \equiv -1 \pmod{4}$. Since $\phi(25) = 20$, we see that $3^{20} \equiv 1 \pmod{25}$. Then for any positive integer of the form $20k + 7$, we have

$$3^{20k+7} = (3^{20})^k 3^7 \equiv 3^7 \equiv 27 \times 27 \times 3 \equiv 12 \pmod{25}.$$

Since 87 is 1 mod 4 and 12 mod 25, we have $3^n \equiv 87 \pmod{100}$. □

Now $3^n \equiv 87 \pmod{100}$ implies $3^n \equiv 7 \pmod{20}$ and so $3^{3^n} \equiv 87 \pmod{100}$ and we may repeat this forever. In other words, $3^{3^3}, 3^{3^{3^3}}, 3^{3^{3^{3^3}}}, \ldots$ all end in 87.

Exercises

8.1 (Correspondence Theorem) Let R be a commutative ring and let I be an ideal of R. Prove that the ideals of R/I are of the form

$$J/I := \{a + I : a \in J\}$$

for some ideal J of R containing I.

8.2 (Second Isomorphism Theorem) Let R be a commutative ring and let I be an ideal of R. Let S be a subring of R. Prove that:

(a) $S + I = \{s + a : s \in S, a \in I\}$ is a subring of R;

(b) $S \cap I$ is an ideal of S;

(c) $(S + I)/I \cong S/(S \cap I)$.

8.3 (Third Isomorphism Theorem) Let R be a commutative ring and let I be an ideal of R. Let J be an ideal of R containing I. Prove that

$$(R/I)/(J/I) \cong R/J.$$

8.4 Let R be a commutative ring and let I be an ideal of R. Let

$$I[x] = \{a_n x^n + \cdots + a_0 \in R[x] : a_i \in I\}.$$

Prove that $R[x]/I[x] \cong (R/I)[x]$.

8.5 Prove that the ideals of $\mathbb{Z}$ are all of the form $d\mathbb{Z}$ for some non-negative integer d. What are the subrings of $\mathbb{Z}$? For a general commutative ring R, which ideal can also be a subring?

8.6 Let R be the ring of continuous (real-valued) functions on $[0, 3]$ with pointwise addition and multiplication, and the constant functions 0 and 1 as 0 and 1. Consider

$$a(x) = \begin{cases} 1 - x & \text{if } 0 \le x \le 1 \\ 0 & \text{if } 1 \le x \le 2 \\ x - 2 & \text{if } 2 \le x \le 3 \end{cases}, \qquad b(x) = \begin{cases} 1 - x & \text{if } 0 \le x \le 1 \\ 0 & \text{if } 1 \le x \le 2 \\ 2 - x & \text{if } 2 \le x \le 3 \end{cases}.$$

Prove that $a(x)R = b(x)R$ but there does not exist a unit $u(x) \in R^\times$ such that $b(x) = a(x)u(x)$.

8.7 Let R be a commutative ring and let $a \in R^\times$ with $o(a)$ finite. Prove that for any $k \in \mathbb{N}$, we have

$$o(a^k) = \frac{o(a)}{\gcd(o(a), k)}.$$

8.8 Let $n = 2 \cdot 11 \cdot 43$. Prove that $n \mid 2^n + 2$.

It is a lot trickier to prove that if n is odd, then it is impossible for $n \mid 2^n + 2$.

8.9 Let c, m be any positive integers. Prove that the sequence $a_1 = c$, $a_{n+1} = c^{a_n}$ is eventually constant mod m.

Lecture 13 Wed 10/04

9 Polynomials over a field

In this section, we focus on the polynomial ring $F[x]$ where F is a field. We saw before that the units of $F[x]$ are the nonzero constants $F^\times$. Recall that the degree of a polynomial $a_n x^n + \cdots + a_0$ is the largest index n such that $a_n \neq 0$. We follow the convention of $\deg(0) = -\infty$.

Proposition 9.1 *(Division algorithm for polynomials) Let R be an integral domain. Let $f(x) \in R[x]$ and let $g(x) \in R[x]$ such that the leading coefficient of g is a unit in R. Then there exist polynomials $q(x), r(x) \in R[x]$ such that*

$$f(x) = g(x)q(x) + r(x), \qquad \text{and} \qquad \deg(r) < \deg(g).$$

Proof: Standard induction on the degree of $f(x)$. Let a denote the leading coefficient of $g(x)$. So $a \in R^\times$. If $g(x) = a$ has degree 0, then we take $q(x) = a^{-1}f(x)$ and $r(x) = 0$. Suppose now $\deg(g) > 0$. We prove by induction on $\deg(f)$. If $\deg(f) < \deg(g)$, we simply take $q = 0$ and $r = f$. Suppose now $\deg(f) \geq \deg(g)$. Let $b \in R$ be the leading coefficient of $f(x)$. Then

$$f(x) - ba^{-1}x^{\deg(f)-\deg(g)}g(x)$$

is a polynomial with less degree than f. Apply induction. □

When $R = \mathbb{Z}$, the condition that the leading coefficient of g is unit means that it is ± 1. When $R = F$ is a field, we just need g to be nonzero. In the language of HW 4 Problem 4, $F[x]$ is a Euclidean domain. All ideals are generated by one element. An integral domain where every ideal is generated by one element is called a **Principal ideal domain** or PID. In a PID R, the ideal (a, b) generated by two elements a, b is of the form (c). Since R is an integral domain, we know that $(c) = (c')$ if and only if $c' = uc$ for some unit $u \in R^\times$. One can choose a generator of the ideal (c) (sometimes the ideal itself) as the gcd of a and b. When $R = \mathbb{Z}$, we can choose the generator to be positive. When $R = F[x]$, we can choose the generator to be monic.

A polynomial $f(x) \in F[x]$ is **irreducible** if $\deg(f) \geq 1$ and there do not exist polynomials $a(x), b(x) \in F[x]$ of degree at least 1 such that $a(x)b(x) = f(x)$. The analogue of Euclid's lemma and the fundamental theorem of arithmetic are left as HW 5 Problem 1.

Proposition 9.2 *Let F be a field.*

(a) Suppose $f(x) \in F[x]$ is irreducible. If $f(x) \mid a(x)b(x)$ in $F[x]$, then $f(x) \mid a(x)$ or $f(x) \mid b(x)$.

(b) Every non-constant polynomial in $F[x]$ can be factored into a product of irreducible polynomials in $F[x]$.

Remark: In general, for a commutative ring R, we say a nonzero element $r \in R$ is *irreducible* if it is not a unit and there do not exist $a, b \in R \backslash R^\times$ such that $r = ab$. We say a nonzero element $r \in R$ is *prime* if whenever $r \mid ab$ for some $a, b \in R$, we have $r \mid a$ or $r \mid b$. In an integral domain, prime implies irreducible. As Exercise 7.10 shows, this is not true if R is not an integral domain. Conversely, as Exercise 7.11 shows, there are also integral domains where irreducible does not imply prime.

For any ring R and any $\alpha \in R$, there is an evaluation homomorphism $\mathrm{ev}_\alpha : R[x] \to R$ sending

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \;\; \mapsto \;\; a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0.$$

We write $f(\alpha) \in R$ for the image of f under this map.

Proposition 9.3 *Let R be an integral domain. Let $f(x) \in R[x]$ and let $c \in R$. The remainder when $f(x)$ is divided by $x - c$ is the constant polynomial $f(c)$.*

Proof: The remainder $r(x)$ satisfies $\deg(r) < \deg(x - c) = 1$. So $r(x) = r_0$ is a constant. Apply ev_c to $f(x) = (x - c)q(x) + r_0$ to get $r_0 = f(c)$. □

Corollary 9.4 *Let R be an integral domain. Let $f(x) \in R[x]$ and let $c_1, \ldots, c_n \in R$ be distinct. Then $c_1, \ldots, c_n$ all are roots of $f(x)$ if and only if $(x - c_1)(x - c_2) \cdots (x - c_n) \mid f(x)$.*

Proof: Only the forwards direction needs to be proved. We prove by induction on n. The case $n = 1$ follows immediately from Proposition 9.3. Suppose now $n \geq 2$. By induction using $c_1, \ldots, c_{n-1}$, we see that there exists $g(x) \in R[x]$ such that $f(x) = (x - c_1) \cdots (x - c_{n-1})g(x)$. Apply ev_{c_n} to get

$$0 = (c_n - c_1) \cdots (c_n - c_{n-1})g(c_n).$$

Since each $c_n - c_i \neq 0$ and R is an integral domain, we see that $g(c_n) = 0$. Then $g(x) = (x - c_n)h(x)$ for some $h \in R[x]$. So $f(x) = (x - c_1) \cdots (x - c_n)h(x)$. □

Corollary 9.5 *Let R be an integral domain. Let $f(x) \in R[x]$ with degree $d \geq 0$. Then $f(x)$ has at most d distinct roots in R.*

Corollary 9.6 *Let F be a field. Linear (degree 1) polynomials in $F[x]$ are all irreducible. Quadratic (degree 2) and cubic (degree 3) polynomials in $F[x]$ are irreducible if and only if they don't have a root in F.*

Proof: Any factorization of a polynomial of degree at most 3 into polynomials of smaller degrees must involve a linear polynomial, which will produce a root of f in F. □

We say $c \in R$ is a repeated root of $f(x)$ if $(x - c)^2 \mid f(x)$. Repeated roots can be checked using the formal **derivative** of $f(x)$ defined as

$$f'(x) = na_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

The word "formal" is referring to the fact that this has nothing to do with taking limits. The same rules of derivatives in calculus apply here:

$$(f + g)'(x) = f'(x) + g'(x), \qquad (fg)'(x) = f(x)g'(x) + f'(x)g(x), \qquad (f \circ g)'(x) = f'(g(x))g'(x).$$

Additivity is easy to check from the definition. Then one can use it to reduce the product rule and the chain rule to the case $f(x) = a_n x^n$.

Proposition 9.7 *Let R be an integral domain. Let $f(x) \in R[x]$ and let $c \in R$. Then c is a repeated root of $f(x)$ if and only if $f(c) = f'(c) = 0$.*

Proof: For both directions, we may assume c is a root. So $f(x) = (x - c)g(x)$ for some $g(x) \in R[x]$. Differentiate it to get $f'(x) = g(x) + (x - c)g'(x)$. Hence $f'(c) = g(c)$. So $g(x)$ has another factor of $x - c$ if and only if $f'(c) = 0$. □

The moral of the story is that $F[x]$ and $\mathbb{Z}$ are very similar, except we have an extra operation of differentiation for $F[x]$. This differentiation allows one to prove versions of the abc conjecture (Mason's Theorem) and Fermat's last theorem over $F[x]$. One can test for existence of repeated roots by applying the Euclidean algorithm to find the gcd of $f(x)$ and $f'(x)$. However, testing for squarefree integers is as difficult as factorization.

The process of turning $\mathbb{Z}$ into $\mathbb{Q}$ is the process of taking the field of fraction. We have

$$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}.$$

We can do the same thing with $F[x]$ (in fact with any integral domains) to define the field $F(x)$ of rational functions:

$$F(x) = \left\{ \frac{a(x)}{b(x)} : a(x), b(x) \in F[x], b(x) \neq 0 \right\}.$$

Arithmetic works just as you expect with fractions. For example

$$\frac{a(x)}{b(x)} + \frac{c(x)}{d(x)} = \frac{a(x)d(x) + b(x)c(x)}{b(x)d(x)}.$$

Remark: To be more precise, we need the notion of *localizations*. Let R be a commutative ring. Let S be a multiplicatively closed subset of R that does not contain 0. In other words, $1 \in S$ and $ab \in S$ for any $a, b \in S$. We denote an element (r, s) of $R \times S$ suggestively as $\frac{r}{s}$, and define a relation $\sim$ on $R \times S$ by

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \iff \exists s_3 \in S,\ s_3(r_1 s_2 - r_2 s_1) = 0.$$

When R is an integral domain, this is equivalent to simply $r_1 s_2 = r_2 s_1$. It is easy to check that $\sim$ defines an equivalence relation on $R \times S$. We define the localization $S^{-1}R$ as the set $(R \times S)/\sim$ of equivalence classes. In other words, one may think of elements of $S^{-1}R$ as fractions r/s where $r \in R$ and $s \in S$, keeping in mind that multiple fractions could correspond to the same elements. We can then define the ring operations on $S^{-1}R$ by

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}, \qquad 0 = \frac{0}{1}, \qquad 1 = \frac{1}{1}.$$

It is easy to check that the above addition and multiplication do not depend on the choice of representatives. In other words,

$$\text{if } \frac{r_1}{s_1} \sim \frac{r_1'}{s_1'} \text{ and } \frac{r_2}{s_2} \sim \frac{r_2'}{s_2'}, \text{ then } \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \sim \frac{r_1' s_2' + r_2' s_1'}{s_1' s_2'} \text{ and } \frac{r_1 r_2}{s_1 s_2} \sim \frac{r_1' r_2'}{s_1' s_2'}.$$

There is a ring homomorphism $R \to S^{-1}R$ sending r to $r/1$. Note that elements of the form $s/1$ where $s \in S$ are units in $S^{-1}R$ since $1/s \in S^{-1}R$. In this sense, one can think of the localization $S^{-1}R$ is an "extension" of R where we add inverses of elements of S, hence the notation. Since elements in S become units, the proper ideals of $S^{-1}R$ correspond to ideals of R disjoint from S, i.e. contained in $R \backslash S$, hence the name "localization".

When R is an integral domain, the set $R\backslash\{0\}$ of nonzero elements of R is multiplicatively closed. In the localization $(R\backslash\{0\})^{-1}R$, we are adding inverses to every nonzero element of R. In this case, $(R\backslash\{0\})^{-1}R$ is a field, and is the proper definition for the *field of fraction* of an integral domain.

Lecture 14 Fri 10/06

We consider the quotient $F[x]/(g(x))$ for some fixed $g(x) \in F[x]$ of degree $d \geq 1$. By the division algorithm, any $f(x) \in F[x]$ is of the form $g(x)q(x) + r(x)$ where $\deg(r) < d$. So

$$f(x) + (g(x)) = r(x) + (g(x)).$$

Moreover, by considering degrees, we see that no two of such $r(x) + (g(x))$ are equal. Hence

$$F[x]/(g(x)) = \{r(x) + (g(x)) \colon \deg(r) \leq d - 1\}.$$

Proposition 9.8 *Let F be a field and let $g(x) \in F[x]$ with degree at least 1. Then the following are equivalent:*

(a) $F[x]/(g(x))$ is a field;

(b) $F[x]/(g(x))$ is an integral domain;

(c) $g(x)$ is irreducible.

Proof: Suppose first that $g(x)$ is not irreducible. Then it factors as $a(x)b(x)$ for some $a(x), b(x) \in F[x]$ with degrees between 1 and $\deg(g) - 1$. Then $a(x) + (g(x))$ and $b(x) + (g(x))$ are nonzero in $F[x]/(g(x))$ but their product is $g(x) + (g(x))$ which is zero. Hence $F[x]/(g(x))$ is not an integral domain. This proves $(b) \Rightarrow (c)$.

Suppose now $g(x)$ is irreducible. Let $f(x) + (g(x)) \in F[x]/(g(x))$ be any nonzero element. The ideal $I = (f(x), g(x))$ is of the form $h(x)$ for some $h(x) \in F[x]$. We prove that $I = F[x]$. From $g(x) \in (h(x))$, we have $g(x) = h(x)j(x)$ for some $j(x) \in F[x]$. Since $g(x)$ is irreducible, we have either $h(x)$ or $j(x)$ is a nonzero constant. If $j(x)$ is a nonzero constant j_0, then it is a unit in $F[x]$ and so $(h(x)) = (g(x))$ contradicting $f \notin (g)$. So $h(x)$ is a nonzero constant, implying that $(f(x), g(x)) = F[x]$. Hence there exist $a(x), b(x) \in F[x]$ such that $a(x)f(x) + b(x)g(x) = 1$. In other words, $a(x)f(x) + (g(x)) = 1 + (g(x))$. Hence $F[x]/(g(x))$ is a field. This proves $(c) \Rightarrow (a)$. Finally $(a) \Rightarrow (b)$ is trivial. □

We consider $F = \mathbb{F}_2 = \{0, 1\}$. There are 4 degree 2 polynomials: x^2, $x^2 + 1$, $x^2 + x$ and $x^2 + x + 1$. The first three are reducible, note that $x^2 + 1 = (x+1)^2$, and the last one is irreducible. The ring $\mathbb{F}_2[x]/(g(x))$ has size 4 and characteristic 2. It is easy to check that

$$f(x) + (x^2) \mapsto f(x+1) + ((x+1)^2)$$

defines an isomorphism $\mathbb{F}_2[x]/(x^2) \cong \mathbb{F}_2[x]/((x+1)^2)$. Note also that $x^2 + x = x(x+1)$ with $(x, x+1) = (1)$. Hence by the Chinese Remainder Theorem,

$$\mathbb{F}_2[x]/(x^2 + x) \cong \mathbb{F}_2[x]/(x) \times \mathbb{F}_2[x]/(x+1) \cong \mathbb{F}_2 \times \mathbb{F}_2.$$

This leaves $\mathbb{F}_2[x]/(x^2 + x + 1)$ as the field $\mathbb{F}_4$. In degree 3, there are two irreducible polynomials $x^3 + x + 1$ and $x^3 + x^2 + 1$. Are the two fields $\mathbb{F}_2[x]/(x^3 + x + 1)$ and $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ of size 8 isomorphic?

Corollary 9.9 *Let p be a prime. Let $g(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree d. Then $\mathbb{F}_p[x]/(g(x))$ is field of p^d elements.*

In HW5, you will prove that any finite commutative ring has a decomposition of the form

$$R \cong R_1 \times R_2 \times \cdots R_r$$

where $|R_i| = p_i^{d_i}$ and $p_1, \ldots, p_r$ are distinct primes. It follows then that any finite field F (i.e. integral domain) has size p^d for some prime p. We saw before that the characteristic of an integral domain is a prime, and in HW4 that the characteristic divides the size of the ring. Hence the prime p is necessarily the characteristic of F. Hence the prime subfield of F is $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Exercise

9.1 Prove that the ideal $(2, x)$ in $\mathbb{Z}[x]$ is not principal.

9.2 What are the irreducible polynomials in $\mathbb{C}[x]$? What are the irreducible polynomials in $\mathbb{R}[x]$?

9.3 Let R be a commutative ring and let I be a proper ideal of R. We say I is a **maximal ideal** of R if there does not exist a proper ideal J such that I is a proper subset of J. Prove that I is maximal if and only if R/I is a field.

There is also a notion of a **prime ideal**. Can you guess what its definition is and how it relates to R/I?

9.4 Give an example of a commutative ring R, a maximal ideal I, and a subring S such that $S \cap I$ is not maximal in S.

9.5 What are all the maximal ideals of $\mathbb{Z}[x]$?

9.6 For any commutative ring R, we write $R[x, y]$ for the ring $(R[x])[y]$. Prove that the maximal ideals of $\mathbb{C}[x, y]$ are of the form $(x - a, y - b)$ for some $a, b \in \mathbb{C}$. (Hint: recall the similarity between $\mathbb{C}[x]$ and $\mathbb{Z}$, and mimic your solution for Exercise 4.)

It is in fact true that the maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ are of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in \mathbb{C}$. This result is known as Hilbert's Nullstellensatz (theorem of zeros in German). The rings $\mathbb{C}[x_1, \ldots, x_{n-1}]$ for $n \geq 3$ are no longer PID so your solutions for Exercise 5 and 6 above likely will not generalize.

9.7 Find all irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$.

9.8 Let p be a prime. Prove that $x^2 + x + 1 \in \mathbb{F}_p[x]$ is irreducible if and only if $p \not\equiv 1 \pmod 3$.

10 Finite fields

The main theorem in the theory of finite fields is:

Theorem 10.1 *For every prime p and every positive integer d, there is a unique field of size p^d up to isomorphism, given by*

$$\mathbb{F}_{p^d} \cong \mathbb{F}_p[x]/(g(x))$$

where $g(x) \in \mathbb{F}_p[x]$ is irreducible of degree d.

The key theorem is the existence of a primitive element.

Theorem 10.2 *Let F be a finite field of size p^n for some prime p and some positve integer n. Then there exists $a \in F^\times$ such that $o(a) = p^n - 1$.*

Such an element a is called a **primitive** element of F as every nonzero element is a power of a:

$$F^\times = \{a, a^2, \ldots, a^{p^n - 1}\}.$$

Proof: Write $m = p^n - 1$. For any positive divisor d of m, let N_d denote the number of elements in F with order exactly d. We prove that $N_d \leq \phi(d)$. If $N_d = 0$, then this is obviously true. Suppose $N_d > 0$ and let α be an element of order d. Any element of order d is a root of the degree d polynomial $x^d - 1 \in F[x]$ and $\alpha, \alpha^2, \ldots, \alpha^d$ already give d of them, which are all distinct since $d = o(\alpha)$. In other words, any element of order d must be one of these d powers of α. Recall from Exercise 8.7 that for any integer k,

$$o(\alpha^k) = \frac{o(\alpha)}{\gcd(k, o(\alpha))}.$$

Hence we see that $o(\alpha^k) = d$ if and only if $\gcd(k, o(\alpha)) = 1$. Therefore, $N_d = \phi(d)$.

Since every element in $F^\times$ has order dividing m, we have

$$m = \sum_{d \mid m} N_d \leq \sum_{d \mid m} \phi(d) = m,$$

by Corollary 6.2. Therefore, $N_d = \phi(d)$ for every $d \mid m$. In particular, $N_m = \phi(m) > 0$. □

Lecture 15 Mon 10/16

Corollary 10.3 *Let F be a finite field of size p^n for some prime p and some positive integer n. Then $F \cong \mathbb{F}_p[x]/(f(x))$ for some irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n.*

Proof: Let $a \in F^\times$ be an element of order $p^n - 1$. Then every element of $F^\times$ is a power of a. Hence the evaluation map $\mathrm{ev}_a : \mathbb{F}_p[x] \to F$ is a surjective homomorphism. The kernel of ev_a is an ideal of $\mathbb{F}_p[x]$ and so is of the form $(f(x))$ for some $f(x) \in \mathbb{F}_p[x]$. By the first isomorphism theorem, F is isomorphic to $\mathbb{F}_p[x]/(f(x))$. In order for this quotient to be a field, $f(x)$ must be irreducible by Proposition 9.8. □

To see that an irreducible polynomial of degree n exists, we need the following result.

Theorem 10.4 *Let p be a prime and let $n \in \mathbb{N}$. Then $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree dividing n.*

For example, when $p = 2$, we have

$$\begin{aligned} x^4 - x &= x(x+1)(x^2+x+1) \\ x^8 - x &= x(x+1)(x^3+x^2+1)(x^3+x+1) \end{aligned}$$

Corollary 10.5 *Let $S_p(n)$ denote the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree n. Then $S_p(n) > 0$ for any $n \in \mathbb{N}$.*

Proof: Since degree is additive, we have

$$p^n = \sum_{d|n} dS_p(d) \qquad \Longrightarrow \qquad nS_p(n) = \sum_{d|n} \mu(d) p^{n/d},$$

by HW 3 Problem 3, where μ is the Mobius function. Note that if $d > 1$, then $n/d \leq n/2$. Hence

$$|p^n - nS_p(n)| = \left| \sum_{d|n, d>1} \mu(d) p^{n/d} \right| \leq p^{\lfloor n/2 \rfloor} + p^{\lfloor n/2 \rfloor - 1} + \cdots + 1 < p^{\lfloor n/2 \rfloor + 1} \leq p^n.$$

This implies that $nS_p(n) > 0$. □

For example

$$S_2(6) = \frac{1}{6}\left(2^6 - 2^3 - 2^2 + 2^1\right) = 9.$$

Corollary 10.6 *Let p be a prime and let $n \in \mathbb{N}$. Let $f(x), g(x) \in \mathbb{F}_p[x]$ be two irreducible polynomials of degree n. Then $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[x]/(g(x))$.*

We need a straightforward lemma on how to define a homomorphism out of these quotients.

Lemma 10.7 *Let p be a prime. Suppose $f(x)$ is an irreducible polynomial in $\mathbb{F}_p[x]$. Suppose R is a ring of characteristic p, so that the prime subfield of R is $\mathbb{F}_p$. Then any ring homomorphism $\mathbb{F}_p[x]/(f(x)) \to R$ is of the form $j(x) + (f(x)) \mapsto j(\alpha)$ for any $j(x) \in \mathbb{F}_p[x]$ where $\alpha \in R$ is a root of $f(x)$. Any such ring homomorphism is automatically injective.*

Proof: Easy exercise. Any ring homomorphism must be identity on the prime subfield $\mathbb{F}_p$. If it sends $x + (f(x))$ to α, then it sends $j(x) + (f(x))$ to $j(\alpha)$ for any $j(x) \in \mathbb{F}_p[x]$. Since $f(x) + (f(x))$ is 0, we must have $f(\alpha) = 0$. The kernel is a proper ideal of the field $\mathbb{F}_p[x]/(f(x))$ and so must be $\{0\}$. □

Proof of Corollary 10.6: Let $F = \mathbb{F}_p[x]/(g(x))$. It suffices to find a root α of $f(x)$ in F, since then we would have an injective homomorphism $\mathbb{F}_p[x]/(f(x)) \to \mathbb{F}_p[x]/(g(x))$, which is also surjective because they have the same size.

We may assume $f(x)$ and $g(x)$ are monic. Every nonzero element $\alpha \in F^\times$ satisfies $\alpha^{p^n - 1} - 1 = 0$. Hence, every element of F is a root of $x^{p^n} - x \in F[x]$. Since $x^{p^n} - x$ has at most p^n roots in F, we see that it splits completely in $F[x]$ as

$$x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha).$$

Hence $f(x)$ as a factor of $x^{p^n} - x$ in $\mathbb{F}_p[x]$, also splits completely in $F[x]$. We may then take any of its root to define the desired isomorphism. □

We collect two important results, which were proved in the above.

Corollary 10.8 *Every irreducible polynomial in $\mathbb{F}_p$ of degree dividing n splits completely in $\mathbb{F}_{p^n}$.*

Corollary 10.9 *Let F be a finite field and let $q = |F|$. Then*

$$x^q - x = \prod_{\alpha \in F} (x - \alpha).$$

Example: The field $\mathbb{F}_8$ is given by $\mathbb{F}_2[x]/(x^3+x+1)$ and also by $\mathbb{F}_2[x]/(x^3+x^2+1)$. Write $\alpha = x+(x^3+x^2+1)$ in $F = \mathbb{F}_2[x]/(x^3+x^2+1)$. Then $\alpha^3 + \alpha^2 + 1 = 0$. The irreducible polynomials x^3+x^2+1 and x^3+x+1 should split completely in F. Let's find their roots. Note that

$$(\alpha+1)^3 + (\alpha+1) + 1 = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha + 1 + 1 = \alpha^3 + \alpha^2 + 1 = 0.$$

Hence, $\alpha + 1$ is a root of $x^3 + x + 1$. The other two roots of $x^3 + x^2 + 1$ in F are α^2 and $\alpha^4 = \alpha^2 + \alpha + 1$. One can check this via

$$(\alpha^2)^3 + (\alpha^2)^2 + 1 = \alpha^6 + \alpha^4 + 1 = (\alpha^3 + \alpha^2 + 1)^2 = 0.$$

The other two roots of $x^3 + x + 1$ are $(\alpha+1)^2 = \alpha^2 + 1$ and $(\alpha+1)^4 = \alpha^4 + 1 = \alpha^2 + \alpha$. In other words, we have the factorizations

$$\begin{aligned} x^3 + x^2 + 1 &= (x+\alpha)(x+\alpha^2)(x+\alpha^2+\alpha+1), \\ x^3 + x + 1 &= (x+\alpha+1)(x+\alpha^2+1)(x+\alpha^2+\alpha). \end{aligned}$$

We make a very important observation. From the binomial expansion, we have

$$(a+b)^{p^n} = \sum_{r=0}^{p^n} \binom{p^n}{r} a^r b^{p^n - r}.$$

Moreover, we know that

$$\nu_p\left(\binom{p^n}{r}\right) = n - \nu_p(r) > 0 \qquad \text{if} \qquad 0 < r < p^n$$

by Corollary 4.4. In other words, all the middle coefficients are divisible by p. Therefore, if we are in characteristic p, then

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

In particular, if $f(x) = a_m x^m + \cdots + a_0 \in \mathbb{F}_{p^n}[x]$, then each $a_i^{p^n} = a_i$ and

$$f(x)^{p^n} = a_m^{p^n} x^{mp^n} + \cdots + a_0^{p^n} = a_m (x^{p^n})^m + \cdots + a_0 = f(x^{p^n}).$$

Lecture 16 Wed 10/18

Proof of Theorem 10.4: We recall a result proved in HW 1:

$$\gcd(p^k - 1, p^\ell - 1) = p^{\gcd(k,\ell)} - 1.$$

In particular,

$$p^k - 1 \mid p^\ell - 1 \quad \Longleftrightarrow \quad k \mid \ell.$$

We first prove that if $f(x) \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree $d \mid n$, then $x^{p^n} - x \in (f(x))$. If $d = 1$, then $f(x) = x - a$ for some $a \in \mathbb{F}_p$, in which case we know $x - a \mid x^{p^n} - x$ because $a^{p^n} = a$. Suppose now $d \geq 2$. Let $F = \mathbb{F}_p[x]/(f(x))$. Let $\alpha = x + (f(x))$. Then $\alpha \neq 0$ and so $\alpha^{p^d - 1} = 1$. Since $d \mid n$, we know that $p^d - 1 \mid p^n - 1$. Hence $\alpha^{p^n - 1} = 1$. So $\alpha^{p^n} = \alpha$. This means that $x^{p^n} - x \in (f(x))$.

Conversely, suppose $x^{p^n} - x \in (f(x))$ for some irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree d. We prove $d \mid n$. Again let $F = \mathbb{F}_p[x]/(f(x))$. Let $\alpha = a(x) + (f(x))$ be a primitive element so that $o(\alpha) = p^d - 1$.

We would be done if we can prove that $\alpha^{p^n} = \alpha$, which implies that $\alpha^{p^n-1} = 1$ and so $p^d - 1 \mid p^n - 1$. We note from last time that if $a(x) = a_m x^m + \cdots + a_0 \in \mathbb{F}_p[x]$, we have

$$a(x)^{p^n} = a_m x^{mp^n} + a_{m-1} x^{(m-1)p^n} + \cdots + a_0.$$

Now each

$$x^{jp^n} - x^j = ((x^{p^n} - x) + x)^j - x^j \in (x^{p^n} - x)$$

and so also in $(f(x))$. Hence we see that

$$a(x)^{p^n} - a(x) = \sum_{j=0}^{m} a_j (x^{jp^n} - x^j) \in (f(x)).$$

In other words, $\alpha^{p^n} = \alpha$ in F.

Finally, we need to prove that $x^{p^n} - x$ has no repeated factors, so that every monic irreducible polynomial of degree dividing n appears exactly once in the factorization of $x^{p^n} - x$. This follows easily from

$$(x^{p^n} - x)' = p^n x^{p^n - 1} - x = -1$$

which shares no common divisor with $x^{p^n} - x$. □

Proposition 10.10 *The field $\mathbb{F}_{p^n}$ has a subring isomorphic to $\mathbb{F}_{p^d}$ if and only if $d \mid n$, in which case, the subring is unique and we say $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$.*

Proof: Consider the subset

$$R = \{\alpha \in \mathbb{F}_{p^n} : \alpha^{p^d} = \alpha\}.$$

Then R has size at most p^d since it is the set of roots of a polynomial of degree p^d. Suppose a homomorphism $\varphi : \mathbb{F}_{p^d} \to \mathbb{F}_{p^n}$ (which is the same as an isomorphism from $\mathbb{F}_{p^d}$ to a subring of $\mathbb{F}_{p^n}$) exists. Then since every element β in $\mathbb{F}_{p^d}$ satisfies $\beta^{p^d} = \beta$, we have $(\varphi(\beta))^{p^d} = \varphi(\beta)$ and so $\varphi(\beta) \in R$. Comparing sizes gives that the image of φ is R. This proves uniqueness. Let β be an element of $\mathbb{F}_{p^d}$ of order $p^d - 1$. Then $\varphi(\beta)$ also has order $p^d - 1$ in $\mathbb{F}_{p^n}$ since φ is injective. Hence $p^d - 1 \mid p^n - 1$, implying that $d \mid n$.

Suppose conversely that $d \mid n$. Then any monic irreducible polynomial of degree dividing d also has degree dividing n. Hence $x^{p^d} - x$, which is a product of monic irreducible polynomials of degree dividing d, splits completely in $\mathbb{F}_{p^n}$ by Corollary 10.8. So the subset

$$R = \{\alpha \in \mathbb{F}_{p^n} : \alpha^{p^d} = \alpha\}$$

has size p^d. Suppose $\alpha, \beta \in R$. Then

$$\begin{aligned} (\alpha + \beta)^{p^d} &= \alpha^{p^d} + \beta^{p^d} = \alpha + \beta, \\ (\alpha\beta)^{p^d} &= \alpha^{p^d} \beta^{p^d} = \alpha\beta, \\ (\alpha^{-1})^{p^d} &= (\alpha^{p^d})^{-1} = \alpha^{-1}. \end{aligned}$$

This proves that R is a subfield of $\mathbb{F}_{p^n}$. It has size p^d and so is isomorphic to $\mathbb{F}_{p^d}$. □

For $n = 1$, we have the factorization

$$x^p - x = x(x-1)\cdots(x-(p-1)).$$

Canceling the x gives

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)),$$

which we already knew from Fermat's little theorem. Setting $x = 0$ gives

$$-1 = (-1)^{p-1}(p-1)! \qquad \text{in } \mathbb{F}_p.$$

Translating it to integer congruences gives Wilson's Theorem

$$(p-1)! \equiv -1 \pmod{p}.$$

There is of course a more direct proof by pairing a and b if $ab \equiv 1 \pmod{p}$. Then only 1 and -1 are left over.

When $n = 2$, we note that every quadratic polynomial over $\mathbb{F}_p$ has a root in $\mathbb{F}_{p^2}$.

Theorem 10.11 *Let p be a prime divisor of $n^3 + n^2 - 2n - 1$ for some integer n. Then $p = 7$ or $p \equiv \pm 1 \pmod{7}$.*

Proof: We have some $n \in \mathbb{F}_p$ such that $n^3 + n^2 - 2n - 1 = 0$. Let $\alpha \in \mathbb{F}_{p^2}$ be a root of $x^2 - nx + 1$. Then $\alpha \neq 0$ and $n = \alpha + \alpha^{-1}$. Now

$$\begin{aligned} 0 &= (\alpha + \alpha^{-1})^3 + (\alpha + \alpha^{-1})^2 - 2(\alpha + \alpha^{-1}) - 1 \\ &= \alpha^3 + 3\alpha + 3\alpha^{-1} + \alpha^{-3} + \alpha^2 + 2 + \alpha^{-2} - 2(\alpha + \alpha^{-1}) - 1 \\ &= \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^{-1} + \alpha^{-2} + \alpha^{-3}. \end{aligned}$$

Multiplying by $\alpha^3(\alpha - 1)$ gives

$$\alpha^7 - 1 = 0.$$

So the order $o(\alpha)$ of α in $\mathbb{F}_{p^2}$ divides 7. If $o(\alpha) = 1$, then $\alpha = 1$, and we get $0 = 7$ and so $p = 7$. Suppose now $o(\alpha) > 1$. Then $o(\alpha) = 7$. Since $o(\alpha) \mid |\mathbb{F}_{p^2}^{\times}|$, we get $7 \mid p^2 - 1$. So $7 \mid (p-1)(p+1)$ and hence $p \equiv \pm 1 \pmod{7}$. □

The key to this cute result is that for the polynomial $f(x) = x^3 + x^2 - 2x - 1$, we have

$$f(x + x^{-1}) = x^{-3}\,\Phi_7(x).$$

It follows from the fact that $\Phi_m(x)$ is reciprocal that for any $m \geq 2$, there exists $f(x) \in \mathbb{Z}[x]$ such that

$$f(x + x^{-1}) = x^{-\phi(m)/2}\,\Phi_m(x).$$

With a little more work (to calculate $f(0)$ which involves calculating $\Phi_m(i)$), one can use this to give a Euclidean proof for the infinitude of primes of the form $qk - 1$ where q is a prime. If m is not a prime, we won't be able to conclude from $m \mid p^2 - 1$ that $p \equiv \pm 1 \pmod{m}$. In HW6, you will work this out for $m = 9$.

Exercise

10.1 Let p be a prime. Prove that there exists $a \in \mathbb{Z}$ such that $p \mid \Phi_{p-1}(a)$.

10.2 Let F be a finite field and let $k \in \mathbb{N}$ such that $\gcd(k, |F| - 1) = 1$. Prove that every element in F is the k-th power of some element in F.

10.3 Let F be a finite field and let $k \in \mathbb{N}$. Let S be the subset of F consists of sums of k-th powers. (Note that an empty sum is 0.) Prove that S is a subfield of F.

10.4 Prove that for any positive integer $n \neq 2$, every element in $\mathbb{F}_{2^n}$ is a sum of cubes. Note that the cubes in $\mathbb{F}_4$ are precisely 0 and 1 and so the subfield of sums of cubes in $\mathbb{F}_4$ is $\mathbb{F}_2$.

10.5 Let F be a finite field with $3 \mid |F| - 1$. Suppose there exist $u, v \in F^{\times}$ such that $u^3 + v^3 = 1$. Let w be an arbitrary element of F. Let

$$A = \{a^3 : a \in F\}, \quad B = \{w + b^3 : b \in F\}, \quad C = \{u^3 w + c^3 : c \in F\}.$$

(a) Prove that A, B, C are not pairwise disjoint.

(b) Prove that w is a sum of two cubes. In other words, every element of F is a sum of two cubes.

10.6 Let F be a finite field with $3 \mid |F|-1$ and $|F|>7$. Suppose there does not exist $u, v \in F^\times$ such that $u^3+v^3=1$. Let $\alpha \in F^\times$ be a primitive element. Let

$$A = \{\alpha^{3k} : k \in \mathbb{Z}\}, \quad D = \{\alpha^{3k+1} : k \in \mathbb{Z}\}, \quad E = \{\alpha^{3k+2} : k \in \mathbb{Z}\}.$$

(a) Prove that at least one of α^3-1, α^3+1, α^6-1 belongs to D, and at least one of them belongs to E.

(b) Prove that every element of F is a sum of two cubes.

10.7 Exercises 10.2, 10.5, 10.6 imply that for any finite field except $\mathbb{F}_4$ and $\mathbb{F}_7$, every element is a sum of two cubes. Prove that for $F=\mathbb{F}_7$, every element is a sum of three cubes, and not every element is a sum of two cubes.

10.8 Prove that for any $\alpha \in \mathbb{F}_7$, the polynomial $x^4-\alpha \in \mathbb{F}_7[x]$ is reducible.

10.9 Let $q=p^n$ be a power of a prime. Let $\alpha \in \mathbb{F}_q$ be a primitive element. Suppose $q \equiv 1 \pmod{d}$ for some positive integer d. Prove that $x^d-\alpha \in \mathbb{F}_q[x]$ is irreducible.

Lecture 17 Fri 10/20

11 Quadratic reciprocity

We say an integer a is a **quadratic residue** mod m (or in $\mathbb{Z}/m\mathbb{Z}$) if the equation $x^2 \equiv a \pmod{m}$ has an integer solution. Otherwise, we say it is a **quadratic non-residue**. We consider the case where $m=p$ is a prime first. When $p=2$, every integer is a quadratic residue. So we assume p is odd.

Stated in terms of the finite field $\mathbb{F}_p$, we are just studying the set $\{b^2 : b \in \mathbb{F}_p\}$. For example in $\mathbb{F}_7$, the set of quadratic residues are $\{0,1,2,4\}$ and the set of quadratic non-residues are $\{3,5,6\}$. Let α be a primitive element in $\mathbb{F}_p^\times$ so that we may write

$$\mathbb{F}_p = \{0, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}.$$

Moreover, we know that $\alpha^k = \alpha^\ell$ if and only if $p-1 \mid k-\ell$.

Lemma 11.1 *Let p be an odd prime and let α be primitive in $\mathbb{F}_p^\times$. For $k=1,\ldots,p-1$, the element α^k is a quadratic residue if and only if k is even.*

Proof: If $k=2\ell$ is even, then $\alpha^k=(\alpha^\ell)^2$. Conversely, if $\alpha^k=(\alpha^\ell)^2$ for some $\ell \in \mathbb{Z}$, then $p-1 \mid k-2\ell$ and so k is even since p is odd. □

Corollary 11.2 *Let p be an odd prime. Let $a \in \mathbb{F}_p$, then*

$$a^{(p-1)/2} = \begin{cases} 1 & \text{if } a \text{ is a nonzero quadratic residue} \\ -1 & \text{if } a \text{ is a quadratic non-residue} \\ 0 & \text{if } a=0. \end{cases}$$

Proof: Let α be a primitive element. Then $(\alpha^{(p-1)/2})^2 = \alpha^{p-1} = 1$. Hence $\alpha^{(p-1)/2} = -1$ since it can't be 1. Now write $a=\alpha^k$ for some $k=0,\ldots,p-2$. If $k=2\ell$ is even, then $a^{(p-1)/2} = \alpha^{(p-1)\ell} = 1$. If $k=2\ell+1$ is odd, then $a^{(p-1)/2} = \alpha^{(p-1)\ell+(p-1)/2} = -1$. □

We define the **Legendre symbol** $\left(\frac{a}{p}\right)$ to be the integer 1, -1 or 0 depending on if a is a nonzero quadratic residue, quadratic non-residue, or 0 in $\mathbb{F}_p$. In other words,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p},$$

from which we see that it is multiplicative:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

so that the product of two quadratic non-residues is a quadratic residue.

Corollary 11.3 *We have that -1 is a quadratic residue mod p if and only if $p = 2$ or $p \equiv 1 \pmod 4$. In other words, for $p \neq 2$,*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Proposition 11.4 *We have that 2 is a quadratic residue mod p if and only if $p = 2$ or $p \equiv \pm 1 \pmod 8$. In other words, for $p \neq 2$,*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Corollary 11.5 *We have that -2 is a quadratic residue mod p if and only if $p = 2$ or $p \equiv 1$ or 3 mod 8.*

Proof: Suppose $p \neq 2$. We know that -2 is a quadratic residue precisely when both -1 and 2 are quadratic residues or when they are both non-residues. The first case corresponds to $p \equiv 1 \pmod 8$ and the second case corresponds to $p \equiv 3 \pmod 8$. □

To prove Proposition 11.4, we use the following lemma, which will also be used a few times later.

Lemma 11.6 *Let p be a prime and let m be a positive integer coprime to p. Then there exists $a \in \mathbb{F}^{\times}_{p^{\phi(m)}}$ such that $o(a) = m$. In fact, such an element exists in $\mathbb{F}^{\times}_{p^{o_m(p)}}$. We call such an element a primitive m-th root of unity.*

Proof: Let $d = o_m(p)$. Then $m \mid p^d - 1$ and $d \mid \phi(m)$ so $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^{\phi(m)}}$. Let α be a primitive element of $\mathbb{F}^{\times}_{p^d}$. Then $o(\alpha) = p^d - 1$. Hence $a = \alpha^{(p^d-1)/m}$ has order m. □

Proof of Proposition 11.4: Suppose p is an odd prime. Let $\alpha \in \mathbb{F}^{\times}_{p^4}$ be a primitive 8-th root of unity. The key idea is to find some $\beta \in \mathbb{F}_{p^4}$ such that $\beta^2 = 2$. Then 2 is a quadratic residue mod p if and only if $\beta \in \mathbb{F}_p$ and we can check if $\beta \in \mathbb{F}_p$ by comparing β^p with β. Take $\beta = \alpha + \alpha^{-1}$. Then

$$\beta^2 = \alpha^2 + 2 + \alpha^{-2}.$$

Since $\alpha^8 = 1$ and $\alpha^4 \neq 1$, we have $\alpha^4 = -1$, and so $\alpha^2 = -\alpha^{-2}$. Hence $\beta^2 = 2$. Since we are in characteristic p, we have $\beta^p = \alpha^p + \alpha^{-p}$. Since $\alpha^8 = 1$, we see that β^p depends only on what p is mod 8. It is now easy to check that if $p \equiv \pm 1 \pmod 8$, then

$$\beta^p = \alpha^1 + \alpha^{-1} = \beta$$

and when $p \equiv \pm 3 \pmod 8$,

$$\beta^p = \alpha^3 + \alpha^{-3} = -\alpha^{-1} - \alpha = -\beta.$$

Therefore, $\beta \in \mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 8$. □

Theorem 11.7 *(Quadratic reciprocity) Suppose p, q are two distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

In particular

$$\begin{aligned}\left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right), \text{ if both } p, q \equiv 3 \pmod 4;\\ \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right), \quad \text{otherwise.}\end{aligned}$$

For example, suppose we want to compute $\left(\frac{11}{29}\right)$. Then we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right) = \left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1.$$

As another example, we can work out when 3 is a quadratic residue mod p. If $p \equiv 1 \pmod 4$, then $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 3$. If $p \equiv 3 \pmod 4$, then $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 2 \pmod 3$. Hence $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$. The case for 5 is easier because $5 \equiv 1 \pmod 4$ and so $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 5$. The case for 7 is similar: if $p \equiv 1 \pmod 4$, we need $\left(\frac{p}{7}\right) = 1$ so $p \equiv 1, 2, 4 \pmod 7$; if $p \equiv 3 \pmod 4$, we need $\left(\frac{p}{7}\right) = -1$ so $p \equiv 3, 5, 6 \pmod 7$.

Corollary 11.8 *We have*

(a) 3 *is a quadratic residue mod* p *if and only if* $p = 3$ *or* $p \equiv \pm 1 \pmod{12}$.

(b) 5 *is a quadratic residue mod* p *if and only if* $p = 5$ *or* $p \equiv \pm 1 \pmod 5$.

(c) 7 *is a quadratic residue mod* p *if and only if* $p = 7$ *or* $p \equiv \pm 1, \pm 9, \pm 25 \pmod{28}$.

Note that for a prime to be ± 1 mod 5, it is equivalent to be ± 1 or ± 9 mod 20. It is then natural to expect the following result, which is actually equivalent to quadratic reciprocity.

Proposition 11.9 *Suppose* p, q *are distinct odd primes. Then* q *is a quadratic residue mod* p *if and only if* $p \equiv \pm a^2 \pmod{4q}$ *for some odd integer* a.

Proof of equivalence: Let

$$p^* = (-1)^{(p-1)/2} p = \left(\frac{-1}{p}\right) p.$$

It is an easy exercise to prove that p^* is a quadratic residue mod q if and only if $p \equiv \pm a^2 \pmod{4q}$ for some odd integer a.

If $p \equiv 1 \pmod 4$, then $p^* = p$. If p is a square mod q, then $p \equiv b^2 \pmod q$ for some integer b. By the Chinese remainder theorem, there exists an integer a that is 1 mod 4 and b mod q. So $p \equiv a^2 \pmod{4q}$. Since p is odd and $4q$ is even, we have a is odd. Conversely, if $p \equiv \pm a^2 \pmod{4q}$ for some odd integer a. If $p \equiv -a^2 \pmod{4q}$, then $p \equiv -a^2 \pmod 4$ but $a^2 \equiv p \equiv 1 \pmod 4$, which is impossible. So $p \equiv a^2 \pmod{4q}$ and thus $p \equiv a^2 \pmod q$. The case for $p \equiv 3 \pmod 4$ is similar.

By multiplicativity, we have

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Hence quadratic reciprocity is equivalent to

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

Lecture 18 Mon 10/23

Proof of Quadratic Reciprocity

Similar to the proof of Proposition 11.4, we let $\alpha \in \mathbb{F}_{p^{q-1}}$ be a primitive q-th root of unity and try to write down a square root of q^*. Then we check whether it is in $\mathbb{F}_p$ by raising it to the power p. We will see in about a month why it is more natural to find $\sqrt{q^*}$ in $\mathbb{F}_{p^{q-1}}$ than $\sqrt{q}$, even though they both are contained in $\mathbb{F}_{p^{q-1}}$ (in fact in $\mathbb{F}_{p^2}$).

We first note that since $\alpha^q = 1$, it makes sense to write α^m for any $m \in \mathbb{F}_q$. In other words, the value α^k is independent of the choice of the integer k in the congruence class of m mod q. We define

$$\beta = \sum_{m \in \mathbb{F}_q} \Big(\frac{m}{q}\Big)\alpha^m.$$

As a running example, we take $p = 7$ and $q = 3$. Then $\alpha \in \mathbb{F}_{49}$ is a primitive cube root of unity. In fact, we may take $\alpha = x + (x^2 + x + 1)$ in $\mathbb{F}_7[x]/(x^2 + x + 1)$. Then

$$\beta = \Big(\frac{0}{3}\Big)\alpha^0 + \Big(\frac{1}{3}\Big)\alpha^1 + \Big(\frac{2}{3}\Big)\alpha^2 = \alpha - \alpha^2 = \alpha - (-\alpha - 1) = 2\alpha + 1.$$

We can now compute

$$\beta^2 = 4\alpha^2 + 4\alpha + 1 = 4(-\alpha - 1) + 4\alpha + 1 = -3 = 3^*.$$

Back to the general case, we square β to get

$$\beta^2 = \sum_{m \in \mathbb{F}_q} \sum_{n \in \mathbb{F}_q} \Big(\frac{m}{q}\Big)\Big(\frac{n}{q}\Big)\alpha^{m+n} = \sum_{m \in \mathbb{F}_q} \sum_{n \in \mathbb{F}_q} \Big(\frac{mn}{q}\Big)\alpha^{m+n}.$$

Now we collect terms with the same power of α. Note that $t = m + n$ takes arbitrary values in $\mathbb{F}_q$:

$$\beta^2 = \sum_{t \in \mathbb{F}_q} \left(\sum_{m \in \mathbb{F}_q} \Big(\frac{m(t-m)}{q}\Big) \right) \alpha^t = \sum_{t \in \mathbb{F}_q} \left(\sum_{m \in \mathbb{F}_q^\times} \Big(\frac{m(t-m)}{q}\Big) \right) \alpha^t$$

where we removed the $m = 0$ term because the legendre symbol $\left(\frac{m(t-m)}{q}\right)$ is 0. Let's see what the inner sum is equal to in our example:

$$\begin{aligned}
t = 0 \quad &: \quad \Big(\frac{1(-1)}{3}\Big) + \Big(\frac{2(-2)}{3}\Big) = \Big(\frac{-1}{3}\Big) \cdot 2 \\
t = 1 \quad &: \quad \Big(\frac{1(0)}{3}\Big) + \Big(\frac{2(-1)}{3}\Big) = \Big(\frac{-1}{3}\Big) \cdot (-1) \\
t = 2 \quad &: \quad \Big(\frac{1(1)}{3}\Big) + \Big(\frac{2(0)}{3}\Big) = \Big(\frac{-1}{3}\Big) \cdot (-1)
\end{aligned}$$

If we then factor out the $\left(\frac{-1}{3}\right)$, we get

$$2 - \alpha - \alpha^2 = 3 - (1 + \alpha + \alpha^2) = 3.$$

In general, as a primitive q-th root of unity, α satisfies

$$1 + \alpha + \cdots + \alpha^{q-1} = 0.$$

This suggests that we should prove

$$\begin{aligned}
t = 0 \quad &: \quad \sum_{m \in \mathbb{F}_q^\times} \Big(\frac{m(t-m)}{q}\Big) = \Big(\frac{-1}{q}\Big) \cdot (q-1), \\
t \neq 0 \quad &: \quad \sum_{m \in \mathbb{F}_q^\times} \Big(\frac{m(t-m)}{q}\Big) = \Big(\frac{-1}{q}\Big) \cdot (-1),
\end{aligned}$$

which would imply that

$$\beta^2 = \Big(\frac{-1}{q}\Big)\left((q-1) - \alpha - \alpha^2 - \cdots - \alpha^{q-1}\right) = \Big(\frac{-1}{q}\Big)q = q^*.$$

Since $m \neq 0$, we have

$$\Big(\frac{m(t-m)}{q}\Big) = \Big(\frac{-m^2(1-tm^{-1})}{q}\Big) = \Big(\frac{-m^2}{q}\Big)\Big(\frac{1-tm^{-1}}{q}\Big) = \Big(\frac{-1}{q}\Big)\Big(\frac{1-tm^{-1}}{q}\Big).$$

If $t = 0$, then we get $\left(\frac{-1}{q}\right)$ for each $m \in \mathbb{F}_q^\times$. There are $q-1$ of them, so we get the desired formula for $t = 0$. When $t \neq 0$, tm^{-1} runs through every element in $\mathbb{F}_q^\times$ and so $1 - tm^{-1}$ runs through every element in $\mathbb{F}_q$ that is not 1. Hence

$$\sum_{m\in\mathbb{F}_q^\times} \Big(\frac{1-tm^{-1}}{q}\Big) = \sum_{s\in\mathbb{F}_q} \Big(\frac{s}{q}\Big) - \Big(\frac{1}{q}\Big) = \sum_{s\in\mathbb{F}_q^\times} \Big(\frac{s}{q}\Big) + \Big(\frac{0}{q}\Big) - \Big(\frac{1}{q}\Big) = -1.$$

Here the first sum is 0 because half the elements of $\mathbb{F}_q^\times$ are quadratic residues and the other halfs are quadratic nonresidues. We have therefore proved that

$$\beta^2 = q^*.$$

We next compare β^p with β to see if β lies in $\mathbb{F}_p$. Since we are in characteristic p and since $\left(\frac{m}{q}\right)$ only takes value in $0, 1, -1$, all of which are fixed by raising to the power p, we have

$$\beta^p = \sum_{m\in\mathbb{F}_q} \Big(\frac{m}{q}\Big)^p \alpha^{mp} = \sum_{m\in\mathbb{F}_q} \Big(\frac{m}{q}\Big)\alpha^{mp}.$$

Since $p \neq q$, as m varies in $\mathbb{F}_q$, mp runs through all values of $\mathbb{F}_q$. Setting $t = mp$, we get

$$\beta^p = \sum_{t\in\mathbb{F}_q} \Big(\frac{tp^{-1}}{q}\Big)\alpha^t = \Big(\frac{p^{-1}}{q}\Big) \sum_{t\in\mathbb{F}_q} \Big(\frac{t}{q}\Big)\alpha^t = \Big(\frac{p}{q}\Big)\beta.$$

Therefore, we conclude that q^* is a quadratic residue in $\mathbb{F}_p$ if and only if $\left(\frac{p}{q}\right) = 1$. In other words,

$$\Big(\frac{q^*}{p}\Big) = \Big(\frac{p}{q}\Big).$$

We now consider $x^2 \equiv a \pmod m$ in general. By the Chinese Remainder Theorem, it suffices to consider the case when $m = p^k$ is the power of a prime p. It is an easy exercise to reduce to the case $p \nmid a$.

Lemma 11.10 *Suppose $p \mid a$. Then $x^2 \equiv a \pmod{p^k}$ has a solution if and only if $\nu_p(a) \geq k$ or if $\nu_p(a)$ is even and*

$$x^2 \equiv a/p^{\nu_p(a)} \pmod{p^{k-\nu_p(a)}}$$

has a solution.

We now assume that $p \nmid a$. The punchline is that the question can be reduced to $m = p$ for p odd, or to $m = 8$ when $p = 2$.

Lecture 19 Wed 10/25

Theorem 11.11 *(Hensel's lemma) Suppose $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let $\alpha \in \mathbb{Z}$. Suppose*

$$\nu_p(f(\alpha)) > 2\nu_p(f'(\alpha)).$$

Then for any $n \in \mathbb{N}$, there exists $\alpha_n \in \mathbb{Z}$ such that $\alpha_n \equiv \alpha \pmod p$,

$$\nu_p(f'(\alpha_n)) = \nu_p(f'(\alpha)) \qquad \text{and} \qquad \nu_p(f(\alpha_n)) \geq \nu_p(f(\alpha)) + n - 1.$$

Corollary 11.12 *Suppose $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let $\alpha \in \mathbb{Z}$. Suppose $f(\alpha) \equiv 0 \pmod{p}$ and $p \nmid f'(\alpha)$. Then for any $n \in \mathbb{N}$, there exists $\alpha_n \in \mathbb{Z}$ such that $\alpha_n \equiv \alpha \pmod{p}$ and $f(\alpha_n) \equiv 0 \pmod{p^n}$.*

Corollary 11.13 *Let p be an odd prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Suppose $x^2 \equiv a \pmod{p}$ has a solution. Then $x^2 \equiv a \pmod{p^n}$ has a solution for any $n \in \mathbb{N}$.*

Proof: Consider $f(x) = x^2 - a \in \mathbb{Z}[x]$. Let $\alpha \in \mathbb{Z}$ be a solution to $x^2 \equiv a \pmod{p}$. Then we have $f(\alpha) = 0 \pmod{p}$. Now $f'(\alpha) = 2\alpha$. Since $p \nmid a$, we have $p \nmid \alpha$. Since p is odd, we have $p \nmid 2$. So $p \nmid f'(\alpha)$. Hence for any $n \in \mathbb{N}$, there exists $\alpha_n \in \mathbb{Z}$ such that $f(\alpha_n) \equiv 0 \pmod{p^n}$, which is the same as $\alpha_n^2 \equiv a \pmod{p^n}$. □

Corollary 11.14 *Let a be an odd integer. Suppose $x^2 \equiv a \pmod{8}$ has a solution. Then $x^2 \equiv a \pmod{2^n}$ has a solution for any integer $n \geq 3$.*

Proof: Consider $f(x) = x^2 - a \in \mathbb{Z}[x]$. Let $\alpha \in \mathbb{Z}$ be a solution to $x^2 \equiv a \pmod{8}$. Then we have $\nu_2(f(\alpha)) \geq 3$. Now $f'(\alpha) = 2\alpha$. Since a is odd, we have α is odd. So $\nu_2(f'(\alpha)) = 1$ which satisfies $\nu_2(f(\alpha)) > 2\nu_2(f'(\alpha))$. Hence by Theorem 11.11, for any integer $n \geq 3$, we have $n - 2 \geq 1$ and there exists $\alpha_{n-2} \in \mathbb{Z}$ such that

$$\nu_2(f(\alpha_{n-2})) = \nu_2(f(\alpha)) + (n-2) - 1 \geq n.$$

In other words, $\alpha_{n-2}^2 \equiv a \pmod{2^n}$. □

It is easy to check that the only odd quadratic residue mod 4 is 1, and the only odd quadratic residue mod 8 is also 1. Note that $x^2 \equiv 5 \pmod{8}$ has no solution but $x^2 \equiv 5 \pmod{4}$ does.

Proof of Theorem 11.11: The important observation is that for any integers a, m, we have

$$f(a+m) \equiv f(a) + f'(a)m \pmod{m^2}.$$

Since both sides are linear in $f(x)$, it is enough to check it for $f(x) = x^n$, in which case $f(a) + f'(a)m = a^n + na^{n-1}m$ are just the first two terms in the binomial expansion for $(a+m)^n$. All the remaining terms are divisible by m^2.

We construct α_n by induction on n. When $n = 1$, we take $\alpha_1 = \alpha$. Suppose now $n \geq 2$ and that α_{n-1} has been constructed with

$$\nu_p(f'(\alpha_{n-1})) = \nu_p(f'(\alpha)) \qquad \text{and} \qquad \nu_p(f(\alpha_{n-1})) \geq \nu_p(f(\alpha)) + n - 2 > 2\nu_p(f'(\alpha_{n-1})).$$

We want to define α_n to be $\alpha_{n-1} + cp^k$ for some integer c not divisible by p and some $k \in \mathbb{N}$, so that

$$\nu_p(f(\alpha_{n-1} + cp^k)) \geq \nu_p(f(\alpha_{n-1})) + 1.$$

Write

$$f(\alpha_{n-1}) = ap^t, \qquad f'(\alpha_{n-1}) = bp^s, \qquad \text{where} \qquad p \nmid ab, \quad t > 2s.$$

Then

$$f(\alpha_{n-1} + cp^k) \equiv ap^t + bp^s cp^k \pmod{p^{2k}}.$$

We take $k = t - s$. Then $2k = 2t - 2s > t$, so $2k \geq t + 1$. We take $c \in \mathbb{Z}$ so that $bc \equiv -a \pmod{p}$, which is possible because $p \nmid b$. So now

$$f(\alpha_{n-1} + cp^k) \equiv ap^t + bp^s cp^k = (a + bc)p^t \pmod{p^{t+1}}$$

is divisible by p^{t+1} as desired. Moreover,

$$f'(\alpha_{n-1} + cp^k) \equiv f'(\alpha_{n-1}) + cp^k f''(\alpha_{n-1}) \pmod{p^{2k}}.$$

Since $k = t - s > s$, we see that

$$\nu_p(cp^k f''(a_{n-1})) > s = \nu_p(f'(\alpha_{n-1})), \qquad \text{and} \qquad 2k > s.$$

So $\nu_p(f'(\alpha_{n-1}+cp^k)) = \nu_p(f'(\alpha_{n-1}))$. Therefore, $\alpha_n = \alpha_{n-1}+cp^k$ satisfies all the desired conditions. □

Example: Consider $f(x) = (x^2-2)(x^2-17)(x^2-34) \in \mathbb{Z}[x]$. Then $f(x) = 0$ has no solution in $\mathbb{Z}$. We claim that it has a solution in $\mathbb{Z}/m\mathbb{Z}$ for any $m \in \mathbb{N}$. By the Chinese Remainder Theorem, it suffices to consider when $m = p^k$ is a power of p. If $p \neq 2, 17$, then at least one of $2, 17, 34$ is a quadratic residue mod p as

$$\left(\frac{34}{p}\right)\left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{2}{p}\right)^2\left(\frac{17}{p}\right)^2 = 1$$

and by Corollary 11.13 is a quadratic residue mod p^k. If $p = 17$, then $2 = 6^2$ is a quadratic residue mod 17 and also mod 17^k. Finally, since $17 \equiv 1 \pmod 8$, it is a quadratic residue mod 8 and so is also mod 2^k.

Remark: It is a fairly nontrivial fact that if $f(x) \in \mathbb{Z}[x]$ is irreducible (in $\mathbb{Q}[x]$), then there are infinitely many primes p for which $f(x)$ has no roots mod p. Theorem 11.15 gives a proof of this in the degree 2 case. An irreducible polynomial in $\mathbb{Z}[x]$ can be reducible mod p for all primes p. As we will learn soon, most cyclotomic polynomials satisfy this.

Theorem 11.15 *Let $a \in \mathbb{N}$. If $x^2 \equiv a \pmod m$ has a solution for every $m \in \mathbb{N}$, then a is a perfect square.*

Proof: Suppose for a contradiction that a is not a perfect square. We find (infinitely many) prime q such that $\left(\frac{a}{q}\right) = -1$. We may assume without loss of generality that a is squarefree. If $a = 2$, we just take $q = 3$. Suppose $a = 2^e p_1 \cdots p_r$ where $e = 0, 1$ and $p_1, \ldots, p_r$ are distinct odd primes with $r \geq 1$. Let s be a quadratic non-residue mod p_r. By the Chinese Remainder Theorem, there exists $b \in \mathbb{N}$ such that

$$\begin{aligned} b &\equiv 1 \pmod 8 \\ b &\equiv 1 \pmod{p_1 \cdots p_{r-1}} \\ b &\equiv s \pmod{p_r} \end{aligned}$$

By Dirichlet's theorem on primes in arithmetic progressions, there exist (infinitely many) primes $q \equiv b \pmod{8p_1 \cdots p_r}$. Then q also satisfies the above congruences. So

$$\left(\frac{2}{q}\right) = 1, \qquad \left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right) = \begin{cases} 1 & \text{if } i = 1, \ldots, r-1 \\ -1 & \text{if } i = r. \end{cases} \qquad \Rightarrow \qquad \left(\frac{a}{q}\right) = -1.$$

Hence $x^2 \equiv a \pmod q$ has no solution. □

Lecture 20 Fri 10/27

If we don't use Dirichlet's theorem, we could factor b as $q_1 \cdots q_t$ into a product of possibly equal odd primes. Then we can generalize the Legendre symbol into the Jacobi symbol

$$\left(\frac{a}{b}\right) := \prod_{j=1}^{t} \left(\frac{a}{q_j}\right).$$

In HW7, you will prove the same quadratic reciprocity laws for the Jacobi symbol and so the same calculation above shows

$$\left(\frac{a}{b}\right) = -1,$$

which implies that a is not a quadratic residue mod b.

Remark: Using the quadratic reciprocity law

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}},$$

one can give a very beautiful proof of the following problem (IMO 2022 shortlist N8):

- For any positive integer n, prove that $2^n + 65 \nmid 5^n - 3^n$.

Suppose for a contradiction that $2^n + 65 \mid 5^n - 3^n$. Since $3 \nmid 5^n - 3^n$ and $2^n + 65 \equiv (-1)^n + 2 \pmod 3$, we see that n is odd and so $2^n + 65 \equiv 1 \pmod 3$. Then since $5^n \equiv 3^n \pmod{2^n + 65}$, we have

$$\Big(\frac{5}{2^n+65}\Big) = \Big(\frac{5^n}{2^n+65}\Big) = \Big(\frac{3^n}{2^n+65}\Big) = \Big(\frac{3}{2^n+65}\Big).$$

Since n is odd and the statement is immediate when $n = 1$, we may assume $n \geq 3$ and so $2^n + 65 \equiv 1 \pmod 4$. Then, we have

$$\Big(\frac{5}{2^n+65}\Big) = \Big(\frac{2^n+65}{5}\Big) = \Big(\frac{2^n}{5}\Big) = \Big(\frac{2}{5}\Big) = -1$$

but

$$\Big(\frac{3}{2^n+65}\Big) = \Big(\frac{2^n+65}{3}\Big) = \Big(\frac{1}{3}\Big) = 1.$$

Contradiction. □

In our proof of the quadratic reciprocity, the value of the sum

$$\sum_{m \in \mathbb{F}_q} \Big(\frac{m(t-m)}{q}\Big)$$

was very important. What about sums of the form

$$\sum_{m \in \mathbb{F}_q} \Big(\frac{am^2+bm+c}{q}\Big)$$

in general, where $a, b, c \in \mathbb{Z}$?

Theorem 11.16 *Let q be an odd prime. Let $a, b, c \in \mathbb{Z}$. Then*

$$\sum_{x \in \mathbb{F}_q} \Big(\frac{ax^2+bx+c}{q}\Big) = \begin{cases} -\Big(\frac{a}{q}\Big) & \text{if } q \nmid b^2 - 4ac \\ (q-1)\Big(\frac{a}{q}\Big) & \text{if } q \mid b^2 - 4ac, q \nmid a. \\ q\Big(\frac{c}{q}\Big) & \text{if } q \mid b^2 - 4ac, q \mid a. \end{cases}$$

As a consequence, if $q \nmid b^2 - 4ac$, then $ax^2 + bx + c$ can be a quadratic residue in $\mathbb{F}_q$ for at most $(q+3)/2$ values of x, which happens when $ax^2 + bx + c$ is reducible.

Proof: If $q \nmid a$, then we can complete the square to get

$$ax^2 + bx + c = a\Big(x + \frac{b}{2a}\Big)^2 - \frac{b^2 - 4ac}{4a^2}.$$

If further $q \mid b^2 - 4ac$, then $\Big(\frac{ax^2+bx+c}{q}\Big) = \Big(\frac{a}{q}\Big)$ when $x \neq -b/2a$ and is 0 when $x = -b/2a$.

If $q \mid a$, then we note that $bx + c$ takes all values in $\mathbb{F}_q$ if $b \neq 0$ and is constant equaling c if $b = 0$. In the first case, the sum is 0 and in the second case, the sum is $q\Big(\frac{c}{q}\Big)$.

The only interesting case is when $q \nmid a$ and $q \nmid b^2 - 4ac$. We have the following equality in $\mathbb{F}_q$:

$$\sum_{x \in \mathbb{F}_q} \Big(\frac{ax^2+bx+c}{q}\Big) = \sum_{x \in \mathbb{F}_q} (ax^2+bx+c)^{(q-1)/2}.$$

In HW 6, you proved that

$$\sum_{x\in\mathbb{F}_q} x^k = \begin{cases} 0 & \text{if } k = 1,\dots,q-2 \\ -1 & \text{if } k = q-1. \end{cases}$$

It is also clear that $\sum_{x\in\mathbb{F}_q} 1 = q = 0$. Hence when we expand $(ax^2+bx+c)^{(q-1)/2}$ and sum over x, only the sum of $a^{(q-1)/2}x^{q-1}$ survives to give $-a^{(q-1)/2}$. Hence in $\mathbb{F}_q$, we have

$$\sum_{x\in\mathbb{F}_q} \Big(\frac{ax^2+bx+c}{q}\Big) = -a^{(q-1)/2} = -\Big(\frac{a}{q}\Big).$$

In other words, as integers, they are congruent mod q. Note that the left hand side is a sum of q numbers of the form $0, -1, 1$ and the right hand side is ± 1. So the only way for them to be not equal is for the left hand side to be $q-1$ or $-(q-1)$. This can only happen when $ax^2+bx+c = 0$ for exactly one $x \in \mathbb{F}_q$, and is a quadratic residue/non-residue for all other $x \in \mathbb{F}_q$. This is impossible because a quadratic has exactly one root if and only if its discriminant $b^2-4ac = 0$, contradicting the assumption that $q \nmid b^2-4ac$. □

Corollary 11.17 *Let $q \geq 5$ be a prime. Let $a, b, c \in \mathbb{Z}$ such that $q \nmid b^2-4ac$. Then ax^2+bx+c cannot be square for $(q+5)/2$ consecutive integers x.*

The weaker result where $(q+5)/2$ is replaced by $2q-1$ is on the 1991 IMO shortlist. The IMO problem is also true for $q = 3$, while the polynomial $2(x-1)(x-2)$ takes square value for $(q+5)/2 = 4$ consecutive integers $x = 0, 1, 2, 3$. It is not hard to give a proof in the $q = 3$ case directly. Let $f(x) = ax^2+bx+c$ with $3 \nmid b^2-4ac$. Suppose $f(x)$ takes five consecutive square values. Then we can find $r, s \in \mathbb{Z}$ that are not congruent mod 3 and a quadratic non-residue α such that

$$f(x) = \alpha(x-r)(x-s) + 3g(x)$$

and $f(r)$ and $f(r+3)$ are squares, for some $g(x) \in \mathbb{Z}[x]$. Then $3g(r)$ is a square implying that $3 \mid g(r)$ and so $3 \mid g(r+3)$. Then

$$\nu_3(f(r+3)) = \nu_3(3\alpha(r+3-s) + 3g(r+3)) = 1.$$

Hence $f(r+3)$ is not a square.

One may ask what happens in the case of a cubic sum. It is a theorem in algebraic geometry that

$$\left|\sum_{x\in\mathbb{F}_q} \Big(\frac{ax^3+bx^2+cx+d}{q}\Big)\right| \leq 2\sqrt{q},$$

when ax^3+bx^2+cx+d has no repeated roots in $\mathbb{F}_q$. The connection to algebraic geometry is in the relation of this sum to the number of $\mathbb{F}_q$-solutions to

$$y^2 = ax^3+bx^2+cx+d$$

which you might recognize as an elliptic curve!

Exercises

11.1 Use Exercise 9.8 to prove that for an odd prime p, we have -3 is a quadratic residue mod p if and only if $p \equiv 1 \pmod 3$.

11.2 Is 91 a quadratic residue mod 253?

11.3 Prove that the polynomial $x^8 - 16$ has a root mod p for all primes p.

11.4 Prove the following more explicit version of Hensel's lemma. Suppose $f(x) \in \mathbb{Z}[x]$ and p is a prime. Suppose $a_1 \in \mathbb{Z}$ such that $f(a_1) \equiv 0 \pmod{p}$ and $p \nmid f'(a_1)$. Then the sequence defined by

$$a_{k+1} \equiv a_k - f(a_k)/f'(a_k) \pmod{p^{k+1}}, \qquad \text{for } k \geq 1$$

satisfies $f(a_k) \equiv 0 \pmod{p^k}$ for all $k \geq 1$.

11.5 Find all solutions to $x^4 + x^3 + 2x^2 + x \equiv 13 \pmod{343}$.

11.6 Find all solutions to $x^3 - 2x - 1 \equiv 0 \pmod{125}$.

11.7 Suppose $a, b \in \mathbb{N}$ are positive integers, neither of which is a perfect square. Prove that there exists a prime q such that a and b are both quadratic non-residues mod q. Conclude that there does not exist a degree 4 reducible polynomial in $\mathbb{Z}[x]$ that has roots mod m for every positive integer m but has no roots in $\mathbb{Z}$.

11.8 Let p be a prime such that the polynomial $x^3 + x + 1$ is irreducible in $\mathbb{F}_p[x]$. Then by HW6 Problem 1, the roots of $x^3 + x + 1$ in $\mathbb{F}_{p^3}$ are of the form $\alpha, \alpha^p, \alpha^{p^2}$ for some $\alpha \in \mathbb{F}_{p^3}$. Let

$$\beta = (\alpha - \alpha^p)(\alpha - \alpha^{p^2})(\alpha^p - \alpha^{p^2}).$$

(a) Prove that $\beta^2 = -31$.

(b) Prove that $\beta \in \mathbb{F}_p$.

(c) Prove that the polynomial $(x^3 + x + 1)(x^2 + 31)$ has a root mod m for every positive integer m.

11.9 Let q be an odd prime and let $a, b, c \in \mathbb{Z}$ with $q \nmid b^2 - 4ac$. Compute

$$\sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \Big(\frac{ax^2 + bxy + cy^2}{q} \Big).$$

Lecture 21 Mon 10/30

12 Schur's Theorem on $mk + a$

We saw in HW 3 Problem 2 that for any non-constant polynomial $f(x) \in \mathbb{Z}[x]$, there are infinitely many primes that divide $f(n)$ for some $n \in \mathbb{Z}$. That was a theorem of Schur, who also proved in the same work:

Theorem 12.1 *Suppose $a, m \in \mathbb{N}$ such that $a^2 \equiv 1 \pmod{m}$. Then there exists $f(x) \in \mathbb{Z}[x]$ such that there infinitely many primes congruent to a mod m that divide $f(n)$ for some $n \in \mathbb{Z}$.*

More precisely:

Theorem 12.2 *Suppose $a, m \in \mathbb{N}$ such that $a^2 \equiv 1 \pmod{m}$. Then there exists $f(x) \in \mathbb{Z}[x]$ with positive leading coefficient and a nonzero integer N such that*

(a) If p is a prime divisor of $f(n)$ for some integer n, then $p \mid N$ or $p \equiv 1$ or a mod m.

(b) If p is a prime congruent to a mod m and coprime to N, then there exists $b \in \mathbb{Z}$ such that $\nu_p(f(b)) = 1$.

(c) All prime divisors of $f(0)$ are congruent to 1 mod m.

In other words, Schur proved that there is a Euclidean polynomial for a mod m if $a^2 \equiv 1 \pmod{m}$. From such a polynomial, we can prove the infinitude of primes congruent to a mod m, assuming that there is at least one coprime to N.

Theorem 12.3 *Suppose $a^2 \equiv 1 \pmod m$ and $a \not\equiv 1 \pmod m$. Suppose there exists a prime q congruent to a mod m that is coprime to the integer N in Theorem 12.2. Then there are infinitely many such primes.*

It is worth noting that Schur's result does not prove the infinitude of primes of the form $mk + a$. We first give a proof of Theorem 12.3 from Theorem 12.2. We recall the following nice property about polynomials with integer coefficients.

Lemma 12.4 *Suppose $f(x) \in \mathbb{Z}[x]$ and $c_1, c_2, k \in \mathbb{Z}$. If $c_1 \equiv c_2 \pmod k$, then $f(c_1) \equiv f(c_2) \pmod k$*

Proof: This is simply the statement $f(c + k\mathbb{Z}) = f(c) + k\mathbb{Z}$ in $\mathbb{Z}/k\mathbb{Z}$ for any $c \in \mathbb{Z}$. □

Proof of Theorem 12.3 from Theorem 12.2: We construct our infinite sequence of pairwise coprime integers each having a prime divisor of the form a mod m. Let k be large even integer such that $f(n) > q$ for all $n \geq mN^k$. This is possible because $f(x)$ has positive leading coefficient. Let $b \in \mathbb{Z}$ with $\nu_q(f(b)) = 1$.

Let $a_1 = 1$. Since q is coprime with a_1, m and N, we see that q is coprime to $mN^k a_1$ and so q^2 is also coprime to $mN^k a_1$. Let c_1 be a positive integer such that $c_1 mN^k a_1 \equiv b \pmod{q^2}$. Then

$$f(c_1 mN^k a_1) \equiv f(b) \pmod{q^2}.$$

Since $\nu_q(f(b)) = 1$, we also have $\nu_q(f(c_1 mN^k a_1)) = 1$. We let $a_2 = f(c_1 mN^k a_1)/q$ so that a_2 is coprime with q. We now repeat this process. More generally for any $n \geq 1$, suppose we have already defined $a_1, \ldots, a_n$ inductively to all be coprime with q, then q^2 is coprime with $mN^k a_1 \cdots a_n$. Let c_n be a positive integer such that

$$c_n mN^k a_1 \cdots a_n \equiv b \pmod{q^2}$$

and we define

$$a_{n+1} = \frac{f(c_n mN^k a_1 \cdots a_n)}{q}.$$

Note that $f(c_n mN^k a_1 \cdots a_n) \equiv f(0) \equiv 1 \pmod m$ and so $a_{n+1} \equiv q^{-1} \equiv a \pmod m$. Suppose now p is a prime divisor of a_{n+1}. Then $p \mid f(c_n mN^k a_1 \cdots a_n)$. If $p \mid N$, then from $f(c_n mN^k a_1 \cdots a_n) \equiv f(0) \pmod N$, we get $p \mid f(0)$ and so p is congruent to 1 or a mod m. If $p \nmid N$, then we know automatically that p is congruent to 1 or a mod m. Hence all the primes divisors of a_{n+1} are congruent to 1 or a mod m. Since $a_{n+1} \not\equiv 1 \pmod m$, we see that not all of the prime divisors of a_{n+1} are 1 mod m. Hence a_{n+1} has a prime divisor of the form a mod m. (Note that a_{n+1} has a prime divisor because $a_{n+1} \geq 2$. This is the purpose of the integer k.)

Finally for $i < j$, we have $a_i \mid c_{j-1} m a_1 \cdots a_{j-1}$ and since $\gcd(a_i, q) = 1$, we have

$$\gcd(a_i, a_j) = \gcd(a_i, qa_j) = \gcd(a_i, f(c_{j-1} m a_1 \cdots a_{j-1})) = \gcd(a_i, f(0)).$$

Since all the prime divisors of $f(0)$ are congruent to 1 mod m, we see that a_i and a_j do not share a prime divisor that is congruent to a mod m. □

We give the construction of $f(x)$ first. Recall that when we considered the polynomial $f(x) = x^3 + x^2 - 2x - 1$ and proved that if p is a prime divisor of $f(n)$, then $p = 7$ or $p \equiv \pm 1 \pmod 7$, we are essentially taking the polynomial in $\mathbb{Q}[x]$ of the smallest degree that has $\zeta_7 + \zeta_7^{-1}$ as a root. In fact, we have the factorization

$$f(x) = (x - (\zeta_7 + \zeta_7^{-1}))(x - (\zeta_7^2 + \zeta_7^{-2}))(x - (\zeta_7^4 + \zeta_7^{-4})).$$

Note that we don't "need" $\zeta_7^j + \zeta_7^{-j}$ for $j = 3, 5, 6$ because they are the same as when $j = 4, 2, 1$ respectively. To say $p \mid f(n)$ is similarly to say that one of $\zeta_7^j + \zeta_7^{-j}$, which a priori lies in $\mathbb{F}_{p^6}$ if $p \neq 7$, actually lies in $\mathbb{F}_p$ for some $j = 1, 2, 4$. We can check whether it lies in $\mathbb{F}_p$ by comparing

$$(\zeta_7^j + \zeta_7^{-j})^p = \zeta_7^{pj} + \zeta_7^{-pj} \qquad \text{with} \qquad \zeta_7^j + \zeta_7^{-j}.$$

As complex numbers, it is easy to see that they are equal if and only if $p \equiv \pm 1 \pmod 7$. One then expects the same is true in $\mathbb{F}_p$, at least for all but finitely many primes p. In the general case of a mod m, it is then natural to take the polynomial in $\mathbb{Q}[x]$ of the smallest degree that has $\zeta_m + \zeta_m^a$ as a root, by taking a product of $(x - (\zeta_m^j + \zeta_m^{ja}))$ for half of the $j \in (\mathbb{Z}/m\mathbb{Z})^\times$, since the other half will just produce the same numbers.

Lemma 12.5 *There exists a subset $S \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$ such that $(\mathbb{Z}/m\mathbb{Z})^\times$ is the disjoint union of S with $Sa = \{ja \colon j \in S\}$.*

Proof: (Exercise) Define a relation on elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ by $j \sim k$ if $j = k$ or $j = ak$. Check this is an equivalence relation so that $(\mathbb{Z}/m\mathbb{Z})^\times$ is a disjoint union of equivalence classes of the form $[j] = \{j, ja\}$. Pick one element from each equivalence class and form S. We will give a more intrinsic meaning to S using the notion of **quotient groups** next time. □

Unlike the case of -1, it is hard to check when $\zeta_m^j + \zeta_m^{ja} = \zeta_m^k + \zeta_m^{ka}$ even in $\mathbb{C}$, but it is easy to check when

$$\zeta_m^j + \zeta_m^{ja} = \zeta_m^k + \zeta_m^{ka} \qquad \text{and} \qquad \zeta_m^k \zeta_m^{ka} = \zeta_m^j \zeta_m^{ja}$$

since this implies that

$$(x - \zeta_m^k)(x - \zeta_m^{ka}) = (x - \zeta_m^j)(x - \zeta_m^{ja}) \in \mathbb{C}[x].$$

Setting $x = \zeta_m^k$ then gives $k = j$ or $k = ja$.

Lemma 12.6 *There exists an integer u such that the numbers*

$$\eta_j = (mu - \zeta_m^j)(mu - \zeta_m^{ja}) \in \mathbb{C}$$

for $j \in S$, are all distinct.

Proof: In order for $\eta_j = \eta_k$ when $j \neq k$, we have

$$mu(\zeta_m^j + \zeta_m^{ja} - \zeta_m^k - \zeta_m^{ka}) = \zeta_m^k \zeta_m^{ka} - \zeta_m^j \zeta_m^{ja}.$$

When viewed as an equation in u, this has at most 1 solution unless

$$\zeta_m^j + \zeta_m^{ja} = \zeta_m^k + \zeta_m^{ka} \qquad \text{and} \qquad \zeta_m^k \zeta_m^{ka} = \zeta_m^j \zeta_m^{ja},$$

in which case we have either $k = j$ or $k = ja$. Since $j, k \in S$, we have $k = j$. Contradiction. Hence, we have the desired u by removing finitely many solutions from infinitely many integers. □

We define

$$f(x) = \prod_{j \in S} (x - \eta_j) = \prod_{j \in S} \Big(x - (mu - \zeta_m^j)(mu - \zeta_m^{ja}) \Big).$$

Note that

$$f(0) = (-1)^{|S|} \prod_{j \in S} (mu - \zeta_m^j)(mu - \zeta_m^{ja}) = (-1)^{|S|} \prod_{j \in (\mathbb{Z}/m\mathbb{Z})^\times} (mu - \zeta_m^j) = (-1)^{|S|} \Phi_m(mu),$$

all of whose prime divisors are 1 mod m. To prove that $f(x) \in \mathbb{Z}[x]$ and the divisibility properties, we need to learn more about groups and fields.

Exercises

12.1 Let m be a positive integer. Give a formula for the number of solutions (mod m) to $x^2 \equiv 1 \pmod{m}$.

12.2 Factor $x^3 - 3x - 1$ in $\mathbb{C}[x]$. (Recall that this polynomial is used to prove the infinitude of primes congruent to 8 mod 9.)

12.3 How many ways are there to pick the set S in Lemma 12.5?

Lecture 22 Wed 11/01

13 Group Theory

A **group** is a set G equipped with one binary operation, one unary operation and one nullary operation:

$$(a,b) \mapsto ab : G \times G \to G \qquad a \mapsto a^{-1} : G \to G, \qquad e \in G$$

such that for any $a, b, c \in G$,

(a) (Associative) $a(bc) = (ab)c$;

(b) (Multiplicative identity) $a \cdot e = a$ and $a \cdot a^{-1} = e$.

With a little bit of work, one can prove that $e \cdot a = a$ and $a^{-1} \cdot a = e$. If $ab = ba$ for all $a, b \in G$, we say G is an **abelian** group. All the groups that we will encounter in this class are abelian groups.

Examples:

1. The group of units $R^\times$ of a commutative ring R is an abelian group with the multiplication, inversion and 1 from the ring R.

2. The additive group of a ring R, where we forget about multiplication and use addition as the binary operation, negation as inversion, and 0 as e, is an abelian group.

3. The additive group of the ring $\mathbb{Z}/m\mathbb{Z}$ for $m \in \mathbb{N}$, is called the **cyclic** group of order m, sometimes denoted C_m.

   The **order** of the group G is the size of G. The order $o(g)$ of an element $g \in G$ is the smallest positive integer d such that $g^d = e$. The cyclic group of order m is the group with an element g of order m, so that $G = \{e, g, g^2, \ldots, g^{m-1}\}$. The group of units $\mathbb{F}_{p^n}^\times$ of a finite field is cyclic of order $p^n - 1$.

   The same argument used to prove that $a^{|R^\times|} = 1$ and $o(a) \mid |R^\times|$ can be used to prove the following result in the case of abelian groups.

   Proposition 13.1 *Let G be a finite group of order m. Then for any $g \in G$, $g^{|G|} = e$ and so $o(g) \mid |G|$. As a consequence, every finite group of prime order is cyclic.*

   To prove this for non-abelian groups, we introduce the notion of a **subgroup** of G, which is a subset H of G closed under the operations of G. That is, it is closed under multiplication, inversion, and contains the identity element. The subgroup generated by an element g is $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. If g has order d, then this is just $\{e, g, \ldots, g^{d-1}\}$.

   In the example of $(\mathbb{Z}/m\mathbb{Z})^\times$, the coset $a + m\mathbb{Z}$ where $a^2 \equiv 1 \pmod{m}$ and $a \not\equiv 1 \pmod{m}$ is an element of order 2. It then generates a subgroup, $\langle a \rangle$, of order 2. In HW 9, you will discover when $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic. In this class, we will only focus on C_m and $(\mathbb{Z}/m\mathbb{Z})^\times$.

   Given any subgroup H of G and an element $g \in G$, we can define the left coset of H containing g as $gH = \{gh : h \in H\}$. Two left cosets $g_1H = g_2H$ if and only if $g_1 \in g_2H$ if and only if $g_2^{-1}g_1 \in H$. It is easy to check that this defines an equivalence relation. Hence G is a disjoint union of left cosets of H. If G (and H) is finite, then all the left cosets of H have the same size and we have proved that $|H|$ divides $|G|$. Taking $H = \langle g \rangle$ proves that $o(g) \mid |G|$.

   We can define the quotient G/H as the set of left cosets of H. To define a group structure on G/H by $g_1H \cdot g_2H = (g_1g_2)H$, we need H to be a **normal** subgroup: for any $g \in G$ and any $h \in H$, we have $ghg^{-1} \in H$. When G is abelian, $ghg^{-1} = h$ and so every subgroup is normal. The set S we saw in Lemma 12.5 is basically $(\mathbb{Z}/m\mathbb{Z})^\times/\langle a \rangle$.

   Group homomorphisms are defined just like ring homomorphisms. Kernels of group homomorphisms are normal subgroups and we have the first isomorphism theorem for groups as well.

4. Traditionally, groups arise as the group of symmetries of certain objects. For example, the symmetric group S_n is the set of bijections from $\{1, 2, \ldots, n\}$ to itself, with composition as the binary operation, inverse as inversion, and the identity map as e. This is an non-abelian group when $n \geq 3$.

   We are more interested in the group $\mathrm{Aut}(E)$ of ring isomorphisms from a field E to itself. These kinds of isomorphisms are called **automorphisms**. If E is a field of containing another field F, we write $\mathrm{Aut}_F(E)$ for the subgroup of $\mathrm{Aut}(E)$ consisting of automorphisms that act as identity on F.

   For example, what is $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$? We know that every complex number is of the form $a + bi$ for some $a, b \in \mathbb{R}$. If $\sigma \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, then

$$\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i).$$

   Now since $i^2 + 1 = 0$, we can apply σ to both sides to get

$$\sigma(i)^2 + 1 = 0.$$

   Hence $\sigma(i) = i$ or $\sigma(i) = -i$. In other words, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ consists of at most two elements, the identity map and complex conjugation. It is easy to check that complex conjugation is in fact an automorphism of $\mathbb{C}$ fixing $\mathbb{R}$. Composing complex conjugation with itself gives the identity map. Therefore,

$$\mathrm{Aut}_{\mathbb{R}}\mathbb{C} \cong C_2.$$

Theorem 13.2 *Let p be a prime and $n \in \mathbb{N}$. Then*

$$\mathrm{Aut}(\mathbb{F}_{p^n}) = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) \cong C_n$$

generated by the Frobenius map $\tau(x) = x^p$.

Proof: Any automorphism of $\mathbb{F}_{p^n}$ sends 1 to 1 and so acts as identity on $\mathbb{F}_p$. So $\mathrm{Aut}(\mathbb{F}_{p^n}) = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$. From $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$, we know that the Frobenius map τ defines a ring homomorphism $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. It is automatically injectively and it is then surjective because an injective map between two finite sets of the same size is surjective. More explicitly, we have for any $a \in \mathbb{F}_{p^n}$,

$$a = a^{p^n} = (a^{p^{n-1}})^p = \tau(a^{p^{n-1}}).$$

Any positive power $\tau^m : x \mapsto x^{p^m}$ of τ is also in $\mathrm{Aut}(\mathbb{F}_{p^n})$. Since every element in $\mathbb{F}_{p^n}$ satisfies $a^{p^n} = a$, we see that τ^n is the identity map. Since there is an element in $\mathbb{F}_{p^n}^\times$ of order $p^n - 1$, we see that no smaller power of τ is the identity map. Hence $\langle \tau \rangle \cong C_n$. It remains to prove that any $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})$ is a power of τ.

Lecture 23 Fri 11/03

Let $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. Then we may identify $\mathbb{F}_{p^n}$ with $\mathbb{F}_p[x]/(f(x))$. Let $\alpha = x + (f(x))$. Then any $\sigma \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p[x]/(f(x)))$ is determined by $\sigma(\alpha)$, which also must be a root of $f(x)$ by Lemma 10.7. Indeed, since σ fixes the coefficients of $f(x)$, we have

$$\sigma(f(\alpha)) = f(\sigma(\alpha)).$$

By HW 6 Problem 1, we know that the roots of $f(x)$ in F are exactly $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$. Hence there is some $m = 0, \ldots, n-1$ such that $\sigma(\alpha) = \alpha^{p^m} = \tau^m(\alpha)$, which implies that $\sigma = \tau^m$. □

What are the subgroups of C_n? Let g be a generator of C_n so that

$$C_n = \langle g \rangle = \{e, g, \ldots, g^{n-1}\}.$$

Let H be a subgroup of C_n. Let d be the smallest positive integer such that $g^d \in H$. Then the usual division algorithm argument implies that if $g^k \in H$, then $d \mid k$. Hence $H = \langle g^d \rangle$. Since $g^n = e \in H$, we have $d \mid n$ and

$$|H| = o(g^d) = \frac{o(g)}{\gcd(d, o(g))} = \frac{n}{d}.$$

In other words, all the subgroups of C_n are cyclic, and there is a unique subgroup of order d for any positive divisor d of n.

What are the subfields of $\mathbb{F}_{p^n}$? We saw before that $\mathbb{F}_{p^n}$ has a (unique) subfield isomorphic to $\mathbb{F}_{p^d}$ if and only if $d \mid n$, in which case this subfield is given by

$$\{a \in \mathbb{F}_{p^n} : a^{p^d} = a\} = \{a \in \mathbb{F}_{p^n} : \tau^d(a) = a\} = \{a \in \mathbb{F}_{p^n} : \sigma(a) = a, \forall \sigma \in \langle \tau^d \rangle\}.$$

On the other hand, by taking a primitive element of $\mathbb{F}_{p^d}$, we know that no smaller positive power of τ fixes $\mathbb{F}_{p^d}$. So we have

$$\mathrm{Aut}_{\mathbb{F}_{p^d}}(\mathbb{F}_{p^n}) = \langle \tau^d \rangle.$$

In other words, there is a natural bijection between subgroups of $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ and subfields of $\mathbb{F}_{p^n}$ (containing $\mathbb{F}_p$). That is, the following two maps are inverses of each other.

$$\begin{array}{rcl} H & \mapsto & \mathbb{F}_{p^n}^H := \{a \in \mathbb{F}_{p^n} : h(a) = a, \forall h \in H\} \\ \mathrm{Aut}_F(\mathbb{F}_{p^n}) & \leftarrow\!\shortmid & F. \end{array}$$

The correspondence between subgroups of the automorphism group $\mathrm{Aut}_F(E)$ and subfields of E containing F is the heart of Galois theory. We will not develop Galois theory but will note an important consequence:

$$E^{\mathrm{Aut}_F(E)} = F.$$

In other words, assuming certain conditions on the field extension E/F, elements of E that are fixed by every automorphism of E fixing F, actually lie in F. We will not use this fact but will point out where this property is reflected. In HW 8, you will consider the notion of normal extensions and separable extensions, which are assumptions the field extension E over F needs to satisfy for Galois theory to work.

Exercises

13.1 Let G be a group and let $g \in G$ with $o(g)$ finite. Prove that for any positive integer k, we have

$$o(g^k) = \frac{o(g)}{\gcd(o(g), k)}.$$

13.2 Let F be any field and let $f(x) \in F[x]$ be a degree 2 irreducible polynomial. Let $E = F[x]/(f(x))$. Prove that $\mathrm{Aut}_F(E) \cong C_2$.

13.3 Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{1\}$.

The following result is beyond our scope: the automorphism group $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$ has cardinality $2^{2^{\aleph_0}}$.

13.4 Let $E = \mathbb{Q}[x]/(x^3 - 2)$. Prove that E is a field and $\mathrm{Aut}_{\mathbb{Q}}(E) = \{1\}$.

13.5 Let $E = \mathbb{Q}[x]/(x^4 + 1)$. Prove that E is a field and $\mathrm{Aut}_{\mathbb{Q}}(E) \cong C_2 \times C_2$.

14 Field extensions

We now expand on some very important ideas illustrated by the examples in the previous section. We say E is a **field extension** of F if F is a subfield of E. We usually write E/F for the field extension. (Not to be confused with ring quotients. After all, fields don't have interesting quotients.)

In both the examples of $\mathbb{C}/\mathbb{R}$ and $\mathbb{F}_{p^n}/\mathbb{F}_p$, there is an isomorphism $E \cong F[x]/(f(x))$ for some irreducible polynomial $f(x)$. Let $\alpha \in E$ corresponds to $x + (f(x))$. Then every element of E is of the form $j(\alpha)$ for some polynomial $j(x) \in F[x]$.

In general, given a field extension E/F and an element $\alpha \in E$, we write $F[\alpha]$ for the smallest subring of E containing F and α. In other words,

$$F[\alpha] = \{j(\alpha) \colon j(x) \in F[x]\}.$$

We write $F(\alpha)$ for the smallest subfield of E containing F and α. In other words,

$$F(\alpha) = \left\{ \frac{j(\alpha)}{k(\alpha)} \colon j(x), k(x) \in F[x], k(\alpha) \neq 0 \right\}.$$

The evaluation map

$$\mathrm{ev}_\alpha : F[x] \to F[\alpha]$$

is a surjective homomorphism. Its kernel is an ideal I of $F[x]$, which is necessarily of the form $(f(x))$. If $f(x) = 0$, then we say α is **transcendental** over F, in which case

$$F[\alpha] \cong F[x] \qquad \text{and} \qquad F(\alpha) \cong F(x),$$

the field of rational functions in x.

If $f(x)$ is nonzero, then we may assume it is monic and $F[x]/(f(x)) \cong F[\alpha]$ is an integral domain since it is a subring of a field. Therefore, $f(x)$ is irreducible and $F[x]/(f(x))$ is a field, which also implies that

$$F(\alpha) \cong F[\alpha] \cong F[x]/(f(x)).$$

In this case, we say α is **algebraic** and we call the monic generator of the kernel of ev_α the **minimal polynomial** of α over F. Equivalently, it is easy to see that the the minimal polynomial of α is the monic irreducible polynomial in $F[x]$ that has α as a root. Moreover, using our usual division algorithm argument, we see that the minimal polynomial $f(x)$ of α is the monic polynomial in $\mathbb{F}[x]$ of the smallest degree that has α has a root; and so if $h(x) \in F[x]$ has α as a root, then $f(x) \mid h(x)$ in $F[x]$.

Proposition 14.1 *Suppose α is algebraic over F with minimal polynomial $f(x)$. Then there is a bijection between $\mathrm{Aut}_F(F(\alpha))$ and the set of distinct roots of $f(x)$ in $F(\alpha)$.*

Proof: Any automorphism σ of $F(\alpha)$ fixing F is determined by $\sigma(\alpha)$, which must also be a root of $f(x)$. Conversely, suppose $\beta \in F(\alpha)$ is a root of $f(x)$. Then there is a homomorphism $F[x]/(f(x)) \to F(\alpha)$ sending $j(x)+(f(x))$ to $j(\beta)$. Composing it with the inverse of the natural isomorphism $F[x]/(f(x)) \to F(\alpha)$ sending $x+(f(x))$ to α, we get a homomorphism $F(\alpha) \to F(\alpha)$ sending α to β. Such a homomorphism is necessarily injective since the domain is a field. To prove that it is surjective, we need to talk about vector spaces. □

It is then fairly natural to imagine that in the framework of Galois theory, we assume that $F(\alpha)$ contains all the roots of $f(x)$ (normal extension), and that $f(x)$ has no repeated roots (separable extension). You will explore these in HW 8.

Lecture 24 Mon 11/06

Given $\alpha_1, \ldots, \alpha_n$ in E, we write

$$\mathrm{Span}_F\{\alpha_1, \ldots, \alpha_n\} = \{c_1\alpha_1 + \cdots + c_n\alpha_n \colon c_1, \ldots, c_n \in F\}$$

for the F-span of $\alpha_1, \ldots, \alpha_n$. It is an F-vector space: closed under addition and closed under multiplication by F. If $\mathrm{Span}_F\{\alpha_1, \ldots, \alpha_n\} = E$, then we call $\{\alpha_1, \ldots, \alpha_n\}$ a **spanning set** and we say E is a **finite** extension of F.

Example: Suppose

$$E = F(\alpha) = F[\alpha] \cong F[x]/(f(x))$$

and $f(x)$ has degree d. Then every element of E is of the form $g(\alpha)$ for some polynomial $g(x) \in F[x]$ of degree less than d. In other words, every element of E is of the form

$$c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1}.$$

So the set $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a spanning set of E. Note also that if such an expression is 0, then α is a root of $c_0 + c_1 x + \cdots + c_{d-1}x^{d-1}$, which must then be divisible by the degree d polynomial $f(x)$; hence we have $c_0 = \cdots = c_{d-1} = 0$.

A set $\{\alpha_1, \ldots, \alpha_n\} \subseteq E$ is said to be **linearly independent** over F if whenever $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$ for some $c_1, \ldots, c_n \in F$, we have $c_1 = \cdots = c_n = 0$. A linearly independent spanning set is called a **basis**.

Lemma 14.2 *If E has a spanning set $\{\alpha_1, \ldots, \alpha_n\}$ of size n, then E has no linearly independent set of size more than n.*

Proof: Suppose for a contradiction that $\{\beta_1, \ldots, \beta_{n+1}\}$ is a linearly independent set of size $n+1$. For each $i = 1, \ldots, n+1$, there exist $c_{i1}, \ldots, c_{in} \in F$ such that

$$\beta_i = c_{i1}\alpha_1 + \cdots + c_{in}\alpha_n.$$

We look for $x_1, \ldots, x_{n+1} \in F$ that are not all 0 such that

$$x_1\beta_1 + \cdots + x_{n+1}\beta_{n+1} = 0.$$

In terms of the coefficients in $\alpha_1, \ldots, \alpha_n$, we see that it suffices to prove that

$$\begin{aligned} x_1 c_{11} + \cdots + x_{n+1} c_{n+1\,1} &= 0 \\ &\vdots \\ x_1 c_{1\,n} + \cdots + x_{n+1} c_{n+1\,n} &= 0 \end{aligned}$$

has a nonzero solution. Note we have n linear equations and $n+1$ unknowns. So we may use standard elimination method for solving systems of linear equations. More precisely, at least one of the c_{ij} is nonzero, for if otherwise all the β_i are 0 and so can't be linearly independent. By renaming, suppose $c_{11} \neq 0$. Then we use the first equation to express

$$x_1 = -c_{11}^{-1}c_{21}x_2 - \cdots - c_{11}^{-1}c_{n+1\,1}x_{n+1}$$

and plug it into the other equations. Now we have $n-1$ linear equations and n unknowns, which must have a nonzero solution in $(x_2, \ldots, x_n)$ by induction. We then use the above formula to find x_1. The base case of 1 equation and 2 unknowns is obvious. □

We list some immediate consequences of Lemma 14.2.

Corollary 14.3 *If E has a spanning set of size n, then any linearly independent set of size n is a basis.*

Proof: Suppose $\{\beta_1, \ldots, \beta_n\}$ is linearly independent over F. If it doesn't span E, then there exists some $\gamma \in E \backslash \mathrm{Span}_F\{\beta_1, \ldots, \beta_n\}$. Then it is easy to see that $\{\beta_1, \ldots, \beta_n, \gamma\}$ is linearly independent over F of size $n+1$. Contradiction. □

Corollary 14.4 *Suppose E/F is finite. Then:*

(a) Any linearly independent set over F can be enlarged into a basis over F.

(b) Any spanning set contains a basis over F.

(c) Any homomorphism $\sigma : E \to E$ fixing F is an isomorphism.

Proof: Let d denote the size of a smallest spanning set of E. A linearly independent set that is not a spanning set can be enlarged by the same procedure as in the proof of the previous corollary. This process terminates when we reach a linearly independent set of size d, which is then a basis.

Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a spanning set of E that is not linearly independent over F. Then there exists $c_1, \ldots, c_n$ not all 0 such that $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$. By renaming, we may assume $c_1 \neq 0$. Then

$$\alpha_1 = -c_1^{-1}c_2\alpha_2 - \cdots - c_1^{-1}c_n\alpha_n.$$

Hence $\{\alpha_2, \ldots, \alpha_n\}$ is a spanning set of E. This process terminates when we reach a linearly independent set that is also a spanning set.

Finally, any field homomorphism is injective. Let $\{\alpha_1, \ldots, \alpha_d\}$ be a basis of E over F. We claim that $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_d)\}$ is linearly independent over F, which then implies that it is a basis and so the image of σ is all of E. Suppose $c_1, \ldots, c_d \in F$ such that

$$c_1\sigma(\alpha_1) + \cdots + c_d\sigma(\alpha_d) = 0.$$

Since σ fixes F, we have

$$\sigma(c_1\alpha_1 + \cdots + c_d\alpha_d) = c_1\sigma(\alpha_1) + \cdots + c_d\sigma(\alpha_d) = 0.$$

Since σ is injective, we see that $c_1\alpha_1 + \cdots + c_d\alpha_d = 0$ and so $c_1 = \cdots = c_d = 0$ by the linear independence of $\{\alpha_1, \ldots, \alpha_d\}$. □

From Lemma 14.2, we see that any two bases of E have the same size: If one has size n and the other has size m, then using the size n spanning set and size m linearly independent set, we get $m \leq n$ and similarly we have $n \leq m$. This common size is the **degree** of the extension, denoted $[E : F]$, or the **dimension** of E as an F-vector space.

Corollary 14.5 *Suppose the minimal polynomial of α has degree d. Then $[F(\alpha) : F] = d$.*

Proposition 14.6 *Suppose L is a finite extension of E and E is a finite extension of F. Then L is a finite extension of F and $[L : F] = [L : E][E : F]$.*

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of L over E and let $\{\beta_1, \ldots, \beta_m\}$ be a basis of E over F. Then it is easy to check that

$$\{\alpha_i\beta_j : i = 1, \ldots, n, j = 1, \ldots, m\}$$

is a basis of L over F. □

Proposition 14.7 *If E/F is finite, then every $\alpha \in E$ is algebraic.*

Proof: Suppose $d = [E : F]$ and $\alpha \neq 0$. Then $\{1, \alpha, \ldots, \alpha^d\}$ is a set of size $d + 1$ and so is not linearly independent. Then $c_0 + c_1\alpha + \cdots + c_d\alpha^d = 0$ for some $c_0, \ldots, c_d \in F$ not all 0. Then α is a root of the nonzero polynomial $c_0 + c_1x + \cdots + c_dx^d$. □

Exercises

14.1 Suppose E/F is finite of degree d. Suppose $|F|$ is finite. Prove that $|E| = |F|^d$, without using the classification theorem of finite fields.

This gives another proof that any finite field has size p^d for some prime p. It also proves that if $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$, then $d \mid n$.

14.2 Find $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$.

14.3 Suppose E/F is a field extension. Let α, β be elements of E. We write $F(\alpha, \beta) = F(\alpha)(\beta)$ for the smallest subfield of E containing α, β and F. Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ (as subfields of $\mathbb{C}$, or $\mathbb{R}$).

14.4 Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}+\sqrt{3})) \cong C_2 \times C_2$.

14.5 Let F be a field and consider $E = F(\alpha)$ where α is algebraic over F. For any intermediate field L in the extension E/F, i.e $F \subseteq L \subseteq E$, we let $f_L(x) \in L[x]$ be the minimal polynomial of α over L.

(a) Prove that for any intermediate fields L and K, we have $L \subseteq K$ if and only if $f_L(x) \in K[x]$.

(b) Prove that for any intermediate fields L and K, we have $L = K$ if and only if $f_L(x) = f_K(x)$.

(c) Prove that there are only finitely many intermediate fields in the extension E/F.

14.6 Suppose E/F is a finite extension where F is infinite. Suppose there are finitely many intermediate fields in the extension E/F. Prove that there exists $\alpha \in E$ such that $E = F(\alpha)$.

Galois theory implies that if F is a finite field or a field of characteristic 0, then a finite extension E/F has finitely many intermediate fields. In other words, they are all of the form $F(\alpha)/F$. Extensions of this form are known as *simple extensions*.

14.7 Consider $F = \mathbb{F}_p(x, y)$, the field of rational functions in two variables x, y over $\mathbb{F}_p$. Let $E = \mathbb{F}_p(t, s)$ with $t^p = x$ and $s^p = y$. In other words, $E = F[T, S]/(T^p - x, S^p - y)$. Prove that E/F is a finite extension and there does not exist $\alpha \in E$ such that $E = F(\alpha)$.

14.8 Let E/F be a field extension. Let

$$L = \{\alpha \in E \colon \alpha \text{ is algebraic over } F\}.$$

Prove that L is a field. Such a field is called the *algebraic closure* of F in E.

Lecture 25 Wed 11/08

15 Cyclotomic extension

In this section, we consider the Cyclotomic extension $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$. Since ζ_m is a root of $\Phi_m(x) \in \mathbb{Z}[x]$, we see that it is algebraic and $\mathbb{Q}(\zeta_m) = \mathbb{Q}[\zeta_m]$. We begin with the irreducibility of $\Phi_m(x)$.

Theorem 15.1 *For any $m \in \mathbb{N}$, $\Phi_m(x)$ is irreducible in $\mathbb{Q}[x]$.*

Since $\Phi_m(x)$ is also monic, we see that it is then the minimal polynomial of ζ_m. The roots of $\Phi_m(x)$ are of the form ζ_m^k where $k \in (\mathbb{Z}/m\mathbb{Z})^\times$, all of which lie in $\mathbb{Q}(\zeta_m)$, and so there is a bijection between $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$ and $(\mathbb{Z}/m\mathbb{Z})^\times$. We write σ_k for the automorphism sending ζ_m to ζ_m^k. For $j, k \in (\mathbb{Z}/m\mathbb{Z})^\times$, we see that

$$\sigma_j(\sigma_k(\zeta_m)) = \sigma_j(\zeta_m^k) = \zeta_m^{jk} = \sigma_{jk}(\zeta_m).$$

Hence the bijection $j \mapsto \sigma_j$ is also a group isomorphism.

Corollary 15.2 *For any integer $m \geq 2$, we have $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ and $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.*

We now work towards the irreducibility of $\Phi_m(x)$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of ζ_m. Then $f(x)$ is a monic irreducible polynomial dividing $\Phi_m(x)$. Write $\Phi_m(x) = f(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. We prove first that $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$.

Given any polynomial $a(x) \in \mathbb{Z}[x]$, we define its **content** to be the gcd of all of its coefficients. We say $a(x)$ is **primitive** if its content is 1. For example, $2x - 3$ is primitive. Any monic polynomial in $\mathbb{Z}[x]$, for example $\Phi_m(x)$, is primitive. For any prime p, let π_p denote the natural homomorphism

$$\pi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x] : a_n x^n + \cdots + a_0 \mapsto a_n x^n + \cdots + a_0.$$

Note that $a(x)$ is primitive if and only if $\pi_p(a(x)) \neq 0$ for all primes p.

Lemma 15.3 *(Gauss) If $a(x)$ and $b(x)$ are primitive, then so is $a(x)b(x)$.*

Proof: Let p be any prime. Since $\mathbb{F}_p$ is a field, $\mathbb{F}_p[x]$ is an integral domain. Hence from $\pi_p(a(x)) \neq 0$ and $\pi_p(b(x)) \neq 0$, we have $\pi_p(a(x)b(x)) = \pi_p(a(x))\pi_p(b(x)) \neq 0$. □

Corollary 15.4 *Suppose $h(x) \in \mathbb{Z}[x]$ is primitive and $j(x), k(x) \in \mathbb{Q}[x]$ are monic polynomials such that $h(x) = j(x)k(x)$. Then $j(x), k(x) \in \mathbb{Z}[x]$.*

Proof: Let c_j and c_k be the smallest positive integers such that $c_j j(x) \in \mathbb{Z}[x]$ and $c_k k(x) \in \mathbb{Z}[x]$. Let $d \in \mathbb{N}$ be the content of $c_j j(x)$. Then d divides the leading coefficient c_j. So now $c_j/d \in \mathbb{N}$ and $(c_j/d)j(x) \in \mathbb{Z}[x]$. By minimality of c_j, we have $d = 1$. So $c_j j(x)$ and similarly $c_k k(x)$ are primitive. By Gauss' Lemma, their product

$$c_j c_k j(x)k(x) = c_f c_g H(x)$$

is primitive. Since $h(x) \in \mathbb{Z}[x]$ is primitive, we have $c_j c_k = 1$. Hence $c_j = c_k = 1$. □

Corollary 15.5 *If $\alpha \in \mathbb{C}$ is the root of a monic polynomial in $\mathbb{Z}[x]$, then the minimal polynomial of α over $\mathbb{Q}$ is in $\mathbb{Z}[x]$. They are called **algebraic integers**.*

Proof: Let $h(x) \in \mathbb{Z}[x]$ be a monic polynomial having α as a root. Then $h(x)$ is primitive. Let $j(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Since $j(x)$ and $h(x)$ are both monic and $j \mid h$ in $\mathbb{Q}[x]$, there exists a monic polnyomial $k(x) \in \mathbb{Q}[x]$ such that $j(x)k(x) = h(x)$. By Corollary 15.4, we have $j(x) \in \mathbb{Z}[x]$. □

Applying Corollary 15.5 to ζ_m, we find that $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$ and are monic.

Proposition 15.6 *Suppose ζ is a root of $f(x)$. Then for any prime $p \nmid m$, ζ^p is also a root of $f(x)$.*

Note that for any positive integer j coprime to m, it can be written as a product of primes $p_1 \cdots p_r$, none of which divides m. Then by repeatedly applying this result, starting from the root ζ_m, we find that $\zeta_m^j = \zeta_m^{p_1 \cdots p_r}$ is a root of $f(x)$. Hence all the roots of $\Phi_m(x)$, which are all distinct, are roots of $f(x)$. So $\Phi_m(x) \mid f(x)$. Since $f(x)$ is irreducible and they are both monic, we have $\Phi_m(x) = f(x)$ is irreducible.

Proof: Since $f(x)$ is monic irreducible, we see that it is also the minimal polynomial of ζ. Since ζ is a root of Φ_m, we know that it is of the form ζ_m^k for some integer k coprime to m. Since $p \nmid m$, we have that pk is also coprime to m and so $\zeta^p = \zeta_m^{pk}$ is a root of $\Phi_m(x)$. Suppose for a contradiction that ζ^p is not a root of $f(x)$. Then it is a root of $g(x)$. Hence ζ is a root of $g(x^p)$, which implies that $g(x^p)$ is divisible by $f(x)$ in $\mathbb{Q}[x]$. Since $f(x)$ is monic and and $g(x^p)$ is a monic polynomial in $\mathbb{Z}[x]$, we have $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$ by Corollary 15.4. Recall that $\Phi_m(x)j(x) = x^m - 1$, where $j(x) \in \mathbb{Z}[x]$ is the product of $\Phi_d(x)$ over all positive divisors $d \mid m$ such that $d \neq m$. In other words, we have

$$\begin{aligned} x^m - 1 &= f(x)g(x)j(x), \\ g(x^p) &= f(x)k(x). \end{aligned}$$

The trick now is to apply π_p to work in $\mathbb{F}_p[x]$. In $\mathbb{F}_p[x]$, we have

$$\pi_p(g(x))^p = \pi_p(g(x^p)) = \pi_p(f(x))\pi_p(k(x)).$$

Let $\ell(x) \in \mathbb{F}_p[x]$ be a monic irreducible divisor of $\pi_p(f(x))$. Then we have $\ell(x) \mid \pi_p(g(x))^p$ and so $\ell(x) \mid \pi_p(g(x))$. However, this implies that $\ell(x)^2 \mid \pi_p(\Phi_m(x)) \mid x^m - 1$ in $\mathbb{F}_p[x]$. So $\ell(x)$ divides the derivative mx^{m-1}. Since $p \nmid m$, we have $\ell(x) = x$, but it can't divide $x^m - 1$. Contradiction. □

There is a very nice irreducibility criterion that can be used to prove that $\Phi_p(x)$ is irreducible when p is prime.

Proposition 15.7 *(Eisenstein's criterion) Suppose $f(x) \in \mathbb{Z}[x]$ of degree n and p is a prime. Suppose $\pi_p(f(x)) = \alpha x^n$ for some $\alpha \in \mathbb{F}_p^\times$ and $\nu_p(f(0)) = 1$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof: Suppose for a contradiction that $f(x) = g(x)h(x)$ where $g(x) \in \mathbb{Q}[x]$ has degree $d \geq 1$ and $h(x) \in \mathbb{Q}[x]$ has degree $e \geq 1$. The same argument as in the proof of Corollary 15.4 implies that we may assume that $g(x), h(x) \in \mathbb{Z}[x]$. Now

$$\pi_p(g(x))\pi_p(h(x)) = \pi_p(f(x)) = \alpha x^n.$$

So we must have $\pi_p(g(x)) = \beta x^d$ and $\pi_p(h(x)) = \gamma x^e$ for some $\beta, \gamma \in \mathbb{F}_p^\times$. Since $d, e \geq 1$, we have $p \mid g(0)$ and $p \mid h(0)$. Then $\nu_p(g(0)h(0)) \geq 2$ contradicting $\nu_p(f(0)) = 1$. $\square$

Note that

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p$$

satisfies the conditions of Eisenstein's criterion. Hence $\Phi_p(x+1)$ is irreducible, and so is $\Phi_p(x)$.

Lecture 26 Fri 11/10

Let's recall the construction of the polynomial in the proof of Schur's theorem. Let m be a positive integer and let $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ be an element of order 2. Fix a subset $S \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$ such that $(\mathbb{Z}/m\mathbb{Z})^\times$ is a disjoint union of S and Sa. Suppose without loss of generatlity that $1 \in S$. Choose an integer u such that

$$\eta_j = (mu - \zeta_m^j)(mu - \zeta_m^{ja}) \in \mathbb{Q}(\zeta_m)$$

for $j \in S$ are all distinct. Note that each η_j is algebraic. We defined

$$f(x) = \prod_{j \in S}(x - \eta_j) = \prod_{j \in S}\Big(x - (mu - \zeta_m^j)(mu - \zeta_m^{ja})\Big).$$

Lemma 15.8 *The minimal polynomial of η_1 over $\mathbb{Q}$ is $f(x)$. In other words, $f(x) \in \mathbb{Q}[x]$ and is irreducible.*

Proof: Recall that we have a group isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$ sending j to the automorphism σ_j where $\sigma_j(\zeta_m) = \zeta_m^j$. Let $g(x) \in \mathbb{Q}[x]$ denote the minimal polynomial of η_1 over $\mathbb{Q}$. Then every element of the form $\sigma_j(\eta_1)$ is a root of $g(x)$. Note that for any $j \in S$,

$$\begin{aligned} \sigma_j(\eta_1) &= (mu - \zeta_m^j)(mu - \zeta_m^{ja}) = \eta_j, \\ \sigma_{ja}(\eta_1) &= (mu - \zeta_m^{ja})(mu - \zeta_m^j) = \eta_j. \end{aligned}$$

Then η_j, for $j \in S$, are all roots of $g(x)$ in $\mathbb{Q}(\zeta_m)$ and we have $f(x) \mid g(x)$ in $\mathbb{Q}(\zeta_m)[x]$. It remains to prove that they have the same degree. Note that

$$[\mathbb{Q}(\eta_1) : \mathbb{Q}] = \deg(g) \geq |S| = \frac{1}{2}\phi(m).$$

Moreover, since $\mathbb{Q}(\eta_1) \subseteq \mathbb{Q}(\zeta_m)$, we have

$$\phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\eta_1)][\mathbb{Q}(\eta_1) : \mathbb{Q}].$$

We now prove that $\mathbb{Q}(\eta_1) \neq \mathbb{Q}(\zeta_m)$. We use σ_a :

$$\sigma_a(\eta_1) = \eta_1, \qquad \text{and} \qquad \sigma_a(\zeta_m) = \zeta_m^a \neq \zeta_m.$$

So σ_a fixes $\mathbb{Q}(\eta_1)$, but not $\mathbb{Q}(\zeta_m)$. Hence $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\eta_1)] \geq 2$ and so $[\mathbb{Q}(\eta_1) : \mathbb{Q}] \leq \phi(m)/2$. Combining this with the above lower bound gives $\deg(g) = \deg(f) = \phi(m)/2$. $\square$

Remark: In fact, we have

$$\mathbb{Q}(\eta_1) = \mathbb{Q}(\zeta_m)^{\langle \sigma_a \rangle}.$$

Since $f(x)$ is fixed by every element in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$, Galois theory would also imply immediately that $f(x) \in \mathbb{Q}[x]$.

We prove next that $f(x) \in \mathbb{Z}[x]$. Consider the ring

$$\mathbb{Z}[\zeta_m] = \{j(\zeta_m) \colon j(x) \in \mathbb{Z}[x]\}.$$

In other words, $\mathbb{Z}[\zeta_m]$ is the smallest subring of $\mathbb{Q}(\zeta_m)$ containing ($\mathbb{Z}$ and) ζ_m. Then we see that $\eta_j \in \mathbb{Z}[\zeta_m]$ for all $j \in S$. Hence $f(x) \in \mathbb{Z}[\zeta_m][x]$.

Lemma 15.9 *We have $\mathbb{Z}[\zeta_m] \cap \mathbb{Q} = \mathbb{Z}$. In particular, $f(x) \in \mathbb{Z}[x]$.*

Proof: Since the minimal polynomial $\Phi_m(x)$ of ζ_m is monic and has integer coefficients, we know that every element in $\mathbb{Z}[\zeta_m]$ is of the form $j(\zeta_m)$ for some polynomial $j(x) \in \mathbb{Z}[x]$ of degree less than $\phi(m)$. Suppose that there exists some $j(x) \in \mathbb{Z}[x]$ with $\deg(j) < \phi(m)$ and $r, s \in \mathbb{Z}$ with $s \neq 0$ such that

$$j(\zeta_m) = \frac{r}{s}.$$

Then $sj(\zeta_m) - r = 0$. Hence $sj(x) - r \in \mathbb{Z}[x]$ is divisible by $\Phi_m(x)$ in $\mathbb{Q}[x]$ but it has degree less than $\deg(\Phi_m(x))$. So $sj(x) - r = 0$. Setting $x = 0$ gives $r = sj(0)$ and so $j(\zeta_m) = j(0) \in \mathbb{Z}$. $\square$

We now consider the divisibility statements: there exists a nonzero integer N such that

(a) If p is a prime divisor of $f(n)$ for some integer n, then $p \mid N$ or $p \equiv 1$ or $a \bmod m$.

(b) If p is a prime congruent to $a \bmod m$ and $p \nmid N$, then there exists $b \in \mathbb{Z}$ such that $\nu_p(f(b)) = 1$.

We give a sketch of the idea first. Suppose $p \mid f(n)$ for some $n \in \mathbb{Z}$. Then we have

$$p \mid \prod_{j \in S} (n - \eta_j).$$

We would like to say that $p \mid n - \eta_j$ for some $j \in S$, which is "like saying" that

$$\eta_j = n \in \mathbb{F}_p \qquad \text{and so} \qquad \eta_j^p = \eta_j.$$

Since we are now in characteristic p, we have

$$\eta_j^p = (mu - \zeta_m^{jp})(mu - \zeta_m^{jap}) = \eta_{jp}.$$

We know that

$$\eta_j = \eta_{jp} \in \mathbb{C} \iff jp = j \text{ or } jp = ja \in (\mathbb{Z}/m\mathbb{Z})^\times \iff p \equiv 1 \text{ or } a \pmod m.$$

We need this to also be true in $\mathbb{F}_p$, except for $p \mid N$ for some nonzero integer N.

To make the first step rigorous, we are looking at a property of the form

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

This is exactly Euclid's lemma for primes, but its proof requires the notion of gcd. However, most $\mathbb{Z}[\zeta_m]$ are not Euclidean domains (we will see that they are for $m = 3, 4$), as most of them are not PIDs. In fact, it is a theorem that $\mathbb{Z}[\zeta_m]$ is a Euclidean domain if and only if it is a PID, and there are only finitely many of them. The way to get around it is to work with prime ideals instead.

Let R be a commutative ring. An ideal I of R is a **prime ideal** if it is a proper ideal and whenever $ab \in I$ for some $a, b \in R$, we have $a \in I$ or $b \in I$. In terms of the quotient R/I, this means that if $(ab) + I = 0 + I$, then $a + I = 0 + I$ or $b + I = 0 + I$. In other words, I is a prime ideal if and only if R/I is an integral domain.

When $R = \mathbb{Z}$, the prime ideals are $p\mathbb{Z}$ and (0). When $R = F[x]$ for some field F, the prime ideals are $(f(x))$ where $f(x)$ is irreducible or 0. We note that in there two examples, if the prime ideal I is not (0), then R/I is actually a field. When $R = \mathbb{Z}[x]$ and $I = (x)$, we have $R/I \cong \mathbb{Z}$ is an integral domain but not a field.

Lecture 27 Mon 11/13

When $R = \mathbb{Z}[\zeta_m]$ and p is a prime, the ideal pR is not necessarily a prime ideal of R. Recall the natural map $\pi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$. Then

$$R/pR \cong \mathbb{F}_p[x]/(\pi_p(\Phi_m(x)))$$

which is not an integral domain if $\pi_p(\Phi_m(x))$ is not irreducible. As you will prove in HW10, $\pi_p(\Phi_m(x))$ is very often reducible.

Theorem 15.10 *Suppose $p \nmid m$. Then $\pi_p(\Phi_m(x))$ factors into a product of $\phi(m)/o_m(p)$ irreducible polynomials in $\mathbb{F}_p[x]$, where $o_m(p)$ is the order of p mod m.*

Note if $o_m(p) = \phi(m)$, then the group $G = (\mathbb{Z}/m\mathbb{Z})^\times$ has an element p whose order equals $|G|$, which implies that $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic. You proved in HW9 that this happens only when $m = 2, 4, q^k, 2q^k$ for some odd prime q.

Example: Consider $\Phi_8(x) = x^4 + 1$. Let's prove that $x^4 + 1$ is reducible in $\mathbb{F}_p[x]$ for every prime p. When $p = 2$, we have $x^4 + 1 = (x + 1)^4$. Suppose p is an odd prime. Then $p^2 \equiv 1 \pmod 8$. So $\mathbb{F}_{p^2}$ contains a primitive 8-th root of unity α. The minimal polynomial of α over $\mathbb{F}_p$ then has degree at most 2 and it divides $x^4 + 1$.

We fix an irreducible factor $g_0(x)$ of $\pi_p(\Phi_m(x))$ and let $g(x) \in \mathbb{Z}[x]$ so that $\pi_p(g(x)) = g_0(x)$. Let

$$I_p = (p, g(\zeta_m))$$

be the ideal of R generated by p and $g(\zeta_m)$. Since $p \in I_p$, we see that I_p does not depend on the choice of the lift $g(x)$. From the isomorphisms

$$R/I_p \cong \mathbb{Z}[x]/(p, g(x), \Phi_m(x)) \cong \mathbb{F}_p[x]/(g_0(x), \pi_p(\Phi_m(x))) = \mathbb{F}_p[x]/(g_0(x)),$$

we see that R/I_p is a finite field of characteristic p and so I_p is a prime ideal. We can now redo the argument from last time using I_p.

Suppose p is a prime and $p \mid f(n)$ for some integer n. Then

$$\prod_{j \in S} (n - \eta_j) \in p\mathbb{Z} \subseteq pR \subseteq I_p.$$

Since I_p is a prime ideal, we see that there exists $j \in S$ such that $n - \eta_j \in I_p$. Write $\bar{r}$ for the coset $r + I_p \in R/I_p$. In other words, $\bar{r}$ is the image of r under the natural map $R \to R/I_p$. Then we have $\overline{\eta_j} = \bar{n}$. Since n is an integer, we have $\bar{n} \in \mathbb{F}_p$. Hence

$$\overline{\eta_j} \in \mathbb{F}_p \qquad \Longrightarrow \qquad \overline{\eta_j}^p = \overline{\eta_j}.$$

On the other hand,

$$\overline{\eta_j}^p = (\overline{mu}^p - \overline{\zeta_m}^{jp})(\overline{mu}^p - \overline{\zeta_m}^{jap}) = \overline{(mu - \zeta_m^{jp})(mu - \zeta_m^{jap})} = \overline{\eta_{jp}},$$

where the first equality holds because R/I_p is a field of characteristic p. Hence we have $\eta_j - \eta_{jp} \in I_p$.

Proposition 15.11 *There exists a nonzero integer N such that if $p \nmid N$, then for distinct $j, k \in S$, we have $\eta_j - \eta_k \notin I_p$.*

We remark that this result is also similar to the statement that every nonzero integer is divisible by only finitely many primes.

Let's see how everything follows from this result. From $\eta_j - \eta_{jp} \in I_p$, we see that: if $jp \in S$, then $jp = j$ and so $p \equiv 1 \pmod m$; if $jp \in Sa$, then $jpa \in S$ and so $jpa = j$, implying that $p \equiv a^{-1} \equiv a \pmod m$. In other words, if $p \nmid N$ is a prime divisor of some $f(n)$, then p is congruent to 1 or a mod m.

Suppose conversely that $p \equiv 1$ or $a \pmod m$ and $p \nmid N$. From $p = 1$ or $p = a$ in $(\mathbb{Z}/m\mathbb{Z})^\times$, we have

$$\overline{\eta_1} = \overline{\eta_p} = \overline{\eta_1}^p.$$

Hence $\overline{\eta_1} \in \mathbb{F}_p$. Let n be an integer such that $\bar{n} = \overline{\eta_1}$. Then we have $n - \eta_1 \in I_p$ and so $f(n) \in I_p$.

Lemma 15.12 *Suppose I is a prime ideal of a commutative ring R_1. Let R_2 be a subring of R_1. Then $I \cap R_2$ is a prime ideal of R_2. (Compare this with Exercise 9.4 about maximal ideals.)*

Proof: It is easy to check that $I \cap R_2$ is a proper (because it doesn't contain 1) ideal of R_2. Suppose $a, b \in R_2$ with $ab \in I \cap R_2$. Then from $ab \in I$, we have $a \in I$ or $b \in I$. So $a \in I \cap R_2$ or $b \in I \cap R_2$. □

As an immediate corollary, we have $I_p \cap \mathbb{Z} = p\mathbb{Z}$ since it is a prime ideal of $\mathbb{Z}$ containing p. Therefore, we have $p \mid f(n)$.

What about $p^2 \nmid f(n)$? Suppose we have $p^2 \mid f(n)$ instead. Then

$$f(n+p) \equiv f(n) + pf'(n) \equiv pf'(n) \pmod{p^2}.$$

So if we have $p \nmid f'(n)$, then $p^2 \nmid f(n+p)$ and we can take $n+p$ instead. Using the product rule, we have

$$f'(x) = \frac{d}{dx}\prod_{j\in S}(x-\eta_j) = \sum_{j\in S}\prod_{k\in S, k\neq j}(x-\eta_k) = \prod_{k\in S,k\neq 1}(x-\eta_k) + (x-\eta_1)(\cdots).$$

We set $x = n$. We know that $n - \eta_1 \in I_p$ and $n - \eta_k \notin I_p$ for any $k \in S$ different from 1 since $\eta_1 - \eta_k \notin I_p$. Then we have $f'(n) \notin I_p$ and so $p \nmid f'(n)$.

Lecture 28 Wed 11/15

It now remains to prove Proposition 15.11. Since I_p is a prime ideal, we see that in order for each $\eta_j - \eta_k \notin I_p$, it is equivalent to require that

$$\prod_{\substack{j,k\in S\\ j\neq k}}(\eta_j - \eta_k) \notin I_p.$$

The punchline is that this product is an integer N. By construction, the η_j are distinct complex numbers, so $N \neq 0$. If a prime p doesn't divide N, then $N \notin p\mathbb{Z} = I_p \cap \mathbb{Z}$. So $N \notin I_p$ and we are done!

We remark that since every element of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$ permutes η_j for $j \in S$, their product is fixed by every element of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$. Hence using Galois theory, we immediately obtain this product is in $\mathbb{Q}$ and since it is also in $\mathbb{Z}[\zeta_m]$, we see that it is an integer.

Without Galois theory, we will use the theory of symmetric polynomials. We note that any permutation of the η_j's leaves the above product unchanged.

Exercise

15.1 Prove that if $r \in \mathbb{Q}$ is an algebraic integer. Then $r \in \mathbb{Z}$.

15.2 Prove that $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$.

15.3 Prove that $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$ as groups.

15.4 For which primes p is $x^6 + x^3 + 1$ irreducible in $\mathbb{F}_p[x]$? For which primes p does $x^6 + x^3 + 1$ have a root in $\mathbb{F}_p$?

15.5 What are all the prime ideals of $\mathbb{Z}[\zeta_m]$ for some fixed $m \geq 2$?

15.6 Let $m \geq 2$ be an integer. Prove that

$$\prod_{1\leq i<j\leq m}(\zeta_m^i - \zeta_m^j)^2 = (-1)^{(m-1)(m+2)/2}m^m.$$

15.7 Suppose $f(x) \in \mathbb{Z}[x]$ is a monic polynomial dividing $x^m - 1$ for some $m \geq 2$. Let p be a prime not dividing m and let ζ be a root of $f(x)$. Let $R = \mathbb{Z}[\zeta_m]$ and let I_p be a prime ideal of R containig p.

(a) Prove that $f(\zeta^p) \in I_p$.

(b) Prove that if $f(\zeta^p) \neq 0$, then $f(\zeta^p) \mid m^m$ in R. Conclude that $f(\zeta^p) = 0$.

This gives another proof of Proposition 15.6.

16 Symmetric polynomials

Let R be a commutative ring. Then we have the polynomial ring $R[x_1, \ldots . x_n]$ in n-variables with coefficients in R. One can also view this as formed from R inductively via

$$R[x_1, \ldots . x_n] = R[x_1, \ldots, x_{n-1}][x_n].$$

Given any bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ and any $f \in R[x_1, \ldots, x_n]$, we define

$$\sigma(f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

We say $f(x_1, \ldots, x_n)$ is **symmetric** in $x_1, \ldots, x_n$ if

$$\sigma(f) = f$$

for any such σ. Here are some examples of symmetric polynomials in 3 variables:

$$1, \qquad x_1 + x_2 + x_3, \qquad x_1^2 + x_2^2 + x_3^2, \qquad x_1x_2 + x_1x_3 + x_2x_3$$

$$x_1^3 + x_2^3 + x_3^3, \qquad x_1^2x_2 + x_2^2x_1 + x_2^2x_3 + x_3^2x_2 + x_1^2x_3 + x_3^2x_1, \qquad x_1x_2x_3.$$

The **elementary symmetric polynomials** are defined as

$$s_k(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k}.$$

For example,

$$\begin{aligned} s_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3 \\ s_2(x_1, x_2, x_3) &= x_1x_2 + x_1x_3 + x_2x_3 \\ s_3(x_1, x_2, x_3) &= x_1x_2x_3 \end{aligned}$$

Alternatively, we let

$$P(t) = (t - x_1) \cdots (t - x_n) \in R[x_1, \ldots, x_n][t].$$

Then $s_k(x_1, \ldots, x_n)$ is the coefficient of $(-1)^k t^k$ in $P(t)$.

Theorem 16.1 *If $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is symmetric in $x_1, \ldots, x_n$, then there exists a polynomial $g \in R[x_1, \ldots, x_n]$ such that $f(x_1, \ldots, x_n) = g(s_1, \ldots, s_n)$.*

For example, we have

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = s_1^2 - 2s_2.$$

Proof: We induct on n and the degree of f viewed as a polynomial in x_1 with coefficient in $R[x_2, \ldots, x_n]$. The base case $f(x_1) = cx_1$ is trivial. Suppose we are in the general case. Then $f(x_1, \ldots, x_{n-1}, 0)$ is symmetric in $x_1, \ldots, x_{n-1}$ and so by induction, there exists $j \in R[x_1, \ldots, x_{n-1}]$ such that

$$f(x_1, \ldots, x_{n-1}, 0) = j(s_1(x_1, \ldots, x_{n-1}), \ldots, s_{n-1}(x_1, \ldots, x_{n-1})).$$

We observe that

$$s_k(x_1, \ldots, x_{n-1}) = s_k(x_1, \ldots, x_{n-1}, 0).$$

Hence

$$f(x_1, \ldots, x_n) - j(s_1(x_1, \ldots, x_n), \ldots, s_{n-1}(x_1, \ldots, x_n))$$

is a polynomial that vanishes when $x_n = 0$. Hence every term has an x_n in it. Since it is symmetric in $x_1, \ldots, x_n$, every term has $x_1 \cdots x_n$ in it. Let $h \in R[x_1, \ldots, x_n]$ be a polynomial such that

$$f(x_1, \ldots, x_n) - j(s_1(x_1, \ldots, x_n), \ldots, s_{n-1}(x_1, \ldots, x_n)) = x_1 \cdots x_n h(x_1, \ldots, x_n).$$

Then h is symmetric in $x_1, \ldots, x_n$ of degree than less than $\deg(f)$. So by induction, there exists $k \in R[x_1, \ldots, x_n]$ such that

$$h(x_1, \ldots, x_n) = k(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)).$$

Then we have

$$f(x_1, \ldots, x_n) = j(s_1, \ldots, s_{n-1}) + s_n k(s_1, \ldots, s_n)$$

is a polynomial in $s_1, \ldots, s_n$. $\square$

An important example is the polynomial

$$\Delta(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{i \ne j} (x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n].$$

of the product of the difference of the variables, when $n \ge 2$. For example,

$$\Delta(x_1, x_2) = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2.$$

Since $\Delta(x_1, \ldots, x_n)$ is symmetric in $x_1, \ldots, x_n$, there is a unique polynomial $G \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$\Delta(x_1, \ldots, x_n) = G(s_1, \ldots, s_n).$$

Now given any polynomial $f(x) = x^n + c_1 x^{n-1} + \cdots + c_n \in R[x]$, we define its **discriminant**

$$\Delta(f) = G(-c_1, c_2, \ldots, (-1)^n c_n) \in R.$$

Lecture 29 Fri 11/17

Suppose now $R = F$ is a field. Let E/F be a splitting field of $f(x)$. In other words, there exist $\alpha_1, \ldots, \alpha_n \in E$ such that

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

Then we have for $k = 1, \ldots, n$,

$$c_k = (-1)^k s_k(\alpha_1, \ldots, \alpha_n).$$

Then

$$\Delta(f) = G(s_1(\alpha_1, \ldots, \alpha_n), \ldots, s_n(\alpha_1, \ldots, \alpha_n)) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Hence $\Delta(f) = 0$ if and only if $f(x)$ has repeated roots in some extension of F. We note that the polynomial G has integer coefficients. This means that if $f(x) \in \mathbb{Z}[x]$ with $\Delta(f) \in \mathbb{Z}$, then $\pi_p(f(x)) \in \mathbb{F}_p[x]$ and

$$\Delta(\pi_p(f)) = \pi_p(\Delta(f)).$$

So $f(x)$ has repeated roots in some extension of $\mathbb{F}_p$ if and only if $p \mid \Delta(f)$.

Recall that $x^m - 1$, and its divisor $\Phi_m(x)$, have no repeated factors mod p for any prime $p \nmid m$. This means that discriminants can only be divisible by the primes divisors of m. In fact,

$$\begin{aligned} \Delta(x^m - 1) &= (-1)^{(m-1)(m+2)/2} m^m, \\ \Delta(\Phi_m(x)) &= (-1)^{\phi(m)/2} \prod_{p \mid m} p^{\phi(m)(\nu_p(m) - \frac{1}{p-1})}, \text{ if } m \ge 3. \end{aligned}$$

The computation of $\Delta(x^m - 1)$ is Exercise 15.6. The computation of $\Delta(\Phi_m(x))$ when $m = p$ is a prime follows similarly. The more general case is beyond the scope of this course. Note that when $m = p$ is an odd prime, we have

$$\Delta(\Phi_p(x)) = (-1)^{(p-1)/2} p^{p-2} = p^*(p^{(p-3)/2})^2.$$

From the definition of Δ, we see that

$$\Delta(\Phi_p(x)) = \left(\prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j) \right)^2$$

is a square in $\mathbb{Q}(\zeta_p)$. In other words, p^* is a square in $\mathbb{Q}(\zeta_p)$. This explains why it was more natural to try to find a square root of p^* when we proved quadratic reciprocity.

In terms of Galois theory, we see that $\mathbb{Q}(\zeta_p)$ contains the quadratic field $\mathbb{Q}(\sqrt{p^*})$ of $\mathbb{Q}$. The automorphism group $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) \cong (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ is cyclic of order $p-1$. It has a unique subgroup of order $(p-1)/2$, whose fixed field is a quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$. In other words, $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$.

Exercise

16.1 Express $x_1^3 + x_2^3 + x_3^3$ and $x_1^4 + x_2^4 + x_3^4$ in terms of the elementary symmetric polynomials in x_1, x_2, x_3.

16.2 Prove that the polynomial g in Theorem 16.1 is unique.

16.3 Find the formula for $\Delta(x^2 + bx + c)$ and $\Delta(x^3 + ax^2 + bx + c)$.

16.4 Prove that $\Delta(x^n + c_1 x^{n-1} + \cdots + c_{n-1}x) = c_{n-1}^2 \Delta(x^{n-1} + c_1 x^{n-2} + \cdots + c_{n-1})$.

16.5 Let $f(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-1}x + c_n \in \mathbb{Z}[x]$ be a polynomial of degree $n \ge 2$. Let p be a prime. Suppose that $p^2 \mid c_n$ and $p \mid c_{n-1}$. Prove that $p^2 \mid \Delta(f)$.

16.6 Prove that for any monic polynomial $f(x) = x^n + c_1 x^{n-1} + \cdots + c_n \in \mathbb{C}[x]$ with roots $\alpha_1, \ldots, \alpha_n$, we have

$$\Delta(f) = \prod_{i=1}^{n} (-1)^{n(n-1)/2} f'(\alpha_i).$$

16.7 Consider the polynomial $f(x) = x^n + ax + b \in \mathbb{C}[x]$. Prove that

$$\Delta(x^n + ax + b) = (-1)^{n(n-1)/2}(n^n b^{n-1} - (n-1)^{n-1}(-a)^n).$$

17 RSA and Shor's algorithm

One does not teach a first year intro to number theory course without mentioning RSA. RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem, one of the oldest, that is widely used for secure data transmission. Let's discuss its setup:

1. Pick two large distinct primes p and q, say on the order of 2^{1024} or approximately 300 digits.

2. Let $n = pq$ so that $\phi(n) = (p-1)(q-1)$.

   Then for any integer M coprime to n, we have $M^{\phi(n)} \equiv 1 \pmod{n}$. Now if $N \equiv 1 \pmod{\phi(n)}$, then $N = 1 + \phi(n)k$ for some $k \in \mathbb{Z}$ so

   $$M^N = M \cdot M^{\phi(n)k} \equiv M \pmod{n}.$$

3. Pick an integer d coprime to $\phi(n)$.

   Then there exist integers e, t such that $de + t\phi(n) = 1$. The integer e can be easily found using the (Extended) Euclidean algorithm. Note that for any integer M coprime to n,

   $$de \equiv 1 \pmod{\phi(n)} \qquad \Longrightarrow \qquad M^{de} \equiv M \pmod{n}.$$

4. Publish (e, n) as the public key. Keep (d, n) (and p, q) hidden as the private key. It is also customary to replace e and d by their remainders mod $\phi(n)$.

Now when someone wants to send a message M to me, they would take my (e, n) and compute

$$C \equiv M^e \pmod{n}$$

and send C to me. When we receive C, we can recover M mod n via

$$C^d \equiv M^{de} \equiv M \pmod{n}.$$

If we further require that $M = 1, \ldots, n$, for example by restricting the size of the message or by breaking it up into multiple messages, we would recover M exactly.

The security of RSA relies on the following:

1. Given the public key (e, n), it is practically impossible to find the private key (d, n).

   Note that we can find d by solving $ex \equiv 1 \pmod{\phi(n)}$ but this requires finding p and q so we can compute $\phi(n) = (p-1)(q-1)$. In other words, factorization should be hard.

2. Given the message M and the encrypted C, it is practically impossible to find d such that $M \equiv C^d \pmod{n}$.

   This problem is known as discrete logarithm.

In the above, practically impossible means that the current best algorithm would take longer than the lifetime of the universe to complete. These algorithms' runtime are exponential in $\log n$, which is basically the number of bits that n has. Even something like e^{100} is already more than 10^{43}.

The efficiency of RSA on the other hand requires the following procedures to have a runtime that is polynomial in $\log n$:

1. Easy to compute M^e mod n. This is also known as discrete exponentiation.

   This can be done using the Square and Multiply method. For example, suppose we want to calculate 452^{1563} mod 2023. Then we first express the exponent 1563 as a sum of powers of 2, which it already was when working with a computer:

   $$1563 = 1024 + 512 + 16 + 8 + 2 + 1.$$

   Then we square 452 repeatedly to find

   $$452, 452^2, 452^4, 452^8, \ldots, 452^{1024} \pmod{2023}.$$

   Note that before computing the next square, we first reduce mod 2023, so that every step is simply the square of a number at most 2023. Finally we multiply the ones that show up in the binary representation of 1563.

2. Easy to generate primes.

   The traditional sieve of Eratosthenes produces all the primes, but is too slow to generate 300 digit primes. From the prime number theorem, we know that roughtly 1 out of $\log n$ numbers up to n are primes. So it is much more efficient to take a bunch of random large numbers and test for primality.

For the rest of the semester, we will discuss:

1. Shor's algorithm for factorization and how quantum computing destroys RSA's security.

2. Fermat and Miller-Rabin primality tests. These are polynomial in runtime but probabilistic. However, the chance of them failing is lower than the chance of computation error.

3. AKS primality test. This is deterministic and polynomial in runtime.

4. Lucas-Lehmer primality test. This only works for Mersenne primes $2^p - 1$.

5. The cyclotomic fields $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_4)$ and $x^3 + y^3 = z^3$.

Lecture 30 Mon 11/20

It turns out that factorization can be reduced to the discrete logarithm problem! First we note that it is easy to check if a positive integer is a perfect power. If $n = a^k$ for some $a, k \geq 2$, then $k \leq \log_2 n$. For each $k \leq \log_2 n$, we can do a binary search to see if $n = a^k$ for some integer a. Here is the algorithm:

1. Set $a_L = 2$ and $a_H = n - 1$. So any solution will lie in $[a_L, a_H]$.

2. Let $c = (a_L + a_H)/2$.

3. If $c^k = n$, then we are done. If $c^k > n$, then c is too big and we replace a_H by c. If $c^k < n$, then c is too small and we replace a_L by c. Go back to step 2.

Suppose we have tested that n is not a prime power. The key idea is to consider the congruence equation $x^2 \equiv 1 \pmod{n}$. It always has ± 1 as solutions. A nontrivial solution is an integer a such that $a^2 \equiv 1 \pmod{n}$ but $a \not\equiv \pm 1 \pmod{n}$.

Lemma 17.1 *Let $n > 1$ be an odd integer with at least 2 prime divisors. The equation $x^2 \equiv 1 \pmod{n}$ has a nontrivial solution. Let a be one such solution. Then $\gcd(a + 1, n)$ and $\gcd(a - 1, n)$ are divisors of n different from 1 or n.*

Proof: There is a factorization of n as dk where $\gcd(d, k) = 1$ and $d, k > 2$. By the Chinese Remainder Theorem, there exists an integer a such that $a \equiv -1 \pmod{d}$ and $a \equiv 1 \pmod{k}$. Since $d, k > 2$, we see that $a \not\equiv 1 \pmod{d}$ and $a \not\equiv -1 \pmod{k}$. Hence $a \not\equiv \pm 1 \pmod{n}$. However, $a^2 \equiv 1 \pmod{d}$ and $a^2 \equiv 1 \pmod{k}$ and so $a^2 \equiv 1 \pmod{n}$.

The second statement is clear from $n \mid (a - 1)(a + 1)$ and $n \nmid a - 1$ and $n \nmid a + 1$ using prime factorization. In fact, we have $n = \gcd(a + 1, n) \gcd(a - 1, n)$. The proof is left as an exercise. □

How to find a nontrivial solution?

1. Pick $b = 1, \ldots, n - 1$ at random.

2. Compute $\gcd(b, n)$. If $\gcd(b, n) > 1$, then it is a nontrivial divisor of n.

3. Suppose $\gcd(b, n) = 1$. Compute $d = o_n(b)$. Note this is basically solving the discrete logarithm problem $b^d \equiv 1 \pmod{n}$.

4. If d is odd, go back to step 1. If d is even, then $b^{d/2}$ is a solution to $x^2 \equiv 1 \pmod{n}$. If $b^{d/2} \equiv \pm 1 \pmod{n}$, then go back to step 1. If $b^{d/2} \not\equiv \pm 1 \pmod{n}$, then we have found a nontrivial solution. (Note that $b^{d/2} \equiv 1 \pmod{n}$ is not possible since $d = o_n(b)$.)

You will prove in HW11 that when n has at least 2 odd prime divisors, there are at most $\frac{1}{2}\phi(n)$ elements $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $o_n(b)$ is odd or $b^{o_n(b)/2} \equiv -1 \pmod{n}$. This means that for a randomly chosen b, there is at least a 50% probability that it produces a nontrivial divisor of n. Hence the probability that no answer is found after k iterations is at most $1/2^k$. For $k \geq 80$, this is less than 10^{-24} which is roughly the probability that a cosmic ray flipping a bit in the computer causing a calculation error. So as long as each iteration is polynomial in the number of digits of n, then we are in good shape.

What can a quantum computer do?

1. It can compute $b^m \bmod n$ for all non-negative integers $m < n$ at the same time.

   However, it will be a superposition of states $|m, b^m \bmod n\rangle$. Measuring the first registry gives a random m_0 and the value $b^{m_0} \bmod n$. Measuring the second registry gives a random c_0 and a superposition of states $|m\rangle$ such that $b^m \equiv c_0 \pmod n$.

   The key is that there is a hidden period in this. In other words, the integers m such that $b^m \equiv c_0 \pmod n$ are of the form

   $$m_0, m_0 + o_n(b), m_0 + 2o_n(b), \ldots$$

2. Quantum Fourier Transform can be used to find this hidden period.

A similar method can be used for the general discrete logarithm problem: given M, C and n, find d such that $M \equiv C^d \pmod n$. We use a two variable version of the above.

1. Compute $M^\alpha C^{-\beta} \bmod n$ for all non-negative integers $\alpha, \beta < o_n(C)$ at the same time.

   We get a superposition of $|\alpha, \beta, M^\alpha C^{-\beta} \bmod n\rangle$. Measuring the third registry gives a random c_0 and superposition of states $|\alpha, \beta\rangle$ such that $M^\alpha C^{-\beta} \equiv c_0 \pmod n$. These pairs of integers (α, β) are of the form

   $$(\alpha_0, \beta_0), (\alpha_0 + 1, \beta_0 + d), (\alpha_0 + 2, \beta_0 + 2d), \ldots$$

2. Apply QFT.

Exercises

17.1 Prove that if n is an odd prime power, then $x^2 \equiv 1 \pmod n$ if and only if $x \equiv \pm 1 \pmod n$.

17.2 Suppose $n = pq$ is a product of two distinct odd primes. Find the number of $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $o_n(b)$ is odd or $b^{o_n(b)/2} \equiv -1 \pmod n$.

Lecture 31 Wed 11/22

18 Probabilistic primality test

In this section, we consider two probabilistic primality tests, the Fermat test and the Miller-Rabin test. They both build upon Fermat's little theorem: $a^{p-1} \equiv 1 \pmod p$ if p is a prime and $a = 1, \ldots, p-1$.

Lemma 18.1 *If $a^{n-1} \equiv 1 \pmod n$ for every $a = 1, \ldots, n-1$, then n is a prime.*

Proof: Every $a = 1, \ldots, n-1$ is invertible in $\mathbb{Z}/n\mathbb{Z}$. □

It is not practical to test all integers less than n (we might as well just check for division in this case). So we use the same probabilistic idea as in Shor's algorithm:

1. Pick $a = 1, \ldots, n-1$ at random.
2. Compute $\gcd(a, n)$. If it is bigger than 1, then n is not a prime.
3. Compute $a^{n-1} \bmod n$. If it is not 1, then n is not a prime. Otherwise, return to step 1.

Let

$$F_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{n-1} = 1\}.$$

We need to know how big F_n is in order to know the probability that a randomly chosen a can be used to prove that n is not a prime.

Lemma 18.2 *The set F_n is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof: Clearly $1 \in F_n$. If $a, b \in F_n$, then $(ab)^{n-1} = a^{n-1}b^{n-1} = 1$ and $(a^{-1})^{n-1} = (a^{n-1})^{-1} = 1$. $\square$

Since the order of a subgroup divides the order of the group, we see that if $F_n \neq (\mathbb{Z}/n\mathbb{Z})^\times$, then $|F_n| \leq \frac{1}{2}\phi(n)$ and we have a probability of at least $1/2$ that a randomly chosen a can be used to prove that n is not a prime. Unfortunately, there exists (infinitely many) odd composite numbers n where $F_n = (\mathbb{Z}/n\mathbb{Z})^\times$. These numbers are called **Carmichael** numbers. The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$. If we attempt to run the Fermat test on a Carmichael number, then we are just hoping to hit integers a that share a prime factor with n. If n is a product of very few large primes, we are in trouble. Carmichael numbers are all squarefree and so have at least 2 distinct prime divisors. In HW11, you will show that they have at least 3 distinct prime divisors.

Proposition 18.3 *If $p^2 \mid n$ for some prime $p \geq 3$, then n is not a Carmichael number.*

Proof: The key observation is that

$$(1+p)^{n-1} = 1 + (n-1)p + \sum_{r=2}^{n-1} \binom{n-1}{r} p^r \equiv 1 + (n-1)p \pmod{p^2}.$$

Since $p \mid n$, we have $p \nmid n-1$ and so $(1+p)^{n-1} \not\equiv 1 \pmod{p^2}$. Hence $(1+p)^{n-1} \not\equiv 1 \pmod{n}$. $\square$

The Miller-Rabin test builds upon this idea and the earlier idea of nontrivial solutions of $x^2 \equiv 1 \pmod{n}$. Since n is assumed to be odd, we write $n - 1 = u \cdot 2^k$ where u is odd and $k \in \mathbb{N}$. Let

$$b_0 \equiv a^u \pmod{n}, \qquad b_i \equiv b_{i-1}^2 \equiv a^{u \cdot 2^i} \pmod{n} \text{ for } i = 1, \ldots, k.$$

Here is the algorithm for the Miller-Rabin test

1. Pick $a = 1, \ldots, n-1$ at random.
2. Compute $\gcd(a, n)$. If it is bigger than 1, then n is not a prime.
3. Compute $b_0 \equiv a^u \bmod n$. If $b_0 \equiv 1 \bmod n$, return to step 1.
4. Repeatedly compute $b_{i+1} \equiv b_i^2 \bmod n$. If $-1 \bmod n$ is reached before $1 \bmod n$, return to step 1. If $1 \bmod n$ is reached before $-1 \bmod n$, then n is not prime because we have a nontrivial solution to $x^2 \equiv 1 \pmod{n}$. If none of $b_0, \ldots, b_{k-1}$ equals $-1 \bmod n$, then n is not a prime.

We now consider the bad set for the Miller-Rabin test. Let

$$M_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^u = 1 \text{ or } a^{u2^i} = -1 \text{ for some } i = 0, \ldots, k-1\}.$$

For any $a \in M_n$, if $a^u = 1$, we set $i(a) = -1$; otherwise, we set $i(a)$ to be the integer $i = 0, \ldots, k-1$ such that $a^{u2^i} = -1$. Note that $(-1)^u = -1$ and $(-1)^{2u} = 1$ and so $i(-1) = 0$. Let $j \leq k-1$ be the largest $i(a)$ over $a \in M_n$. Then $j \geq i(-1) = 0$. For any $a \in M_n$, since $i(a) \leq j$, we have $a^{u2^j} = \pm 1$. In other words, M_n is a subset of

$$E_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{u \cdot 2^j} = \pm 1\}.$$

It is easy to see that E_n is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 18.4 *Suppose n is a positive odd number with at least two distinct prime divisors (for example if n is a Carmichael number). Then E_n is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. As a result, $|M_n|/\phi(n) \leq \frac{1}{2}$.*

Proof: We write $n = m_1 m_2$ where m_1 and m_2 are coprime odd integers. Let $a_0 \in M_n$ with $i(a_0) = j$. Then $a_0^{u2^j} = -1$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. By the Chinese Remainder Theorem, there exists an integer a such that

$$\begin{aligned} a &\equiv a_0 \pmod{m_1} \\ a &\equiv 1 \pmod{m_2}. \end{aligned}$$

Then $a^{u \cdot 2^j}$ is $-1 \bmod m_1$ and $1 \bmod m_2$. So it can't be $\pm 1 \bmod m_1 m_2$. Hence $a \notin E_n$. $\square$

Exercises

1. Let G be a finite group and let H be a non-empty subset. Prove that if $\forall a, b \in H, ab \in H$, then H is a subgroup.

2. Let n be an odd positive integer. Let

$$F_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{(n-1)/2} = \left(\frac{a}{n}\right)\}$$

where $\left(\frac{a}{n}\right)$ is the Jacobi symbol. Prove that F_n is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, and that it is a proper subgroup when n is composite.

Since the Jacobi symbols can be quickly computed using quadratic reciprocity (see HW 7 Problem 2), this gives another probabilistic primality test (Solovay-Strassen) with polynomial runtime.

3. Let $n > 1$ be an integer. Let $a \in \mathbb{N}$ and let p be a prime number such that:

- $a^{n-1} \equiv 1 \pmod{n}$;
- $p \mid n-1$ and $p > \sqrt{n} - 1$;
- $\gcd(a^{(n-1)/p} - 1, n) = 1$.

Prove that n is a prime.

This result can be used to recursively generate candidates for primes with deterministic proofs: given a large prime p, consider $n = 2pq + 1$ where q is some large random natural number less than $p/2$.

19 Agrawal-Kayal-Saxena primality test

The AKS primality test is a deterministic primality test whose run time is polynomial in $\log n$.

For any commutative ring R and any $a, b, m_1, \ldots, m_r \in R$, we write

$$a \equiv b \pmod{m_1, \ldots, m_r} \qquad \Longleftrightarrow \qquad a - b \in (m_1, \ldots, m_r).$$

Recall that when $n = p$ is a prime, we have for any $a \in \mathbb{Z}$, the following congruence in $\mathbb{Z}[x]$,

$$(x + a)^p \equiv x^p + a^p \equiv x^p + a \pmod{p}.$$

Lecture 32 Fri 11/24

Lemma 19.1 *Let $n \geq 2$ be an integer such that for some $a \in \mathbb{Z}$ coprime to n,*

$$(x + a)^n \equiv x^n + a \pmod{n}.$$

Then n is a prime.

Proof: Suppose for a contradiction that n is not a prime. Let $p < n$ be a prime divisor of n. Let k be a positive integer such that $p^k \leq n < p^{k+1}$. Then by Corollary 4.3, we have $p \nmid \binom{n}{p^k}$. Since a is coprime to n, we have $p \nmid \binom{n}{p^k} a^{n-p^k}$. This gives a nonzero middle term if $p^k < n$. If $p^k = n$, then by Corollary 4.4, we have $\nu_p(\binom{n}{p}) = k - 1 < \nu_p(n)$ and so $n \nmid \binom{n}{p} a^{n-p}$. □

The key idea of the AKS test is to check the congruence

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}$$

for a suitably chosen $r \leq (\log_2 n)^5$ and for positive integers $a \leq \sqrt{\phi(r)} \log_2 n \leq (\log_2 n)^{3.5}$. We can use the usual square and multiply method to compute $(x+a)^n \bmod (x^r - 1, n)$ in polynomial time for each a. Hence the full algorithm is in polynomial time. In what follows, we write $\log n$ for $\log_2 n$.

Lemma 19.2 *For $n \geq 3$, there exists a positive integer $r \leq (\log n)^5$ such that either $\gcd(r,n) > 1$ or $o_r(n) > (\log n)^2$.*

Proof: Suppose for a contradiction that for all positve integer $r \leq (\log n)^5$, we have $\gcd(r,n) = 1$ and $r \mid n^d - 1$ for some $d \leq (\log n)^2$. Let $m = \lfloor (\log n)^5 \rfloor$. Then $L_m = \mathrm{lcm}(1, 2, \ldots, m)$ divides

$$\prod_{1 \leq d \leq (\log n)^2} (n^d - 1) \leq n^{\sum_{1 \leq d \leq (\log n)^2} d} \leq n^{(\log n)^4 - 1} = 2^{(\log n)^5 - (\log n)}.$$

Recall from HW 2 that $L_m \geq 2^m$ for any integer $m \geq 7$. From $n \geq 3$, we have $m \geq 10$, so

$$L_m \geq 2^m \geq 2^{(\log n)^5 - 1}.$$

We now have a contradiction because $(\log n)^5 - 1 > (\log n)^5 - (\log n)$ for $n \geq 4$. □

Remark: The bound

$$\sum_{1 \leq d \leq (\log n)^2} d \leq (\log n)^4 - 1$$

can be improved to about $\frac{1}{2}(\log n)^4$for large n and we can improve the bound on r to about $\frac{1}{2}(\log n)^5$.

Step 1 of AKS: Find the smallest positive integer r such that $\gcd(r,n) > 1$ or $o_r(n) > (\log n)^2$.

We know we only need to test at most $(\log n)^5$ different r. For each r, we simply compute $r, r^2, r^3, \ldots r^{\lfloor (\log n)^2 \rfloor} \mod n$ to see if any of them is 1. Hence this step can be done in polynomial time. If $n < (\log n)^5$ is small (only happens when $n < 10^7$) so that this step does not terminate before $r \geq n$, then we have checked that $\gcd(r,n) = 1$ for all $r < n$ and so n is prime. If this step terminates at an r with $\gcd(r,n) > 1$, then n is composite. Suppose now we have found a positive integer $r \leq (\log n)^5$ coprime with n with $o_r(n) > (\log n)^2$. Note this also implies that $\phi(r) > (\log n)^2$. Since $n \not\equiv 1 \pmod{r}$, we see that n has a prime divisor $p \not\equiv 1 \pmod{r}$ so that $o_r(p) > 1$.

Step 2 of AKS: For every positive integer $a \leq r$, check if $\gcd(a,n) = 1$.

Suppose Step 2 is passed. Then that means we may assume $p > r$. So we have

$$\sqrt{\phi(r)} \log n < \phi(r) < r < p.$$

Step 3 of AKS: For every positive integer $a \leq \sqrt{\phi(r)} \log n$, check if $\gcd(a,n) = 1$ and if so, check the congruence

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}.$$

Theorem 19.3 *Suppose positive integers n, r and prime p satisfy:*

- $o_r(n) > (\log n)^2$
- $p \mid n$, $p > r$ *and* $o_r(p) > 1$
- *For all positive integers $a < \sqrt{\phi(r)} \log n$, the congruence $(x + a)^n \equiv x^n + a \pmod{x^r - 1, p}$.*

Then n is a power of p.

Step 0 of AKS: Check if n is a perfect power.

It remains now to prove Theorem 19.3. We may assume that $n \geq 4$. The congruence mod $(x^r - 1, p)$ suggests to look inside $\mathbb{F}_p[x]$ and consider r-th roots of unities. Let $d = o_r(p) > 1$. We know that the finite field $\mathbb{F}_{p^d}$ is the smallest field that contains a primitive r-th root of unity α_0, and thus all the r-th roots of unities as powers of α_0. Let

$$\mu_r = \langle \alpha_0 \rangle = \{\alpha_0^k \colon k \in \mathbb{Z}/r\mathbb{Z}\}$$

be the subgroup of all r-th roots of unities. Let $\ell = \lfloor \sqrt{\phi(r)} \log n \rfloor < p$. The congruence

$$(x+a)^n \equiv x^n + a \pmod{x^r - 1, p}$$

translates to: for every $f(x) \in S := \{x, x+1, \ldots, x+\ell\} \subseteq \mathbb{F}_p[x]$,

$$f(x)^n - f(x^n) = j(x)(x^r - 1)$$

for some $j(x) \in \mathbb{F}_p[x]$. In other words, we have for every $f(x) \in S$,

$$f(\alpha)^n = f(\alpha^n) \in \mathbb{F}_{p^d}, \text{ for every } \alpha \in \mu_r.$$

Note since $\ell < p$, the set S contains $\ell + 1$ distinct linear polynomials.

We say a polynomial $g(x) \in \mathbb{F}_p[x]$ *commutes* with a positive integer m if

$$g(\alpha)^m = g(\alpha^m) \in \mathbb{F}_{p^d}, \text{ for every } \alpha \in \mu_r.$$

Hence, every element in S commutes with n. The following lemmas are immediate:

Lemma 19.4 *Any $g \in \mathbb{F}_p[x]$ commutes with p and 1.*

Lemma 19.5 *If $g_1, g_2 \in \mathbb{F}_p[x]$ both commute with m, then $g_1 g_2$ commutes with m*

Lecture 33 Mon 11/27

The next two are less immediate.

Lemma 19.6 *If $g \in \mathbb{F}_p[x]$ commutes with m_1 and m_2, then g commutes with $m_1 m_2$.*

Proof: For any $\alpha \in \mu_r$, we have

$$g(\alpha)^{m_1 m_2} = (g(\alpha^{m_1}))^{m_2} = g(\alpha^{m_1 m_2})$$

since $\alpha^{m_1} \in \mu_r$. □

Lemma 19.7 *If $g \in \mathbb{F}_p[x]$ commutes with m and $p \mid m$, then g commutes with m/p.*

Proof: For any $\alpha \in \mu_r$, we have

$$\big(g(\alpha)^{m/p}\big)^p = g(\alpha)^m = g(\alpha^m) = g(\alpha^{m/p})^p.$$

Hence $g(\alpha)^{m/p} = g(\alpha^{m/p})$ because raising to the power p is an automorphism and thus injective on $\mathbb{F}_{p^d}$. □

Let $\bar{S}$ denote the set of polynomials in $\mathbb{F}_p[x]$ that are products of elements in S. So

$$\bar{S} = \{x^{n_0}(x+1)^{n_1} \cdots (x+\ell)^{n_\ell} : n_0, \ldots, n_\ell \geq 0\}.$$

Then every element in $\bar{S}$ commutes with every positive integer of the form $(n/p)^i p^j$. Suppose for a contradiction that n is not a power of p. Then the integers $(n/p)^i p^j$ are all distinct for distinct pairs (i, j). However, α_0^m only takes r possible values. In other words, the set

$$T = \{\alpha_0^{(n/p)^i p^j} : i, j \geq 0\} \subseteq \mu_r$$

is finite. Let $m_1 > m_2$ to two integers of the form $(n/p)^i p^j$ such that $\alpha_0^{m_1} = \alpha_0^{m_2}$. Note that this condition is equivalent to $m_1 \equiv m_2 \pmod{r}$. Then for any $g \in \bar{S}$, we have

$$g(\alpha_0)^{m_1} = g(\alpha_0^{m_1}) = g(\alpha_0^{m_2}) = g(\alpha_0)^{m_2}.$$

Recall that F_{p^d} is the smallest field that contains a primitive r-th root of unity and any $g \in \bar{S}$ splits in $\mathbb{F}_p$. Hence all the roots of $g(x)$ are in $\mathbb{F}_p$ while $\alpha_0 \notin \mathbb{F}_p$. So $g(\alpha_0) \neq 0$ and we have

$$g(\alpha_0)^{m_1 - m_2} = 1.$$

On the other hand, when can $g(\alpha_0) = h(\alpha_0)$ for $g, h \in \bar{S}$? We know that for every integer m of the form $(n/p)^i p^j$, we have

$$g(\alpha_0^m) = g(\alpha_0)^m = h(\alpha_0)^m = h(\alpha_0^m).$$

In other words, every $\alpha \in T$ is a root of $g(x) - h(x)$. Hence if we further require that $\deg(g)$ and $\deg(h)$ are less than $|T|$, then $g = h$. Let $N = |T|$ and let $C(\ell + 1, N - 1)$ be the number of elements in $\bar{S}$ of degree at most $N - 1$. Then we have

$$|\{g(\alpha_0) \colon g \in \bar{S}\}| \geq C(\ell + 1, N - 1).$$

Hence, if we can find m_1 and m_2 so that

$$m_1 - m_2 < C(\ell + 1, N - 1),$$

then we would have too many solutions to $x^{m_1 - m_2} = 1$, which is a contradiction!

We note that

$$N = |\{\alpha_0^{(n/p)^i p^j} : i, j \geq 0\}| = |\{(n/p)^i p^j \bmod r \colon i, j \geq 0\}|.$$

For $i, j = 0, \ldots, \lfloor \sqrt{N} \rfloor$, we have $(\lfloor \sqrt{N} \rfloor + 1)^2 > N$ distinct integers of the form $(n/p)^i p^j$. There are only N possible congruence classes mod r that they can take. Hence, by the Pigeonhole principle, there exist two distinct integers $m_1 > m_2$ among them that are congruent mod r. Moreover,

$$m_1 - m_2 < m_1 \leq (n/p)^{\lfloor \sqrt{N} \rfloor} p^{\lfloor \sqrt{N} \rfloor} = n^{\lfloor \sqrt{N} \rfloor}.$$

Therefore, it remains to prove that

$$n^{\lfloor \sqrt{N} \rfloor} \leq C(\ell + 1, N - 1).$$

Let's estimate the sizes of the variables involved. By taking $i = j$, we see that $(n/p)^i p^j = n^i$. So we have

$$\{n^i \bmod r \colon i \geq 0\} \subseteq \{(n/p)^i p^j \bmod r \colon i, j \geq 0\} \subseteq (\mathbb{Z}/r\mathbb{Z})^\times.$$

In other words,

$$(\log n)^2 < o_r(n) \leq N \leq \phi(r).$$

Let $M = \lfloor \lfloor \sqrt{N} \rfloor \log n \rfloor$. Then

$$\begin{aligned} n^{\lfloor \sqrt{N} \rfloor} &= 2^{\lfloor \sqrt{N} \rfloor \log n} \leq 2^{M+1}, \\ \ell + 1 &= \lfloor \sqrt{\phi(r)} \log n \rfloor + 1 \geq \lfloor \sqrt{N} \log n \rfloor + 1 \geq M + 1, \\ N - 1 &> \sqrt{N} \log n - 1 \geq M - 1, \\ C(\ell + 1, N - 1) &\geq C(M + 1, M). \end{aligned}$$

Hence, it is enough to prove that

$$C(M + 1, M) \geq 2^{M+1}.$$

Since $x, x + 1, \ldots, x + M$ are all distinct linear polynomials in $\mathbb{F}_p[x]$, $C(M + 1, M)$ is the same as the number of monomials of the form $x_1^{a_1} \cdots x_{M+1}^{a_{M+1}}$ in $M + 1$ variables of degree $a_1 + \cdots + a_{M+1}$ at most M. By adding in one more variable x_0 and setting $a_0 = M - (a_1 + \cdots + a_{M+1})$, this is the same as the number of monomials of the form $x_0^{a_0} x_1^{a_1} \cdots x_{M+1}^{a_{M+1}}$ in $M + 2$ variables of degree exactly M.

Theorem 19.8 *The number of monomials of the form $x_1^{a_1} \cdots x_k^{a_k}$ in k variables of degree $d = a_1 + \cdots + a_k$ is $\binom{d+k-1}{k-1}$.*

In particular, we have

$$C(M+1,M) = \binom{2M+1}{M+1} = \binom{2M+1}{M} > \frac{4^M}{M+1} \geq 2^{M+1}$$

when $2^M \geq 2(M+1)$, which is true for $M \geq 3$. Since $n \geq 4$, we have $\log n \geq 2$ and $M \geq 4$.

The standard proof of Theorem 19.8 is the stars and bars method. Imagining placing d stars and $k-1$ bars in $d+k-1$ slots. The number of ways to do this is $\binom{d+k-1}{k-1}$. The number of stars before the first bar is the exponent of x_1. The number of stars between the i-th bar and the $(i+1)$-st bar is the exponent of x_{i+1} for $i = 1, \ldots, k-2$. The number of stars after the last bar is the exponent of x_k.

Lecture 34 Wed 11/29

20 Lucas-Lehmer primality test

A Mersenne number is a number of the form $M_n = 2^n - 1$ for some $n \in \mathbb{N}$. Note since $2^d - 1 \mid 2^n - 1$ whenever $d \mid n$, in order for $2^n - 1$ to be a prime, n itself must be a prime. However, when $n = p$ is a prime, $M_p = 2^p - 1$ is not necessarily a prime. For example, $M_{11} = 2047 = 23 \times 89$.

A Sophie Germain prime is a prime p such that $2p+1$ is also prime. The above $p = 11$ is one such example with $2p + 1 = 23$ appearing in the factorization of M_p. The infinitude of Sophie Germain primes is an open conjecture. The heuristic count for the number of them less than x is about $1.32032\, x/(\ln x)^2$.

Proposition 20.1 *Suppose $p \equiv 3 \pmod 4$ is a Sophie Germain prime. Then $2p+1 \mid M_p$ and so M_p is not prime for $p > 3$.*

Proof: From $p \equiv 3 \pmod 4$, we get $2p + 1 \equiv 7 \pmod 8$. Hence 2 is a quadratic residue mod $2p+1$. Let a be an integer such that $2 \equiv a^2 \pmod{2p+1}$. Then

$$2^p \equiv a^{2p} \equiv 1 \pmod{2p+1}$$

by Fermat's little theorem. Then $2p + 1 \mid 2^p - 1$. □

The Lucas-Lehmer primality test is used in general to see whether a Mersenne number $M_p = 2^p - 1$ is prime. The current record for the largest proved prime number is

$$2^{82589933} - 1.$$

In the Lucas-Lehmer test, we define the sequence

$$a_0 = 4, \qquad a_{n+1} = a_n^2 - 2 \text{ for } n \geq 0.$$

We let $\omega = 2 + \sqrt{3}$. Then $\omega^{-1} = 2 - \sqrt{3}$. In other words, ω is a unit in the ring

$$R = \mathbb{Z}[\sqrt{3}] = \{j(\sqrt{3})\colon j(x) \in \mathbb{Z}[x]\} = \{a + b\sqrt{3}\colon a, b \in \mathbb{Z}\} \cong \mathbb{Z}[x]/(x^2 - 3).$$

It is easy to check via induction that

$$a_n = \omega^{2^n} + \omega^{-2^n} = \omega^{-2^n}(\omega^{2^{n+1}} + 1).$$

Consider

$$a_{p-2} = \omega^{-2^{p-2}}(\omega^{2^{p-1}} + 1).$$

Theorem 20.2 *Let p be an odd prime. The Mersenne number $M_p = 2^p - 1$ is prime if and only if $a_{p-2} \equiv 0 \pmod{M_p}$.*

Proof: Let $q = M_p$. Then $qR = \{qa + qb\sqrt{3} \colon a, b \in \mathbb{Z}\}$. Hence we see that

$$a_{p-2} \in q\mathbb{Z} \iff a_{p-2} \in qR \iff \omega^{2^{p-1}} = -1 \text{ in } R/qR \iff \omega^{\frac{q+1}{2}} = -1 \text{ in } R/qR.$$

Suppose first that $a_{p-2} \in q\mathbb{Z}$ and suppose for a contradiction that q is not a prime. Let $r \leq \sqrt{q}$ be a prime divisor of q. Then we also have $a_{p-2} \in r\mathbb{Z}$ and so $\omega^{2^{p-1}} = -1$ in R/rR. Then $\omega^{2^p} = 1$ in R/rR. The order $o(\omega)$ of ω in $(R/rR)^\times$ is then a divisor of 2^p that doesn't divide 2^{p-1}. Hence it equals 2^p, which then must divide $|(R/rR)^\times|$. However, we have a contradiction now because

$$|(R/rR)^\times| \leq |R/rR| - 1 = r^2 - 1 \leq q - 1 = 2^p - 2.$$

Suppose conversely that q is a prime. Since p is odd, we see that

$$2^p - 1 \equiv 7 \pmod{12}, \qquad 2^p - 1 \equiv 7 \pmod{8}.$$

So by quadratic reciprocity,

$$\left(\frac{3}{q}\right) = -1, \qquad \left(\frac{2}{q}\right) = 1.$$

This means that the polynomial $x^2 - 3$ is irreducible in $\mathbb{F}_q[x]$ and so

$$R/qR \cong \mathbb{F}_q[x]/(x^2 - 3) \cong \mathbb{F}_{q^2}.$$

The Frobenius map $a \mapsto a^q$ sends $\sqrt{3}$ to $-\sqrt{3}$. This can also be seen from

$$\sqrt{3}^{q-1} = 3^{(q-1)/2} = -1 \in R/qR.$$

For any $a + b\sqrt{3}$ in R/qR, we then have

$$(a + b\sqrt{3})^q = a^q + b^q\sqrt{3}^q = a - b\sqrt{3}$$

and so

$$(a + b\sqrt{3})^{q+1} = (a + b\sqrt{3})^q(a + b\sqrt{3}) = (a - b\sqrt{3})(a + b\sqrt{3}) = a^2 - 3b^2.$$

We note that $(3 + \sqrt{3})^2 = 12 + 6\sqrt{3} = 6\,\omega$. Hence

$$\omega^{(q+1)/2} = \frac{(3 + \sqrt{3})^{q+1}}{6^{(q-1)/2} \cdot 6} = \frac{3^2 - 3 \cdot 1^2}{2^{(q-1)/2}3^{(q-1)/2} \cdot 6} = \frac{6}{-6} = -1,$$

as desired. □

In the above proof, the fact that $(a + b\sqrt{3})^{q+1} \in \mathbb{F}_q$ is a consequence of a more general construction. We note that $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^2}) = \{\mathrm{id}, \tau\}$ where τ denotes the Frobenius map and

$$(a + b\sqrt{3})^{q+1} = \mathrm{id}(a + b\sqrt{3}) \cdot \tau(a + b\sqrt{3}) = \prod_{\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^2})} \sigma(a + b\sqrt{3}).$$

It is then not surprising that it is fixed by every element in $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^2})$ and so it must lie in $\mathbb{F}_q$. In general, given a Galois extension E/F, we have the norm

$$N_{E/F}(\alpha) = \prod_{\sigma \in \mathrm{Aut}_F(E)} \sigma(\alpha) \in F.$$

For $\mathbb{C}/\mathbb{R}$, this is simply

$$N_{\mathbb{C}/\mathbb{R}}(z) = z \cdot \bar{z} = |z|^2.$$

We next consider $\mathbb{Q}(\zeta_4)$ and $\mathbb{Q}(\zeta_3)$, which both have degree 2 over $\mathbb{Q}$, and where the non-identity automorphism is complex conjugation. So their norm maps are also just the complex modulus squared.

Lecture 35 Fri 12/01

21 $\mathbb{Q}(\zeta_4)$ and $\mathbb{Q}(\zeta_3)$

In this section, we consider the two cyclotomic extensions of degree 2. We have

$$\begin{aligned}\mathbb{Q}[x]/(x^2+1) &\cong \mathbb{Q}(\zeta_4) = \{a+bi\colon a,b\in\mathbb{Q}\} = \mathbb{Q}(i)\\ \mathbb{Q}[x]/(x^2+x+1) &\cong \mathbb{Q}(\zeta_3) = \{a+b\zeta_3\colon a,b\in\mathbb{Q}\} = \mathbb{Q}(-\frac{1}{2}+\frac{\sqrt{3}}{2}i)\end{aligned}$$

Note that $\phi(6)=2$ so $\mathbb{Q}(\zeta_6)$ also has degree 2, but $\zeta_6 = \frac{1}{2}+\frac{\sqrt{3}}{2}i = \zeta_3+1$. So $\mathbb{Q}(\zeta_6)=\mathbb{Q}(\zeta_3)$. Let τ denote the non-identity element of the automorphism groups $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_4))$ and $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_3))$. For $\mathbb{Q}(\zeta_4)$, we have for any $a,b\in\mathbb{Q}$,

$$\tau(i) = i^3 = -i \qquad \Longrightarrow \qquad \tau(a+bi) = a-bi,$$

and for $\mathbb{Q}(\zeta_3)$, we have

$$\tau(\zeta_3) = \zeta_3^2 = -1-\zeta_3 = -\frac{1}{2}-\frac{\sqrt{3}}{2}i = \overline{\zeta_3} \qquad \Longrightarrow \qquad \tau(a+b\zeta_3) = a-b-b\zeta_3.$$

In other words, τ is complex conjugation for both of them. Define the **norm** of an element in either field as

$$N(\alpha) = \tau(\alpha)\alpha = |\alpha|^2 : \qquad N(a+bi) = a^2+b^2, \qquad N(a+b\zeta_3) = (a-\frac{b}{2})^2+\frac{3}{4}b^2 = a^2-ab+b^2.$$

Note that the norm function is multiplicative: $N(\alpha\beta)=N(\alpha)N(\beta)$. So from

$$(a+bi)(c+di) = ac-bd+(ad+bc)i$$

we have the well-known formula

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2;$$

and from

$$(a+b\zeta_3)(c+d\zeta_3) = ac+(bc+ad)\zeta_3+bd(-1-\zeta_3) = ac-bd+(bc+ad-bd)\zeta_3$$

we have the less-known formula

$$(a^2-ab+b^2)(c^2-cd+d^2) = (ac-bd)^2-(ac-bd)(bc+ad-bd)+(bc+ad-bd)^2.$$

If we use the above formula with $a,b,c,d\in\mathbb{Z}$, we see that the sets

$$\begin{aligned}S_4 &= \{a^2+b^2\colon a,b\in\mathbb{Z}\}\\ S_3 &= \{a^2-ab+b^2\colon a,b\in\mathbb{Z}\}\end{aligned}$$

are closed under multiplication. Hence to understand what they are, it remains to understand which prime powers do S_4 and S_3 contain. They clearly contain p^2 for every prime p by taking $a=p$ and $b=0$. It is easy to check that $2\in S_4$, $2\notin S_3$ and $3\in S_3$.

Suppose $p>2$ is a prime and $p=a^2+b^2$ for some $a,b\in\mathbb{Z}$. Then $a^2\equiv -b^2 \pmod p$. If $p\mid b$, then $p\mid a^2$ implying that $p\mid a$ and so $p^2\mid a^2+b^2$ which is not possible. So $p\nmid b$ and we have $(ab^{-1})^2\equiv -1 \pmod p$. Hence $p\equiv 1 \pmod 4$. Similarly, if $p=a^2-ab+b^2$ for $a,b\in\mathbb{Z}$ and $p>2$ prime. We have $p\nmid b$ and $(2ab^{-1}-1)^2\equiv -3 \pmod p$. It then follows from quadratic reciprocity that $p=3$ or $p\equiv 1 \pmod 3$. The converse is also true.

Theorem 21.1 *If p is a prime congruent to 1 mod 4, then there exist $a,b\in\mathbb{Z}$ such that $p=a^2+b^2$.*

Theorem 21.2 *If p is a prime congruent to 1 mod 3, then there exist $a,b\in\mathbb{Z}$ such that $p=a^2-ab+b^2$.*

We give a ring-theoretic proof of these results. There is also a "descent"-type proof. We note that if $p \equiv 1 \pmod{m}$, then $m \mid p-1$ so $\mathbb{F}_p$ contains a primitive m-th root of unity. In other words, $\pi_p(\Phi_m(x))$ splits completely in $\mathbb{F}_p[x]$. Let $x-n$ be an irreducible factor of it. Then we have a prime ideal $I_p = (p, \zeta_m - n)$ in $\mathbb{Z}[\zeta_m]$.

Proposition 21.3 *The rings $\mathbb{Z}[\zeta_4]$ and $\mathbb{Z}[\zeta_3]$ are Euclidean domains with respect to the norm function.*

As a consequence, we see that $\mathbb{Z}[\zeta_m]$ is a PID for $m = 3$ and 4. There then exists some $\alpha \in \mathbb{Z}[\zeta_m]$ such that $I_p = (\alpha)$. We write $p = \alpha\beta$ for some $\beta \in \mathbb{Z}[\zeta_m]$. Taking norm gives $p^2 = N(\alpha)N(\beta)$. Next we note that if $N(\gamma) = 1$ for some $\gamma \in \mathbb{Z}[\zeta_m]$, then $\gamma \cdot \tau(\gamma) = 1$ and so γ is a unit. (**Exercise**: Conversely, if γ is a unit, then $N(\gamma) = 1$.) Since I_p is a proper ideal, we see that α can't be a unit. If β is a unit, then $I_p = (p)$ but $p \nmid \zeta_m - n$. So neither $N(\alpha)$ nor $N(\beta)$ can be 1 but they multiply to p^2 and p is a prime. So $N(\alpha) = N(\beta) = p$. Upon writing $\alpha = a + b\zeta_m$ for $a, b \in \mathbb{Z}$, we have

$$p = a^2 + b^2 \text{ for } m = 4, \qquad \text{and} \qquad p = a^2 - ab + b^2 \text{ for } m = 3.$$

Proof of Proposition 21.3: Let $\alpha, \beta \in \mathbb{Z}[\zeta_m]$ where $m = 3$ or 4 and $\alpha \neq 0$. We divide β by α in the field $\mathbb{Q}(\zeta_m) = \mathbb{Q}[\zeta_m]$ to get

$$\frac{\beta}{\alpha} = t + s\zeta_m, \qquad r, s \in \mathbb{Q}.$$

Let $a \in \mathbb{Z}$ be an integer that is the closest to t and let $b \in \mathbb{Z}$ be an integer that is the closest to s. (In other words, either the floor or ceiling of t and s.) Hence

$$\frac{\beta}{\alpha} = (a + b\zeta_m) + \big((t-a) + (s-b)\zeta_m\big), \qquad |t-a| \leq \frac{1}{2}, \qquad |s-b| \leq \frac{1}{2}.$$

Then

$$N\big((t-a) + (s-b)\zeta_m\big) \leq |t-a|^2 + |t-a||s-b| + |s-b|^2 \leq \frac{3}{4} < 1.$$

We let $q = a + b\zeta_m \in \mathbb{Z}[\zeta_m]$ and $r = \beta - \alpha q = \alpha\big((t-a) + (s-b)\zeta_m\big) \in \mathbb{Z}[\zeta_m]$. Then $N(r) < N(\alpha)$. □

Remark: When $t = 1/2$ for example, there are two choices for a. Hence the "quotient" and "remainder" are not unique in this division algorithm. The same argument also works for $\mathbb{Z}[\sqrt{2}i]$, $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$.

Lecture 36 Mon 12/04

The units in $\mathbb{Z}[\zeta_m]$ for $m = 3, 4$ are elements of the form $a + b\zeta_m$ with norm dividing 1, and so equaling 1 since it is non-negative. It is easy to check that

$$\begin{aligned} \mathbb{Z}[i]^\times &= \{1, -1, i, -i\} = \mu_4, \\ \mathbb{Z}[\zeta_3]^\times &= \{1, -1, \zeta_3, -\zeta_3, 1+\zeta_3, -1-\zeta_3\} = \mu_6. \end{aligned}$$

There is an intrinsic reason for this. The roots of unities are clearly units. The norms for these rings are sums of squares and so there are only finitely many integer solutions to $N = 1$, implying that the group of units is finite. Every element of a finite group has a finite order, and is thus a root of unity.

Since $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_3]$ are PIDs, we can define prime elements (generate a prime ideal), gcds and we have unique factorization into primes up to units. We use this property of $\mathbb{Z}[\zeta_3]$ to prove that there are no integer solutions to $x^3 + y^3 = z^3$ with $xyz \neq 0$. We write ζ for ζ_3 and write $\gcd(\alpha, \beta)$ for some element that generates the ideal (α, β) in $\mathbb{Z}[\zeta]$.

Theorem 21.4 *There do not exist nonzero $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta]$ and a unit $\epsilon \in \mathbb{Z}[\zeta]^\times$ such that*

$$\alpha^3 + \beta^3 + \epsilon\gamma^3 = 0.$$

Suppose a solution $(\alpha, \beta, \gamma, \epsilon)$ exists. We take one so that $N(\alpha\beta\gamma)$ is the smallest. If there is a prime $\pi \in \mathbb{Z}[\zeta]$ dividing two of α, β, γ, then it divides the cube of the third and so also the third, but then $(\alpha/\pi, \beta/\pi, \gamma/\pi, \epsilon)$ is a smaller solution. Hence α, β, γ are pairwise coprime. We use a descent argument: we construct another solution $(\alpha', \beta', \gamma', \epsilon')$ with $N(\alpha'\beta'\gamma') < N(\alpha\beta\gamma)$.

Let $\pi = \sqrt{3}\, i = 1 + 2\zeta$. Then $N(\pi) = 1 - 2 + 2^2 = 3$ and $\pi^2 = -3$. Hence π is a prime and we have an isomorphism

$$\mathbb{Z}[\zeta]/(\pi) \cong \mathbb{F}_3$$

sending $a + b\zeta + (\pi)$ to $b - 2a$.

Lemma 21.5 *If $\delta \equiv e \pmod{\pi}$ where $e = \pm 1$, then $\delta^3 \equiv e \pmod{9}$.*

Proof: Suppose $\delta = e + \pi\eta$ for some $\eta \in \mathbb{Z}[\zeta]$. Using $e^2 = 1$ and $e^3 = e$, we have

$$\delta^3 = e + 3\pi\eta + 3e(-3)\eta^2 - 3\pi\eta^3 \equiv e + 3\pi(\eta - \eta^3) \pmod{9}.$$

Since $\mathbb{Z}[\zeta]/(\pi) \cong \mathbb{F}_3$, we have $\eta^3 \equiv \eta \pmod{\pi}$ and so $3\pi^2 \mid 3\pi(\eta - \eta^3)$ but $3\pi^2 = -9$. $\square$

Lemma 21.6 *If $\epsilon \in \mathbb{Z}[\zeta]^\times$, then $\pm 1 \pm 1 \pm \epsilon \not\equiv 0 \pmod{9}$. Moreover, if $\pm 1 + \epsilon(\pm 1) \equiv 0 \pmod{3}$, then $\epsilon = \pm 1 = \epsilon^3$.*

As a result, we see that π divides exactly one of α, β, γ. If $\pi \mid \alpha$ so that $3 \mid \alpha^3$, then we have $\epsilon = \epsilon^3$ so that $(\beta, \epsilon\gamma, \alpha, 1)$ is a solution where π divides the third argument. Hence, we may assume without loss of generality that $\pi \mid \gamma$. Now from $\pi \mid \alpha^3 + \beta^3$, we have $\pi \mid \alpha + \beta$ since $(\alpha^3 + \beta)^3 \equiv (\alpha + \beta)^3 \pmod{\pi}$. So we may assume $\alpha \equiv 1 \pmod{\pi}$ and $\beta \equiv -1 \pmod{\pi}$. This then gives $\alpha^3 + \beta^3 \equiv 0 \pmod{9}$ and so we must have $\pi^2 \mid \gamma$. In other words, we have

$$\alpha \equiv 1 \pmod{\pi}, \qquad \beta \equiv -1 \pmod{\pi}, \qquad \pi^2 \mid \gamma.$$

We now factor

$$-\epsilon\gamma^3 = (\alpha + \beta)(\alpha^2 - \alpha\beta + \beta^2) = (\alpha + \beta)(\alpha + \beta\zeta)(\alpha - \beta(1 + \zeta)).$$

Note that since $\zeta \equiv 1 \pmod{\pi}$, we see that all three factors are divisible by π. Hence we have

$$(\pi) \supseteq (\alpha + \beta, \alpha + \beta\zeta) \supseteq (\alpha(\zeta - 1), \beta(\zeta - 1)) = (\zeta - 1) = (\pi).$$

The same is true for any two terms in the product. In other words, once we remove one factor of π from each of them, we have three pairwise coprime elements that multiply to a cube, up to a unit. Hence they must each be a cube, up to a unit. In other words, we have the following factorization:

$$\begin{aligned} \alpha + \beta &= \epsilon_1\pi\delta^3 \\ \alpha + \beta\zeta &= \epsilon_2\pi\eta^3 \\ \alpha - \beta(1 + \zeta) &= \epsilon_3\pi\rho^3 \\ \gamma &= \pi\delta\eta\rho \end{aligned}$$

where $\delta, \eta, \rho \in \mathbb{Z}[\zeta]$ are pairwise coprime and $\epsilon_1, \epsilon_2, \epsilon_3$ are units. Note since $\pi^2 \mid \gamma$, axactly one of δ, η, ρ is divisible by π. Multiplying the second equation by ζ and the third by ζ^2, which are both units, we have

$$\begin{aligned} \alpha + \beta &= \epsilon_1\pi\delta^3 \\ \alpha\zeta + \beta\zeta^2 &= \epsilon_4\pi\eta^3 \\ \alpha\zeta^2 + \beta\zeta &= \epsilon_5\pi\rho^3 \end{aligned}$$

for some units ϵ_4, ϵ_5. Adding them gives

$$\epsilon_1\pi\delta^3 + \epsilon_4\pi\eta^3 + \epsilon_5\pi\rho^3 = 0$$

which looks very much like the original equation! Suppose without loss of generality that $\pi \mid \rho$ and $\pi \nmid \delta, \eta$. We divide the above equation by $\epsilon_1 \pi$ to get

$$\delta^3 + \epsilon_6 \eta^3 + \epsilon_7 \rho^3 = 0,$$

for some units ϵ_6, ϵ_7. From $\pi \mid \rho$, we get $\pm 1 + \epsilon_6(\pm 1) \equiv 0 \pmod 3$ and so $\epsilon_6 = \pm 1 = \epsilon_6^3$. Then $(\delta, \epsilon_6 \eta, \rho, \epsilon_7)$ is another but smaller solution:

$$N(\delta \cdot \epsilon_6 \eta \cdot \rho) = N(\delta \eta \rho) = N(\gamma/\pi) < N(\gamma) \leq N(\alpha\beta\gamma).$$