Scribe Notes for *Algorithmic Number Theory*
Class 13—June 4, 1998

Scribes: Cara Struble and Craig Struble

Abstract

Today we finish Chapter 5, covering Sections 5.6 on the multiplicative structure of $\mathbb{Z}/(n)^*$, 5.7 on quadratic residues, and 5.8 on the Legendre symbol.

1 The Multiplicative Structure of $(\mathbb{Z}/(n))^*$

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the prime factors of n. Since $\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{e_1}) \oplus \mathbb{Z}/(p_2^{e_2}) \oplus \cdots \oplus \mathbb{Z}/(p_k^{e_k})$ as rings, we have this isomorphism of the multiplicative group:

$$(\mathbb{Z}/(n))^* \cong (\mathbb{Z}/(p_1^{e_1}))^* \times (\mathbb{Z}/(p_2^{e_2}))^* \times \cdots \times (\mathbb{Z}/(p_k^{e_k}))^*.$$

Example 1.1. $n = 60 = 2^2 \cdot 3 \cdot 5$, $\phi(60) = 16$, $\phi(4) = 2$, $\phi(3) = 2$, $\phi(5) = 4$

$(\mathbb{Z}/(60))^*$	$\cong$	$(\mathbb{Z}/(4))^*$	$\times$	$(\mathbb{Z}/(3))^*$	$\times$	$(\mathbb{Z}/(5))^*$
$\overline{1}$		$\overline{1}$		$\overline{1}$		$\overline{1}$
$\overline{7}$		$\overline{3}$		$\overline{1}$		$\overline{2}$
$\overline{11}$		$\overline{3}$		$\overline{2}$		$\overline{1}$
$\overline{13}$		$\overline{1}$		$\overline{1}$		$\overline{3}$
$\overline{17}$		$\overline{1}$		$\overline{2}$		$\overline{2}$
$\overline{19}$		$\overline{3}$		$\overline{1}$		$\overline{4}$
$\overline{23}$		$\overline{3}$		$\overline{2}$		$\overline{3}$
$\overline{29}$		$\overline{1}$		$\overline{2}$		$\overline{4}$
$\overline{31}$		$\overline{3}$		$\overline{1}$		$\overline{1}$
$\overline{37}$		$\overline{1}$		$\overline{1}$		$\overline{2}$
$\overline{41}$		$\overline{1}$		$\overline{2}$		$\overline{1}$
$\overline{43}$		$\overline{3}$		$\overline{1}$		$\overline{3}$
$\overline{47}$		$\overline{3}$		$\overline{2}$		$\overline{2}$
$\overline{49}$		$\overline{1}$		$\overline{1}$		$\overline{4}$
$\overline{53}$		$\overline{1}$		$\overline{2}$		$\overline{3}$
$\overline{59}$		$\overline{3}$		$\overline{2}$		$\overline{4}$

Hence, it suffices to consider $G = (\mathbb{Z}/(p^e))^*$ where p is prime and $e \geq 1$. G has $\phi(p^e) = p^{e-1}(p-1)$ elements.
If $e = 1$, then G is a cyclic group.
If $p \geq 3$, then G is a cyclic group.
If $p = 2$ and $e = 2$, then G is cyclic and generated by $\overline{3}$.
If $p = 2$ and $e \geq 3$, then $G \cong C_2 \times C_{2^{e-2}}$, where C_2 is a cyclic group of order 2 and $C_{2^{e-2}}$ is a cyclic group of order 2^{e-2}.

Example 1.2. This is an example of the last case above. Consider $(\mathbb{Z}/(8))^*$. Here $p = 2$ and $e = 3$. We have

$(\mathbb{Z}/(8))^*$	$\cong$	$(\mathbb{Z}/(2))^*$	$\times$	$(\mathbb{Z}/(2))^*$
$\overline{1}$		$\overline{1}$		$\overline{1}$
$\overline{3}$		$\overline{3}$		$\overline{1}$
$\overline{5}$		$\overline{1}$		$\overline{5}$
$\overline{7}$		$\overline{3}$		$\overline{5}$

$\overline{3}, \overline{5}, \overline{7}$ are all of order 2. We get 3 subgroups of order 2: $\{\overline{1}, \overline{3}\}, \{\overline{1}, \overline{5}\}, \text{and}\{\overline{1}, \overline{7}\}$. The direct product of any two of these gives $(\mathbb{Z}/(8))^*$.

Now we present a proof of the first case above: If $e = 1$ then G is a cyclic group. This is exercises 14 through 18 in Chapter 5.

Proof. View $\mathbb{Z}/(p)$ as a field. Any polynomial of degree d over $\mathbb{Z}/(p)$ has at most d roots. The polynomial $X^{p-1} - 1$ over $\mathbb{Z}/(p)$ has exactly $p - 1$ roots by Fermat's Theorem. If $d|(p-1)$ then $(X^d - 1)|(X^{p-1} - 1)$ because

$$X^{p-1} - 1 = (X^d - 1) \sum_{i=0}^{\frac{p-1}{d}-1} X^{di}.$$

Hence $X^d - 1$ has exactly d roots in $\mathbb{Z}/(p)$. If $q^e|(p-1)$ where q is prime and $e \geq 1$, then we show by induction that $(\mathbb{Z}/(p))^*$ contains an element of order q^e.
$X^q - 1$ has q roots, all but 1 have order q.
$X^{q^2} - 1$ has q^2 roots, $q^2 - q$ have order q^2.
$\vdots$
$X^{q^e} - 1$ has q^e roots, $q^e - q^{e-1}$ have order q^e.

Let $p - 1 = q_1^{e_1} q_2^{e_2} \dots q_k^{e_k}$ be the prime factorization of $p - 1$. Choose for each i, $1 \leq i \leq k$, an element $q_i \in (\mathbb{Z}/(p))^*$ of order $q_i^{e_i}$. Then $g_1 g_2 \dots g_k$ has order $p - 1$ in $(\mathbb{Z}/(p))^*$. So $(\mathbb{Z}/(p))^*$ is cyclic and has $\phi(p-1)$ generators. □

2 Quadratic Residues

Definition 5.7.1 in the text defines an m^{th} power reside (mod n). Suppose $m, n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ with gcd(a,n) = 1. Then a is an m^{th} **power residue (mod n)** if there is an x such that $x^m \equiv a$ (mod n). Alternatively, $\overline{a}$ has an m^{th} root in $(\mathbb{Z}/(n))^*$.

Special case: Suppose p is prime and gcd(m,$p-1$) = 1. Look at the m^{th} power map

$$f : (\mathbb{Z}/(p))^* \to (\mathbb{Z}/(p))^*$$

defined by $f(\overline{c}) = \overline{c}^m$. This is a permutation of $(\mathbb{Z}/(p))^*$ since $(\mathbb{Z}/(p))^*$ is a cyclic group of order relatively prime to m. Every element of $(\mathbb{Z}/(p))^*$ has a unique m^{th} root.

Example 2.1. $p = 7, p - 1 = 2 \cdot 3, m = 5$ The following table shows the application of the fifth power map to $\overline{c}$.

$\overline{c}$	$\overline{c}^5$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{5}$
$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{3}$
$\overline{6}$	$\overline{6}$

Theorem 2.2 (Theorem 5.7.2). *Suppose* $(\mathbb{Z}/(n))^*$ *is cyclic and* $\gcd(a, n) = 1$. *Then, a is an* m^{th} *power residue modulo n if and only if*

$$a^{\varphi(n)/d} \equiv 1 \pmod{n},$$

where $d = \gcd(m, \varphi(n))$.

Proof. Write $m = dk$. If a has a d^{th} root modulo n, called b, then $b^d \equiv a \pmod{n}$ and $b^{\varphi(n)} \equiv 1 \pmod{n}$ by the Euler-Fermat theorem. So $a^{\varphi(n)/d} \equiv 1 \pmod{n}$.

Conversely, if $a^{\varphi(n)/d} \equiv 1 \pmod{n}$, then a has a d^{th} root modulo n. This is because $(\mathbb{Z}/(n))^*$ is cyclic with order $\phi(n)$. Take a generator γ for $(\mathbb{Z}/(n))^*$, which must have order $\phi(n)$. Then $a = \gamma^z$ where z is divisible by d. Then $\gamma^{z/d}$ is a d^{th} root of a.

We have $\gcd(k, \varphi(n)) = 1$. The map $\alpha \to \alpha^k$ is a permutation. Hence a has an m^{th} root modulo n. □

Suppose $\gcd(a, n) = 1$. Then a is a **quadratic residue** $\pmod{n}$ if a is a second power residue $\pmod{n}$, and otherwise a is a **quadratic nonresidue**.

Corollary 2.3 (Corollary 5.7.3: Euler's Criterion). *Let p be an odd prime and a be such that* $\gcd(a, p) = 1$. *Then, a is a quadratic residue modulo p if*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

and is a quadratic nonresidue $\pmod{p}$ *if*

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Corollary 2.4 (Corollary 5.7.4). *There are* $(p-1)/2$ *quadratic residues and* $(p-1)/2$ *quadratic nonresidues modulo an odd prime p.*

Example 2.5. Let $p = 11$. The following table shows the squares modulo 11.

a	$a^2 \pmod{11}$
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

We see that the quadratic residues $\pmod{11}$ are $\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$ and the quadratic nonresidues modulo 11 are $\{\overline{2}, \overline{6}, \overline{7}, \overline{8}, \overline{10}\}$.

Corollary 2.6 (Corollary 5.7.5). *We can find a quadratic nonresidue* $\pmod{p}$ *with a Las Vegas algorithm with expected* $O((\lg p)^2)$ *bit operations.*

3 Legendre Symbol

Let $a \in \mathbb{Z}$ and p be an odd prime. The **Legendre symbol** is notation useful for summations and other functions counting quadratic residues, and is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue;} \\ -1, & \text{if } a \text{ is a quadratic nonresidue;} \\ 0, & \text{if } p \mid a. \end{cases}$$

The following theorem provides ways of computing the Legendre symbol

Theorem 3.1 (Theorem 5.8.1). *Let p and q be odd primes. Then*

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$; *(Euler's Criterion)*
   $$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}; \end{cases}$$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$;
3. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *if* $a \equiv b \pmod{p}$;
4. $$\left(\frac{a^2}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a; \\ 0 & \text{if } p \mid a; \end{cases}$$
5. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$;

6. If $p \neq q$*, then* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Example 3.2. Using Theorem 5.8.1, we compute the Legendre symbol $\left(\frac{105}{11}\right)$.

$$\begin{aligned}
\left(\frac{105}{11}\right) &= \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) && (\textit{Rules } 3,\ 2)\\
&= \left(\frac{-8}{11}\right)(-1)^{(11^2-1)/8} && (\textit{Rules } 3,\ 5)\\
&= \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)\left(\frac{4}{11}\right)(-1) && (\textit{Rule } 2)\\
&= (-1)(-1)(1)(-1) = -1. && (\textit{Rules } 1,\ 2,\ 4)
\end{aligned}$$

Example 3.3. Using Theorem 5.8.1, we compute the Legendre symbol $\left(\frac{11}{13}\right)$.

$$\begin{aligned}
\left(\frac{11}{13}\right) &= \left(\frac{13}{11}\right)(-1)^{\frac{13-1}{2}\frac{11-1}{2}} && (\textit{Rule } 6)\\
&= \left(\frac{2}{11}\right) = -1. && (\textit{Rules } 3,\ 5)
\end{aligned}$$

Example 3.4. Using Theorem 5.8.1, we compute the Legendre symbol $\left(\frac{11}{19}\right)$.

$$\begin{aligned}
\left(\frac{11}{19}\right) &= \left(\frac{19}{11}\right)(-1)^{\frac{19-1}{2}\frac{11-1}{2}} && (\textit{Rule } 6)\\
&= \left(\frac{6}{11}\right)(-1) = (-1)(-1) = 1. && (\textit{Rule } 3)\\
7^2 = 49 &\equiv 11 \pmod{19}.
\end{aligned}$$