CS 70 Spring 2020 — Discrete Mathematics and Probability Theory — Quiz 4

1. [Mod Math, Fermat, CRT]

(a) What is 70^{2014} mod 11?

(b) What is 70^{2014} mod 77?

Solution:

(a) $70^{2014} \equiv 4^{2014} \equiv 4^{10\cdot 200+4} \equiv 4^4 \equiv 256 \equiv 3 \bmod 11$

(b) By CRT, decompose into 70^{2014} mod 7 and 70^{2014} mod 11 since $77 = 7 \cdot 11$. $70^{2014} \equiv 0$ mod 7, and $70^{2014} \equiv 3$ mod 11 from part (a).

Hence, $70^{2014} \equiv 3 \cdot 7 \cdot [7^{-1}]_{11} \equiv 3 \cdot 7 \cdot 8 \equiv 14 \bmod 77$

---

2. [Modular Arithmetic]:

(a) Compute $11^{13} \pmod{100}$ using repeated squaring. Show your intermediate results.

(b) State Fermat's Little Theorem, and then use it to give a careful proof of the following claim.

Claim: If p is prime and b, c are positive integers such that $b = c \pmod{p-1}$, then $a^b = a^c \pmod{p}$ for any integer a.

(c) Find $8^{(321^{49})} \pmod{11}$.

NOTE: You should use part (b). It is possible to figure out this question in two lines. If you are doing a lot of calculations, you are probably on the wrong track. Write no more than five lines.

Solution:

(a) By repeated squaring we compute:

$$11^2 = 121 \equiv 21 \pmod{100}$$
$$11^4 \equiv 21^2 \equiv 41 \pmod{100}$$
$$11^8 \equiv 41^2 \equiv 81 \pmod{100}$$

$$\begin{aligned} 11^{13} &= 11^{1+4+8} \\ &= 11^1 \times 11^4 \times 11^8 \\ &\equiv 11 \times 41 \times 81 \\ &\equiv 51 \times 81 \\ &\equiv 31 \pmod{100} \end{aligned}$$

(b) Fermat's Little Theorem states that for any prime p, for any $a \in \{1,2,...,p-1\}$,

$$a^{p-1} = 1 \pmod p$$

. We prove by cases:

- Case 1: $a = 0 \pmod p$. Then $a^b = 0 = a^c \pmod p$ for any positive integers b and c.
- Case 2: $a \neq 0 \pmod p$. Since $b = c \pmod{p-1}$, we have $b = c + k(p-1)$ for some integer k, so

$$a^b = a^{c+k(p-1)} = a^c \times (a^{k(p-1)}) \underbrace{=}_{(*)} a^c \times 1^k = a^c \pmod p,$$

where the equality $(*)$ comes from Fermat's Little Theorem.

(c) Using part (b) with $p = 11$, the first step is to calculate:

$$321^{49} = (32 \times 10 + 1)^{49} \equiv 1^{49} = 1 \pmod{10}.$$

Then by part (b) we have

$$8^{(321^{49})} = 8^1 \equiv 8 \pmod{11}.$$

---

3. Show that if p is prime, then $(p-1) \equiv (p-1)! \pmod p$.
(HINT: what can you say about the inverses of numbers x between 2 and $p-2$ mod p?)

Solution: First, consider the set $S = 1,...,(p-1)$. Since every element in S is coprime with p, we know that each one has a unique multiplicative inverse $\pmod p$ that is also in the set S. To prove that they are unique,suppose that $a, b \in 1,...,(p-1)$ have the same multiplicative inverse, m.

$$\begin{aligned} a \cdot m &\equiv 1 \pmod p \\ b \cdot m &\equiv 1 \pmod p \\ m \cdot (a-b) &\equiv 0 \pmod p \\ m \equiv 0 \pmod p \text{ or } (a-b) &\equiv 0 \pmod p \end{aligned}$$

Since m is not divisible by p, $(a-b)$ must be divisible by p. Since $|(a-b)| < p-2$, $a-b$ must equal zero.Therefore, if a and b have the same multiplicative inverse, then $a = b$.

Note that since every number in S has a unique multiplicative inverse from S, taking the multiplicativeinverse is a bijection. There are two cases: a number has a multiplicative inverse $\pmod p$ that is itself, or a number has an inverse $\pmod p$ that is different from itself. Let's look at some number x in the set S that has an inverse $\pmod p$ that is itself.

$$\begin{aligned} x^2 &\equiv 1 \pmod p \\ x^2 - 1 &\equiv 0 \pmod p \\ (x+1)(x-1) &\equiv 0 \pmod p \\ x+1 \equiv 0 \pmod p \text{ or } x-1 &\equiv 0 \pmod p \\ x &\equiv \pm 1 \pmod p \end{aligned}$$

This shows that only 1 and $p-1$ are their own inverses. Each of the numbers $2,3,\ldots,(p-3),(p-2)$ have a unique inverse which is not themselves.

Now going back to the statement $(p-1) \equiv (p-1)! \pmod{p}$, there are two cases to show.

- $p=2$: $(2-1)=1 \equiv 1! \pmod{p}$. So, true.
- $p>2$: We know for every such p, p is an odd number. Then there are an even number of terms in $(p-2)(p-3)\cdots(3)(2)$. Since we have shown each number in this term has a unique inverse $\pmod{p}$, each term will pair up with its multiplicative inverse and result in $1 \cdot 1 \cdots 1 \cdot 1 \equiv (p-2)(p-3)\cdots(3)(2) \pmod{p}$. We now have $(p-1)! \pmod{p} \equiv (p-1) \cdot 1 = (p-1)$. So, again, the statement is true.

CS 70 Discrete Mathematics and Probability Theory
Spring 2020 DIS 4A

1 RSA Warm-Up

Consider an RSA scheme with modulus $N = pq$, where p and q are distinct prime numbers larger than 3.

(a) What is wrong with using the exponent $e = 2$ in an RSA public key?

(b) Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

(c) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

(d) What is the private key?

(e) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message $E(x)$ she sends using the public key?

(f) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message? and what is the decrypted message?

Solution:

(a) To find the private key d from the public key (N, e), we need $\gcd(e, (p-1)(q-1)) = 1$. However, $(p-1)(q-1)$ is necessarily even since p, q are distinct odd primes, so if $e = 2$, $\gcd(e, (p-1)(q-1)) = 2$, and a private key does not exist. (Note that this shows that e should more generally never be even.)

(b) Both p and q must be of the form $3k+2$. $p = 3k+1$ is a problem since then $p-1$ has a factor of 3 in it. $p = 3k$ is a problem because then p is not prime.

(c) $N = p \cdot q = 85$ and $e = 3$ are displayed publicly. Note that in practice, p and q should be much larger (512-bit) numbers. We are only choosing small numbers here to allow manual computation.

(d) We must have $ed = 3d \equiv 1 \pmod{64}$, so $d = 43$. Reminder: we would do this by using extended gcd with $x = 64$ and $y = 3$. We get $\gcd(x, y) = 1 = ax + by$, and $a = 1$, $b = -21$.

(e) We have $E(x) = x^3 \pmod{85}$, where $E(x)$ is the encryption function. $10^3 \equiv 65 \pmod{85}$, so $E(x) = 65$.

(f) We have $D(y) = y^{43} \pmod{85}$, where $D(y)$ is the decryption function, the inverse of $E(x)$.

$$x \equiv 24^{43} \pmod{85}$$

From CRT we know that for coprime numbers p and q if

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

then

$$x = aqq_1 + bpp_1 \pmod{pq}$$

where $p_1 = p^{-1} \pmod{q}$ and $q_1 = q^{-1} \pmod{p}$.
In our case we have $p = 5$ and $q = 17$. So

$$x \equiv 24^{43} \equiv (-1)^{43} \equiv -1 \equiv 4 \pmod{5}$$

and

$$\begin{aligned}
x &= 24^{43} \pmod{17}\\
x &= (7)^{43} \pmod{17}\\
x &= (7^2)^{21} \cdot 7 \pmod{17}\\
x &\equiv (-2)^{21} \cdot 7 \pmod{17}\\
x &= ((-2)^4)^5 \cdot (-2) \cdot 7 \pmod{17}\\
x &\equiv (-1)^5 \cdot (-14) \pmod{17}\\
x &\equiv 14 \pmod{17}
\end{aligned}$$

Hence

$$x = a = 4 \pmod{5} \qquad x = b = 14 \pmod{17}$$

and

$$\begin{aligned}
p_1 &= p^{-1} \pmod{17} = 5^{-1} \pmod{17} = 7\\
q_1 &= q^{-1} \pmod{5} = 17^{-1} \pmod{5} = 3
\end{aligned}$$

So we have

$$\begin{aligned}
x &\equiv aqq_1 + bpp_1 \pmod{pq}\\
x &= 4 \cdot 17 \cdot 3 + 14 \cdot 5 \cdot 7 \pmod{85}\\
x &= 4 \cdot 17 \cdot 3 + 490 \pmod{85}\\
x &= 17 \cdot (12) + 490 \pmod{85}\\
x &= 17 \cdot (10 + 2) + 490 \pmod{85}\\
x &\equiv 34 + (-20) \pmod{85}\\
x &= 14 \pmod{85}
\end{aligned}$$

so $D(y) = 14$.

2 RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(N_1,e),\dots,(N_k,e)$ where no two N_i's are the same. Assume that the message is x such that $0 \le x < N_i$ for every i.

(a) Suppose Eve sees the public keys $(p_1q_1,7)$ and $(p_1q_2,7)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of p_1,q_1,q_2 as massive 1024-bit numbers. Assume p_1,q_1,q_2 are all distinct and are valid primes for RSA to be carried out.

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(p_1q_1,3)$, $(p_2q_2,3)$, and $(p_3q_3,3)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume p_1,p_2,p_3,q_1,q_2,q_3 are all distinct and are valid primes for RSA to be carried out.

(c) Let's say the secret x was not changed, so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x?

Solution:

(a) Normally, the difficulty of cracking RSA hinges upon the believed difficulty of factoring large numbers. If Eve were given just p_1q_1, she would (probably) not be able to figure out the factors.

However, Eve has access to two public keys, so yes, she will be able to figure it out. Note that $\gcd(p_1q_1,p_1q_2) = p_1$. Taking GCDs is actually an efficient operation thanks to the Euclidean Algorithm. Therefore, she can figure out the value of p_1, and from there figure out the value of q_1 and q_2 since she has p_1q_1 and p_1q_2.

(b) Since none of the N's have common factors, she cannot find a GCD to divide out of any of the Ns. Hence the approach above does not work.

(c) Eve observes $x^3 \pmod{N_1}$, $x^3 \pmod{N_2}$, $x^3 \pmod{N_3}$. Since all N_1,N_2,N_3 are pairwise relatively prime, Eve can use the Chinese Remainder Theorem to figure out $x^3 \pmod{N_1N_2N_3}$. However, once she gets that, she knows x, since $x < N_1$, $x < N_2$, and $x < N_3$, which implies $x^3 < N_1N_2N_3$. Uh oh!
(Side note: for a more concrete walk through of CRT, refer to the Chinese Remainder Problem in discussion 2C.)

3 RSA for Concert Tickets

Alice wants to tell Bob her concert ticket number, m, which is an integer between 0 and 100 inclusive. She wants to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know her ticket number.

(a) Bob announces his public key $(N = pq, e)$, where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's ticket number is. How did she do it?

(b) Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm, encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r. How can she figure out m?

Solution:

(a) There are only 101 possible values for Alice's ticket number, so Eve can try encrypting all 101 values with Bob's public key and find out which one matches the one Alice sent.

(b) Alice sends $x = r^e \pmod{pq}$, as well as $y = (rm)^e = r^e m^e = xm^e \pmod{pq}$. We can find $x^{-1} \pmod{N}$ using the Extended Euclidean Algorithm, and multiplying this value by y gives us $m^e \pmod{N}$. Now we proceed as in the previous part to find m.