PMATH 340 Number Theory, Solutions to the Exercises for Chapter 5

1: (a) Let $p = 47$, $q = 61$, $e = 43$ and $n = pq$. Encrypt the 2-letter message GO using the RSA public key (e, n) (first replace GO by the number $m = 0715$ because G and O are the 7^{th} and 15^{th} letters of the alphabet).

Solution: Note that $n = pq = 47 \cdot 61 = 2867$. 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.

(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 $\varphi(n) = \varphi(41)\varphi(67) = 40 \cdot 66 = 2640$. To decypher c we can use $d = e^{-1} \big(\bmod\, \varphi(n)\big)$, 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 $d = e^{-1} \big(\bmod\, \lambda(n)\big)$ where $\lambda(n) = \text{lcm}\big(\varphi(41), \varphi(67)\big) = \text{lcm}(40, 66) = 1320$, 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.

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

Solution: Using $n = pq$ we have

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

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 $\varphi(n)$ we have

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

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 $\varphi = \varphi(n)$ must be kept secret, and part (b) illustrates that the two primes p and q must not be chosen too close together).

3: (a) Show that 91 is a pseudo-prime to the base 3.

Solution: Note that $91 = 7 \cdot 13$, so 91 is composite and we have $\lambda(91) = \psi(91) = \text{lcm}(6, 12) = 12$. Since $91 = 7 \bmod 12$, we have $3^{91} = 3^7 = 2187 = 3 \bmod 91$, so 91 passes the base 3 test.

(b) Find a prime p such that $n = 5 \cdot 29 \cdot p$ is a Carmichael number.

Solution: For $n = 5 \cdot 29 \cdot p$ to be a Carmichael number, we need to have $4 \big| (n-1)$, $28 \big| (n-1)$ and $(p-1) \big| (n-1)$. Note that

$$4 \big| (n-1) \Longrightarrow n = 1 \bmod 4 \Longrightarrow 5 \cdot 29 \cdot p = 1 \bmod 4 \Longrightarrow p = 1 \bmod 4 \text{ , and}$$

$$28 \big| (n-1) \Longrightarrow n = 1 \bmod 28 \Longrightarrow 5 \cdot 29 \cdot p = 1 \bmod 28 \Longrightarrow 5p = 1 \bmod 28 \Longrightarrow p = 17 \bmod 28$$

so we need to have $p = 17 \bmod 28$, that is $p = 17, 45, 73, 101, 129, \cdots$. By trying some of the primes in this list we find that $p = 17$ and $p = 73$ both satisfy $(p-1) \big| (n-1)$, so they both yield Carmichael numbers. The corresponding Carmichael numbers are $n = 5 \cdot 29 \cdot 17 = 7395$ and $n = 5 \cdot 29 \cdot 73 = 10585$.

Alternatively, rather than simply trying some of the (infinitely many) primes in the list, we can be more selective as follows. Note that $n - 1 = 5 \cdot 29 \cdot p - 1 = 145\,p - 1 = 145(p-1) + 144$ and so

$$(p-1) \big| (n-1) \iff (p-1) \big| \big(145(p-1) + 144\big) \iff (p-1) \big| 144 \, .$$

Thus it is enough to test each of the (finitely many) primes $p = 17 \bmod 28$ with $p \leq 145 = 5 \cdot 29$ to see whether $(p-1) \big| 144$. In particular, this shows that $p = 17$ and $p = 73$ are the *only* two primes for which $n = 5 \cdot 29 \cdot p$ is a Carmichael number.

(c) Show that 217 is a strong pseudoprime for the base 6.

Solution: Note that $217 = 7 \cdot 31$, so 217 is composite and we have $\gcd(6, 217) = 1$. We need to show that either $6^{216} = -1 \bmod 217$ or $6^{108} = -1 \bmod 217$ or $6^{54} = -1 \bmod 217$ or $6^{27} = \pm 1 \bmod 217$. Modulo 7 we have $6^{27} = (-1)^{217} = -1$. Modulo 31 we have

k	0	1	2	3	4	5	6
6^k	1	6	5	-1	-6	-5	1

so the powers of 6 modulo 31 repeat every 6 terms beginning with 6^0 and so $6^{27} = 6^3 = -1$. Since $6^{27} = -1 \bmod 7$ and $6^{27} = -1 \bmod 31$ we have $6^{27} = -1 \bmod 217$ by the CRT. Thus 217 is a strong pseudoprime for the base 6.

4: (a) Show that there are infinitely many primes of the form $6k+5$, where k is an integer.

Solution: Every odd integer is of one of the forms $6k+1$, $6k+3$ or $6k+5$. Since $3\big|(6k+3)$, every prime other than 2 and 3 is either of the form $6k+1$ or of the form $6k+5$. Suppose, for a contradiction, that there are only finitely many primes of the form $6k+5$, say $p_1, p_2, \cdots, p_l$. Consider the number $n = 6\,p_1p_2\cdots p_l - 1$. Since n is odd, its prime factors are odd. Note that 3 is not a factor of n (the remainder when n is divided by 3 is equal to 2), so the pime factors of n are all of one of the forms $6k+1$ or $6k+5$. None of the primes p_i is a factor of n (since the remainder when n is divided by p_i is $p_i - 1$) and so all of the prime factors of n must be of the form $6k+1$. But since $(6k+1)(6l+1) = 6(6kl+k+l)+1$, we see that a product of terms of the form $6k+1$ is also of the form $6k+1$. This shows that n must be of the form $6k+1$. But n is of the form $6k-1$, so it is not of the form $6k+1$, and we have the desired contradiction.

(b) Show that the sequence $\{6k+5\}$ contains arbitrarily long strings of consecutive terms which are all composite. In other words, show that for every positive integer n there exists a value of k such that the n integers $6k+5, 6k+11, 6k+17, \cdots, 6k+6n-1$ are all composite.

Solution: For any positive integer n, the numbers $(6n)!+2, (6n)!+3, (6n)!+4, \cdots, (6n)!+6n$ are all composite since for $2 \leq k \leq 6n$ we have $k\big|(6n)!+k$. In particular, the n integers

$$(6n)!+5,\ (6n)!+11,\ (6n)!+17,\ \cdots,\ (6n)!+(6n-1)$$

are all composite.

5: (a) Show that there are infinitely many primes of the form $8k-1$ with $k \in \mathbf{Z}$.

Solution: Let $p_1, p_2, \cdots, p_l$ be primes of the form $8k-1$ with $k \in \mathbf{Z}$, and let $n = (p_1p_2\cdots p_l)^2 - 2$. Note that since $p_i = -1 \bmod 8$ for all i, we have ${p_i}^2 = 1 \bmod 8$ and so $n = {p_1}^2{p_2}^2\cdots{p_l}^2 - 2 = 1 - 2 = -1 \bmod 8$. Let p be a prime factor of n Note that p is odd since n is odd, and note also that $p \neq p_i$ for any i, since $n = -2 \bmod p_i$ so p_i is not a factor of n. We have $n = 0 \bmod p$, so $(p_1p_2\cdots p_l)^2 = 2 \bmod p$, so $2 \in Q_p$. Since $2 \in Q_p$ we must have $p = \pm 1 \bmod 8$. Since $n = -1 \bmod 8$ it is not possible that every prime factor of n is of the form $p = 1 \bmod 8$, and so n must have at least one prime factor of the form $p = -1 \bmod 8$. Thus we have found another prime of the form $8k-1$.

(b) Show that there are infinitely many primes of the form $8k+5$ with $k \in \mathbf{Z}$.

Solution: Let $p_1, p_2, \cdots, p_l$ be primes of the form $8k+5$ with $k \in \mathbf{Z}$, and let $n = (p_1p_2\cdots p_l)^2 + 4$. Note that each $p_i = 5 \bmod 8$ so ${p_i}^2 = 1 \bmod 8$ so $n = 5 \bmod 8$. Let p be a prime factor of n. Note that p is odd (since n is odd) and that $p \neq p_i$ for any i (since no p_i is a factor of n). We have

$$\begin{aligned} n = 0 \bmod p &\Longrightarrow (p_1p_2\cdots p_l)^2 = -4 \bmod p \Longrightarrow -4 \in Q_p \\ &\Longrightarrow 1 = \left(\tfrac{-4}{p}\right) = \left(\tfrac{-1}{p}\right)\left(\tfrac{2}{p}\right)^2 = \left(\tfrac{-1}{p}\right) \\ &\Longrightarrow p = 1 \bmod 4 \Longrightarrow p = 1 \text{ or } 5 \bmod 8 \end{aligned}$$

Since $n = 5 \bmod 8$ it is not possible that every prime factor of n is of the form $p = 1 \bmod 8$, and so n must have at least one prime factor of the form $p = 5 \bmod 8$. Thus we have found another prime of the form $p = 8k+5$ with $k \in \mathbf{Z}$.