Introduction to Number Theory

Mike Reiter

Based partially on Chapters 1-2 of N. Koblitz, A course in number theory and cryptography, and on Chapter 9 of Bellare and Rogaway.

Prime Numbers

- An integer $p > 1$ is a prime number iff its only divisors are $\pm 1$ and $\pm p$
- Any integer $a > 1$ can be factored in a unique way as
  \[ a = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t} \]
  where $p_1 < p_2 < \ldots < p_t$ are primes and each $a_i$ is a positive integer
- Alternatively, if $P$ is the set of all primes, then any positive integer can be written uniquely in the form
  \[ a = \prod_{p \in P} p^{\alpha_p} \]
  where each $\alpha_p \geq 0$
  and where only finitely many exponents are nonzero.
Prime Numbers

- Let

\[ a = \prod_{p \in P} p^{\alpha_p} \quad b = \prod_{p \in P} p^{\beta_p} \]

- Then

\[ a \cdot b = \prod_{p \in P} p^{\alpha_p + \beta_p} \]

\[ \gcd(a, b) = \prod_{p \in P} p^{\min(\alpha_p, \beta_p)} \]

Fermat’s Little Theorem

- Theorem: Let \( p \) be a prime. For any integer \( a \),

\[ a^p \equiv a \mod p \]

\textbf{Proof:} If \( p \) divides \( a \), then it is trivially true.

Now suppose that \( p \) does not divide \( a \).

First note that \( 0 \cdot a, 1 \cdot a, \ldots, (p - 1) \cdot a \) constitute the integers mod \( p \), since if

\[ i \cdot a = j \cdot a \mod p \]

then \( p \mid (i-j) \cdot a \) and so \( p \mid (i-j) \). Since \( i, j < p \), this happens only if \( i = j \).

Since \( 0 \cdot a = 0 \mod p \), \{1 \cdot a, \ldots, (p - 1) \cdot a\} = \{1, \ldots, p - 1\} \). Multiplying both sets, we get \( a^{p-1} \cdot (p - 1)! \equiv (p - 1)! \mod p \) and so \( a^{p-1} \equiv 1 \mod p \).\[ \square \]
Fermat’s Little Theorem

**Corollary:** If \( n \equiv m \mod (p - 1) \) then \( a^n \equiv a^m \mod p \).

\[ n = m + c \cdot (p - 1) \]

So, multiplying

\[ a^{p-1} = 1 \mod p \]

by itself \( c \) times, and then by

\[ a^m = a^m \mod p \]

gives the result.

---

Chinese Remainder Theorem

**Theorem:** Consider the system of congruences

\[
\begin{align*}
x &\equiv a_1 \mod m_1 \\
x &\equiv a_2 \mod m_2 \\
& \quad \vdots \\
x &\equiv a_r \mod m_r
\end{align*}
\]

and suppose that \( \gcd(m_i, m_j) = 1 \) for each \( i, j, i \neq j \). There exists a simultaneous solution \( x \) to all the congruences, and any two solutions are congruent modulo \( M = m_1 \cdot m_2 \cdot \ldots \cdot m_r \).
Chinese Remainder Theorem

Proof:

First we prove uniqueness mod $M$. We need the following lemma.

**Lemma:** If $a \equiv b \mod m$ and $a \equiv b \mod n$, and if $\gcd(m, n) = 1$, then $a \equiv b \mod mn$.

- Proof: Since $\gcd(m, n) = 1$, $m | (a - b)$ and $n | (a - b)$ implies that $a - b = lm + nx$ for some $l, x, y > 0$

  and so $mn | (a - b)$.

Let $x'$ and $x''$ be two solutions, and let $x = x' - x''$.

Then $x \equiv 0 \mod m_j$ for each $m_j$. By the above lemma, $x \equiv 0 \mod M$.

Now we prove existence.

Let $M_j = M/m_j$. Clearly $\gcd(m_j, M_j) = 1$, and so there is an integer $N_j$ such that

$$M_j N_j \equiv 1 \mod m_j$$

Now set

$$x = \sum_i a_i M_i N_i$$

Since $m_j | M_j$, for any $i \neq j$,

$$x \equiv a_i M_i N_i \equiv a_i \mod m_i$$
Euler Totient Function

- For any positive integer \( n \), let \( \varphi(n) \) denote the number of nonnegative integers less than \( n \) that are relatively prime to \( n \)

\[
\varphi(n) = \left| \{ b : 0 \leq b < n \land \gcd(b, n) = 1 \} \right|
\]

- Properties of \( \varphi(n) \)
  - \( \varphi(1) = 1 \)
  - \( \varphi(p) = p - 1 \) for any prime \( p \)
  - \( \varphi(p^\alpha) = p^\alpha - p^{\alpha - 1} = p^{\alpha}(1 - 1/p) \)
    - The numbers from 0 to \( p^\alpha - 1 \) that are not relatively prime to \( p \) are those that are divisible by \( p \), and there are \( p^{\alpha - 1} \) of those

---

Euler Totient Function

- **Theorem**: If \( \gcd(m, n) = 1 \), then \( \varphi(mn) = \varphi(m) \varphi(n) \).

  - **Proof**: By the CRT, for each pair \( j_1 \in [0, m - 1] \) and \( j_2 \in [0, n - 1] \), there is exactly one \( j \in [0, mn - 1] \) such that \( j \equiv j_1 \mod m \) and \( j \equiv j_2 \mod n \).

    \[
    \gcd(j_1, m) > 1 \Rightarrow \gcd(j, m) > 1 \Rightarrow \gcd(j, mn) > 1
    \]
    \[
    \gcd(j_2, n) > 1 \Rightarrow \gcd(j, n) > 1 \Rightarrow \gcd(j, mn) > 1
    \]

    In addition,

    \[
    \gcd(j, mn) > 1
    \]
    \[
    \Rightarrow \gcd(j, m) > 1 \text{ or } \gcd(j, n) > 1
    \]
    \[
    \Rightarrow \gcd(j_1, m) > 1 \text{ or } \gcd(j_2, n) > 1
    \]

    So, \( \gcd(j, mn) = 1 \) iff \( \gcd(j_1, m) = 1 \) and \( \gcd(j_2, n) = 1 \).
Euler Totient Function

- **Corollary**: Let 

\[ n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \]

be the prime factorization of \( n \). Then 

\[ \varphi(n) = p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r} \left(1 - \frac{1}{p_r}\right) = \prod_{p^n} \left(1 - \frac{1}{p}\right) \]

Euler’s Theorem

- **Theorem**: If \( \gcd(a, m) = 1 \), then \( a^{\varphi(m)} \equiv 1 \mod m \).

\[ a \varphi(p^{\alpha}) \equiv a^{p^{\alpha-1}} \equiv 1 \mod p^{\alpha-1} \]

That is, for some integer \( b \),

\[ a^{p^{\alpha-1}(p-1)} = 1 + bp^{\alpha-1} \]
Euler’s Theorem

Now we use the binomial theorem:

Lemma: For any positive integer \( n \), \((x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\).

By this, we get

\[
\alpha^{\varphi(p^\alpha)} = \left(\alpha^{p^{\alpha-1}(p-1)}\right)^p = \left(1 + b p^{\alpha-1}\right)^p = \sum_{k=0}^{p} \binom{p}{k} (b p^{\alpha-1})^k
\]

This completes case 1.

Euler’s Theorem

Case 2: \( m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \)

We know from case 1 that

\[
\alpha^{\varphi(p_i^{\alpha_i})} \equiv 1 \mod p_i^{\alpha_i}
\]

and from multiplicativity of the totient function that

\[
\varphi(m) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \ldots \varphi(p_r^{\alpha_r})
\]

So,

\[
\alpha^{\varphi(m)} \equiv \left(\alpha^{\varphi(p_i^{\alpha_i})}\right) \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) \equiv (1) \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) \equiv 1 \mod p_i^{\alpha_i}
\]

Since the prime powers are relatively prime, the result follows.
Useful Facts

- **Fact 1**: Let $p$ be a prime. Then $(\mathbb{Z}_p^*, \cdot)$ is a cyclic group of order $\varphi(p) = p - 1$.
- **Fact 2**: Let $G$ be a group of prime order. Then $G$ is cyclic.
- **Fact 3**: Let $G$ be a group of order $m$. Then $a^m = 1$ for any $a \in G$.
  - As a result, for any integer $i$, $a^i = a^{i \mod m}$.
- **Fact 4**: Let $G$ be a group and let $S$ be a subgroup of $G$. Then the order of $S$ divides the order of $G$.
- **Fact 5**: Let $(F, +, \cdot)$ be a finite field, and let $F^* = F - \{0\}$. Then $(F^*, \cdot)$ is a cyclic group.
  - Note that this implies Fact 1, since $(\mathbb{Z}_p^*, +, \cdot)$ is a finite field.

Finding a Generator of a Group

- **Proposition**: Let $G$ be a cyclic group of order $m$. Let

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

be the prime factorization of $m$, and let $m_i = m/p_i$. Then $g$ is a generator of $G$ if and only if

$$g^{m_i} \neq 1$$

for each $i$, $1 \leq i \leq r$.

- **Proof**: First suppose that $g$ is a generator of $G$. Then, the smallest positive integer $j$ such that $g^j = 1$ is $j = m$. Since each $m_i$ satisfies $0 < m_i < m$, it must be that

$$g^{m_i} \neq 1$$
Finding a Generator of a Group

Now suppose that for each $m_i$,

$$g^{m_i} \neq 1$$

and let $j$ be the order of $g$, the smallest positive integer such that $g^j = 1$. Then $j \mid m$ and so

$$j = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$$

where each $\beta_i$ satisfies $0 \leq \beta_i \leq \alpha_i$.

If $j < m$ then there must be some $i$ such that $\beta_i < \alpha_i$, but this would imply that $j \mid m_i$ and so

$$g^{m_i} = 1$$

As a result, it must be that $j = m$.

Finding a Generator of a Group

■ **Proposition:** Let $G$ be a cyclic group of order $m$, and let $g$ be a generator of $G$. Define $\text{Gen}(G)$ to be the set of all generators of $G$. Then,

$$\text{Gen}(G) = \{g^i : i \in \mathbb{Z}_m^*\}$$

and so

$$|\text{Gen}(G)| = \varphi(m)$$

\(\blacktriangledown\) Proof: We first show that if $i \in \mathbb{Z}_m^*$ then $h = g^i$ is a generator. To see this, let $j \in \mathbb{Z}_m$ be such that $h^j = 1$, i.e.,

$$1 = h^j = g^{ij}$$

Since $g$ is a generator, it must be the case that $ij \equiv 0 \mod m$, i.e., $m \mid ij$.

Since $i \in \mathbb{Z}_m^*$, it must be that $m \mid j$.

But since $j \in \mathbb{Z}_m$, it follows that $j = 0$. That is, the only possible value of $j \in \mathbb{Z}_m$ for which $h^j = 1$ is $j = 0$, and so $h$ is a generator.
Finding a Generator of a Group

We now show that if \( i \in \mathbb{Z}_m \setminus \mathbb{Z}_m^* \), then \( h = g^i \) is not a generator. Let \( d = \gcd(i, m) \). Then, \( d > 1 \), and so \( j = m/d \) is an element of \( \mathbb{Z}_m \). Then,

\[
h^j = g^{ij} = g^{im/d} = (g^m)^{i/d} = 1^{i/d} = 1
\]

That is, there is a nonzero \( j \in \mathbb{Z}_m \) such that \( h^j = 1 \), and so \( h \) is not a generator.

So, one way to find a generator of a group \( G \) of order \( m \) is to simply choose random elements of \( G \) and test them. Each is a generator with probability \( \varphi(m)/m \), and so one will be found in roughly \( m/\varphi(m) \) attempts.

Finding a Generator of a Group

- When we work with a group in cryptography, we often choose the group to be \( (\mathbb{Z}_p^*, \cdot) \)
- In order to make finding a generator as efficient as possible, we typically choose \( p \) so that \( \varphi(p) = p - 1 \) has few prime factors
  - A common choice is \( p = 2q + 1 \) where \( q \) is prime
  - A randomly chosen group element (excluding 1 and \( p - 1 \)) is a generator with probability \( \varphi(2q)/(p - 3) = (q - 1)/(2q - 2) = 1/2 \)
Squares and Non-squares

An element \(a\) of a group \(G\) is called a square or quadratic residue if there is a \(b \in G\) such that \(a = b^2\).

- We denote the squares of \(G\) by \(\text{QR}(G)\).
- The non-squares of \(G\) are \(G \setminus \text{QR}(G)\).

We are mainly interested in the case where \(G = \mathbb{Z}_N^*\) for some integer \(N\).

Proposition: Let \(p > 2\) be a prime and let \(g\) be a generator of \(\mathbb{Z}_p^*\). Then

\[
\text{QR}(\mathbb{Z}_p^*) = \{g^i \mod p : i \in \mathbb{Z}_{p-1} \text{ and } i \text{ is even}\}
\]

and

\[
|\text{QR}(\mathbb{Z}_p^*)| = (p-1)/2.
\]

Plus, every square mod \(p\) has two distinct square roots mod \(p\).

Proof: Let \(E = \{g^i \mod p : i \in \mathbb{Z}_{p-1} \text{ and } i \text{ is even}\}\). We show that \(E = \text{QR}(\mathbb{Z}_p^*)\) by showing that \(E \subseteq \text{QR}(\mathbb{Z}_p^*)\) and then that \(E \supseteq \text{QR}(\mathbb{Z}_p^*)\).

First, consider an \(a \in E\), and suppose that \(a \equiv g^i \mod p\). Since \(a \in E\), we know that \(i\) is even. Let \(j = i/2\), and note that \(j \in \mathbb{Z}_{p-1}\).

Then, \(a \in \text{QR}(\mathbb{Z}_p^*)\) since

\[
(g^j)^2 \equiv g^{2j} \mod p 
\]

\[
\equiv a \mod p
\]
Squares and Non-squares

Now, to show that $E \supseteq \text{QR}(Z_p^*)$, consider any $b \in Z_p^*$. We will show that $b^2 \in E$.

Suppose $b \equiv g^i \mod p$. Then,

$$b^2 \equiv (g^i)^2 \equiv g^{2i} \mod p$$

and it is easy to verify that $2j \mod p-1$ is even since $p-1$ is.

This completes the argument that $E = \text{QR}(Z_p^*)$.

The claim that $|\text{QR}(Z_p^*)| = (p-1)/2$ follows immediately since exactly $(p-1)/2$ elements of $Z_{p-1}$ are even.

Squares and Non-squares

Now we have to prove that every element of $\text{QR}(Z_p^*)$ has exactly two square roots mod $p$.

Consider $a \in \text{QR}(Z_p^*)$ and suppose that $a \equiv g^i \mod p$. By the preceding, we know that $i$ is even. So, $g^i \mod p$ with $x = i/2$ is a square root of $a$.

In addition, consider $y \equiv x + (p-1)/2 \mod p-1$. Note that

$$(g^i)^2 \equiv (g^x + (p-1)/2)^2 \equiv g^x g^{p-1} \equiv a \mod p$$

and so $y$ is a square root of $a \mod p$.

Since $i$ is even and in $Z_{p-1}$, we get $0 \leq x < (p-1)/2$. Then, it follows that $(p-1)/2 \leq y < p-1$. So, $x$ and $y$ are distinct square roots of $a$. 

Copyright © 2018 by Michael Reiter
All rights reserved.
Let \( p \) be a prime number. We define a function\( J_p : \mathbb{Z}_p^* \to \{1, -1\} \)
by
\[
J_p(a) = \begin{cases}
1 & \text{if } a \in \text{QR}(\mathbb{Z}_p^*) \\
-1 & \text{if } a \notin \text{QR}(\mathbb{Z}_p^*)
\end{cases}
\]
This is called the \textbf{Legendre symbol} of \( a \).

By the previous result, if \( a \equiv g^i \mod p \), then \( J_p(a) = (-1)^i \)
However, computing \( J_p(a) \) this way is not efficient, since it requires computing the discrete logarithm of \( a \).

\textbf{Proposition:} Let \( p > 2 \) be a prime. Then for any \( a \in \mathbb{Z}_p^* \),
\[
J_p(a) \equiv a^{(p-1)/2} \mod p
\]
\textbf{Proof:} The proof uses the following lemma.

\textbf{Lemma:} Let \( p > 2 \) be a prime, and let \( g \) be a generator of \( \mathbb{Z}_p^* \). Then
\[
g^{(p-1)/2} \equiv -1 \mod p
\]
Proof: First note that 1 and \(-1 = p - 1\) are the two square roots of 1 \( \mod p \), and are distinct since \( p > 2 \). Now set
\[
b = g^{(p-1)/2} \mod p
\]
Then \( b^2 \equiv 1 \mod p \), and so \( b \) equals 1 or \(-1\). However, \( b \) is not 1, since the smallest \( j \) such that \( g^j \equiv 1 \mod p \) is \( j = p - 1 \).
Legendre Symbol

Now suppose \( a \in \mathbb{Z}_p^* \), and let \( g \) be a generator of \( \mathbb{Z}_p^* \). Suppose \( a \equiv g^i \mod p \).

If \( a \in \text{QR}(\mathbb{Z}_p^*) \), then \( i \) is even. In this case
\[
a \equiv (g^i)^{(p-1)/2} \equiv (g^{(p-1)/2})^i \equiv 1 \mod p
\]
as needed.

If \( a \not\in \text{QR}(\mathbb{Z}_p^*) \), then \( i \) is odd. In this case
\[
a \equiv (g^i)^{(p-1)/2} = g^{(i-1)p-1/2} = (g^{p-1})^{(i-1)/2} = -1 \mod p
\]
as needed.

Legendre Symbol

\[\text{Proposition: Let } p > 2 \text{ be a prime. For any } a, b \in \mathbb{Z}_p^*, J_p(ab \mod p) = J_p(a) \cdot J_p(b)\]

\[\text{Proof: } J_p(ab \mod p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \equiv J_p(a) \cdot J_p(b) \mod p\]

Then, the range of \( J_p \) is \( \{1, -1\} \), equality holds.

\[\text{Proposition: Let } p > 2 \text{ be a prime, and let } g \text{ be a generator of } \mathbb{Z}_p^*. \text{ Then, for any } x, y \in \mathbb{Z}_{p-1}, J_p(g^{xy} \mod p) = 1 \text{ iff } J_p(g^x \mod p) = 1 \text{ or } J_p(g^y \mod p) = 1\]

\[\text{Proof: } \text{Since } p-1 \text{ is even, } x \text{ mod } p-1 \text{ is even iff } xy \text{ is even}\]
\[\text{iff } x \text{ is even or } y \text{ is even.}\]
Legendre Symbol

- **Proposition:** Let $p > 2$ be a prime, and let $g$ be a generator of $\mathbb{Z}_p^*$.
  \[
  \Pr[J_p(g^{xy} \mod p) = 1 \mid x \leftarrow_{R \mathbb{Z}_{p-1}} ; y \leftarrow_{R \mathbb{Z}_{p-1}}] = \frac{3}{4}.
  \]

  □ Proof: It suffices to show that
  \[
  \Pr[J_p(g^x \mod p) = 1 \text{ or } J_p(g^y \mod p) = 1 \mid x \leftarrow_{R \mathbb{Z}_{p-1}} ; y \leftarrow_{R \mathbb{Z}_{p-1}}] = \frac{3}{4}.
  \]
  Setting the above to $1 - \alpha$, we get that
  \[
  \alpha = \Pr[J_p(g^x \mod p) = -1 \text{ and } J_p(g^y \mod p) = -1 \mid x \leftarrow_{R \mathbb{Z}_{p-1}} ; y \leftarrow_{R \mathbb{Z}_{p-1}}] \\
  = \Pr[J_p(g^x \mod p) = -1 \mid x \leftarrow_{R \mathbb{Z}_{p-1}}] \cdot \Pr[J_p(g^y \mod p) = -1 \mid y \leftarrow_{R \mathbb{Z}_{p-1}}] \\
  = (|\text{QNR}(\mathbb{Z}_p^*)|/(p-1)) \cdot (|\text{QNR}(\mathbb{Z}_p^*)|/(p-1)) \\
  = [(p-1)/2]/(p-1) \cdot [(p-1)/2]/(p-1) \\
  = \frac{1}{4}.
  \]

- This is bad news for “Diffie Hellman” keys, as it shows they are not uniformly distributed in $\mathbb{Z}_p^*$

Groups of Prime Order

- In cryptography, it is often useful to employ a group of prime order

- A common way to obtain such a group is to use a prime-order subgroup of a group of integers modulo a prime

- **Example**
  □ Pick a prime $p = 2q + 1$ where $q$ is a prime
  □ Then $\text{QR}(\mathbb{Z}_p^*)$ is a group of order $q$, with group operation multiplication mod $p$
  □ A generator for this group is $g^2 \mod p$ for any generator $g$ of $\mathbb{Z}_p^*$
Groups of Prime Order

1. Why are groups of prime order useful?
2. Let $G$ be a group of prime order $p$, with generator $g$
3. Then arithmetic “in the exponents” is performed modulo $p$
4. Since $p$ is prime, we can also divide in the exponents

---

Groups of Prime Order

- Proposition: Suppose $G$ is a group of prime order $q$. Let $g$ be a generator of $G$. Then for any $a \in G$ we have

$$\Pr[g^x = a | x \leftarrow \mathbb{Z}_q, y \leftarrow \mathbb{Z}_q] = \begin{cases} \frac{1}{q} \left( 1 - \frac{1}{q} \right) & \text{if } a \neq 1 \\ \frac{1}{q} \left( 2 - \frac{1}{q} \right) & \text{if } a = 1 \end{cases}$$

- Proof: First suppose that $a = 1$. Then $g^x = 1$ iff $x = 0$ or $y = 0$. Then,

$$\Pr[x = 0 \text{ or } y = 0] = \Pr[x = 0] + \Pr[y = 0] - \Pr[x = 0 \text{ and } y = 0] = \frac{1}{q} + \frac{1}{q} - \frac{1}{q^2}$$
Groups of Prime Order

Now consider $a \neq 1$, and suppose $g^{z} = a$. Then,

$$g^{xy} = a \text{ iff } xy \equiv z \mod q$$

For any $x \in \mathbb{Z}_q^*$, there is exactly one $y \in \mathbb{Z}_q$ for which $xy \equiv z \mod q$, since $q$ is prime.

Now consider $x$ chosen at random from $\mathbb{Z}_q$. If $x = 0$, then $xy$ and $z$ are not equivalent mod $q$, no matter what $y$ is, since $z \neq 0$.

If $x \neq 0$, then $y$ will be selected so that $xy \equiv z \mod q$ with probability $1/q$. So,

$$\Pr[xy \equiv z \mod q] = \frac{q-1}{q} \cdot \frac{1}{q} = \frac{1}{q} \left( \frac{1}{q} \right)$$

Euler Totient Function

**Proposition:** Let $n$ be the product of two distinct primes $n = pq$. Knowledge of $\varphi(n)$ and $(p, q)$ are “equivalent” in the sense that given one, the other can be efficiently computed.

Proof: Result is trivial if $n$ is even: $p = 2$, $q = n/2$ and $\varphi(n) = n/2 - 1$.

Now suppose $n$ is odd. If we are given $(p, q)$, then we can compute $\varphi(n)$ directly using $\varphi(n) = (p - 1)(q - 1) = n + 1 - (p + q)$.

If we are given $\varphi(n)$ then we know the following two equations:

$$pq = n \quad \quad p + q = n + 1 - \varphi(n)$$

Let $2b = n + 1 - \varphi(n)$ since it is even. Then two numbers whose sum is $2b$ and product is $n$ must be the roots of $x^2 - 2bx + n = 0$. So, $p$ and $q$ equal

$$b \pm \sqrt{b^2 - n}$$