1 Classical Cryptosystems

(Continued from Lecture 1.)

1.1 Interlude: Modular Arithmetic

One fundamental idea in number theory, which is used in cryptography, is modular arithmetic.

1.1.1 Quotients and Remainders

Lemma 1.1: Euclid's Division

For any integer a and positive integer n, there exists a unique pair of integers q and r such that $0 \leq r < n$ and $a = qn + r$. The integers q and r are called the quotient and remainder, respectively. We also write $a \pmod{n}$ to refer to the remainder.

For the proof, the dea is that we can keep subtracting, or adding, n from a until we end up in the range $[0, n)$. Therefore, the number of times we had to subtract, or add, n is the *quotient*, and the number in the range $[0, n)$ that we end up with at the end is the *remainder*.

(Example.) Divide $a = 17$ by $n = 5$. Find the quotient and remainder.

Using the proof idea, we note that:

- Subtracting 5 to a once gives us 12.
- Subtracting 5 to a twice gives us 7.
- Subtracting 5 to a thrice gives us 2.

It took us 3 subtractions to get to a number that's in the range $[0, 5)$, so the quotient is $\boxed{3}$ and the remainder is $\boxed{2}$.

We should note that this is pretty standard when $a \geq 0$. However, for $a < 0$, it might be less familiar, albeit the same process.

(Example.) Divide $a = -7$ by $n = 5$. Find the quotient and remainder.

Using the proof idea, we note that:

- Adding 5 to a once gives us 2.
- Adding 5 to a twice gives us 3.

It took us 2 additions to get to a number that's in the range $[0, 5)$, so the quotient is $\boxed{-2}$ (because we had to *add*, not subtract) and the remainder is $\boxed{3}$.

Remark:

- If we have to **add** n to a x times to get a number that's in the range $[0, n)$, then our final quotient will be negative (that is, $-x$).
- If we have to **subtract** n from a x times to get a number that's in the range $[0, n)$, then our final quotient will be positive (that is, x).

(Exercise.) For each of the following, calculate the quotient and remainder when a is divided by n. Do these calculations by hand.

- $a = 13$, $n = 3$.

  We know that $13/3 = 4$, and $13-(3\cdot 4) = 1 \in [0,3)$. So, the quotient is $\boxed{4}$ and the remainder is $\boxed{1}$.

- $a = 134$, $n = 10$.

  We know that $134/10 = 13$ and $134 - (10 \cdot 13) = 4 \in [0, 10)$. So, the quotient is $\boxed{13}$ and remainder is $\boxed{4}$.

- $a = -37$, $n = 10$.

  We know that we need to add n to a **4** times to get a number, 3, that is in the range $[0, 10)$. To be precise,
  $$-37 + 10 + 10 + 10 + 10 = -37 + 40 = 3 \in [0, 10).$$
  Therefore, the quotient is $\boxed{-4}$ and the remainder is $\boxed{3}$.

- $a = -15$, $n = 60$.

  We have to add n to a **1** time to get $45 \in [0, 60)$. Therefore, the quotient is $\boxed{01}$ and the remainder is $\boxed{45}$.

- $a = 13$, $n = 12$.

  We know that $13/12 = 1$ and $13 - (12 \cdot 1) = 1$. So, the quotient is $\boxed{1}$ and the remainder is $\boxed{1}$.

Proposition. *Suppose a and n are integers and $n > 0$. All the following statements are equivalent:*

- $a \pmod n = 0$.
- *There is no remainder when a is divided by n.*
- *a is a multiple of n.*
- *a is divisible by n.*
- *n is a divisor of a.*
- *n is a factor of a.*
- *n divides a (in notation[1]: $n|a$).*
- *a/n is an integer.*

[1] Note that | is read as "*divides*."

1.1.2 Congruences

Definition 1.1: Congruence

Fix a positive integer n. If a and b are integers, we say that "a is **congruent** to b mod n," or that "a and b are congruent mod n," if a and b have the same remainder when each is divided by n. This can be denoted in symbols as follows:

$$a \equiv b \pmod{n}.$$

For example, $19 \equiv 7 \pmod{4}$ since 19 and 7 both have remainder 3 when divided by 4. Observe also that $19 - 7 = 12$ is a multiple of 4. This can be generalized:

Lemma 1.2

Fix a positive integer n. Two integers a and b are congruent mod n if and only if $a - b$ is a multiple of n.

Proof. Divide a and b by n to write $a = q_1 n + r_1$ and $b = q_2 n + r_2$. If

$$a \equiv b \pmod{n},$$

this by definition means that $r_1 = r_2$ so

$$a - b = (q_1 n + r_1) - (q_2 n + r_2) = q_1 n - q_2 n = n(q_1 - q_2).$$

So, $a - b$ is a multiple of n. Conversely, suppose $a - b$ is a multiple of n. Then,

$$(a - b) - (q_1 - q_2)n = ((q_1 n + r_1) - (q_2 n + r_2)) - (q_1 - q_2)n = r_1 - r_2$$

is a multiple of n. Since $0 \le r_1, r_2 < n$, however, we must have $|r_1 - r_2| < n$. The only way that $r_1 - r_2$ can be a multiple of n is if $r_1 - r_2 = 0$, i.e., if $r_1 = r_2$. That means $a \equiv b \pmod{n}$. $\square$

Theorem 1.1: Modular Arithmetic Theorem

Fix a positive integer n. Suppose a, a', b, b' are integers such that

$$a \equiv a' \pmod{n}$$

$$b \equiv b' \pmod{n}$$

and k is any positive integer. Then, all of the following are also true:

$$a + b \equiv a' + b' \pmod{n}$$

$$a - b \equiv a' - b' \pmod{n}$$

$$ab \equiv a'b' \pmod{n}$$

$$a^k \equiv (a')^k \pmod{n}$$

(Exercise.) Use the Modular Arithmetic Theorem to quickly calculate the following.

- $417 \cdot 22 \pmod{10}$.

$$\begin{aligned} 417 \cdot 22 &\equiv 7 \cdot 2 \\ &= 14 \\ &\equiv 4 \pmod{10}. \end{aligned}$$

- $333333 + 666 \pmod 3$.

$$\begin{aligned} 333333 + 666 &\equiv 0 + 0 \\ &\equiv 0 \pmod 3. \end{aligned}$$

- $7^{202320232023} \pmod 6$.

$$\begin{aligned} 7^{202320232023} &= 7 \cdot 7 \cdot \ldots \cdot 7 \\ &\equiv 1 \cdot 1 \cdot \ldots \cdot 1 \\ &= 1 \pmod 6. \end{aligned}$$

(Exercise.) Fix positive integers k and n. Suppose a and a' are integers such that $a \equiv a' \pmod n$. It is not true in general that $k^a \equiv k^{a'} \pmod n$. Show this by example: in other words, find k, n, a, and a' such that $a \equiv a' \pmod n$ but $k^a \not\equiv k^{a'} \pmod n$.

Let $k = 2$, $n = 5$, $a = 6$, and $a' = 1$ so that

$$6 \equiv 1 \pmod 5.$$

Then, we note that

$$k^a = 2^6 = 64$$

and

$$k^{a'} = 2^1 = 2.$$

From this, it's clear that

$$64 \not\equiv 2 \pmod 5.$$

(Exercise.) *Suppose that the number $273x49y5$, where x and y are unknown digits, is divisible by 495. Find x and y.*

We are asked to solve

$$273x49y5 \equiv 0 \mod 495.$$

We can write $273x49y5$ as

$$20000000 + 7000000 + 300000 + 10000x + 4000 + 900 + 10000y + 5.$$

With this in mind, we have

$$\begin{aligned} 20000000 + 7000000 + 300000 + 10000x + 4000 + 900 + 10y + 5 \\ &\equiv 20 + 205 + 30 + 100x + 40 + 405 + 10y + 5 \\ &= 705 + 100x + 10y \\ &\equiv 210 + 100x + 10y \mod 495. \end{aligned}$$

We note that the next multiple of 495 is 990. So, effectively, we want to find some x and y such that $0 \le x < 10$ and $0 \le y < 10$ and

$$210 + 100x + 10y = 990.$$

This gives us

$$100x + 10y = 780.$$

One obvious solution is $x = 7$ and $y = 8$.

1.1.3 Revisiting the Caesar Cipher

Suppose we identify the letters A through Z with the numbers 0 through 25. In other words, we have $A \mapsto 0$, $B \mapsto 1$, and so on. Suppose we want to apply the Caesar cipher with a shift of 5 to encrypt the letter Y. Consider the following

$$E(x) = (x + 5) \pmod{26}.$$

We note that Y corresponds to the number 24. Then, it follows that

$$E(24) = (24 + 5) \pmod{26} = 29 \pmod{26} = 3.$$

The number 3 corresponds to the letter D, the desired result. In other words, if we can identify the letters with numbers, the function E is the encryption function of the Caesar cipher with a shift of 5.

The decryption function is given by

$$D(y) = (y - 5) \pmod{26}.$$

So, if we wanted to decrypt the letter D, which corresponds to the number 3, then

$$D(3) = (3 - 5) \pmod{26} = -2 \pmod{26} = 24,$$

which corresponds to Y.

What we just did is actually a consequence of the Modular Arithmetic Theorem; for a quick little "proof," notice how

$$\begin{aligned} D(E(x)) &= D(y) \\ &\equiv (y - 5) \pmod{26} \\ &\equiv ((x + 5) - 5) \pmod{26} \\ &= x. \end{aligned}$$