MATH 135 Algebra, Solutions to Assignment 10

1: (a) The name of a mathematician was encoded using a Caesar cypher to give the cyphertext below. Decrypt the cyphertext.

ZPXGDY

Solution: We list all 26 possibilities.

ZPXGDY	GWENKF	NDLURM	TJRAXS
AQYHEZ	HXFOLG	OEMVSN	UKSBYT
BRZIFA	IYGPMH	PFNWTO	VLTCZU
CSAJGB	JZHQNI	QGOXUP	WMUDAV
DTBKHC	KAIROJ	RHPYVQ	XNVEBW
EUCLID	LBJSPK	SIQZWR	YOWFCX
FVDMJE	MCKTQL		

The only famous mathematician on the list is Euclid (the mathematician Kairoj is not as well known).

(b) Two quotes from Bertrand Russell were encoded using a substitution cypher to give the cyphertext below. Use the fact that the most frequently occurring letters in English text are the letters E, T and A (in that order) to help decrypt the cyphertext.

GMQEUBQI MWJMVI QMWS BZ XVUYL ZBE QOCUE PBDYQEV
HDQ YCTCE BZ SUWWUYL ZBE QOCUE PBDYQEV.

RMQOCRMQUPI RMV HC XCZUYCX MI QOC IDHACPQ UY JOUPO
JC YCTCE SYBJ JOMQ JC MEC QMWSUYL MHBDQ,
YBE JOCQOCE JOMQ JC MEC IMVUYL UI QEDC.

Solution: By counting the number of occurrences of each letter, we find that C occurs most frequently, followed by Q and then by M, so we guess that we should make the substitutions C→E, Q→T and M→A. Then the coded word QOC in the second quote will become QOC→T–E so we guess that O→H so that QOC→THE (we could also have O→I or O→O, but O→H seems the most likely). The coded word JOMQ on the last line will then become JOMQ→–HAT, so we guess that J→W so that JOMQ→WHAT. Similarly, from JOCQOCE→WHETHE–, we guess that E→ *R*, then from QOCUE→THE–R, we guess that U→I, then from QEDC→TR–E, we guess that D→U, then from JOUPO→WHI–H, we guess that P→C, from RMQOCRMQUPI→–ATHE–ATIC–, we guess that R→M and I→S. After a few more such guesses, we find that the first quote becomes

"Patriots always talk of dying for their country but never of killing for their country",

and the second quote becomes

"Mathematics may be defined as the subject in which we never know
what we are talking about nor whether what we are saying is true."

(In this second quote, Bertrand Russel is stating a logical fact about mathematics: we do not know what we are talking about because all mathematical objects are defined in terms of sets, but sets are never defined, and we do not know whether what we are saying is true since by Gödel's Incompleteness Theorem, if our rules of mathematical proof can only be used to prove true statements, then it is impossible to prove that our rules only prove true statements).

2: (a) Find $1263^{1842} \pmod{2357}$ using the square and multiply algorithm.

Solution: We make a list of powers of 1263 modulo 2357.

k	1263^k	k	1263^k
1	1263	64	915
2	1837	128	490
4	1702	256	2043
8	51	512	1959
16	244	1024	485
32	611		

Note that $1842 = 1024 + 512 + 256 + 32 + 16 + 2$, so we have

$$\begin{aligned} 1263^{1842} &\equiv 1263^{1024} \cdot 1263^{512} \cdot 1263^{256} \cdot 1263^{32} \cdot 1263^{16} \cdot 1263^{2} \\ &\equiv (485 \cdot 1957)(2043 \cdot 611)(244 \cdot 1837) \\ &\equiv 244 \cdot 1420 \cdot 398 \equiv 398 \pmod{2357}\,. \end{aligned}$$

(b) Use Fermat's Little Theorem and the Square and Multiply Algorithm to show that the integer 2479 is not prime (without testing each prime $p \leq \sqrt{2479}$ to see if is a factor).

Solution: We calculate $2^{2478} \pmod{2479}$. We make a list of powers of 2 modulo 2479.

k	2^k	k	2^k
1	2	64	419
2	4	128	2031
4	16	256	2384
8	256	512	1588
16	1082	1024	601
32	636	2048	1746

Note that $2478 = 2048 + 256 + 128 + 32 + 8 + 4 + 2$ so we have

$$\begin{aligned} 2^{2478} &\equiv 2^{2048} \cdot 2^{256} \cdot 2^{128} \cdot 2^{32} \cdot 2^{8} \cdot 2^{4} \cdot 2^{2} \\ &\equiv (1746 \cdot 2384)(2031 \cdot 636)(256 \cdot 16 \cdot 4) \\ &\equiv 223 \cdot 157 \cdot 1510 \equiv 1935\,. \end{aligned}$$

Since $2^{2478} \not\equiv 1 \pmod{2479}$ we know that 2479 cannot be prime, by Fermat's Little Theorem.
(We remark that this idea is used in algorithms which test a large integer to determine whether it is prime without factoring it. Such algorithms are used to select the two prime numbers p and q in the RSA Scheme).

3: (a) Encrypt the 1-letter message R using the RSA public key $(e, n) = (13, 77)$.

Solution: Since R is the 18^{th} letter of the alphabet, we replace the letter R by the message $m = 18$. We must find $c \equiv m^e \pmod{n}$, that is $c \equiv 18^{13} \pmod{77}$. We make a list of powers of 18 modulo 77.

k	18^k
1	18
2	16
4	25
8	9

Since $13 = 8 + 4 + 1$ we have

$$c \equiv 18^{13} \equiv 18^8 \cdot 18^4 \cdot 18^1 \equiv 9 \cdot 25 \cdot 18 \equiv 46 \pmod{77}.$$

Thus the cyphertext is $c = 46$.

(b) Let $p = 47$, $q = 61$, $e = 43$ and $n = pq$. Encrypt the 2-letter message GO using the RSA public key (e, n).

Solution: Note that $n = pq = 47 \cdot 61 = 2867$. Since G and O are the 7^{th} and 15^{th} letters of the alphabet, we replace the word GO by the message $m = 0715$. We must find $c \equiv m^e \pmod{n}$, that is $c \equiv 715^{43} \pmod{2867}$. We make a list of powers of 715 modulo 2867.

k	715^k
1	715
2	899
4	2574
8	2706
16	118
32	2456

Since $43 = 32 + 8 + 2 + 1$ we have

$$c \equiv 715^{43} \equiv 715^{32} \cdot 715^8 \cdot 715^2 \cdot 715^1 \equiv (2456 \cdot 2706)(899 \cdot 715) \equiv 230 \cdot 577 \equiv 828 \pmod{2867}.$$

Thus the cyphertext is 828.

4: (a) Decrypt the cyphertext $c = 41$ which was encoded from a 1-letter message using the RSA public key $(e, n) = (29, 65)$.

Solution: Note that $n = 65 = 5 \cdot 13$ so that $\phi(n) = \phi(5)\phi(13) = 4 \cdot 12 = 48$. To decypher c we can use $d = e^{-1} \pmod{\phi(n)}$, that is $d = 29^{-1} \pmod{48}$. We consider the equation $29x + 48y = 1$. The Euclidean Algorithm gives

$$48 = 1 \cdot 29 + 19 \ , \quad 29 = 1 \cdot 19 + 10 \ , \quad 19 = 1 \cdot 10 + 9 \ , \quad 10 = 1 \cdot 9 + 1$$

so we have $\gcd(29, 48) = 1$, and then Back-Substitution gives

$$1 \ , \quad -1 \ , \quad 2 \ , \quad -3 \ , \quad 5$$

so we have $(29)(5) + (48)(-3) = 1$. Thus $29^{-1} \equiv 5 \pmod{40}$ so we can take $d = 5$. (Alternatively, we could use $d = e^{-1} \pmod{\psi(n)}$ where $\psi(n) = \text{lcm}(\phi(5), \phi(13)) = \text{lcm}(4, 12) = 12$, that is $d = 5^{-1} \pmod{12}$, so we can take $d = 5$ by inspection). We must find $m \equiv c^d \pmod{n}$, that is $m \equiv 41^5 \pmod{65}$. We make a list of powers of 41 modulo 65.

k	41^k
1	41
2	56
3	21
4	16
5	6

Thus the message was $m = 6$, which corresponds to the single letter F.

(b) Let $p = 41$, $q = 67$, $e = 217$ and $n = pq$. Decrypt the cyphertext $c = 811$ which was encoded from a 2-letter message using the RSA public key (e, n).

Solution: We have $n = pq = 41 \cdot 67 = 2747$, and we have $\phi(n) = \phi(41)\phi(67) = 40 \cdot 66 = 2640$. To decypher c we can use $d = e^{-1} \pmod{\phi(n)}$, that is $d = 217^{-1} \pmod{2640}$. We consider the equation $217x + 2640y = 1$. The Euclidean Algorithm gives $2640 = 12 \cdot 217 + 36$ and $217 = 6 \cdot 36 + 1$ so we have $\gcd(217, 2640) = 1$, and then Back-Substitution gives the sequence 1, -6, 73 so we have $(217)(73) + (2640)(-6) = 1$. Thus we have $217^{-1} \equiv 73 \pmod{2640}$ and we can take $d = 73$. (Alternatively, we could use $d = e^{-1} \pmod{\psi(n)}$ where $\psi(n) = \text{lcm}(\phi(41), \phi(67)) = \text{lcm}(40, 66) = 1320$, but as it happens, this gives the same value $d = 73$). We must find $m \equiv c^d \pmod{n}$, that is $m \equiv 811^{73} \pmod{2747}$. We make a list of powers of 811 modulo 2747.

k	811^k
1	811
2	1188
4	2133
8	657
16	370
32	2297
64	1969

Since $73 = 64 + 8 + 1$ we have

$$w \equiv 811^{73} \equiv 811^{64} \cdot 811^8 \cdot 811^1 \equiv 1969 \cdot 657 \cdot 811 \equiv 2123 \pmod{2747} \, .$$

Thus the message is $m = 2123$ which corresponds to the 2-letter message UW.

5: (a) Let $n = 459061$. Given that $n = pq$ for some primes $p < q$ and that $\phi(n) = 457612$, find the prime factorization of n.

Solution: Using $n = pq$ we have

$$\begin{aligned}(p-1)(q-1) &= \phi(n)\\ pq - p - q + 1 &= \phi(n)\\ n - p - q + 1 &= \phi(n)\\ q + p &= n - \phi(n) + 1\,.\end{aligned}$$

Also, we have

$$\begin{aligned}(q-p)^2 &= (q+p)^2 - 4pq\\ q - p &= \sqrt{(q+p)^2 - 4n}\end{aligned}$$

Using the given values of n and $\phi(n)$ we have

$$q + p = (n - \phi(n) + 1) = 1450 \text{ and } q - p = \sqrt{(q+p)^2 - 4n} = \sqrt{(1450)^2 - 4(459061)} = 516\,.$$

Thus $p = \frac{(q+p)-(q-p)}{2} = \frac{1450-516}{2} = 467$ and $q = 516 + p = 516 + 467 = 983$.

(b) Let $n = 806437$. Given that $n = pq$ for some primes $p < q$ with $q - p \leq 100$, find the prime factorization of n.

Solution: We have

$$(q-p)^2 = (q+p)^2 - 4pq = (q+p)^2 - 4n\,.$$

Since the left side is positive, we must have $(q+p)^2 > 4n$, so $(q+p) \geq \left\lceil \sqrt{4n} \right\rceil = \left\lceil \sqrt{4(806437)} \right\rceil = 1797$. We have $1797^2 - 4n = 3461$, which is not a square, and $1798^2 - 4n = 7056 = 84^2$, and $1799^2 - 4n = 10653 > 100^2$, so we must have $q + p = 1798$ and $q - p = 84$. Thus $p = \frac{(q+p)-(q-p)}{2} = \frac{1798-84}{2} = 857$ and $q = 84 + p = 941$. (We remark that part (a) illustrates that in the RSA Scheme, the value of $\phi = \phi(n)$ must be kept secret, and part (b) illustrates that the two primes p and q must not be chosen too close together).