§1. Some facts about $\mathbb{Z}/n\mathbb{Z}$

(1.1) Let $n \geq 2$ be a positive integer, and let

$$n = p_1^{e_1} \cdots p_a^{e_a}$$

be the primary factorization of $n$, where $p_1, \ldots, p_r$ are distinct prime numbers, and $e_1, \ldots, e_r \geq 1$ are positive integers. The Chinese Remainder Theorem asserts that the canonical map

$$\mathbb{Z}/n\mathbb{Z} \rightarrow (\mathbb{Z}/p_1^{e_1}) \times \cdots \times (\mathbb{Z}/p_r^{e_r})$$

is an isomorphism. Therefore we get a canonical isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/p_1^{e_1})^\times \times \cdots \times (\mathbb{Z}/p_r^{e_r})^\times$$

on the group of units.

(1.2) By definition, the Euler’s function $\phi$ has value $\phi(n) := \text{Card}((\mathbb{Z}/n\mathbb{Z})^\times)$ for every positive integer $n$. The Chinese remainder theorem tells us that $\phi$ is a multiplicative function: if $(m, n) = 1$, then $\phi(mn) = \phi(m) \phi(n)$. Consequently if $n = p_1^{e_1} \cdots p_a^{e_a}$ is the primary factorization of $n$, then

$$\phi(n) = (p_1 - 1) \cdots (p_a - 1) p_1^{e_1 - 1} \cdots p_a^{e_a - 1}.$$  

(1.3) Lemma (Fermat’s little theorem) Let $p$ be a prime number. Then $a^p \equiv a \pmod{p}$ for every integer $a$. Equivalently, $a^{p-1} \equiv 1 \pmod{p}$ for every integer $a$ with $(a, p) = 1$.

Proof. The group of units $\mathbb{F}_p^\times$ in $\mathbb{F}_p$ is a group with $p - 1$ elements. □

Fermat’s little theorem, although fairly easy from the point of view of group theory, is useful in elementary primality test: Given a natural number $n$, select a a relatively small number of natural numbers $a_i$ such that $a_i < n$ for each $i$, and test whether $a_i^{n-1} \equiv 1 \pmod{n}$. If $a_i^{n-1} \not\equiv 1 \pmod{n}$ for some $i$, then $n$ is not a prime number. On the other hand, if $a_i^{n-1} \equiv 1 \pmod{n}$ for each $i$, then one knows the chance for $n$ to be a prime number is quite good. Since computing $a_i^{n-1}$ modulo $n$ can be done quickly, this method provides a fast albeit unsophisticated probabilistic test for primality.
(1.4) For any prime number \( p > 0 \), the group \((\mathbb{Z}/p\mathbb{Z})^\times\) is a cyclic group of order \( p - 1 \). Actually this statement holds for all finite fields: The group of units for any finite field \( \mathbb{F}_q^\times \) is cyclic. The standard proof uses the fact that over any field \( k \), every polynomial of degree \( d > 0 \) with coefficients in \( k \) has at most \( d \) distinct roots in \( k \). Most “elementary” proofs uses this method in some disguise.

Let \( p \) be a prime number, \( e \geq 1 \). Consider the group \((\mathbb{Z}/p^e\mathbb{Z})^\times\) and its subgroup \((\mathbb{Z}/p^e\mathbb{Z})_1^\times\) of principal units, consisting of all elements of \( x \in (\mathbb{Z}/p^e\mathbb{Z})^\times \) with \( x \equiv 1 \pmod{p} \).

(1.5) Proposition

(i) Let \( p \) be an odd prime number. Then \((\mathbb{Z}/p^e\mathbb{Z})_1^\times\) is a cyclic group of order \( p^{e-1} \), generated by the element represented by \( 1 + p \).

(ii) For an odd prime number \( p \), the group \((\mathbb{Z}/p^e\mathbb{Z})^\times\) is cyclic of order \((p - 1)p^{e-1}\).

(iii) For the case \( p = 2 \), assume that \( e \geq 2 \). Then the subgroup \((\mathbb{Z}/2^e\mathbb{Z})_2^\times\) of \((\mathbb{Z}/2^e\mathbb{Z})^\times\) consisting of all elements \( x \in (\mathbb{Z}/2^e\mathbb{Z})^\times \) with \( x \equiv 1 \pmod{4} \) is cyclic order \( 2^{e-2} \). The element 5 is a generator of \((\mathbb{Z}/2^e\mathbb{Z})_2^\times\). The group \((\mathbb{Z}/2^e\mathbb{Z})_1^\times = (\mathbb{Z}/2^e\mathbb{Z})^\times\) is the direct product of \((\mathbb{Z}/2^e\mathbb{Z})_2^\times\) with \( \{\pm 1\} \).

When \( p \) is odd, the elements of \((\mathbb{Z}/p^e\mathbb{Z})^\times\) whose order divides \( p - 1 \) is the product of all Sylow-\( \ell \)-subgroups of \((\mathbb{Z}/p^e\mathbb{Z})^\times\), where \( \ell \) runs over all primes divisors of \( p - 1 \). It is a cyclic group of order \( p - 1 \) by Proposition 1.4.

§2. Sum of squares

(2.1) The equation \( x^2 + y^2 = z^2 \) is familiar from Pythagoras’s theorem. The identity \((a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2\) produces lots of integer solutions of the above equation, and all non-trivial integer solutions can be obtained this way.

(2.2) One question that traces back to the ancient time is: Which whole numbers are sum of two squares? In other words, given a positive number \( n \), we would like to know whether there exist integers \( x, y \) such that \( n = x^2 + y^2 \).

(2.3) Proposition

(i) Let \( p \) be an odd prime number. Then \( p \) is a sum of two squares if and only if \( p \equiv 1 \pmod{4} \).

(ii) Let \( n \) be a positive integer and let \( n = p_1^{e_1} \cdots p_a^{e_a} \) be its primary factorization. Then \( n \) is a sum of two squares if and only if \( e_i \equiv 0 \pmod{2} \) for each \( i \) with \( p_i \equiv 3 \pmod{4} \).
§3. The Legendre symbol

(3.1) Definition Let \( p \) be an odd prime number. For every \( a \in \mathbb{Z} \), define

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } \bar{a} \in (\mathbb{F}_p^\times)^2 \\
-1 & \text{if } \bar{a} \in (\mathbb{F}_p^\times \smallsetminus \mathbb{F}_p^\times)^2 \\
0 & \text{if } a \equiv 0 \pmod{p} 
\end{cases}
\]

The function \( \left( \frac{\cdot}{p} \right) \) is called the Legendre symbol for the prime number \( p \).

(3.2) Lemma Let \( p \) be an odd prime number.

(i) If \( a \in \mathbb{Z} \) and \( (a,p) = 1 \), then \( \left( \frac{a}{p} \right) = 1 \) if and only if

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

(ii) If \( a,b \in \mathbb{Z} \) and \( (ab,p) = 1 \), then

\[ \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right). \]

PROOF. The group \( \mathbb{F}_p^\times \) is a cyclic group of order \( p - 1 \).

The values of \( \left( \frac{-1}{p} \right) \) and \( \left( \frac{2}{p} \right) \) are given below.

(3.3) Corollary Let \( p \) be an odd prime number. Then

\[ \left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}. \]

In other words, \( \left( \frac{-1}{p} \right) = 1 \) if and only if \( a^{\frac{p-1}{2}} \equiv 0 \pmod{p} \).

(3.4) Proposition Let \( p \) be an odd prime number. Then

\[ \left( \frac{2}{p} \right) = (-1)^{\frac{p^2 - 1}{2}}. \]

In other words, \( \left( \frac{2}{p} \right) = 1 \) if and only if \( p \equiv \pm 1 \pmod{p} \).

Gauss’s famous quadratic reciprocity theorem gives an effective way to compute the Legendre symbol. He gave four different proof of it.

(3.5) Theorem (Quadratic reciprocity) Let \( \ell \) and \( p \) be two distinct odd prime numbers. Then

\[ \left( \frac{\ell}{p} \right) = \left( \frac{p}{\ell} \right) (-1)^{\frac{(\ell-1)(p-1)}{4}}. \]
(3.6) Example  Both 257 and 101 are prime numbers. We have

\[
\left( \frac{101}{257} \right) = \left( \frac{55}{101} \right) = \left( \frac{5}{101} \right) \left( \frac{11}{101} \right) = \left( \frac{1}{5} \right) \left( \frac{2}{11} \right) = -1.
\]

(3.7) Remark Most books on elementary number theory covers the above material, and more. A succinct eight-page treatment can be found in the book “A Course in Arithmetic” by J.-P. Serre.