MODULAR ARITHMETIC

MIGUEL A. LERMA

(Last updated: April 21, 2005)

1. Modular Arithmetic

1. Congruences Modulo m. Given an integer $m \ge 2$, we say that a is congruent to b modulo m, written $a \equiv b \pmod{m}$, if m divides 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.

For instance 6 and 21 are congruent modulo 5 because when divided by 5 both have the same remainder of 1.

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							
 -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 is denoted $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. For instance, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

MIGUEL A. LERMA

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 rby including " (mod 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 mod 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 mod 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 mod 5 = -1

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

$$[x] + [y] = [x + y];$$
 $[x] \cdot [y] = [x \cdot y]$

As an example, tables 1 and 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

TABLE 1. Operational tables for \mathbb{Z}_5

+	0	1	2	3	4	5]	•	0	1	2	3	4	
0	0	1	2	3	4	5		0	0	0	0	0	0	
1	1	2	3	4	5	0		1	0	1	2	3	4	
2	2	3	4	5	0	1		2	0	2	4	0	2	
3	3	4	5	0	1	2		3	0	3	0	3	0	
4	4	5	0	1	2	3		4	0	4	2	0	4	
5	5	0	1	2	3	4		5	0	5	4	3	2	

TABLE 2. Operational tables for \mathbb{Z}_6

2

MODULAR ARITHMETIC

A difference between these 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. $2^{-1} = 4$ (mod 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 multiplied 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:

$$\mathbb{Z}_2^* = \{1\}$$

$$\mathbb{Z}_3^* = \{1, 2\}$$

$$\mathbb{Z}_4^* = \{1, 3\}$$

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

$$\mathbb{Z}_6^* = \{1, 5\}$$

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

$$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$$

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:

Now we compute backward:

$$1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 1 \cdot 13) = 4 \cdot 13 - 3 \cdot 17$$

= 4 \cdot (64 - 3 \cdot 17) - 3 \cdot 17 = 4 \cdot 64 - 15 \cdot 17.

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 $17^{-1} \mod 64 = 49$.

2. Euler's Phi Function. The number of units (invertible elements) 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 $1 \le a \le m$ and gcd(a, m) = 1. That number is given by the so called *Euler's phi* function:

$\phi(m)$ = number of positive integers not greater than mand 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 $s \ge 1$, 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

$$\phi(m) = m (1 - 1/p_1) (1 - 1/p_2) \dots (1 - 1/p_k).$$

4

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

For instance

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

3. Euler's Theorem. If a and m are two relatively prime positive integers, $m \ge 2$, 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

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

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:

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

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

 $3^{9734888} \mod 100 = 3^{9734888 \mod \phi(100)} \mod 100$ = $3^{9734888 \mod 40} \mod 100 = 3^8 \mod 100 = 6561 \mod 100 = 61$.

Fermat's Little Theorem can be used as test of primality, or rather as test of *non-primality*. *Example*: Prove that 716311796279 is not prime. *Answer*: We have that²

$$2^{716311796279-1} = 2^{716311796278} \equiv 127835156517 \pmod{716311796279}.$$

But if 716311796279 were prime, $2^{716311796279-1}$ would be congruent to 1 modulo m. Warning: Note that $a^{m-1} \equiv 1 \pmod{m}$ does not imply that m is prime; the only thing that we can say is that if $a^{m-1} \not\equiv 1 \pmod{m}$ (and $\gcd(a, m) = 1$) then m is not prime.

²Given a power a^x , there is an efficient method (easy to implement as an algorithm) to reduce a^x modulo m.

4. The Chinese Remainder Theorem. Let m_1, m_2, \ldots, m_k be pairwise relatively prime integers greater than or equal to 2. The following system of congruences

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ x \equiv r_2 \pmod{m_2} \\ \dots \\ x \equiv r_k \pmod{m_k} \end{cases}$$

has a unique solution modulo $M = m_1 m_2 \dots m_k$.

We can find a solution to that system in the following way. Let $M_i = M/m_i$, and $s_i =$ the inverse of M_i in \mathbb{Z}_{m_i} . Then

$$x = M_1 s_1 r_1 + M_2 s_2 r_2 + \dots + M_k s_k r_k$$

is a solution of the system.

Example: A group of objects can be arranged in 3 rows leaving 2 left, in 5 rows leaving 4 left, and in 7 rows leaving 6 left. How many objects are there? *Answer*: We must solve the following system of congruences:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

We have: $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 105/3 = 35 \equiv 2 \pmod{3}$, $M_2 = 105/5 = 21 \equiv 1 \pmod{5}$, $M_3 = 105/7 = 15 \equiv 1 \pmod{7}$; $s_1 =$ "inverse of 2 in \mathbb{Z}_3 " = 2, $s_2 =$ "inverse of 1 in \mathbb{Z}_5 " = 1, $s_3 =$ "inverse of 1 in \mathbb{Z}_7 " = 1. Hence the solution is

$$x = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 4 + 15 \cdot 1 \cdot 6 = 314 \equiv 104 \pmod{105}$$

Hence, any group of 104 + 105 k objects is a possible solution to the problem.