**Topic: Number Theory**

**Lec-1**

**Course: Discrete Mathematics**

## Introduction

In the next sections we will review concepts from **Number Theory**, the branch of mathematics that deals with integer numbers and their properties.

We will be covering the following topics:

1. Divisibility and Modular Arithmetic
2. Prime Numbers, Greatest Common Divisors (GCD) and Euclidean Algorithm.
3. Applications: solving congruences, applications, cryptography.

# Divisibility

When dividing an integer by a second nonzero integer, the quotient may or may not be an integer.
For example, $12/3 = 4$ while $9/4 = 2.25$.

### Definition

If $a$ and $b$ are integers with $a \neq 0$, we say that $a$ *divides* $b$ if there exists an integer $c$ such that $b = ac$. When $a$ divides $b$ we say that $a$ is a *factor* of $b$ and that $b$ is a *multiple* of $a$.
The notation $a \mid b$ denotes $a$ divides $b$ and $a \nmid b$ denotes $a$ does not divide $b$.

Back to the above examples, we see that $3$ divides $12$, denoted as $3 \mid 12$, and $4$ does not divide $9$, denoted as $4 \nmid 9$.

Activate Win
Go to Settings to

**Example.** The following examples illustrate the concept of divisibility of integers: $13 \mid 182$, $-5 \mid 30$, $17 \mid 289$, $6 \nmid 44$, $7 \nmid 50$, $-3 \mid 33$, and $17 \mid 0$.

**Example.** The divisors of 6 are $\pm 1$, $\pm 2$, $\pm 3$, and $\pm 6$. The divisors of 17 are $\pm 1$ and $\pm 17$. The divisors of 100 are $\pm 1, \pm 2, \pm 4$, $\pm 5$, $\pm 10$, $\pm 20$, $\pm 25$, $\pm 50$, and $\pm 100$.

**Proposition 1.3.** If $a$, $b$, and $c$ are integers with $a \mid b$ and $b \mid c$, then $a \mid c$.

*Proof.* Since $a \mid b$ and $b \mid c$, there are integers $e$ and $f$ with $ae = b$ and $bf = c$. Hence, $bf = (ae)f = a(ef) = c$, and we conclude that $a \mid c$. $\square$

**Example.** Since $11 \mid 66$ and $66 \mid 198$, Proposition 1.3 tells us that $11 \mid 198$.

**Proposition 1.4.** If $a$, $b$, $m$, and $n$ are integers, and if $c \mid a$ and $c \mid b$, then $c \mid (ma+nb)$.

*Proof.* Since $c \mid a$ and $c \mid b$, there are integers $e$ and $f$ such that $a = ce$ and $b = cf$. Hence, $ma + nb = mce + ncf = c(me+nf)$. Consequently, we see that $c \mid (ma+nb)$. □

**Example.** Since $3 \mid 21$ and $3 \mid 33$, Proposition 1.4 tells us that

$$3 \mid (5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6 .$$

## The division algorithm

*Let $a$ be an integer and $d$ a positive integer. Then, there are unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = dq + r$.*

- $d$ is called the *divisor*;
- $a$ is called the *dividend*;
- $q$ is called the *quotient*; this can be expressed $q = a \ \mathbf{div} \ d$;
- $r$ is called the *remainder*; this cane be expressed $r = a \ \mathbf{mod} \ d$;

**Example:**

If $a = 7$ and $d = 3$, then $q = 2$ and $r = 1$, since $7 = (2)(3) + 1$.

If $a = -7$ and $d = 3$, then $q = -3$ and $r = 2$, since $-7 = (-3)(3) + 2$.

Try a=57, d=9

a=-57, d=9

a=3,d=8

## Greatest Common Divisors

**Definition**. The *greatest common divisor* of two integers $a$ and $b$, that are not both zero, is the largest integer which divides both $a$ and $b$.

The greatest common divisor of $a$ and $b$ is written as $(a, b)$.

**Example**. The common divisors of 24 and 84 are $\pm 1$, $\pm 2$, $\pm 3$, $\pm 4$, $\pm 6$, and $\pm 12$. Hence $(24, 84) = 12$. Similarly, looking at sets of common divisors, we find that $(15, 81) = 3$, $(100, 5) = 5$, $(17, 25) = 1$, $(0, 44) = 44$, $(-6, -15) = 3$, and $(-17, 289) = 17$.

We are particularly interested in pairs of integers sharing no common divisors greater than 1. Such pairs of integers are called *relatively prime*.

**Definition**. The integers $a$ and $b$ are called *relatively prime* if $a$ and $b$ have greatest common divisor $(a, b) = 1$.

**Example**. Since $(25, 42) = 1$, 25 and 42 are relatively prime.

**Definition.** Let $a_1, a_2, \ldots, a_n$ be integers, that are not all zero. The *greatest common divisor* of these integers is the largest integer which is a divisor of all of the integers in the set. The greatest common divisor of $a_1, a_2, \ldots, a_n$ is denoted by $(a_1, a_2, \ldots, a_n)$.

**Example.** We easily see that $(12, 18, 30) = 6$ and $(10, 15, 25) = 5$.

**The Euclidean Algorithm.** Let $r_0 = a$ and $r_1 = b$ be nonnegative integers with $b \neq 0$. If the division algorithm is successively applied to obtain $r_j = r_{j+1}q_{j+1} + r_{j+2}$ with $0 < r_{j+2} < r_{j+1}$ for $j = 0,1,2,\ldots,n-2$ and $r_n = 0$,

$a = bq_1 + r_2 \quad 0 < r_2 < b$

then $(a, b) = r_{n-1}$, the last nonzero remainder.

**Example.** To find $(252, 198)$, we use the division algorithm successively to obtain

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18. \end{aligned}$$

Hence $(252, 198) = 18$.

## Theorem (A)

*If $a$ and $b$ are positive integers, then there exist integers $s$ and $t$ such that gcd$(a, b) = sa + tb$.*

Example:

$\gcd(252, 198) = 18 = 4 \cdot 252 - 5 \cdot 198$

Consider the steps of the Euclidean algorithm for $\gcd(252, 198)$:

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 \end{aligned}$$

$$\begin{aligned} \gcd(252, 198) = 18 &= 54 - 1 \cdot 36 \\ &= 54 - 1(198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198 \end{aligned}$$

Therefore, $\gcd(252, 198) = 4 \cdot 252 - 5 \cdot 198$.

## The Fundamental Theorem of Arithmetic

**The Fundamental Theorem of Arithmetic.** Every positive integer can be written uniquely as a product of primes, with the prime factors in the product written in order of nondecreasing size.

**Example.** The factorizations of some positive integers are given by

$$240 = 2\cdot2\cdot2\cdot2\cdot3\cdot5 = 2^4\cdot3\cdot5,\ 289 = 17\cdot17 = 17^2,\ 1001 = 7\cdot11\cdot13\ .$$

To describe, in general, how prime factorizations can be used to find greatest common divsors, let $\min(a, b)$ denote the smaller or minimum, of the two numbers $a$ and $b$. Now let the prime factorizations of $a$ and $b$ be

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

$$(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)},$$

# Modular Arithmetic

**Definition**

If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is *congruent to* $b$ *modulo* $m$ if $m$ divides $a-b$. We use the notation $a \equiv b \pmod{m}$ if this is the case, and $a \not\equiv b \pmod{m}$, otherwise.

Example: $10$ and $26$ are congruent modulo $8$, since their difference is $16$ or $-16$, which is divisible by $8$. When dividing $10$ and $26$ by $8$ we get $10 = 1 \cdot 8 + 2$ and $26 = 4 \cdot 8 + 2$. So $10 \textbf{ mod } 8 = 2 = 26 \textbf{ mod } 8$.

Activate Windo
Go to Settings to act

**Example.** We have $22 \equiv 4 \pmod 9$, since $9 \mid (22-4) = 18$. Likewise $3 \equiv -6 \pmod 9$ and $200 \equiv 2 \pmod 9$.

Congruences often arise in everyday life. For instance, clocks work either modulo 12 or 24 for hours, and modulo 60 for minutes and seconds, calendars work modulo 7 for days of the week and modulo 12 for months. Utility meters often operate modulo 1000, and odometers usually work modulo 100000.

Let $m$ be a positive integer. The integers $a$ and $b$ are congruent modulo $m$ if and only if there is an integer $k$ such that $a = b + km$

Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Let $m$ be a positive integer and let $a$ and $b$ be integers. Then,

$$(a + b) \mathbf{\ mod\ } m = ((a \mathbf{\ mod\ } m) + (b \mathbf{\ mod\ } m)) \mathbf{\ mod\ } m$$

$$ab \mathbf{\ mod\ } m = ((a \mathbf{\ mod\ } m)(b \mathbf{\ mod\ } m)) \mathbf{\ mod\ } m$$

**Proposition 3.2.** Let $m$ be a positive integer. Congruences modulo $m$ satisfy the following properties:

(i) *Reflexive property*. If $a$ is an integer, then $a \equiv a \pmod{m}$.

(ii) *Symmetric property*. If $a$ and $b$ are integers such that $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(iii) *Transitive property*. If $a, b,$ and $c$ are integers with $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

*Proof.*

(i) We see that $a \equiv a \pmod{m}$, since $m \mid (a-a) = 0$.

(ii) If $a \equiv b \pmod{m}$, then $m \mid (a-b)$. Hence, there is an integer $k$ with $km = a - b$. This shows that $(-k)m = b - a$, so that $m \mid (b-a)$. Consequently, $b \equiv a \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a-b)$ and $m \mid (b-c)$. Hence, there are integers $k$ and $\ell$ with $km = a - b$ and $\ell m = b - c$. Therefore, $a - c = (a-b) + (b-c) = km + \ell m = (k+\ell)m$. Consequently, $m \mid (a-c)$ and $a \equiv c \pmod{m}$. □

**Theorem 3.1.** If $a, b, c$, and $m$ are integers with $m > 0$ such that $a \equiv b \pmod{m}$, then

(i) $a + c \equiv b + c \pmod{m}$,

(ii) $a - c \equiv b - c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

**Example.** Since $19 \equiv 3 \pmod{8}$, it follows from Theorem 3.1 that

$26 = 19 + 7 \equiv 3 + 7 = 10 \pmod{8}$, $15 = 19 - 4 \equiv 3 - 4 \equiv -1 \pmod{8}$, and $38 = 19 \cdot 2 \equiv 3 \cdot 2 = 6 \pmod{8}$.

What happens when both sides of a congruence are divided by an integer? Consider the following example.

**Example.** We have $14 = 7 \cdot 2 \equiv 4 \cdot 2 = 8 \pmod{6}$. But $7 \not\equiv 4 \pmod{6}$.

**Theorem 3.2.** If $a, b, c$ and $m$ are integers such that $m > 0$, $d = (c,m)$, and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m/d}$.

*Proof.* If $ac \equiv bc \pmod{m}$, we know that $m \mid (ac-bc) = c(a-b)$. Hence, there is an integer $k$ with $c(a-b) = km$. By dividing both sides by $d$, we have $(c/d)(a-b) = k(m/d)$. Since $(m/d, c/d) = 1$, from Proposition 2.1 it follows that $m/d \mid (a-b)$. Hence, $a \equiv b \pmod{m/d}$. $\square$

**Example.** Since $50 \equiv 20 \pmod{15}$ and $(10,5) = 5$, we see that $50/10 \equiv 20/10 \pmod{15/5}$, or $5 \equiv 2 \pmod 3$.

**Corollary 3.1.** If $a$, $b$, $c$, and $m$ are integers such that $m > 0$, $(c,m) = 1$, and $ac \equiv bc \pmod m$, then $a \equiv b \pmod m$.

**Example.** Since $42 \equiv 7 \pmod 5$ and $(5,7) \equiv 1$, we can conclude that $42/7 \equiv 7/7 \pmod 5$, or that $6 \equiv 1 \pmod 5$.

**Theorem 3.3.** If $a, b, c, d$, and $m$ are integers such that $m > 0$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then

(i) $a + c \equiv b + d \pmod{m}$,

(ii) $a - c \equiv b - d \pmod{m}$,

(iii) $ac \equiv bd \pmod{m}$.

**Example.** Since $13 \equiv 8 \pmod{5}$ and $7 \equiv 2 \pmod{5}$, using Theorem 3.3 we see that $20 = 13 + 7 \equiv 8 + 2 \equiv 0 \pmod{5}$, $6 = 13 - 7 \equiv 8 - 7 \equiv 1 \pmod{5}$, and $91 = 13 \cdot 7 \equiv 8 \cdot 2 = 16 \pmod{5}$.

**Theorem 3.5.** If $a$, $b$, $k$, and $m$ are integers such that $k > 0$, $m > 0$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ .

*Proof.* Because $a \equiv b \pmod{m}$, we have $m \mid (a - b)$. Since

$$a^k - b^k = (a-b)(a^{k-1}+a^{k-2}b+\cdots+ab^{k-2}+b^{k-1}),$$

we see that $(a - b) \mid (a^k - b^k)$. Therefore, from Proposition 1.2 it follows that $m \mid (a^k - b^k)$. Hence, $a^k \equiv b^k \pmod{m}$. □

**Example.** Since $7 \equiv 2 \pmod{5}$, Theorem 3.5 tells us that $343 = 7^3 \equiv 2^3 \equiv 8 \pmod{5}$.

**Theorem 3.6.** If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots,$ $a \equiv b \pmod{m_k}$ where $a, b, m_1, m_2, \ldots, m_k$ are integers with $m_1, m_2, \ldots, m_k$ positive, then

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]},$$

where $[m_1, m_2, \ldots, m_k]$ is the least common multiple of $m_1, m_2, \ldots, m_k$.

**Corollary 3.2.** If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, \ldots,$ $a \equiv b \pmod{m_k}$ where $a$ and $b$ are integers and $m_1, m_2, \ldots, m_k$ are relatively prime positive integers, then

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

In our subsequent studies, we will be working with congruences involving large powers of integers. For example, we will want to find the least positive residue of $2^{644}$ modulo 645. If we attempt to find this least positive residue by first computing $2^{644}$, we would have an integer with 194 decimal digits, a most undesirable thought. Instead, to find $2^{644}$ modulo 645 we first express the exponent 644 in binary notation:

$$(644)_{10} = (1010000100)_2 .$$

Next, we compute the least positive residues of $2, 2^2, 2^4, 2^8, \ldots, 2^{512}$ by successively squaring and reducing modulo 645. This gives us the congruences

$$\begin{aligned}
2 &\equiv 2 \pmod{645},\\
2^2 &\equiv 4 \pmod{645},\\
2^4 &\equiv 16 \pmod{645},\\
2^8 &\equiv 256 \pmod{645},\\
2^{16} &\equiv 391 \pmod{645},\\
2^{32} &\equiv 16 \pmod{645},\\
2^{64} &\equiv 256 \pmod{645},\\
2^{128} &\equiv 391 \pmod{645},\\
2^{256} &\equiv 16 \pmod{645},\\
2^{512} &\equiv 256 \pmod{645}.
\end{aligned}$$

We can now compute $2^{644}$ modulo 645 by multiplying the least positive residues of the appropriate powers of 2. This gives

$$\begin{aligned}
2^{644} = 2^{512+128+4} = 2^{512}2^{128}2^4 &\equiv 256 \cdot 391 \cdot 16\\
&= 1601536 \equiv 1 \pmod{645}.
\end{aligned}$$

Activate Winc
Go to Settings to

We have just illustrated a general procedure for *modular exponentiation*, that is, for computing $b^N$ modulo $m$ where $b$, $m$, and $N$ are positive integers. We first express the exponent $N$ in binary notation, as $N = (a_k a_{k-1} \ldots a_1 a_0)_2$. We then find the least positive residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo $m$, by successively squaring and reducing modulo $m$. Finally, we multiply the least positive residues modulo $m$ of $b^{2^j}$ for those $j$ with $a_j = 1$, reducing modulo $m$ after each multiplication.

## Linear Congruences

A congruence of the form

$$ax \equiv b \pmod{m},$$

How can we solve it, i.e. find all integers $x$ that satisfy it?

One possible method is to multiply both sides of the congruence by an inverse $\overline{a}$ of $a \pmod{m}$ if one such inverse exists:
$\overline{a}$ is an **inverse** of $a \pmod{m}$ if $\overline{a}a \equiv 1 \pmod{m}$.

Example:
$5$ is an inverse of $3 \pmod{7}$, since $5 \cdot 3 \equiv 15 \equiv 1 \pmod{7}$.
Using this we can solve:

$$\begin{aligned} 3x &\equiv 4 \pmod{7} \\ 5 \cdot 3x &\equiv 5 \cdot 4 \pmod{7} \\ 1 \cdot x &\equiv 20 \pmod{7} \\ x &\equiv 6 \pmod{7} \end{aligned}$$

Substitute back into the original linear congruence to check that $6$ is a solution:

$$3 \cdot 6 \equiv 18 \equiv 4 \pmod{7}.$$

For a simple example, you can easily check by inspection that the linear congruence

$$6x \equiv 4 \pmod{10}$$

has solutions $x = 4, 9$. Already we see a difference from ordinary algebra: linear congruences can have more than one solution!

Are these the *ONLY* solutions? No. In fact, any integer which is congruent to either 4 or 9 mod 10 is also a solution. You should check this for yourself now.

So any integer of the form $4 + 10k$ or of the form $9 + 10k$ where $k \in \mathbb{Z}$ is a solution to the given linear congruence. The above linear congruence has *infinitely many* integer solutions.

Theorem 20.1.7: **A linear congruence $ax \equiv b \bmod m$ has solutions if and only if $gcd(a, m) \mid b$.**
**(in which case it has precisely $gcd(a, m)$ different solutions modulo $m$)**

Examples:

a) Solve $14x \equiv 21 \; mod \; 35$.
Note: gcd(14,35)=7, which divides 21, so there should be 7 solutions modulo 35.

Solutions mod 35: $x \equiv 4, 9, 14, 19, 24, 29, or\ 34 \;\; mod\ 35$

b) Solve $14x \equiv 16 \mod 35$.

**To be continued……**

Thanks for watching

Have a nice day