# MODULAR ARITHMETIC 

MIGUEL A. LERMA

(Last updated: April 21, 2005)

## 1. Modular Arithmetic

1. Congruences Modulo m. Given an integer $m \geq 2$, we say that $a$ is congruent to $b$ modulo $m$, written $a \equiv b(\bmod m)$, if $m$ divides $a-b$. Note that the following conditions are equivalent
(1) $a \equiv b(\bmod m)$.
(2) $a=b+k m$ 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

$$
[x]=[x]_{m}=\{x+k m \mid k \in \mathbb{Z}\} .
$$

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

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

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, $\mathbb{Z}_{5}=\{0,1,2,3,4\}$.

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 " $(\bmod p)$ " at some point. For instance $8=3(\bmod p)$. Note that in " $a \equiv b(\bmod m)$ ", $a$ and $b$ represent integers, while in " $a=b(\bmod m)$ " 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 " 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 $4\left(\mathbb{Z}_{5}=\{0,1,2,3,4\}\right)$, then $9 \bmod 5=4$. Another possibility is to choose the representatives in the interval from -2 to $2\left(\mathbb{Z}_{5}=\right.$ $\{-2,-1,0,1,2\}$ ), so that $9 \bmod 5=-1$

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

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

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 |


| $\cdot$ | 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 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 |$\quad \quad$| $\cdot$ | 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 2. Operational tables for $\mathbb{Z}_{6}$

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. $2^{-1}=4$ $(\bmod 5)$. 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. $2 \cdot 3=0(\bmod 6)$. 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 $\operatorname{gcd}(a, m)=1$.
(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 $\operatorname{gcd}(a, m)$, since that algorithm also provides a solution to the equation $a x+m y=\operatorname{gcd}(a, m)=1$, which is equivalent to $a x \equiv 1(\bmod m)$.

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

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

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 $(-15) \cdot 17 \equiv 1(\bmod 64)$, but $-15 \equiv 49(\bmod 64)$, so the inverse of 17 in $\left(\mathbb{Z}_{64}^{*}, \cdot\right)$ is 49 . We will denote this by writing $17^{-1}=49$ $(\bmod 64)$, or $17^{-1} \bmod 64=49$.
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 $1 \leq a \leq m$ and $\operatorname{gcd}(a, m)=1$. That number is given by the so called Euler's phi function:

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

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 $\phi\left(p^{s}\right)=p^{s}-p^{s-1}=$ $p^{s}(1-1 / p)$. In particular $\phi(p)=p-1$.
(2) If $m_{1}, m_{2}$ are two relatively prime positive integers, then $\phi\left(m_{1} m_{2}\right)=$ $\phi\left(m_{1}\right) \phi\left(m_{2}\right) .{ }^{1}$
(3) If $m=p_{1}^{s_{1}} p_{2}^{s_{2}} \ldots p_{k}^{s_{k}}$, where the $p_{k}$ are prime and the $s_{k}$ are positive, then

$$
\phi(m)=m\left(1-1 / p_{1}\right)\left(1-1 / p_{2}\right) \ldots\left(1-1 / p_{k}\right) .
$$

[^0]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, $m \geq 2$, then

$$
a^{\phi(m)} \equiv 1 \quad(\bmod m) .
$$

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

$$
a^{p-1} \equiv 1 \quad(\bmod p)
$$

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

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

$$
x \equiv y \quad(\bmod \phi(m)) \quad \Rightarrow \quad a^{x} \equiv a^{y} \quad(\bmod m)
$$

Consequently, the following function is well defined:

$$
\begin{aligned}
\mathbb{Z}_{m}^{*} \times \mathbb{Z}_{\phi(m)} & \rightarrow \mathbb{Z}_{m}^{*} \\
\left([a]_{m},[x]_{\phi(m)}\right) & \mapsto\left[a^{x}\right]_{m}
\end{aligned}
$$

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

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

if $\operatorname{gcd}(a, m)=1$. For instance:
$3^{9734888} \bmod 100=3^{9734888 \bmod \phi(100)} \bmod 100$

$$
=3^{9734888 \bmod 40} \bmod 100=3^{8} \bmod 100=6561 \bmod 100=61
$$

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 that ${ }^{2}$

$$
2^{716311796279-1}=2^{716311796278} \equiv 127835156517 \quad(\bmod 716311796279)
$$

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

[^1]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
\[

\left\{$$
\begin{array}{rlll}
x & \equiv & r_{1} & \left(\bmod m_{1}\right) \\
x & \equiv & r_{2} & \left(\bmod m_{2}\right) \\
& \cdots & & \\
x & \equiv & r_{k} & \left(\bmod m_{k}\right)
\end{array}
$$\right.
\]

has a unique solution modulo $M=m_{1} m_{2} \ldots m_{k}$.
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

$$
x=M_{1} s_{1} r_{1}+M_{2} s_{2} r_{2}+\cdots+M_{k} s_{k} r_{k}
$$

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:

$$
\left\{\begin{array}{l}
x \equiv 2 \quad(\bmod 3) \\
x \equiv 4 \quad(\bmod 5) \\
x \equiv 6 \quad(\bmod 7)
\end{array}\right.
$$

We have: $M=3 \cdot 5 \cdot 7=105, M_{1}=105 / 3=35 \equiv 2(\bmod 3)$, $M_{2}=105 / 5=21 \equiv 1(\bmod 5), M_{3}=105 / 7=15 \equiv 1(\bmod 7) ; s_{1}=$ "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

$$
x=35 \cdot 2 \cdot 2+21 \cdot 1 \cdot 4+15 \cdot 1 \cdot 6=314 \equiv 104 \quad(\bmod 105) .
$$

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


[^0]:    ${ }^{1}$ A function $f(x)$ of positive integers such that $\operatorname{gcd}(a, b)=1 \Rightarrow f(a b)=f(a) f(b)$ is called multiplicative.

[^1]:    ${ }^{2}$ Given a power $a^{x}$, there is an efficient method (easy to implement as an algorithm) to reduce $a^{x}$ modulo $m$.

