# MATH 135 S 2016: Assignment 9 Solutions

---

1. Prove that for any integer $n$,

$$441n^{43} + 374n^{35} + 285n^{23} \equiv 0 \pmod{55}.$$

**Solution:** Since $55 = 5 \times 11$ and $\gcd(5, 11) = 1$, we may use the *Splitting Modulus* proposition and work with respect to modulo 5 and modulo 11 respectively. Let $n \in \mathbb{Z}$.

In modulo 5: note that $441 \equiv 1 \pmod 5$, $374 \equiv (-1) \pmod 5$ and $285 \equiv 0 \pmod 5$. If $n \equiv 0 \pmod 5$, then of course the expression $441n^{43} + 374n^{35} + 285n^{23}$ is congruent to 0 modulo 5 by the *Properties of Congruence*. On the other hand, if $n \not\equiv 0 \pmod 5$, and since 5 is a prime, then we may use reduction by *Fermat's ℓittle Theorem*, and get that $n^{43} \equiv n^{4\times 10+3} \equiv n^3 \pmod 5$ and $n^{35} \equiv n^{4\times 8+3} \equiv n^3 \pmod 5$. Thus, we get $441n^{43} + 374n^{35} + 285n^{23} \equiv (1)n^3 + (-1)n^3 + 0n^{23} \equiv 0 \pmod 5$.

In modulo 11: note that $441 \equiv 1 \pmod{11}$, $374 \equiv 0 \pmod{11}$ and $285 \equiv (-1) \pmod{11}$, so we have $441n^{43} + 374n^{35} + 285n^{23} \equiv (1)n^{43} + 0n^{35} + (-1)n^{23} \pmod{11}$. Again, if $n \equiv 0 \pmod{11}$, the result is obviously true, so we consider the case when $n \not\equiv 0 \pmod{11}$. Then, as 11 is a prime, we use $F\ell T$ again to get, $n^{43} \equiv n^{10\times 4+3} \equiv n^3 \pmod{11}$ and $n^{23} \equiv n^{10\times 2+3} \equiv n^3 \pmod{11}$. This means $441n^{43} + 374n^{35} + 285n^{23} \equiv (1)n^{43} + (-1)n^{23} \equiv n^3 - n^3 \equiv 0 \pmod{11}$.

Finally, by using *Splitting Modulus* again, this time to recombine the modulo back to 55, we have $441n^{43} + 374n^{35} + 285n^{23} \equiv 0 \pmod{55}$.

2. Suppose you are given $p = 7$ and $q = 11$ for an RSA scheme. Given a public key $(e, n) = (13, 77)$, find the corresponding private key. Make sure to justify your steps.

**Solution:** First, we compute $(p-1)(q-1) = (7-1)(11-1) = (6)(10) = 60$.

We need to find and integer $2 \le d \le 60$ such that

$$13d \equiv 1 \pmod{60}.$$

We may rewrite this as a linear Diophantine equation $13d + 60y = 1$. Using the *Extended Euclidean Algorithm (EEA) Table*, we get

| $x$ | $y$ | $r$ | $q$ | Division Algorithm |
|---|---|---|---|---|
| 1 | 0 | 60 | . | . |
| 0 | 1 | 13 | . | . |
| 1 | $-4$ | 8 | 4 | $60 = 4(13) + 8$ |
| $-1$ | 5 | 5 | 1 | $13 = 1(8) + 5$ |
| 2 | $-9$ | 3 | 1 | $8 = 1(5) + 3$ |
| $-3$ | 14 | 2 | 1 | $5 = 1(3) + 2$ |
| 5 | $-23$ | 1 | 1 | $3 = 1(2) + 1$ |

Therefore, $60(5) + 13(-23) = 1$. In other words,

$$(13)(-23) \equiv 1 \pmod{60}.$$

Since, $(-23) \equiv 37 \pmod{60}$, we get $d = 37$. Hence the corresponding private key is $(37, 77)$.

3. Professor $X$ and Professor Zoom have both set up their own RSA keys: X's public key is $(e_X, n_X) = (887, 15833)$, and Zoom's public key is $(e_Y, n_Y) = (977, 13019)$. Zoom wants to send X the answer to the first exam question of MATH 135, which is $M = 3141$. What is the ciphertext that Zoom needs to send to X? Show the set up of the calculations and the results. You may use a computer to perform the calculations.

   **Solution:** Zoom needs to use X's public key to encrypt her message. He needs to send $C \equiv M^{e_X} \pmod{n_X}$, which is $C \equiv 3141^{887} \pmod{15833}$. This gives us $C = 2054$.

4. Suppose you receive the cipher-text $C = 47$ (note $0 \leq C < 55$). Decrypt the message using your private key $(27, 55)$. Show the details of your computation; do not use a calculator or a computer.

   **Solution:** We are trying to solve for $R \equiv C^d \pmod{n}$, that is, $R \equiv (47)^{27} \pmod{55}$, where we require $0 < R < n$.

   Since $55 = 5 \times 11$ and $\gcd(5, 11) = 1$, therefore to find the value of $R$, we would solve the simultaneous congruences

$$\begin{aligned} R &\equiv (47)^{27} \equiv (2)^{27} \pmod{5} \\ \text{and } R &\equiv (47)^{27} \equiv 3^{27} \pmod{11}. \end{aligned}$$

   Since 5 and 11 are both prime numbers, we start using *Fermat's little Theorem (FlT)*. Since $5 \nmid 2$, we get that $2^4 \equiv 1 \pmod{5}$. Similarly, $11 \nmid 3$ gives us $3^{10} \equiv 1 \pmod{11}$.

   Using $27 = (6)(4) + 3$ in the first congruence, we get

$$R \equiv \left(2^4\right)^6 \left(2^3\right) \equiv (1)\left(2^3\right) \equiv 8 \equiv 3 \pmod{5}.$$

   Similarly, from $27 = 2(10) + 7$ , the second congruence becomes

$$R \equiv \left(3^{10}\right)^2 \left(3^7\right) \equiv (1)(3^7) \pmod{11}$$

   Now, notice that $3^7 = (3^3) \cdot (3^3) \cdot (3)$, so

$$R \equiv (3^3)(3^3)(3) \equiv (27)(27)(3) \equiv (5)(5)(3) \equiv (5)(15) \equiv (5)(4) \equiv 20 \equiv 9 \pmod{11}.$$

   So, we finally have to solve the simultaneous congruences

$$\begin{aligned} R &\equiv 3 \pmod{5} \\ \text{and } R &\equiv 9 \pmod{11}. \end{aligned}$$

   $R \equiv 9 \pmod{11}$ gives $R = 9 + 11s$ for some integer $s$. Then, simplifying the other congruence we get $s \equiv 4 \pmod{5}$.

   Thus, we may write $s = 4 + 5t$ for some integer $t$. Consequently,

$$R = 9 + 11(4 + 5t) = 9 + 44 + 55t = 53 + 55t.$$

   As a result, $R \equiv 53 \pmod{55}$. Since we need $0 \leq R < 55$, we obtain the decrypted message

$$R = 53.$$

5. Researchers have analyzed many public RSA keys generated by some cheap routers. Suppose the $i^{th}$ router generates the key $(e_i, n_i)$. To their shock, the researchers recently discovered that some of the different $n_i$'s were generated using a common prime factor.

(a) Let $p, q$ and $r$ be distinct odd primes. Suppose $n = pq$ and $m = pr$. Given that you know that $m$ and $n$ share a common prime factor, but that you do not know the values of $p, q, r$, explain how you may obtain the prime factors of $m$ and $n$ without using the method of prime factorization?

**Solution:** Suppose $p, q$ and $r$ are distinct primes where $n = pq$ and $m = pr$. Since we have the prime factorizations of $n$ and $m$, so $\gcd(n, m) = p$. To find the GCD, we may simply run the *Euclidean algorithm* (which is a much faster process than prime factorization) to figure out what $p$ is, and then we can easily obtain $q$ and $r$ by dividing $n$ and $m$ by $p$ respectively.

(b) The numbers 41685823 and 39034579 share a common prime factor. Use your method described in part (a) to factor $n = 41685823$ and $m = 39034579$. Make sure to show all your steps.

**Solution:** Given $n = 41685823$ and $m = 39034579$, we simply run the *Euclidean Algorithm* to get

$$\begin{aligned}
41685823 &= (1)(39034579) + 2651244 \\
39034579 &= (14)(2651244) + 1917163 \\
2651244 &= (1)(1917163) + 734081 \\
1917163 &= (2)(734081) + 449001 \\
734081 &= (1)(449001) + 285080 \\
449001 &= (1)(285080) + 163921 \\
285080 &= (1)(163921) + 121159 \\
163921 &= (1)(121159) + 42762 \\
121159 &= (2)(42762) + 35635 \\
42763 &= (1)(35635) + 7127 \\
35635 &= (5)(7127) + 0.
\end{aligned}$$

Hence $\gcd(n, m) = 7127$, that is, $p = 7127$. Using long division, we may then find $41685823 = (7127)(5849)$ and $39034579 = (7127)(5477)$. Therefore $q = 5849$ and $r = 5477$.

6. Sam and Tim have set up their RSA keys $(e_S, n), (e_T, n)$, respectively, where the $n$-value is the same. Furthermore, it happens that $\gcd(e_S, e_T) = 1$. Suppose that their friend Rob wants to send both Sam and Tim a message $M$ that is coprime with $n$. Rob encrypts $M$ using Sam and Tim's public keys, producing the ciphertexts $C_S$ and $C_T$ respectively.

Prove that anyone who eavesdrops and obtains the values of both $C_S$ and $C_T$ can determine the message $M$ using the public keys of Sam and Tim, without knowing their private keys or factoring $n$.

**Solution:** From the RSA algorithm, $C_S \equiv M^{e_S} \pmod{n}$ and $C_T \equiv M^{e_T} \pmod{n}$. Since $\gcd(e_S, e_T) = 1$, by EEA, there exist integers $x, y$ such that $e_S x + e_T y = 1$. Now one of $x, y$ is positive and the other is negative. Without loss of generality, assume that $y$ is negative. Then $e_S x = 1 - e_T y$ (where $-e_T y$ is now positive). Then

$$M^{e_S x} \equiv M^{1 - e_T y} \pmod{n}$$

or

$$M^{e_S x} \equiv M \cdot M^{-e_T y} \pmod{n}.$$

Then

$$C_S^x \equiv M \cdot C_T^{-y} \pmod{n}.$$

We can calculate the values of $C_S^x$ and $C_T^{-y}$, so this is simply a linear congruence with $M$ as our variable. Since $M$ is coprime with $n$, and $C_T^{-y} \equiv M^{-e_T y} \pmod{n}$, then $C_T^{-y}$ is also coprime with $n$, so an integer solution exists. We can then obtain $M$ from solving this congruence.

7. Let $p$ and $q$ be distinct odd primes. Define $n = pq$. The security of RSA relies on the fact that, given the value of $n$, it is difficult to find the factors $p$ and $q$.

However, if the value of $\phi = (p-1)(q-1)$ is also known, here we will see that the values of $p$ and $q$ may be obtained without factoring $n$.

(a) Show that

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

**Solution:** Given $n = pq$ and $\phi = (p-1)(q-1)$, and assuming $p \geq q$, we have

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

and

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

(b) Use your answer from part (a) to express the primes $p$ and $q$ in terms of $n$ and $\phi$.

**Solution:** We have $p + q = n - \phi(n) + 1$ and $p - q = \sqrt{(p+q)^2 - 4n}$. Adding these, we get

$$\begin{aligned} 2p &= (n - \phi(n) + 1) + \sqrt{(p+q)^2 - 4n} \\ \implies p &= \frac{1}{2}\left((n - \phi(n) + 1) + \sqrt{((n - \phi(n) + 1))^2 - 4n}\right). \end{aligned}$$

Taking the difference of the two equations, we get

$$\begin{aligned} 2q &= (n - \phi(n) + 1) - \sqrt{(p+q)^2 - 4n} \\ \implies q &= \frac{1}{2}\left((n - \phi(n) + 1) - \sqrt{((n - \phi(n) + 1))^2 - 4n}\right). \end{aligned}$$