Number theory and Cryptography May 9th, 2024

Lecture 2 : Congruences Modulo n

Instructor: Chao Qin *Notes written by: Wenhao Tong and Yingshu Wang*

Definition (Group)**.** *A* group *is a set G equipped with a binary operation $G \times G \to G$ (denoted by multiplication below) and an identity element $1 \in G$ such that:*

1. *For all $a, b, c \in G$, we have $(ab)c = a(bc)$.*
2. *For each $a \in G$, we have $1a = a1 = a$, and there exists $b \in G$ such that $ab = 1$.*

Definition (Abelian Group)**.** *An* abelian group *is a group G such that $ab = ba$ for every $a, b \in G$.*

Definition (Ring)**.** *A* ring *R is a set equipped with binary operations $+$ and $\times$ and elements $0, 1 \in R$ such that R is an abelian group under $+$, and for all $a, b, c \in R$ we have*

- $1a = a1 = a$
- $(ab)c = a(bc)$
- $a(b + c) = ab + ac$.

If, in addition, $ab = ba$ for all $a, b \in R$, then we call R a commutative ring.

Definition (Integers Modulo n)**.** *The ring n of integers modulo n is the set of equivalence classes of integers modulo n. It is equipped with its natural ring structure:*

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (a \cdot b) + n\mathbb{Z}.$$

Example 1. *For example,*

$$Z/3Z = \{\{\ldots, -3, 0, 3, \ldots\}, \{\ldots, -2, 1, 4, \ldots\}, \{\ldots, -1, 2, 5, \ldots\}\}$$

Definition (Field)**.** *A field K is a ring such that for every nonzero element $a \in K$ there is an element $b \in K$ such that $ab = 1$.*

For example, if p is a prime, then p is a field

Definition (Reduction Map and Lift)**.** *We call the natural reduction map $\mathbb{Z} \to n\mathbb{Z}$, which sends a to $a + nZ$, reductionmodulo n. We also say that a is a lift of $a + n\mathbb{Z}$. Thus, e.g., 7 is a lift of 1 mod 3, since $7 + 3\mathbb{Z} = 1 + 3\mathbb{Z}$.*

We can use that arithmetic in n is well defined to derive tests for divisibility by n

Theorem. *A number $n \in \mathbb{Z}$ is divisible by 3 if and only if the sum of the digits ofn is divisible by 3.*

Theorem (Cancellation)**.** *If $gcd(c, n) = 1$ and*

$$ac \equiv bc \pmod{n},$$

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

Proof. By definition

$$n \mid ac - bc = (a - b)c.$$

Since $\gcd(n, c) = 1$, it follows from FTA that $n \mid a - b$, so

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

as claimed. □

Definition (Complete Set of Residues)**.** *We call a subset $R \subset \mathbb{Z}$ of size n whose reductions modulo n are pairwise distinct from a completesetofresidues modulo n. In other words, a complete set of residues is a choice of representative for each equivalence class in $\mathbb{Z}/n\mathbb{Z}$.*

Lemma. *If R is a complete set of residues modulo n and $a \in Z$ with $\gcd(a, n) = 1$, then $aR = \{ax : x \in R\}$ is also a complete set of residues modulo n.*

Theorem (Units)**.** *If $\gcd(a, n) = 1$, then the equation $ax \equiv b \pmod{n}$ has a solution, and that solution is unique modulo n.*

Proof. Let R be a complete set of residues modulo n, so there is a unique element of R that is congruent to b modulo n. By Lemma2.1.12, aR is also a complete set of residues modulo n, so there is a unique element $ax \in aR$ that is congruent to b modulo n, and we have $ax \equiv b \pmod{n}$. □

Theorem (Solvability)**.** *The equation* $ax \equiv b \pmod{n}$ *has a solution if and only if* $\gcd(a, n)$ *divides* b*.*

Definition (Order of an Element)**.** *Let* $n \in \mathbb{N}$ *and* $x \in \mathbb{Z}$ *and suppose that* $\gcd(x, n) = 1$*. The* order *of* x *modulo* n *is the smallest* $m \in \mathbb{N}$ *such that*

$$x^m \equiv 1 \pmod{n}.$$

Definition (Euler's φ-function)**.** *For* $n \in \mathbb{N}$*, let*

$$\varphi(n) = \#\{a \in N : a \leq n \text{ and } \gcd(a, n) = 1\}.$$

For example,

$$\begin{aligned} \varphi(1) &= \#\{1\} = 1, \\ \varphi(2) &= \#\{1\} = 1, \\ \varphi(5) &= \#\{1, 2, 3, 4\} = 4, \\ \varphi(12) &= \#\{1, 5, 7, 11\} = 4. \end{aligned}$$

Theorem (Euler's Theorem)**.** *If* $\gcd(x, n) = 1$*, then*

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Theorem. *An integer* $p > 1$ *is prime if and only if* $(p-1)! \equiv -1 \pmod{p}$.

For example, if $p = 3$, then $(p-1)! = 2 \equiv -1 \pmod{3}$. If $p = 17$, then

$$(p-1)! = 20922789888000 \equiv -1 \pmod{17}.$$

But if $p = 15$, then

$$(p-1)! = 87178291200 \equiv 0 \pmod{15},$$

so 15 is composite. Thus Wilson's theorem could be viewed as a primality test, though, from a computational point of view, it is probably one of the world's **least efficient** primality tests since computing $(n-1)!$ takes so many steps.