Number theory and Cryptography May 16th, 2024

Lecture 4: Structure of $\mathbb{Z}/p\mathbb{Z}$

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

Definition (Primitive Root)**.** *A* primitive root *modulo an integer n is an element of $(\mathbb{Z}/n\mathbb{Z})^*$ of order $\varphi(n)$.*

Proposition. *Let p be a prime number and let d be a divisor of $p-1$. Then $f = x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ has exactly d roots in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Let $e = (p-1)/d$. We have

$$\begin{aligned} x^{p-1} - 1 &= (x^d)^e - 1 \\ &= (x^d - 1)((x^d)^{e-1} + (x^d)^{e-2} + \cdots + 1) \\ &= (x^d - 1)g(x), \end{aligned}$$

where $g \in (\mathbb{Z}/p\mathbb{Z})[x]$ and $\deg(g) = de - d = p-1-d$. Fetmat's Little Theorem implies that $x^{p-1} - 1$ has exactly $p-1$ roots in $\mathbb{Z}/p\mathbb{Z}$, since every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ is a root! Since g has *at most* $p-1-d$ roots and $x^d - 1$ has at most d roots. Since a root of $(x^d-1)g(x)$ is a root of either $x^d - 1$ or $g(x)$ and $x^{p-1} - 1$ has $p-1$ roots, g must have exactly $p-1-d$ roots and $x^d - 1$ must have exactly d roots, as claimed. □

Lemma. *Suppose $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ have orders r and s, respectively, and that* $\gcd(r, s) = 1$*. Then ab has order rs.*

Theorem (Primitive Roots)**.** *There is a primitive root modulo any prime p. In particular, the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.*

Example 1. *We illustrate the proof of Theorem when $p = 13$. We have*

$$p - 1 = 12 = 2^2 \cdot 3.$$

The polynomial $x^4 - 1$ has roots $\{1, 5, 8, 12\}$ and $x^2 - 1$ has roots $\{1, 12\}$, so we may take $a_1 = 5$. The polynomial $x^3 - 1$ has roots $\{1, 3, 9\}$, and we set $a_2 = 3$. Then $a = 5 \cdot 3 = 15 \equiv 2$ is a primitive root. To verify this, note that the successive powers of $2 \pmod{13}$ *are*

$$2,\ 4,\ 8,\ 3,\ 6,\ 12,\ 11,\ 9,\ 5,\ 10,\ 7,\ 1.$$

Example 2. *Theorem is false if, for example, p is replaced by a power of* 2 *bigger than* 4*. For example, the four elements of* $(\mathbb{Z}/8\mathbb{Z})^*$ *each have order dividing* 2*, but* $\varphi(8) = 4$*.*

Theorem (Primitive Roots mod p^n)**.** *Let* p^n *be a power of an odd prime. Then there is a primitive root modulo* p^n*.*

Proposition (Number of Primitive Roots)**.** *If there is a primitive root modulo n, then there are exactly* $\varphi(\varphi(n))$ *primitive roots modulo n.*

Proof. The primitive roots modulo n are the generators of $(\mathbb{Z}/n\mathbb{Z})^*$, which by assumption is cyclic of order $\varphi(n)$. Thus they are in bijection with the generators of any cyclic group of order $\varphi(n)$. In particular, the number of primitive roots modulo n is the same as the number of elements of $\mathbb{Z}/\varphi(n)\mathbb{Z}$ with additive order $\varphi(n)$. An element of $\mathbb{Z}/\varphi(n)\mathbb{Z}$ has additive order $\varphi(n)$ if and only if it is coprime to $\varphi(n)$. There are $\varphi(\varphi(n))$ such elements, as claimed. □

Example 3. *For example, there are* $\varphi(\varphi(17)) = \varphi(16) = 2^4 - 2^3 = 8$ *primitive roots mod* 17*, namely* $3, 5, 6, 7, 10, 11, 12, 14$*. The* $\varphi(\varphi(9)) = \varphi(6) = 2$ *primitive roots modulo* 9 *are* 2 *and* 5*. There are no primitive roots modulo* 8*, even though* $\varphi(\varphi(8)) = \varphi(4) = 2 > 0$*.*