3.3. Modular Arithmetic, RSA Algorithm

3.3.1. Congruences Modulo m. Given an integer $m \geq 2$, we say that a is congruent to b modulo m, written $a \equiv b \pmod{m}$, if $m|(a-b)$. Note that the following conditions are equivalent

1. $a \equiv b \pmod{m}$.
2. $a = b + km$ for some integer k.
3. a and b have the same remainder when divided by m.

The relation of congruence modulo m is an equivalence relation. It partitions $\mathbb{Z}$ into m equivalence classes of the form

$$[x] = [x]_m = \{x + km \mid k \in \mathbb{Z}\}\,.$$

For instance, for $m = 5$, each one of the following rows is an equivalence class:

...	-10	-5	0	5	10	15	20	...
...	-9	-4	1	6	11	16	21	...
...	-8	-3	2	7	12	17	22	...
...	-7	-2	3	8	13	18	23	...
...	-6	-1	4	9	14	19	24	...

Each equivalence class has exactly a representative r such that $0 \leq r < m$, namely the common remainder of all elements in that class when divided by m. Hence an equivalence class may be denoted $[r]$ or $x + m\,\mathbb{Z}$, where $0 \leq r < m$. Often we will omit the brackets, so that the equivalence class $[r]$ will be represented just r. The set of equivalence classes (i.e., the quotient set of $\mathbb{Z}$ by the relation of congruence modulo m) is denoted $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. For instance, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Remark: When writing "r" as a notation for the class of r we may stress the fact that r represents the class of r rather than the integer r by including " $\pmod{p}$" at some point. For instance $8 = 3 \pmod{p}$. Note that in "$a \equiv b \pmod{m}$", a and b represent integers, while in "$a = b \pmod{m}$" they represent elements of $\mathbb{Z}_m$.

Reduction Modulo m: Once a set of representatives has been chosen for the elements of $\mathbb{Z}_m$, we will call "r *reduced modulo* m", written "$r \bmod m$", the chosen representative for the class of r. For instance, if we choose the representatives for the elements of $\mathbb{Z}_5$ in the interval from 0 to 4 ($\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$), then $9 \bmod 5 = 4$. Another possibility is to choose the representatives in the interval from -2 to 2 ($\mathbb{Z}_5 = \{-2, -1, 0, 1, 2\}$), so that $9 \bmod 5 = -1$

In $\mathbb{Z}_m$ it is possible to define an *addition* and a *multiplication* in the following way:

$$[x] + [y] = [x + y]\,; \qquad [x] \cdot [y] = [x \cdot y]\,.$$

As an example, tables 3.3.1 and 3.3.2 show the addition and multiplication tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$ respectively.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

TABLE 3.3.1. Operational tables for $\mathbb{Z}_5$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

TABLE 3.3.2. Operational tables for $\mathbb{Z}_6$

A difference between this two tables is that in $\mathbb{Z}_5$ every non-zero element has a multiplicative inverse, i.e., for every $x \in \mathbb{Z}_5$ such that $x \neq 0$ there is an x^{-1} such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$; e.g. $2^{-1} = 4 \pmod 5$. However in $\mathbb{Z}_6$ that is not true, some non-zero elements like 2 have no multiplicative inverse. Furthermore the elements without multiplicative inverse verify that they can be multiply by some other non-zero element giving a product equal zero, e.g. $2 \cdot 3 = 0 \pmod 6$. These elements are called divisors of zero. Of course with this definition zero itself is a divisor of zero. Divisors of zero different from zero are called *proper divisors of zero*. For instance in $\mathbb{Z}_6$ 2 is a proper divisor of zero. In $\mathbb{Z}_5$ there are no proper divisors of zero.

In general:

1. The elements of $\mathbb{Z}_m$ can be classified into two classes:

   (a) *Units*: elements with multiplicative inverse.
   (b) *Divisors of zero*: elements that multiplied by some other non-zero element give product zero.
2. An element $[a] \in \mathbb{Z}_m$ is a unit (has a multiplicative inverse) if and only if $\gcd(a, m) = 1$.
3. All non-zero elements of $\mathbb{Z}_m$ are units if and only if m is a prime number.

The set of units in $\mathbb{Z}_m$ is denoted $\mathbb{Z}_m^*$. For instance:

$$\begin{aligned}
\mathbb{Z}_2^* &= \{1\} \\
\mathbb{Z}_3^* &= \{1, 2\} \\
\mathbb{Z}_4^* &= \{1, 3\} \\
\mathbb{Z}_5^* &= \{1, 2, 3, 4\} \\
\mathbb{Z}_6^* &= \{1, 5\} \\
\mathbb{Z}_7^* &= \{1, 2, 3, 4, 5, 6\} \\
Z_8^* &= \{1, 3, 5, 7\} \\
Z_9^* &= \{1, 2, 4, 5, 7, 8\}
\end{aligned}$$

Given an element $[a]$ in $\mathbb{Z}_m^*$, its inverse can be computed by using the Euclidean algorithm to find $\gcd(a, m)$, since that algorithm also provides a solution to the equation $ax + my = \gcd(a, m) = 1$, which is equivalent to $ax \equiv 1 \pmod{m}$.

Example: Find the multiplicative inverse of 17 in $\mathbb{Z}_{64}^*$. *Answer*: We use the Euclidean algorithm:

$$\begin{array}{rcll}
64 &=& 3 \cdot 17 + 13 & \rightarrow \quad r = 13 \\
17 &=& 1 \cdot 13 + 4 & \rightarrow \quad r = 4 \\
13 &=& 3 \cdot 4 + 1 & \rightarrow \quad r = 1 \\
4 &=& 4 \cdot 1 + 0 & \rightarrow \quad r = 0
\end{array}$$

Now we compute backward:

$$\begin{aligned}
1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 1 \cdot 13) &= 4 \cdot 13 - 3 \cdot 17 \\
&= 4 \cdot (64 - 3 \cdot 17) - 3 \cdot 17 = 4 \cdot 64 - 15 \cdot 17 \,.
\end{aligned}$$

Hence $(-15) \cdot 17 \equiv 1 \pmod{64}$, but $-15 \equiv 49 \pmod{64}$, so the inverse of 17 in $(\mathbb{Z}_{64}^*, \cdot)$ is 49. We will denote this by writing $17^{-1} = 49 \pmod{64}$, or $17^{-1} \bmod 64 = 49$.

3.3.2. Euler's Phi Function. The number of units in $\mathbb{Z}_m$ is equal to the number of positive integers not greater than and relatively prime to m, i.e., the number of integers a such that $1 \leq a \leq m$ and $\gcd(a, m) = 1$. That number is given by the so called *Euler's phi function*:

$$\phi(m) = \text{number of positive integers not greater than } m \text{ and relatively prime to } m\,.$$

For instance, the positive integers not greater than and relatively prime to 15 are: $1, 2, 4, 7, 8, 11, 13, 14$, hence $\phi(15) = 8$.

We have the following results:

1. If p is a prime number and $s \geq 1$, then $\phi(p^s) = p^s - p^{s-1} = p^s(1 - 1/p)$. In particular $\phi(p) = p - 1$.
2. If m_1, m_2 are two relatively prime positive integers, then $\phi(m_1 m_2) = \phi(m_1)\,\phi(m_2)$.[1]
3. If $m = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, where the p_k are prime and the s_k are positive, then
$$\phi(m) = m\,(1 - 1/p_1)\,(1 - 1/p_2)\,\dots\,(1 - 1/p_k)\,.$$

For instance

$$\phi(15) = \phi(3 \cdot 5) = \phi(3) \cdot \phi(5) = (3 - 1) \cdot (5 - 1) = 2 \cdot 4 = 8\,.$$

3.3.3. Euler's Theorem. If a and m are two relatively prime positive integers, $m \geq 2$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}\,.$$

The particular case in which m is a prime number p, Euler's theorem is called *Fermat's Little Theorem*:

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

For instance, if $a = 2$ and $p = 7$, then we have, in fact, $2^{7-1} = 2^6 = 64 = 1 + 9 \cdot 7 \equiv 1 \pmod 7$.

A consequence of Euler's Theorem is the following. If $\gcd(a, m) = 1$ then

$$x \equiv y \pmod{\phi(m)} \quad \Rightarrow \quad a^x \equiv a^y \pmod{m}\,.$$

[1] A function $f(x)$ of positive integers such that $\gcd(a, b) = 1 \Rightarrow f(ab) = f(a)f(b)$ is called *multiplicative*.

Consequently, the following function is well defined:

$$\mathbb{Z}_m^* \times \mathbb{Z}_{\phi(m)} \to \mathbb{Z}_m^*$$
$$([a]_m, [x]_{\phi(m)}) \mapsto [a^x]_m$$

Hence, we can compute powers modulo m in the following way:

$$a^n = a^{n \bmod \phi(m)} \pmod{m},$$

if $\gcd(a, m) = 1$. For instance:

$$\begin{aligned} 3^{9734888} \bmod 100 &= 3^{9734888 \bmod \phi(100)} \bmod 100 \\ &= 3^{9734888 \bmod 40} \bmod 100 = 3^8 \bmod 100 = 6561 \bmod 100 = 61\,. \end{aligned}$$

An even more efficient way to compute powers modulo m is given in Appendix A, paragraph A.1.

3.3.4. Application to Cryptography: RSA Algorithm. The RSA algorithm is an encryption scheme designed in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman. It allows encrypting a message with a key (the *encryption key*) and decrypting it with a different key (the *decryption key*). The encryption key is public and can be given to everybody. The decryption key is private and is known only by the recipient of the encrypted message.

The RSA algorithm is based on the following facts. Given two prime numbers p and q, and a positive number m relatively prime to p and q, Euler's theorem tells us that:

$$m^{\phi(pq)} = m^{(p-1)(q-1)} = 1 \pmod{pq}.$$

Assume now that we have two integers e and d such that $e \cdot d = 1 \pmod{\phi(pq)}$. Then we have that

$$(m^e)^d = m^{e \cdot d} = m \pmod{pq}.$$

So, given m^e we can recover m modulo pq by raising to the dth power.

The RSA algorithm consists of the following:

1. Generate two large primes p and q. Find their product $n = pq$.
2. Find two numbers e and d (in the range from 2 to $\phi(n)$) such that $e \cdot d = 1 \pmod{\phi(n)}$. This requires some trial and error. First e is chosen at random, and the Euclidean algorithm is used to find $\gcd(e, m)$, solving at the same time the equation $ex + my = \gcd(e, m)$. If $\gcd(e, m) = 1$ then the value obtained

for x is d. Otherwise, e is no relatively prime to $\phi(n)$ and we must try a different value for e.

3. The *public encryption key* will be the pair (n, e). The *private decryption key* will be the pair (n, d). The encryption key is given to everybody, while the decryption key is kept secret by the future recipient of the message.

4. The message to be encrypted is divided into small pieces, and each piece is encoded numerically as a positive integer m smaller than n.

5. The number m^e is reduced modulo n; $m' = m^e \bmod n$.

6. The recipient computes $m'' = m'^d \bmod n$, with $0 \leq m'' < n$.

It remains to prove that $m'' = m$. If m is relatively prime to p and q, then from Euler's theorem we get that $m'' = m \pmod{n}$, and since both are in the range from 0 to $n - 1$ they must be equal. The case in which p or q divides m is left as an exercise.