PMATH 340 Number Theory, Solutions to Assignment 4

1: (a) Let $n = 493$, $e = 85$ and $c = 261$. Decipher the ciphertext c to recover the original message m that was encrypted using the RSA scheme with the public key (n, e).

Solution: First we factor n. Since $\sqrt{n} < 25$ we only need to look for prime factors p with $p \le 23$. By trial and error, we find that $n = pq$ where $p = 17$ and $q = 29$. We let $\psi = \mathrm{lcm}(p-1, q-1) = \mathrm{lcm}(16, 28) = 16 \cdot 7 = 112$. Next we need to find $d = e^{-1} \bmod \psi$. To do this we solve $85x + 112y = 1$. The Euclidean Algorithm gives

$$112 = 85 \cdot 1 + 27 \;,\; 85 = 27 \cdot 3 + 4 \;,\; 27 = 4 \cdot 6 + 3 \;,\; 4 = 3 \cdot 1 + 1$$

then Back-Substitution gives the sequence $1, -1, 7, -22, 29$ so we have $85 \cdot 29 + 122 \cdot 22 = 1$. This shows that $d = e^{-1} = 29 \bmod 112$. To decode the ciphertext c we need to calculate $m = c^d \bmod n$. Using a hand calculator, this can be done using the Square and Multiply Algorithm. Without a calculator, it is easier to use the fact that $493 = 17 \cdot 29$ and calculate $c^d \bmod 17$ and $c^d \bmod 29$. Since $c = 261 = 6 \bmod 17$ we have $c^d = 6^{29} \bmod 17$. We list some powers of 6 modulo 17.

k	1	2	4	8	16
6^k	6	2	4	-1	1

Since $29 = 16 + 8 + 4 + 1$ we have $c^d = 6^{29} = 6^{16} \cdot 6^8 \cdot 6^4 \cdot 6^1 = (1)(-1)(4)(6) = -24 = 10 \bmod 17$. Also, since $c = 261 = 0 \bmod 29$ we have $c^d = 0^{29} = 0 \bmod 29$. We can find $c^d \bmod n$ by solving the pair of congruences $x = 10 \bmod 17$ and $x = 0 \bmod 29$. We need $x = 10 + 17k$ and $x = 0 + 29\ell$ so we solve $17k - 29\ell = -10$. The Euclidean Algorithm gives $29 = 17 \cdot 1 + 12$, $17 = 12 \cdot 1 + 5$, $12 = 5 \cdot 2 + 2$, $5 = 2 \cdot 2 + 1$ and then Back-Substitution gives the sequence $1, -2, 5, -7, 12$ so we have $17 \cdot 12 - 29 \cdot 7 = 1$. Multiply by -10 to get $(17)(-120) - (29)(-70) = -10$. By the Linear Diophantine Equations Theorm, the general solution to the equation $17k - 29\ell = -10$ is given by $(k, \ell) = (-120, -70) + t(29, 17)$, $t \in \mathbb{Z}$. Taking $t = 5$ gives the solution $(k, \ell) = (25, 15)$. Thus $x = 10 + 17k = 10 + 17 \cdot 25 = 435$ is one solution to the pair of congruences $x = 10 \bmod 17$, $x = 0 \bmod 19$. Thus $c^d = x = 435 \bmod 493$, so the original message was $m = 435$.

(b) Show that if many users choose a small value for their encryption key then the RSA scheme can be weak. To be specific, show that if A sends the same short message m to three individuals B_1, B_2 and B_3 who have public keys (n_i, e_i) with n_1, n_2 and n_3 distinct, and with $e_1 = e_2 = e_3 = 3$, then an eavesdropper E who intercepts the three encrypted messages $c_i = m^{e_i} = m^3 \bmod n_i$ can recover the original message m.

Solution: Suppose that $0 \le m < n_i$ for all i and that E knows the values of $c_i = m^3 \bmod n_i$ for all i. First, E can use the Euclidean Algorithm to determine whether the numbers n_1, n_2 and n_3 are coprime.

Case 1: Suppose that two of the numbers n_i are not coprime, say $\gcd(n_1, n_2) \ne 1$. Since $n_1 \ne n_2$ and each of n_1 and n_2 is a product of two primes, it follows that $p = \gcd(n_1, n_2)$ is a prime and that $n_1 = pq_1$ and $n_2 = pq_2$ where p, q_1, q_2 are distinct primes. After finding $p = \gcd(n_1, n_2)$ (using the Euclidean Algorithm), E obtains $q_1 = n_1/p$ and then E can calculate $\psi_1 = \mathrm{lcm}(p-1, q_1-1)$, then $d_1 = {e_1}^{-1} \bmod \psi_1$, then $m = {c_1}^{d_1} \bmod n_1$.

Case 2: Suppose that all three of the numbers n_1, n_2 and n_3 are coprime. Then E can solve the system of congruences $x = c_i \bmod n_i$, $i = 1, 2, 3$ (by solving linear diophantine equations using the Euclidean algorithm). If $x = u$ is a solution then the general solution is $x = u \bmod n_1n_2n_3$, so E can find the unique solution $x = v$ with $0 \le v < n_1n_2n_3$. Since $m^3 = c_i \bmod n_i$ for all i, we see that m^3 is a solution to the system. Assuming that $0 \le m < n_i$ for all i, we have $0 \le m^3 < n_1n_2n_3$. Since $0 \le v < n_1n_2n_3$ and $0 \le m^3 < n_1n_2n_3$ with $m^3 = v \bmod n_1n_2n_3$, we have $m^3 = v$ in $\mathbb{Z}$. Thus E can recover the message m by calculating the cubed root of v in $\mathbb{Z}$.

2: (a) Use Fermat's Little Theorem and the Square and Multiply Algorithm to show that 2479 is not prime (without testing each prime $p \leq \sqrt{2479}$ to see if is a factor). You can use a calculator for this problem.

Solution: We calculate 2^{2478} mod 2479 using the Square and Multiply Algorithm. We have

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

$$\begin{aligned} 2^{2478} &\equiv 2^{2048} \cdot 2^{256} \cdot 2^{128} \cdot 2^{32} \cdot 2^8 \cdot 2^4 \cdot 2^2 \\ &= (1746 \cdot 2384)(2031 \cdot 636)(256 \cdot 16 \cdot 4) \\ &= 223 \cdot 157 \cdot 1510 = 1935 \text{ mod } 2479\,. \end{aligned}$$

Since $2^{2478} \not\equiv 1$ mod 2479 we know that 2479 cannot be prime, by Fermat's Little Theorem.

(b) Determine whether 561 is a pseudo-prime, and whether 561 is a strong pseudoprime, for the base 5.

Solution: Note that 561 is composite with $561 = 3 \cdot 11 \cdot 13$ and that to carry out the Fermat Test and the Miller-Rabin Test, we need to consider each of $5^{560}, 5^{280}\, 5^{140}\, 5^{70}, 5^{35}$ mod 561. Modulo 3, we have $5^2 = 1$ so that $\text{ord}_3(5) = 2$. Modulo 11, we have $5^2 = 3$, $5^3 = 4$, $5^4 = 9$ and $5^5 = 1$, so that $\text{ord}_{11}(5) = 5$. Modulo 13, we have $5^2 = -1$, $5^3 = -5$ and $5^4 = 1$ so that $\text{ord}_{13}(5) = 4$. Since $5^{35} = 5^3 = 4 \neq \pm 1$ mod 13, we have $5^{35} \neq \pm 1$ mod 561. Since $5^{70} = 1 \neq -1$ mod 3, we have $5^{70} \neq -1$ mod 561. Since $5^{140} = 1$ mod 3, mod 11 and mod 13, we have $5^{140} = 1$ mod 561. Since $5^{140} = 1$ mod 561, we also have $5^{280} = 5^{560} = 1$ mod 561. Thus 561 is a pseudoprime for the base 5 (because $5^{560} = 1$ mod 561), but 561 is not a strong pseudoprime for the base 5 (because modulo 561 we have $5^{280} \neq -1$, $5^{140} \neq -1$, $5^{70} \neq -1$ and $5^{35} \neq \pm 1$).

(c) Find every prime number p such that $7 \cdot 19 \cdot p$ is a Carmichael number.

Solution: Let $n = 7 \cdot 19 \cdot p$ where p is prime number. By Theorem 5.16, n is a Carmichael number when $p \neq 2, 7$ or 19, and $6\big|(n-1)$, $18\big|(n-1)$ and $(p-1)\big|(n-1)$. We have $6\big|(n-1) \iff n = 1 \text{ mod } 6 \iff 7 \cdot 19 \cdot p = 1 \text{ mod } 6 \iff p = 1 \text{ mod } 6$, and we have $18\big|(n-1) \iff n = 1 \text{ mod } 18 \iff 7 \cdot 19 \cdot p = 1 \text{ mod } 18 \iff 7p = 1 \text{ mod } 18 \iff p = 13 \text{ mod } 18$. Thus we have $6\big|(n-1)$ and $18\big|(n-1)$ when $p = 13$ mod 18. Also, we have $(p-1)\big|(n-1) \iff (p-1)\big|(133p-1) \iff (p-1)\big|\big(133(p-1)+132\big) \iff (p-1)\big|132$. By making a short list, we find that the only positive integers p with $p = 13$ mod 18 and $(p-1)\ \big|132$ are $p = 13$ and $p = 67$, and these are both prime. Thus $p = 13$ and $p = 67$ are the only two prime numbers for which $7 \cdot 19 \cdot p$ is a Carmichael number.

3: (a) Let $a \geq 2$ and $m \geq 1$ be integers. Show that if $a^m + 1$ is prime, then a must be even and m must be a power of 2.

Solution: Note that since $a \geq 2$ and $m \geq 1$ we have $a^m + 1 \geq 2^1 + 1 = 3$. If a is odd, then a^m is also odd, so $a^m + 1$ is even and not equal to 2, so $a^m + 1$ is not prime.

Suppose that m is not a power of 2. Then we can write $m = 2^k q$ for some $k \geq 0$ and some odd number $q \geq 3$. Recall that when $q \geq 3$ is odd and $x \geq 2$, the number $x^q + 1$ is not prime since $(x^q + 1) = (x+1)(x^{q-1} - x^{q-2} + \cdots - x + 1)$. In particular, taking $x = a^{2^k}$ so that $x^q + 1 = a^{2^k q} + 1 = a^m + 1$, we see that $a^m + 1$ is not prime.

(b) Show that the Mersenne number M_{13} is prime and that the Mersenne number M_{23} is composite. You can use a calculator for this problem.

Solution: We have $M_{13} = 8191$. We know (from Theorem 1.17) that if M_{13} is composite then it must have a prime divisor q with $q \leq \lfloor\sqrt{8191}\rfloor = 90$, and we know (by the Primality Test for Mersenne Numbers, given in Example 5.37), that if q is a prime divisor of M_{13} then we must have $q = 1 \bmod 26$. The only primes $q \leq 90$ with $q = 1 \bmod 26$ are $q = 53, 79$, and since neither 53 nor 79 divides $M_{13} = 8191$, it follows that M_{13} is prime.

It was pointed out to me by some students that M_{23} is shown to be composite in Example 5.38 in the lecture notes, but let us repeat the solution here: We have $M_{23} = 2^{23} - 1 = 8388607$. Using the result of Example 5.37, if q is a prime factor of M_{23}, then we must have $q = 1 \bmod 46$, so $q = 1, 47, 93, 139, \cdots$. We try $q = 47$ and find that $M_{23} = 43 \cdot 178481$.

(c) Show that if n is a pseudoprime for the base 2 then so is the Mersenne number $M_n = 2^n - 1$.

Solution: Let n be a pseudoprime for the base 2. This means n is composite, $\gcd(2, n) = 1$, and $2^{n-1} = 1 \bmod n$. Let $M_n = 2^n - 1$. Note that M_n is odd, and so we have $\gcd(2, M_n) = 1$. Since n is composite, we can write $n = kl$ with $1 < k, l < n$, and then we have $M_n = 2^n - 1 = 2^{kl} - 1 = (2^k - 1)\big(2^{k(l-1)} + 2^{k(l-2)} + \cdots + 2^2 + 1 + 1\big)$ and so M_n is composite. It remains to show that $2^{M_n - 1} = 1 \bmod M_n$. Since $2^{n-1} = 1 \bmod n$ we can choose $t \in \mathbb{Z}^+$ such that $2^{n-1} = 1 + nt$. We then have

$$\begin{aligned} 2^{M_n - 1} - 1 = 2^{2^n - 2} - 1 = 2^{2(2^{n-1} - 1)} - 1 = 2^{2nt} - 1 &= (2^{nt} - 1)(2^{nt} + 1) \\ &= (2^n - 1)\big(2^{n(t-1)} + 2^{n(t-2)} + \cdots + 2 + 1\big)(2^{nt} + 1) \\ &= M_n\big(2^{n(t-1)} + 2^{n(t-2)} + \cdots + 2 + 1\big)(2^{nt} + 1). \end{aligned}$$

Thus we have $M_n \big| 2^{M_n - 1} - 1$, and so $2^{M_n - 1} = 1 \bmod M_n$, as required.

4: (a) Show that there are infinitely many primes of the form $12k+7$ with $k \in \mathbb{Z}$.

Solution: Suppose there are only finitely many primes p with $p = 7 \text{mod } 12$, say $p_1, p_2, \cdots, p_\ell$ are all such primes. Let $n = (2p_1p_2\cdots p_\ell)^2 + 3$. Note that for all k we have $p_k = 7\text{mod } 12 \Longrightarrow {p_k}^2 = 49 = 1\text{mod } 12$ and so $n = 2^2{p_1}^2{p_2}^2\cdots {p_\ell}^2 + 3 = 2^2 + 3 = 7\text{mod } 12$. Also note that $n = 3\text{mod } p_k$ so p_k is not a factor of n. Let p be any prime factor of n. Note that p is odd (since n is odd) and $p \neq p_k$ for any k (since p_k is not a factor of n). We have $p \big| n \Longrightarrow n = 0\text{mod } p \Longrightarrow (2p_1p_2\cdots p_\ell)^2 = -3\text{mod } p \Longrightarrow -3 \in Q_p \Longrightarrow p = 1$ or $7\text{mod } 12$ by Assignment 2, Problem 3(d). Since $n = 7\text{mod } 12$, not every prime factor of n can be equal to $1\text{mod } 12$, so n must have at least one prime factor $p = 7\text{mod } 12$. Thus we have found another prime $p = 7\text{mod } 12$ which is not in the list $p_1, p_2, \cdots, p_\ell$.

(b) Find (with proof, of course) the smallest positive integer k with the property that there exists a prime p such that the six numbers p, $p+k$, $p+2k$, $p+3k$, $p+4k$ and $p+5k$ are all prime.

Solution: We claim that when p and q are prime numbers and $k \in \mathbb{Z}^+$, if k is not a multiple of q then one of the q numbers p, $p+k$, $p+2k$, $\cdots$, $p+(q-1)k$ must be a multiple of q. Suppose k is not a multiple of q. Then we have $\gcd(k,q) = 1$, and so we can find integers u and v such that $ku + qv = p$. Then use the division Algorithm to write $-u = qr + s$ with $0 \leq s < q$, and we have $p + sk = p + (-u - qr)k = p - uk - qrk = qv - qrk$, which is a multiple of q. This proves the claim.

Now, let p be prime, and suppose that the 6 numbers p, $p+k$, $\cdots$, $p+5k$ are all prime. We claim that k must be a multiple of 30.

Suppose, for a contradiction, that k is not a multiple of 2. Then one of the 2 numbers p and $p+k$ is a multiple of 2, and since 2 is the only prime which is a multiple of 2, we must have $p = 2$. But then the third number is $p + 2k = 2 + 2k$, which is not prime. Thus k is a multiple of 2.

Suppose, for a contradiction, that k is not a multiple of 3. Then, by the above claim, one of the 3 numbers p, $p+k$ and $p+2k$ is a multiple of 3, and since 3 is the only prime which is a multiple of 3, we must have $p = 3$. But then the fourth number on the list is $p + 3k = 3 + 3k$, which is not prime. Thus k must be a multiple of 3. Since k is a multiple of 2 and of 3, k must be a multiple of 6.

Suppose, for a contradiction, that k is not a multiple of 5. Then, by the above claim, one of the 5 numbers p, $p+k$, $p+2k$, $p+3k$ and $p+4k$ must be a multiple of 5. Since 5 is the only prime which is a multiple of 5, and since $k \geq 6$, we must have $p = 5$. But then the sixth number on the list is $p + 5k = 5 + 5k$, which is not prime. Thus k is a multiple of 5.

Since k is a multiple of 2, 3 and 5, it must be a multiple of 30, as claimed. Finally, note that taking $p = 7$ and $k = 30$, gives the 6 primes 7, 37, 67, 97, 127 and 157 (each of these numbers is easily verified to be prime: for example, if 157 was composite it would have a prime factor $p \leq \lfloor\sqrt{157}\rfloor = 12$, but the only such primes are $p = 2, 3, 5, 7$ and 11, and these do not divide 157).