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

\[
\begin{array}{cccc}
\mathbb{Z}/(60)^* & \cong & (\mathbb{Z}/(4))^* & \times \ (\mathbb{Z}/(3))^* & \times \ (\mathbb{Z}/(5))^* \\
1 & 1 & 1 & 1 \\
7 & 3 & 1 & 2 \\
11 & 3 & 2 & 1 \\
13 & 1 & 1 & 3 \\
17 & 1 & 2 & 4 \\
19 & 3 & 2 & 3 \\
23 & 3 & 2 & 3 \\
29 & 1 & 2 & 1 \\
31 & 3 & 1 & 1 \\
37 & 1 & 1 & 2 \\
41 & 1 & 2 & 1 \\
43 & 3 & 1 & 3 \\
47 & 3 & 2 & 5 \\
49 & 1 & 1 & 4 \\
53 & 1 & 2 & 3 \\
59 & 3 & 2 & 4 \\
\end{array}
\]

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 \( 3 \).
- 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

\[
(\mathbb{Z}/(8))^* \cong (\mathbb{Z}/(2))^* \times (\mathbb{Z}/(2))^*
\]

\[
\begin{array}{ccc}
\overline{1} & \overline{1} & \overline{1} \\
\overline{3} & \overline{3} & \overline{1} \\
\overline{5} & \overline{1} & \overline{5} \\
\overline{7} & \overline{3} & \overline{5}
\end{array}
\]

\(\overline{3}, \overline{5}, \overline{7}\) 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 \(X^{p-1} - 1 \text{ over } \mathbb{Z}/(p)\) has exactly \(p - 1\) roots by Fermat's Theorem. If \(d\) divides \((p - 1)\) then \((X^d - 1)(X^{p-1} - 1)\) because

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

Hence \(X^d - 1\) has exactly \(d\) roots in \(\mathbb{Z}/(p)\). If \(q^e\) divides \((p - 1)\) 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 \(p - 1 = q_1^{\xi_1} q_2^{\xi_2} \cdots q_k^{\xi_k}\) 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 \(q_i^{\xi_i}\). Then \(g_1 g_2 \cdots g_k\) has order \(p - 1\) in \((\mathbb{Z}/(p))^*\). So \((\mathbb{Z}/(p))^*\) is cyclic and has \(\phi(p - 1)\) generators.

\section{Quadratic Residues}

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

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

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

defined by \(f(\overline{a}) = \overline{a}^m\). 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 \(m\textsuperscript{th}\) 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 $\mathbb{F}$.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

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

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

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 $a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n}$.

Conversely, if $a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod{n}$, then $a$ has a $d^{th}$ root modulo $n$. This is because $(\mathbb{Z}/(n))^*$ is cyclic with order $\phi(n)$. Take a generator $\gamma$ 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

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$
<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^2 \pmod{11}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>

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

**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. $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p};$  \hspace{1cm} (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. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$;

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 \( \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \).

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

\[
\left( \frac{105}{11} \right) = \left( \frac{6}{11} \right) = \left( \frac{2}{11} \right) \left( \frac{3}{11} \right) \quad (\text{Rules 3, 2})
\]
\[
= \left( \frac{-8}{11} \right) (-1)^{(11^2-1)/8} \quad (\text{Rules 3, 5})
\]
\[
= \left( \frac{-1}{11} \right) \left( \frac{2}{11} \right) \left( \frac{4}{11} \right) (-1) \quad (\text{Rule 2})
\]
\[
= (-1)(-1)(1)(-1) = -1. \quad (\text{Rules 1, 2, 4})
\]

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

\[
\left( \frac{11}{13} \right) = \left( \frac{13}{11} \right) (-1)^{\frac{13-1}{2} \cdot \frac{11-1}{2}} \quad (\text{Rule 6})
\]
\[
= \left( \frac{2}{11} \right) = -1. \quad (\text{Rules 3, 5})
\]

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

\[
\left( \frac{11}{19} \right) = \left( \frac{19}{11} \right) (-1)^{\frac{19-1}{2} \cdot \frac{11-1}{2}} \quad (\text{Rule 6})
\]
\[
= \left( \frac{6}{11} \right) (-1) = (-1)(-1) = 1. \quad (\text{Rule 3})
\]
\[
7^2 = 49 \equiv 11 \pmod{19}.
\]