# Chapter 6. Congruences and Modular Arithmetic

**6.1 Definition:** Let $n \in \mathbf{Z}^+$. For $a, b \in \mathbf{Z}$ we say that $a$ is equal (or **congruent**) to $b$ **modulo** $n$, and we write $a = b$ mod $n$, when $n | (a - b)$ or, equivalently, when $a = b + kn$ for some $k \in \mathbf{Z}$.

**6.2 Theorem:** *Let $n \in \mathbf{Z}^+$. For $a, b \in \mathbf{Z}$ we have $a = b$ mod $n$ if and only if $a$ and $b$ have the same remainder when divided by $n$. In particular, for every $a \in \mathbf{Z}$ there is a unique $r \in \mathbf{Z}$ with $a = r$ mod $n$ and $0 \le r < n$.*

Proof: Let $a, b \in \mathbf{Z}$. Use the Division Algorithm to write $a = qn + r$ with $0 \le r < n$ and $b = pn + s$ with $0 \le s < n$. We need to show that $a = b$ mod $n$ if and only if $r = s$. Suppose that $a = b$ mod $n$, say $a = b + kn$ where $k \in \mathbf{Z}$. Then since $a = qn + r$ and $a = b + kn = (pn + s) + kn = (p + k)n + s$ with $0 \le r < n$ and $0 \le s < n$, it follows that $q = p + s$ and $r = s$ by the uniqueness part of the Division Algorithm. Conversely, suppose that $r = s$. Then we have $0 = r - s = (a - qn) - (b - pn)$ so that $a = b + (q - p)n$, and hence $a = b$ mod $n$.

**6.3 Example:** Find 117 mod 35.

Solution: We are being asked to find the unique integer $r$ with $0 \le r < n$ such that $117 = r$ mod 35 or, in other words, to find the remainder $r$ when 117 is divided by 35. Since $117 = 3 \cdot 35 + 12$ we have $117 = 12$ mod 35.

**6.4 Definition:** An **equivalence relation** on a set $S$ is a binary relation $\sim$ on $S$ such that

E1. $\sim$ is reflexive: for every $a \in S$ we have $a \sim a$,
E2. $\sim$ is symmetric: for all $a, b \in S$, if $a \sim b$ then $b \sim a$, and
E3. $\sim$ is transitive: for all $a, b, c \in S$, if $a \sim b$ and $b \sim c$ then $a \sim c$.

When $\sim$ is an equivalence relation on $S$ and $a \in S$, the **equivalence class** of $a$ in $S$ is the set
$$[a] = \{x \in S \, | \, x \sim a\}.$$

**6.5 Theorem:** *Let $n \in \mathbf{Z}^+$. Then congruence modulo $n$ is an equivalence relation on $\mathbf{Z}$.*

Proof: Let $a \in \mathbf{Z}$. Since $a = a + 0 \cdot n$ we have $a = a$ mod $n$. Thus congruence modulo $n$ satisfies Property E1. Let $a, b \in \mathbf{Z}$ and suppose that $a = b$ mod $n$, say $a = b + kn$ with $k \in \mathbf{Z}$. Then $b = a + (-k)n$ so we have $b = a$ mod $n$. Thus congruence modulo $n$ satisfies Property E2. Let $a, b, c \in \mathbf{Z}$ and suppose that $a = b$ mod $n$ and $b = c$ mod $n$. Since $a = b$ mod $n$ we can choose $k \in \mathbf{Z}$ so that $a = b + kn$. Since $b = c$ mod $n$ we can choose $\ell \in \mathbf{Z}$ so that $b = c + \ell n$. Then $a = b + kn = (c + \ell n) + kn = c + (k + \ell)n$ and so $a = c$ mod $n$. Thus congruence modulo $n$ satisfies Property E3.

**6.6 Definition:** A **partition** of a set $S$ is a set $\mathcal{P}$ of nonempty disjoint subsets of $S$ whose union is $S$. This means that

P1. for all $A \in \mathcal{P}$ we have $\emptyset \ne A \subseteq S$,
P2. for all $A, B \in \mathcal{P}$, if $A \ne B$ then $A \cap B = \emptyset$, and
P3. for every $a \in S$ we have $a \in A$ for some $A \in \mathcal{P}$.

**6.7 Example:** $\mathcal{P} = \{\{1, 3, 5\}, \{2\}, \{4, 6\}\}$ is a partition of $S = \{1, 2, 3, 4, 5, 6\}$.

**6.8 Theorem:** *Let $\sim$ be an equivalence relation on a set $S$. Then $\mathcal{P} = \{[a]\big| a \in S\}$ is a partition of $S$.*

Proof: For $a \in S$, it is clear from the definition of $[a]$ that $[a] \subseteq S$, and we have $[a] \neq \emptyset$ because $a \sim a$ so $a \in [a]$. This shows that $\mathcal{P}$ satisfies P1.

Let $a, b \in S$. We claim that $a \sim b$ if and only if $[a] = [b]$. Suppose that $a \sim b$. Let $x \in S$. Suppose that $x \in [a]$. Then $x \sim a$ by the definition of $[a]$. Since $x \sim a$ and $a \sim b$ we have $x \sim b$ since $\sim$ is transitive. Since $x \sim b$ we have $x \in [b]$. This shows that $[a] \subset [b]$. Since $a \sim b$ implies that $b \sim a$ by symmetry, a similar argument shows that $[b] \subseteq [a]$. Thus we have $[a] = [b]$. Conversely, suppose that $[a] = [b]$. Then since $a \sim a$ we have $a \in [a]$. Since $a \in [a]$ and $[a] = [b]$, we have $a \in [b]$. Since $a \in [b]$, we have $a \sim b$. Thus $a \sim b$ if and only if $[a] = [b]$, as claimed.

Let $a, b \in S$. We claim that if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$. Suppose that $[a] \cap [b] \neq \emptyset$. Choose $c \in [a] \cap [b]$. Since $c \in [a]$ so that $c \sim a$ we have $[c] = [a]$ (by the above claim). Since $c \in [b]$ so that $c \sim b$ we have $[c] = [b]$. Thus $[a] = [c] = [b]$, as required. This completes the proof that $\mathcal{P}$ satisfies P2.

Finally, note that $\mathcal{P}$ satisfies P3 because given $a \in S$ we have $a \in [a] \in P$.

**6.9 Definition:** Let $\sim$ be an equivalence relation on a set $S$. The **quotient** of the set $S$ by the relation $\sim$, denoted by $S/\!\sim$, is the partition $\mathcal{P}$ of the above theorem, that is

$$S/\!\sim \; = \big\{[a]\big| a \in S\big\}.$$

**6.10 Remark:** In Appendix 1, the above quotient construction is used to define $\mathbf{Z}$ from $\mathbf{N}$ and to define $\mathbf{Q}$ from $\mathbf{Z}$.

**6.11 Definition:** Let $n \in \mathbf{Z}^+$. Let $\sim$ be the equivalence relation on $\mathbf{Z}$ defined for $a, b \in \mathbf{Z}$ by $a \sim b \Longleftrightarrow a = b \bmod n$, and write $[a] = \{x \in \mathbf{Z} | x \sim a\} = \{x \in \mathbf{Z} | x = a \bmod n\}$. The set of **integers modulo n**, denoted by $\mathbf{Z}_n$, is defined to be the quotient set

$$\mathbf{Z}_n = \mathbf{Z}/\!\sim \; = \big\{[a]\big| a \in \mathbf{Z}\big\}.$$

Since every $a \in \mathbf{Z}$ is congruent modulo $n$ to a unique $r \in \mathbf{Z}$ with $0 \leq r < n$, we have

$$\mathbf{Z}_n = \big\{[0], [1], [2], \cdots, [n-1]\big\}$$

and the elements listed in the above set are distinct so that $\mathbf{Z}_n$ is an $n$-element set.

**6.12 Example:** We have

$$\mathbf{Z}_3 = \big\{[0], [1], [2]\big\} = \big\{\{\cdots, -3, 0, 3, 6, \cdots\}, \{\cdots, -2, 1, 4, 7, \cdots\}, \{\cdots, -1, 2, 5, 8, \cdots\}\big\}.$$

**6.13 Theorem:** *(Addition and Multiplication Modulo $n$) Let $n \in \mathbf{Z}^+$. For $a, b, c, d \in \mathbf{Z}$, if $a = c$ mod $n$ and $b = d$ mod $n$ then $a + b = c + d$ mod $n$ and $ab = cd$ mod $n$. It follows that we can define addition and multiplication operations on $\mathbf{Z}_n$ by defining*

$$[a] + [b] = [a + b] \quad \text{and} \quad [a]\,[b] = [ab]$$

*for all $a, b \in \mathbf{Z}$. When $n \geq 2$, the set $\mathbf{Z}_n$ is a commutative ring using these operations with zero and identity elements $[0]$ and $[1]$.*

Proof: Let $a, b, c, d \in \mathbf{Z}$. Suppose that $a = c$ mod $n$ and $b = d$ mod $n$. Since $a = c$ mod $n$ we can choose $k \in \mathbf{Z}$ so that $a = c + kn$. Since $b = d$ mod $n$ we can choose $\ell \in \mathbf{Z}$ so that $b = d + \ell n$. Then $a + b = (c + kn) + (d + \ell n) = (c + d) + (k + \ell)n$ so that $a + b = c + d$ mod $n$, and $ab = (c + kn)(d + \ell n) = cd + c\ell n + knd + kn\ell n = cd + (kd + \ell c + k\ell n)n$ so that $ab = cd$ mod $n$.

    It follows that we can define addition and multiplication operations in $\mathbf{Z}_n$ by defining $[a] + [b] = [a + b]$ and $[a]\,[b] = [ab]$ for all $a, b \in \mathbf{Z}$. It is easy to verify that these operations satisfy all of the Axioms R1 - R8 which define a commutative ring. As a sample proof, we shall verify that one half of the distributivity Axiom R7 is satisfied. Let $a, b, c \in \mathbf{Z}$. Then

$$
\begin{aligned}
[a]\big([b] + [c]\big) &= [a]\,[b + c] \text{ , by the definition of addition in } \mathbf{Z}_n \\
&= \big[a(b + c)\big] \text{ , by the definition of multiplication in } \mathbf{Z}_n, \\
&= [ab + ac] \text{ , by distributivity in } \mathbf{Z}. \\
&= [ab] + [ac] \text{ , by the definition of addition in } \mathbf{Z}_n, \\
&= [a]\,[b] + [a]\,[c] \text{ , by the definition of multiplication in } \mathbf{Z}_n.
\end{aligned}
$$

**6.14 Note:** When no confusion arises, we shall often omit the square brackets from our notation so that for $a \in \mathbf{Z}$ we write $[a] \in \mathbf{Z}_n$ simply as $a \in \mathbf{Z}_n$. Using this notation, for $a, b \in \mathbf{Z}$ we have $a = b$ in $\mathbf{Z}_n$ if and only if $a = b$ mod $n$ in $\mathbf{Z}$.

**6.15 Example:** Addition and multiplication in $\mathbf{Z}_6$ are given by the following tables.

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 4 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| × | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

**6.16 Example:** Find $251 \cdot 329 + (41)^2$ mod 16.

Solution: Since $251 = 15 \cdot 16 + 11$ and $329 = 20 \cdot 16 + 9$ and $41 = 2 \cdot 16 + 9$, working in $\mathbf{Z}_{16}$ we have $251 = 11$ and $329 = 41 = 9$ so that

$$251 \cdot 329 + (41)^2 = 11 \cdot 9 + 9^2 = (11 + 9) \cdot 9 = 20 \cdot 9 = 4 \cdot 9 = 36 = 4.$$

Thus $251 \cdot 329 + (41)^2 = 4$ mod 16.

**6.17 Example:** Show that for all $a \in \mathbf{Z}$, if $a = 3$ mod 4 then $a$ is not equal to the sum of 2 perfect squares.

Solution: In $\mathbf{Z}_4$ we have $0^2 = 0$, $1^2 = 1$, $2^2 = 4 = 0$ and $3^2 = 9 = 1$ so that $x^2 \in \{0, 1\}$ for all $x \in \mathbf{Z}_4$. It follows that for all $x, y \in \mathbf{Z}_4$ we have $x^2 + y^2 \in \{0+0, 0+1, 1+0, 1+1\} = \{0, 1, 2\}$ so that $x^2 + y^2 \neq 3$. Equivalently, for all $x, y \in \mathbf{Z}$ we have $x^2 + y^2 \neq 3$ mod 4.

**6.18 Example:** Show that there do not exist integers $x$ and $y$ such that $3x^2 + 4 = y^3$.

Solution: In $\mathbf{Z}_9$ we have

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $x^2$ | 0 | 1 | 4 | 0 | 7 | 7 | 0 | 4 | 1 |
| $x^3$ | 0 | 1 | 8 | 0 | 1 | 8 | 0 | 1 | 8 |
| $3x^2$ | 0 | 3 | 3 | 0 | 3 | 3 | 0 | 3 | 3 |
| $3x^2 + 4$ | 4 | 7 | 7 | 4 | 7 | 7 | 4 | 7 | 7 |

From the table we see that for all $x, y \in \mathbf{Z}_9$ we have $3x^2 + 4 \in \{4, 7\}$ and $y^3 \in \{0, 1, 8\}$ and so $3x^2 + 4 \neq y^3$. It follows that for all $x, y \in \mathbf{Z}$ we have $3x^2 + 4 \neq y^3$.

**6.19 Example:** There are several well known tests for divisibility which can be easily explained using modular arithmetic. Suppose that a positive integer $n$ is written in decimal form as $n = d_\ell \cdots d_1 d_0$ where each $d_i$ is a decimal digit, that is $d_i \in \{0, 1, \cdots, 9\}$. This means that

$$n = \sum_{k=0}^{\ell} 10^i d_i.$$

Since $2 \big| 10$ we have $10 = 0 \bmod 2$. It follows that in $\mathbf{Z}_2$ we have $10 = 0$ so $n = \sum_{i=0}^{\ell} 10^i d_i = d_0$. Thus in $\mathbf{Z}$, we have $2|n \Longleftrightarrow n = 0 \bmod 2 \Longleftrightarrow d_0 = 0 \bmod 2 \Longleftrightarrow 2|d_0$. In other words,

$$\text{2 divides } n \text{ if and only if 2 divides the final digit of } n.$$

More generally for $k \in \mathbf{Z}$ with $1 \leq k \leq \ell$, since $2^k \big| 10^k$ it follows that in $\mathbf{Z}_{2^k}$ we have $10^k = 0$, hence $10^i = 0$ for all $i \geq k$, and so $n = \sum_{i=0}^{\ell} 10^i d_i = \sum_{i=0}^{k-1} 10^i d_i$. Thus in $\mathbf{Z}$, we have $2^k \big| n$ if and only if $2^k \big| \sum_{i=0}^{k-1} 10^i d_i$. In other words,

$$2^k \text{ divides } n \text{ if and only if } 2^k \text{ divides the tailing } k\text{-digit number of } n.$$

Similarly, since $5^k \big| 10^k$ it follows that

$$5^k \text{ divides } n \text{ if and only if } 5^k \text{ divides the tailing } k\text{-digit number of } n.$$

Since $10 = 1 \bmod 3$ it follows that in $\mathbf{Z}_3$ we have $10 = 1$ so that $n = \sum_{i=1}^{\ell} 10^i d_i = \sum_{i=0}^{\ell} d_i$. Thus in $\mathbf{Z}$, $3|n \Longleftrightarrow n = 0 \bmod 3 \Longleftrightarrow \sum_{i=0}^{\ell} d_i = 0 \bmod 3 \Longleftrightarrow 3 \big| \sum_{i=0}^{\ell}$. In other words, 3 divides $n$ if and only if 3 divides the sum of the digits of $n$. Similarly, since $10 = 1 \bmod 9$,

$$\text{9 divides } n \text{ if and only if 9 divides the sum of the digits of } n.$$

Since $10 = -1 \bmod 11$, in $\mathbf{Z}_{11}$ we have $10 = -1$ so that $n = \sum_{i=0}^{\ell} 10^i d_i = \sum_{i=0}^{\ell} (-1)^i d_i$. Thus in $\mathbf{Z}$, $11 \big| n \Longleftrightarrow 11 \big| \sum_{i=0}^{\ell} (-1)^i d_i$. In other words,

$$\text{11 divides } n \text{ if and only if 11 divides the alternating sum of the digits of } n.$$

**6.20 Exercise:** Use the divisibility tests described in the above example to find the prime factorization of the number 28880280. Also, consider the problem of factoring the number 28880281.

**6.21 Remark:** For $a, b \in \mathbf{Z}$ and $n \in \mathbf{Z}^+$ note that if $a = b$ mod $n$ so that $[a] = [b] \in \mathbf{Z}_n$ then we have $\gcd(a, n) = \gcd(b, n)$ and so it makes sense to define $\gcd([a], n) = \gcd(a, n)$.

**6.22 Theorem:** *(Inverses Modulo n) Let $n \in \mathbf{Z}$ with $n \geq 2$. For $a \in \mathbf{Z}$, $[a]$ is a unit in $\mathbf{Z}_n$ if and only if $\gcd(a, n) = 1$ in $\mathbf{Z}$.*

Proof: Let $a \in \mathbf{Z}$ and let $d = gcd(a, n)$. Suppose that $[a]$ is a unit in $\mathbf{Z}_n$. Choose $b \in \mathbf{Z}$ so that $[a][b] = [1] \in \mathbf{Z}_n$. Then $[ab] = [1] \in \mathbf{Z}_n$ and so $ab = 1$ mod $n$ in $\mathbf{Z}$. Since $ab = 1$ mod $n$ we can choose $k$ so that $ab = 1 + kn$. Then we have $ab - kn = 1$. Since $d|a$ and $d|n$ it follows that $d|(ax + ny)$ for all $x, y \in \mathbf{Z}$ so in particular $d|(ab - kn)$, that is $d|1$. Since $d|1$ and $d \geq 0$, we must have $d = 1$.

Conversely, suppose that $d = 1$. By the Euclidean Algorithm with Back-Substitution, we can choose $s, t \in \mathbf{Z}$ so that $as + nt = 1$. Then we have $as = 1 - nt$ so that $as = 1$ mod $n$. Thus in $\mathbf{Z}_n$, we have $[as] = [1]$ so that $[a][s] = [1]$. Thus $[a]$ is a unit with $[a]^{-1} = [s]$.

**6.23 Example:** Determine whether $125$ is a unit in $\mathbf{Z}_{471}$ and if so find $125^{-1}$.

Solution: The Euclidean Algorithm gives

$$471 = 3 \cdot 125 + 96 \ , \ \ 125 = 1 \cdot 96 + 29 \ , \ \ 96 = 3 \cdot 29 + 9 \ , \ \ 29 = 3 \cdot 9 + 2 \ , \ \ 9 = 4 \cdot 2 + 1$$

and so $d = \gcd(125, 471) = 1$ and it follows that $125$ is a unit in $\mathbf{Z}_{471}$. Back-Substitution gives the sequence

$$1 \ , \ -4 \ , \ 13 \ , \ -43 \ , \ 56 \ , \ -211$$

so we have $125(-211) + 471(56) = 1$. It follows that in $\mathbf{Z}_{471}$ we have $125^{-1} = -211 = 260$.

**6.24 Example:** Solve the pair of equations $3x + 4y = 7$ (1) and $11x + 15y = 8$ (2) for $x, y \in \mathbf{Z}_{20}$.

Solution: We work in $\mathbf{Z}_{20}$. Since $3 \cdot 7 = 21 = 1$ we have $3^{-1} = 7$. Multiply both sides of Equation (1) by 7 to get $x + 8y = 9$, that is $x = 9 - 8y$ (3). Substitute $x = 9 - 8y$ into Equation (2) to get $11(9 - 8y) + 15y = 8$, that is $19 - 8y + 15y = 8$ or equivalently $7y = 9$ (4). Multiply both sides of Equation (4) by $7^{-1} = 3$ to get $y = 7$. Put $y = 7$ into Equation (3) to get $x = 9 - 8 \cdot 7 = 9 - 16 = 13$. Thus the only solution is $(x, y) = (13, 7)$.

**6.25 Definition:** A **group** is a set $G$ with an element $e \in G$ and a binary operation $* : G \times G \to G$, where for $a, b \in G$ we write $*(a, b)$ as $a * b$ or simply as $ab$, such that

G1. $*$ is associative: for all $a, b, c \in G$ we have $(ab)c = a(bc)$,

G2. $e$ is an identity element: for all $a \in G$ we have $ae = ea = a$, and

G3. every $a \in G$ has an inverse: for every $a \in G$ there exists $b \in G$ such that $ab = ba = e$.

A group $G$ is called **abelian** when

G4. $*$ is commutative: for all $a, b \in G$ we have $ab = ba$.

**6.26 Definition:** When $R$ is a ring under the operations $+$ and $\times$, the set $R$ is also a group under the operation $+$ with identity element 0. The group $R$ under $+$ is called the **additive group** of $R$. The set $R$ is not a group under the operation $\times$ because not every element $a \in R$ has an inverse under $\times$ (in particular, the element 0 has no inverse). The set of all invertible elements in $R$, however, is a group under multiplication, and we denote it by $R^*$, so we have

$$R^* = \big\{ a \in R \big| a \text{ is a unit} \big\}.$$

The group $R^*$ is called the **group of units** of $R$.

**6.27 Example:** When $F$ is a field, every nonzero element in $F$ is invertible so we have $F^* = F \setminus \{0\}$. In $\mathbf{Z}$, the only invertible elements are $\pm 1$ and so $\mathbf{Z}^* = \{1, -1\}$.

**6.28 Definition:** For $n \in \mathbf{Z}$ with $n \geq 2$, the group of units of $\mathbf{Z}_n$ is called the **group of units modulo** $n$ and is denoted by $U_n$. Thus

$$U_n = \big\{a \in \mathbf{Z}_n \,\big|\, \gcd(a,n) = 1\big\}.$$

For convenience, we also let $U_1$ be the trivial group $U_1 = \mathbf{Z}_1 = \{1\}$. For a set $S$, let $|S|$ denote the cardinality of $S$, so that in particular when $S$ is a finite set, $|S|$ denotes the number of elements in $S$. We define the **Euler phi function**, also called the **Euler totient function**, $\varphi : \mathbf{Z}^+ \to \mathbf{Z}^+$ by

$$\varphi(n) = \big|U_n\big|$$

so that $\varphi(n)$ is equal to the number of elements $a \in \{1, 2, \cdots, n\}$ such that $\gcd(a, n) = 1$.

**6.29 Example:** Since $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ we have $\varphi(20) = 8$.

**6.30 Example:** When $p$ is a prime number and $k \in \mathbf{Z}^+$ notice that

$$U_{p^k} = \{1, 2, 3, \cdots, p^k\} \setminus \{p, 2p, 3p, \cdots, p^k\}$$

and so

$$\varphi(p^k) = p^k - p^{k-1}.$$

**6.31 Theorem:** *(Fermat's Little Theorem) Let $p$ be a prime number. Then*
*(1) For all $a \in \mathbf{Z}$ with $\gcd(a,p) = 1$ we have $a^{p-1} = 1 \bmod p$.*
*(2) For all $a \in \mathbf{Z}$ we have $a^p = a \bmod p$.*

Proof: To prove Part (1), let $a \in \mathbf{Z}$ with $\gcd(a,p) = 1$. Then we have $a \in U_p$. Define $F : U_p \to U_p$ by $F(x) = ax$ (note that when $a$ and $x$ are units in a ring, the product $ax$ is also a unit with $(ax)^{-1} = x^{-1}a^{-1}$, so the map $F$ is well-defined). Notice that $F$ is bijective with inverse $G : U_p \to U_p$ given by $G(x) = a^{-1}x$. Since $F$ is bijective, it follows that the list of elements $1a, 2a, 3a, \cdots, (p-1)a$ is a permutation (that is a a re-orderring) of the list $1, 2, 3, \cdots, p-1$. Thus in $U_p$ we have

$$1a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$$
$$(p-1)! \, a^{p-1} = (p-1)!$$

Multiply both sides by the inverse of $(p-1)!$ in $U_p$ to get $a^{p-1} = 1$ in $U_p$, as required.

To prove Part (2), let $a \in \mathbf{Z}$ be arbitrary. If $\gcd(a,p) = 1$ then by Part (1) we have $a^{p-1} = 1 \bmod p$ and so we can multiply by $a$ to get $a^p = a \bmod p$. If $\gcd(a,p) \neq 1$ then since $p$ is prime it follows that $p|n$ and so we have $a = 0 \bmod p$ hence $a^p = 0^p = 0 = a \bmod p$. In either case, we have $a^p = a \bmod p$, as required.

**6.32 Example:** If today is Tuesday, then what day will it be in $2^{100}$ days?

Solution: By Fermat's Little Theorem we have $2^6 = 1 \bmod 7$. It follows that the list of powers of 2 repeats every 6 terms in $\mathbf{Z}_7$. Since $100 = 16 \cdot 6 + 4$ so that $100 = 4 \bmod 6$, it follows that $2^{100} = 2^4 = 16 = 2 \bmod 7$. Thus in $2^{100}$ days it will be Thursday.

**6.33 Example:** Show that $2^{70} + 3^{70}$ is not prime.

Solution: In $\mathbf{Z}_2$ we have $2^{70} + 3^{70} = 0^{70} + 1^{70} = 1 \neq 0$. In $\mathbf{Z}_3$, we have $2^{70} + 3^{70} = (-1)^{70} + 0^{70} = 1 \neq 0$. In $\mathbf{Z}_5$, by Fermat's Little Theorem the list of powers of 2 and 3 repeats every 4 terms, and $70 = 2$ mod 4, so we have $2^{70} + 3^{70} = 2^2 + 3^2 = 4 + 9 = 3 \neq 0$. In $\mathbf{Z}_7$, the list of powers of 2 and 3 repeats every 6 terms, and $70 = 4$ mod 6, so we have $2^{70} + 3^{70} = 2^4 + 3^4 = 4^2 + 9^2 = 4^2 + 2^2 = 2 + 4 = 6 \neq 0$. In $\mathbf{Z}_{11}$, the list of powers of 2 and 3 repeats every 10 terms, and $70 = 0$ mod 10, so we have $2^{70} + 3^{70} = 2^= + 3^0 = 1 + 1 = 2 \neq 0$. In $\mathbf{Z}_{13}$, the list of powers of 2 and 3 repeats every 12 terms, and $70 = 10$ mod 12, so we have $2^{70} + 3^{70} = 2^{10} + 3^{10} = 2^4 \cdot 2^4 \cdot 2^2 + 3^3 \cdot 3^3 \cdot 3^1 = 3 \cdot 3 \cdot 4 + 1 \cdot 1 \cdot 3 = 10 + 3 = 0$. Since $2^{70} + 3^{70} = 0 \in \mathbf{Z}_{13}$ it follows that $13 | (2^{70} + 3^{70})$ in $\mathbf{Z}$, and so $2^{70} + 3^{70}$ is not prime.

**6.34 Theorem:** *(Euler-Fermat) Let $n \in \mathbf{Z}^+$. For all $a \in \mathbf{Z}$ with $\gcd(a, n) = 1$ we have $a^{\varphi(n)} = 1$ mod $n$.*

Proof: Let $a \in \mathbf{Z}$ with $\gcd(a, n) = 1$. Then we have $a \in U_n$. Let $\varphi = \varphi(n)$ and let $x_1, x_2, \cdots, x_\varphi$ be a list of all the elements in $U_n$. Define $F : U_n \to U_n$ by $F(x) = ax$. Then $F$ is bijective with inverse $G : U_n \to U_n$ given by $G(x) = a^{-1}x$. Since $F$ is bijective, it follows that the list $ax_1, ax_2, \cdots, ax_\varphi$ is a permutation of the list $x_1, x_2, \cdots, x_\varphi$, and so in $U_n$ we have

$$ax_1 \cdot ax_2 \cdot \ldots \cdot ax_\varphi = x_1 \cdot x_2 \cdot \ldots \cdot x_\varphi$$

$$\Big( \prod_{i=1}^{\varphi} x_i \Big) a^\varphi = \prod_{i=1}^{\varphi} x_i$$

Multiply both sides by the inverse of $\prod_{i=1}^{\varphi} x_i$ in $U_n$ to get $a^\varphi = 1$ in $U_n$, as required.

**6.35 Remark:** For any finite abelian group $G$, the above proof is valid and it shows that $a^{|G|} = e$ for all $a \in G$. The same result holds even in non-abelian finite groups, but a different proof is required.

**6.36 Theorem:** *(The Linear Congruence Theorem) Let $n \in \mathbf{Z}^+$, let $a, b \in \mathbf{Z}$, and let $d = \gcd(a, n)$. Consider the congruence $ax = b$ mod $n$.*
*(1) The congruence has a solution $x \in \mathbf{Z}$ if and only if $d | b$, and*
*(2) if $x = u$ is one solution to the congruence, then the general solution is*

$$x = u \text{ mod } \tfrac{n}{d}.$$

Proof: Suppose that the congruence $ax = b$ mod $n$ has a solution. Let $x = u$ be a solution so we have $au = b$ mod $n$. Since $au = b$ mod $n$ we can choose $k \in \mathbf{Z}$ so that $au = b + kn$, that is $au - nk = b$. Since $d | a$ and $d | n$ it follows that $d | (ax + ny)$ for all $x, y \in \mathbf{Z}$, and so in particular $d | (au - nk)$, hence $d | b$. Conversely, suppose that $d | b$. By the Linear Diophanitine Equation Theorem, the equation $ax + ny = b$ has a solution. Choose $u, v \in \mathbf{Z}$ so that $au + nv = b$. Then since $au = b - nv$ we have $au = b$ mod $n$ and so the congruence $ax = b$ mod $n$ has a solution (namely $x = u$).

Suppose that $x = u$ is a solution to the given congruence, so we have $au = b$ mod $n$. We need to show that for every $k \in \mathbf{Z}$ if we let $x = u + k\frac{n}{d}$ then we have $ax = b$ mod $n$ and, conversely, that for every $x \in \mathbf{Z}$ such that $ax = b$ mod $n$ there exists $k \in \mathbf{Z}$ such that $x = u + k\frac{n}{d}$. Let $k \in \mathbf{Z}$ and let $x = u + k\frac{n}{d}$. Then $ax = a\big(u + k\frac{n}{d}\big) = au + \frac{ka}{d}n$. Since $ax = au + \frac{ka}{d}n$ and $d | a$ so that $\frac{ka}{d} \in \mathbf{Z}$, it follows that $ax = au$ mod $n$. Since $ax = au$ mod $n$ and $au = b$ mod $n$ we have $ax = b$ mod $n$, as required.

Conversely, let $x \in \mathbf{Z}$ and suppose that $ax = b$ mod $n$. Since $ax = b$ mod $n$ and $au = b$ mod $n$ we have $ax = au$ mod $n$. Since $ax = au$ mod $n$ we can choose $\ell \in \mathbf{Z}$ so that $ax = au + \ell n$. Then we have $a(x - u) = \ell n$ and so $\frac{a}{d}(x - u) = \frac{n}{d}\ell$. Since $\frac{n}{d}|\frac{a}{d}(x - u)$ and $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, it follows that $\frac{n}{d}|(x - u)$. Thus we can choose $k \in \mathbf{Z}$ so that $x - u = k\frac{n}{d}$ and then we have $x = u + k\frac{n}{d}$, as required.

**6.37 Example:** Solve $221x = 595$ mod $323$.

Solution: The Euclidean Algorithm gives

$$323 = 1 \cdot 221 + 102 \ , \ \ 221 = 2 \cdot 102 + 17 \ , \ \ 102 = 6 \cdot 17 + 0$$

and so $\gcd(221, 323) = 17$. Note that $\frac{595}{17} = 35$, so the congruence has a solution. Back-Substitution gives the sequence

$$1 \ , \ -2 \ , \ 3$$

so we have $221 \cdot 3 - 323 \cdot 2 = 17$. Multiply by 35 to get $221 \cdot 105 - 323 \cdot 70 = 595$. Thus one solution to the given congruence is $x = 105$. Since $\frac{323}{17} = 19$ and $105 = 5 \cdot 19 + 10$, the general solution is given by $x = 105 = 10$ mod 19.

**6.38 Theorem:** *(The Chinese Remainder Theorem) Let $n, m \in \mathbf{Z}^+$ and let $a, b \in \mathbf{Z}$. Consider the pair of congruences*

$$x = a \text{ mod } n,$$
$$x = b \text{ mod } m.$$

*(1) The pair of congruences has a solution $x \in \mathbf{Z}$ if and only if $\gcd(n, m)|(b - a)$, and*
*(2) if $x = u$ is one solution, then the general solution is $x = u$ mod $\text{lcm}(n, m)$.*

Proof: Suppose that the given pair of congruences has a solution and let $d = \gcd(n, m)$. Let $x = u$ be a solution, so we have $u = a$ mod $n$ and $u = b$ mod $m$. Since $u = a$ mod $n$ we can choose $k \in \mathbf{Z}$ so that $u = a + kn$. Since $u = b$ mod $m$ we can choose $\ell \in \mathbf{Z}$ so that $u = b + \ell m$. Since $u = a + kn = b + \ell n$ we have $b - a = nk - m\ell$. Since $d|n$ and $d|m$ it follows that $d|(nx + my)$ for all $x, y \in \mathbf{Z}$ so in particular $d|(nk - m\ell)$, hence $d|(b - a)$. Conversely, suppose that $d|(b - a)$. By the Linear Diophantine Equation Theorem, the equation $nx + my = b - a$ has a solution. Choose $k, \ell \in \mathbf{Z}$ so that $nk - m\ell = b - a$. Then we have $a + nk = b + m\ell$. Let $u = a + nk = b + m\ell$. Since $u = a + nk$ we have $u = a$ mod $n$ and since $u = b + m\ell$ we have $u = b$ mod $m$. Thus $x = u$ is a solution to the pair of congruence.

Now suppose that $u = a$ mod $n$ and $u = b$ mod $m$. Let $\ell = \text{lcm}(n, m)$. Let $k \in \mathbf{Z}$ be arbitrary and let $x = u + k\ell$. Since $x - u = k\ell$ we have $\ell|(x - u)$. Since $n|\ell$ and $\ell|(x - u)$ we have $n|(x - u)$ so that $x = u$ mod $n$. Since $x = u$ mod $n$ and $u = a$ mod $n$ we have $x = a$ mod $n$. Similarly $x = b$ mod $m$.

Conversely, let $x \in \mathbf{Z}$ and suppose that $x = a$ mod $n$ and $x = b$ mod $m$. Since $x = a$ mod $n$ and $u = a$ mod $n$ we have $x = u$ mod $n$ so that $n|(x - u)$. Since $x = b$ mod $m$ and $u = b$ mod $m$ we have $x = u$ mod $m$ so that $m|(x - u)$. Since $n|(x - u)$ and $m|(x - u)$ and $\ell = \text{lcm}(n, m)$, it follows that $\ell|(x - u)$ so that $x = u$ mod $\ell$.

**6.39 Example:** Solve the pair of congruences $x = 2 \bmod 15$ and $x = 13 \bmod 28$.

Solution: We want to find $k, \ell \in \mathbf{Z}$ such that $x = 2+15k = 13+28\ell$. We need $15k-28\ell = 11$. The Euclidean Algorithm gives

$$28 = 1 \cdot 15 + 13 \ , \ \ 15 = 1 \cdot 13 + 2 \ , \ \ 13 = 6 \cdot 2 + 1$$

so that $\gcd(15, 28) = 1$ and Back-Substitution gives the sequence

$$1 \ , \ -6 \ , \ 7 \ , \ -13$$

so that $(15)(-13) + (28)(7) = 1$. Multiplying by 11 gives $(15)(-143) + (28)(77) = 11$, so one solution to the equation $15k - 28\ell = 11$ is given by $(k, l) = (-143, 77)$. It follows that one solution to the pair of congruences is given by $u = 2 + 15k = 2 - 15 \cdot 143 = -2143$. Since $\mathrm{lcm}(15, 28) = 15 \cdot 28 = 420$, and $-2143 = -6 \cdot 420 + 377$, the general solution to the pair of congruences is $x = -2143 = 377 \bmod 420$.

**6.40 Exercise:** Solve the congruence $x^3 + 2x = 18 \bmod 35$.

**6.41 Exercise:** Find the last 2 digits of $14^{14^{14}}$ in its decimal representation.

**6.42 Theorem:** *(The Generalized Chinese Remainder Theorem) Let $\ell \in \mathbf{Z}^+$, let $n_i \in \mathbf{Z}^+$ and $a_i \in \mathbf{Z}$ for all indices $i$ with $1 \leq i \leq \ell$. Consider the system of $\ell$ congruences $x = a_i \bmod n_i$ for all indices $i$ with $1 \leq i \leq \ell$.*

*(1) The system has a solution $x$ if and only if $\gcd(n_i, n_j) \big| (a_i - a_j)$ for all $i, j$, and*
*(2) if $x = u$ is one solution then the general solution is $x = u \bmod \mathrm{lcm}(n_1, n_2, \cdots, n_\ell)$.*

Proof: The proof is left as an exercise.

**6.43 Exercise:** Solve the system $x = 17 \bmod 25$, $x = 14 \bmod 18$ and $x = 22 \bmod 40$.

**6.44 Theorem:** *Let $n = \displaystyle\prod_{i=1}^{\ell} p_i{}^{k_k}$ where $\ell \in \mathbf{Z}^+$ and the $p_i$ are distinct primes and each $k_i \in \mathbf{Z}^+$. Then*

$$\varphi(n) = \prod_{i=1}^{\ell} \varphi\big(p_i{}^{k_i}\big).$$

Proof: I may include a proof later.

**6.45 Example:** When $p$ and $q$ are distinct primes, we have $\varphi(pq) = (p-1)(q-1)$.