

Lecture 3: The Ring of Integers Modulo n

Instructor: Chao Qin

Notes written by: Wenhao Tong and Yingshu Wang

Theorem (Chinese Remainder Theorem). *Let $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{N}$ such that $\gcd(n, m) = 1$. Then there exists $x \in \mathbb{Z}$ such that*

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n}. \end{aligned}$$

Moreover x is unique modulo mn .

Proof. If we can solve for t in the equation

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

then $x = a + tm$ will satisfy both congruences. To see that we can solve, subtract a from both sides and use Unit Proposition together with our assumption that $\gcd(n, m) = 1$ to see that there is a solution.

For uniqueness, suppose that x and y solve both congruences. Then $z = x - y$ satisfies $z \equiv 0 \pmod{m}$ and $z \equiv 0 \pmod{n}$, so $m \mid z$ and $n \mid z$. Since $\gcd(n, m) = 1$, it follows that $nm \mid z$, so $x \equiv y \pmod{nm}$. \square

Lemma. *Suppose that $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$. Then the map*

$$\psi : (\mathbb{Z}/mn\mathbb{Z})^* \rightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*. \quad (1)$$

defined by

$$\psi(c) = (c \bmod m, c \bmod n)$$

is a bijection.

Definition (Multiplicative Function). *A function $f : \mathbb{N} \rightarrow \mathbb{C}$ is multiplicative if, whenever $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$, we have*

$$f(mn) = f(m) \cdot f(n).$$

Proposition (Multiplicativity of φ). *The function φ is multiplicative.*

Proof. The map ψ of Lemma is a bijection, so the set on the left in (1) has the same size as the product set on the right in (1). Thus

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

□

Proposition (Extended Euclidean Representation). *Suppose $a, b \in \mathbb{Z}$ and let $g = \gcd(a, b)$. Then there exists $x, y \in \mathbb{Z}$ such that*

$$ax + by = g.$$

Proof of Euclid Proposition. Let $g = \gcd(a, b)$. Then $\gcd(a/g, b/g) = 1$, so by Solvability Proposition, the equation

$$\frac{a}{g} \cdot x \equiv 1 \pmod{\frac{b}{g}} \quad (2)$$

has a solution $x \in \mathbb{Z}$. Multiplying (2) through by g yields $ax \equiv g \pmod{b}$, so there exists y such that $b \cdot (-y) = ax - g$. Then $ax + by = g$, as required. □

Example 1. *Suppose $a = 5$ and $b = 7$. Here we underline certain numbers, because it clarifies the subsequent back substitution we will use to find x and y .*

$$\begin{array}{ll} \underline{7} = 1 \cdot \underline{5} + \underline{2} & \text{so } \underline{2} = \underline{7} - \underline{5} \\ \underline{5} = 2 \cdot \underline{2} + \underline{1} & \text{so } \underline{1} = \underline{5} - 2 \cdot \underline{2} = \underline{5} - 2(\underline{7} - \underline{5}) = 3 \cdot \underline{5} - 2 \cdot \underline{7} \end{array}$$

On the right, we have back-substituted in order to write each partial remainder as a linear combination of a and b . In the last step, we obtain $\gcd(a, b)$ as a linear combination of a and b , as desired.

Example 2. *That example was not too complicated, so we try another one. Let $a = 130$ and $b = 61$. We have*

$$\begin{array}{ll} \underline{130} = 2 \cdot \underline{61} + \underline{8} & \underline{8} = \underline{130} - 2 \cdot \underline{61} \\ \underline{61} = 7 \cdot \underline{8} + \underline{5} & \underline{5} = -7 \cdot \underline{130} + 15 \cdot \underline{61} \\ \underline{8} = 1 \cdot \underline{5} + \underline{3} & \underline{3} = 8 \cdot \underline{130} - 17 \cdot \underline{61} \\ \underline{5} = 1 \cdot \underline{3} + \underline{2} & \underline{2} = -15 \cdot \underline{130} + 32 \cdot \underline{61} \\ \underline{3} = 1 \cdot \underline{2} + \underline{1} & \underline{1} = 23 \cdot \underline{130} - 49 \cdot \underline{61} \end{array}$$

Thus $x = 23$ and $y = -49$ is a solution to $130x + 61y = 1$.

Example 3. Solve $17x \equiv 1 \pmod{61}$. First, we use Euclid Algorithm to find x, y such that $17x + 61y = 1$:

$$\begin{array}{ll} \underline{61} = 3 \cdot \underline{17} + \underline{10} & \underline{10} = \underline{61} - 3 \cdot \underline{17} \\ \underline{17} = 1 \cdot \underline{10} + \underline{7} & \underline{7} = -\underline{61} + 4 \cdot \underline{17} \\ \underline{10} = 1 \cdot \underline{7} + \underline{3} & \underline{3} = 2 \cdot \underline{61} - 7 \cdot \underline{17} \\ \underline{3} = 2 \cdot \underline{3} + \underline{1} & \underline{1} = -5 \cdot \underline{61} + 18 \cdot \underline{17} \end{array}$$

Thus $17 \cdot 18 + 61 \cdot (-5) = 1$ so $x = 18$ is a solution to $17x \equiv 1 \pmod{61}$.

Theorem (Pseudoprimality). An integer $p > 1$ is prime if and only if for every $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. If p is prime, then the statement follows from Fermat's Little Theorem. If p is composite, then there is a divisor a of p with $2 \leq a < p$. If $a^{p-1} \equiv 1 \pmod{p}$, then $p \mid a^{p-1} - 1$. Since $a \mid p$, we have $a \mid a^{p-1} - 1$, hence there exists an integer k such that $ak = a^{p-1} - 1$. Subtracting, we see that $a^{p-1} - ak = 1$, so $a(a^{p-2} - k) = 1$. This implies that $a \mid 1$, which is a contradiction since $a \geq 2$. \square

Example 4. Is $p = 323$ prime? We compute $2^{322} \pmod{323}$. Making a table as above, we have

i	m	ε_i	$2^{2^i} \pmod{323}$
0	322	0	2
1	161	1	4
2	80	0	16
3	40	0	256
4	20	0	290
5	10	0	120
6	5	1	188
7	2	0	137
8	1	1	35

Thus

$$2^{322} \equiv 4 \cdot 188 \cdot 35 \equiv 157 \pmod{323},$$

so 323 is not prime, though this computation gives no information about how 323 factors as a product of primes. In fact, one finds that $323 = 17 \cdot 19$.