M328K: Homework 4

Katherine Ho

September 30, 2024

1. Show that if $d \mid n$, then $\phi(d) \mid \phi(n)$.

Proof. d and n can each be written as a product of primes. Given $d \mid n$:

$$d = (p_1^{a_1}) \dots (p_i^{a_i})$$
$$n = (p_1^{b_1}) \dots (p_i^{b_i}) \cdot (q_1^{c_1}) \dots (q_j^{c_j})$$

where $b_i \geq a_i$.
Then, since ϕ is multiplicative,

$$\phi(d) = \phi(p_1^{a_1}) \dots \phi(p_i^{a_i})$$
$$\phi(n) = \phi(p_1^{b_1}) \dots \phi(p_i^{b_i}) \cdot \phi(q_1^{c_1}) \dots \phi(q_j^{c_j})$$

Since each factor is prime,

$$\begin{aligned}
\phi(d) &= (p_1^{a_1} - p_1^{a_i - 1}) \dots (p_i^{a_i} - p_i^{a_i - 1}) \\
&= (p_1^{a_1}(1 - \frac{1}{p_1})) \dots (p_i^{a_i}(1 - \frac{1}{p_i})) \\
\phi(n) &= (p_1^{b_1} - p_1^{b_i - 1}) \dots (p_i^{b_i} - p_i^{b_i - 1}) \cdot (q_1^{c_1} - q_j^{c_j - 1}) \dots (q^{c_j} - q^{c_j - 1}) \\
&= (p_1^{b_1}(1 - \frac{1}{p_1})) \dots (p_i^{b_i}(1 - \frac{1}{p_i})) \cdot (q_1^{c_1}(1 - \frac{1}{q_1})) \dots (q_j^{c_j}(1 - \frac{1}{q_j}))
\end{aligned}$$

Since $b_i \geq a_i$, every factor of $\phi(d)$ divides a factor of $\phi(n)$. Thus $\phi(d) \mid \phi(n)$.

□

2. Find the smallest positive integer x satisfying the system of linear congruences

$$3x \equiv 10 \pmod{19}$$
$$4x \equiv 1 \pmod{23}.$$

Proof. First we can isolate x on the left side of each congruence by multiplying by the multiplicative inverse.

(a) $3^{-1} \pmod{19}$:

$$\begin{aligned}
3x &\equiv 1 \pmod{19} \\
3x - 19y &= 1 \\
19 &= 3(6) + 1 \\
1 &= 19 - 3(6) \\
1 &= 3(-6) - 19(-1)
\end{aligned}$$

We have $x = -6 \equiv 13 \equiv 3^{-1} \pmod{19}$. We can multiply by $3x \equiv 10 \pmod{19}$ to get

$$x \equiv 130 \pmod{19}$$

(b) $4^{-1} \pmod{23}$

$$\begin{aligned} 4x &\equiv 1 \pmod{23} \\ 4x - 23y &= 1 \\ 23 &= 4(5) + 3 \\ 4 &= 3(1) + 1 \\ 1 &= 4 - 3(1) \\ 1 &= 4 - (23 - 4(5)) \\ 1 &= 4(6) - 23(1) \end{aligned}$$

We have $x = 6 \equiv 4^{-1} \pmod{23}$. We can multiply by $4x \equiv 1 \pmod{23}$ to get

$$x \equiv 6 \pmod{23}$$

Now the system is

$$\begin{aligned} x &\equiv 130 \pmod{19} \\ x &\equiv 6 \pmod{23} \end{aligned}$$

Since $\gcd(19, 23) = 1$, there is a unique solution for $x \pmod{19 \cdot 23 = 437}$ by the Chinese Remainder theorem.
By Bezout's Theorem, there exist integers y_1, y_2 such that $19y_1 + 23y_2 = 1$.
By the Euclidean Algorithm,

$$\begin{aligned} 23 &= 19(1) + 4 \\ 19 &= 4(4) + 3 \\ 4 &= 3(1) + 1 \\ 1 &= 4 - 3(1) \\ 1 &= (23 - 19) - (19 - 4(4)) \\ 1 &= 23 - 2(19) + 4(4) \\ 1 &= 23 - 2(19) + 4(23 - 19) \\ 1 &= 23(5) - 6(19) \\ 1 &= 19(-6) + 23(5) \end{aligned}$$

So $y_1 = -6, y_2 = 5$. Then, $x = a_2 n_1 y_1 + a_1 n_2 y_2$ is a solution where $n_1 = 19, n_2 = 23$.

$$\begin{aligned} x &= (6)(19)(-6) + 130(23)(5) \\ &= -684 + 14950 \\ &= 14266 \\ x &\equiv 282 \pmod{437} \end{aligned}$$

Thus the smallest value of x satisfying the system of congruences is 282.

$\square$

3. Calculate $3^{434} \mod 1022$ using binary exponentiation.

Proof. The binary expansion of 3^{434} is

$$3^{256} \cdot 3^{128} \cdot 3^{32} \cdot 3^{16} \cdot 3^{2}$$

Then, we can find what each term is congruent to $\pmod{1022}$.

$$\begin{aligned}
3 &\equiv 3 \\
3^2 &\equiv 9 \\
3^4 &\equiv 81 \\
3^8 &\equiv 81^2 \equiv 6,561 \equiv 429 \\
3^{16} &\equiv 429^2 \equiv 184,041 \equiv 81 \\
3^{32} &\equiv 81^2 \equiv 6,561 \equiv 429 \\
3^{64} &\equiv 429^2 \equiv 184,041 \equiv 81 \\
3^{128} &\equiv 81^2 \equiv 6,561 \equiv 429 \\
3^{256} &\equiv 429^2 \equiv 184,041 \equiv 81
\end{aligned}$$

Then substitute back into the binary expansion of 3^{434}.

$$\begin{aligned}
3^{434} &\equiv 81 \cdot 429 \cdot 429 \cdot 81 \cdot 9 \pmod{1022} \\
3^{434} &\equiv 10,867,437,009 \pmod{1022}
\end{aligned}$$

$$\boxed{3^{434} \equiv 9 \pmod{1022}}$$

□

4. Using RSA, decipher the critically important message someone is sending if $n = 7417 \cdot 8363$, exponent $E = 100019$, and you receive 23451141. To fully decrypt, pair digits (padding at the beginning with 0 if necessary) and interpret as 01 = A, 26 = Z. Write down the intermediate steps you used. (Note: You may use computers/calculators to perform the divison algorithm and to reduce integers mod n. You may find the Wolfram Alpha command `Mod[a,n]` particularly useful.

Proof. First, we have the public key $(n, E) = (7417 \cdot 8362, 100019) = (62028371, 100019)$.
Then, we compute $\phi(n) = (7417 - 1) \cdot (8363 - 1) = 62012592$.
We use this result to find the decryption exponent D.

$$D = E^{-1} \pmod{\phi(n)} = 100019^{-1} \pmod{62012592} = 12142859$$

Now we have the private key $(n, D) = (62028371, 12142859)$.
To recover the message W from $Z = 23451141$, we can use the private key to compute:

$$\begin{aligned}
Z^D &\equiv W \pmod{n} \\
23451141^{12142859} &\equiv W \pmod{62028371} \\
&\equiv 12130115
\end{aligned}$$

To decrypt the message:

$$\begin{array}{c} 12 \mid 13 \mid 01 \mid 15 \\ L \mid M \mid A \mid O \end{array}$$

The message is LMAO. $\square$