1: Modular Arithmetic & Number Theory

In general, public-key cryptography relies on computational problems from abstract algebra. Of the techniques currently known for public-key crypto, RSA uses some of the simplest mathematical ideas, so it’s an ideal place to start. We will be working with modular arithmetic, so please review the section on modular arithmetic from the first lecture! We need to understand the behavior of the four basic arithmetic operations in the set \( \mathbb{Z}_n = \{0, \ldots, n - 1\} \).

Every element \( x \in \mathbb{Z}_n \) has an inverse with respect to addition mod \( n \): namely \(-x \mod n\). For example, the additive inverse of 11 mod 14 is \(-11 \equiv 14 \mod 3\). However, multiplicative inverses are not so straight-forward.

Greatest Common Divisors

If \( d \mid x \) and \( d \mid y \), then \( d \) is a common divisor of \( x \) and \( y \). The largest possible such \( d \) is called the greatest common divisor (GCD), denoted \( \gcd(x,y) \). If \( \gcd(x,y) = 1 \), then we say that \( x \) and \( y \) are relatively prime. The oldest “algorithm” ever documented is the one Euclid described for computing GCDs (ca. 300 BCE):

\[
\text{GCD}(x,y): \quad \text{// Euclid’s algorithm}
\]
\[
\text{if } y = 0 \text{ then return } x
\]
\[
\text{else return } \text{GCD}(y, x \mod y)
\]

Multiplicative Inverses

We let \( \mathbb{Z}_n^* \) denote the set \( \{x \in \mathbb{Z}_n | \gcd(x,n) = 1\} \), the multiplicative group modulo \( n \). This group is closed under multiplication mod \( n \), which just means that if \( x,y \in \mathbb{Z}_n^* \) then \( xy \in \mathbb{Z}_n^* \), where \( xy \) denotes multiplication mod \( n \). Indeed, if \( \gcd(x,n) = \gcd(y,n) = 1 \), then \( \gcd(xy,n) = 1 \) and thus \( \gcd(xy \mod n,n) = 1 \) by Euclid’s algorithm.
In abstract algebra, a group is a set that is closed under its operation (in this case multiplication mod $n$), and is also closed under inverses. So if $\mathbb{Z}^*_n$ is really a group under multiplication mod $n$, then for every $x \in \mathbb{Z}^*_n$, there must be a $y \in \mathbb{Z}^*_n$ so that $xy \equiv 1$. In other words, $y$ is the multiplicative inverse of $x$ (and we would give it the name $x^{-1}$).

The fact that we can always find a multiplicative inverse for elements of $\mathbb{Z}^*_n$ is due to the following theorem:

**Theorem 13.1: Bezout’s Theorem**

For all integers $x$ and $y$, there exist integers $a$ and $b$ such that $ax + by = \gcd(x, y)$. In fact, $\gcd(x, y)$ is the smallest positive integer that can be written as an integral linear combination of $x$ and $y$.

What does this have to do with multiplicative inverses? Take any $x \in \mathbb{Z}^*_n$; we will show how to find its multiplicative inverse. Since $x \in \mathbb{Z}^*_n$, we have $\gcd(x, n) = 1$. From Bezout’s theorem, there exist integers $a, b$ satisfying $ax + bn = 1$. By reducing both sides of this equation modulo $n$, we have

$$1 \equiv_n ax + bn \equiv_n ax + 0$$

(since $bn \equiv_n 0$). Thus the integer $a$ guaranteed by Bezout’s theorem is the multiplicative inverse of $x$ modulo $n$.

We have shown that every $x \in \mathbb{Z}^*_n$ has a multiplicative inverse mod $n$. That is, if $\gcd(x, n) = 1$, then $x$ has a multiplicative inverse. But might it be possible for $x$ to have a multiplicative inverse mod $n$ even if $\gcd(x, n) \neq 1$?

Suppose that we have an element $x$ with a multiplicative inverse; that is, $xx^{-1} \equiv_1 1$. Then $n$ divides $xx^{-1} - 1$, so we can write $xx^{-1} - 1 = kn$ (as an expression over the integers) for some integer $k$. Rearranging, we have that $xx^{-1} - kn = 1$. That is to say, we have a way to write 1 as an integral linear combination of $x$ and $n$. From Bezout’s theorem, this must mean that $\gcd(x, n) = 1$. Hence, $x \in \mathbb{Z}^*_n$. We conclude that:

$$\mathbb{Z}^*_n \overset{\text{def}}{=} \{ x \in \mathbb{Z}_n \mid \gcd(x, n) = 1 \} = \{ x \in \mathbb{Z}_n \mid \exists y \in \mathbb{Z}_n : xy \equiv_n 1 \}.$$

The elements of $\mathbb{Z}^*_n$ are exactly those elements with a multiplicative inverse mod $n$.

Furthermore, multiplicative inverses can be computed efficiently using an extended version of Euclid’s GCD algorithm. While we are computing the GCD, we can also keep track of integers $a$ and $b$ from Bezout’s theorem at every step of the recursion; see below:

```
Example \(
\\PageIndex{1}\\)
```

Below is a table showing the computation of EXTGCD(35,144). Note that the columns $x, y$ are computed from the top.
down (as recursive calls to EXTCD are made), while the columns $d$, $a$, and $b$ are computed from bottom up (as recursive calls return). Also note that in each row, we indeed have $d = ax + by$.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$\lfloor \frac{x}{y} \rfloor$</th>
<th>$x \mod y$</th>
<th>$d$</th>
<th>$a$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>144</td>
<td>0</td>
<td>35</td>
<td>1</td>
<td>-37</td>
<td>9</td>
</tr>
<tr>
<td>144</td>
<td>35</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>9</td>
<td>-37</td>
</tr>
<tr>
<td>35</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>1</td>
<td>-1</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

The final result demonstrates that $35^{-1} \equiv 144 \equiv 107$.

The Totient Function

Euler's totient function is defined as $\phi(n) \equiv |\mathbb{Z}_n^*|$, in other words, the number of elements of $\mathbb{Z}_n$ which are relatively prime to $n$. As an example, if $p$ is a prime, then $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$ because every integer in $\mathbb{Z}_n$ apart from zero is relatively prime to $p$. Therefore,

$$\lfloor \phi(p) = p - 1. \rfloor$$

We will frequently work modulo $n$ where $n$ is the product of two distinct primes $n = pq$. In that case, $\phi(n) = (p - 1)(q - 1)$.

To see why, let's count how many elements in $\mathbb{Z}_{pq}$ share a common divisor with $pq$ (i.e., are not in $\mathbb{Z}^*_{pq}$).

- The multiples of $p$ share a common divisor with $pq$. These include $0, p, 2p, 3p, \ldots, (q - 1)p$. There are $q$ elements in this list.
- The multiples of $q$ share a common divisor with $pq$. These include $0, q, 2q, 3q, \ldots, (p - 1)q$. There are $p$ elements in this list.

We have clearly double-counted element $0$ in these lists. But no other element is double counted. Any item that occurs in both lists would be a common multiple of both $p$ and $q$, but the least common multiple of $p$ and $q$ is $pq$ since $p$ and $q$ are relatively prime. But $pq$ is larger than any item in these lists.

We count $p + q - 1$ elements in $\mathbb{Z}_{pq}$ which share a common divisor with $pq$. That leaves the rest to reside in $\mathbb{Z}^*_{pq}$, and there are $pq - (p + q - 1) = (p - 1)(q - 1)$ of them. Hence

$$\lfloor \phi(pq) = (p - 1)(q - 1). \rfloor$$

General formulas for $\phi(n)$ exist, but they typically rely on knowing the prime factorization of $n$. We will see more connections between the difficulty of computing $\phi(n)$ and the difficulty of factoring $n$ later in this part of the course.

Here's an important theorem from abstract algebra:

Theorem 13.2: Euler's Theorem
If $x \in \mathbb{Z}_n^*$ then $x^{\varphi(n)} \equiv_1 1$.

As a final corollary, we can deduce Fermat’s "little theorem," that $x^p \equiv_p x$ for all $x$, when $p$ is prime.\textsuperscript{2}

\textsuperscript{2}You have to handle the case of $x \equiv_p 0$ separately, since $0 \notin \mathbb{Z}_p^*$ so Euler’s theorem doesn’t apply to it.