Faculty of Computer Science and Information Technology

Discrete Mathematics

Lecture 5

Number Theory

Division

- **Definition:**

If a and b are integers with $a \neq 0$, $\frac{b}{a} = c$ $\underline{b = ac}$

we say that a *divides* b if there is an integer c such that

$b = ac$. (or equivalently, if $\frac{b}{a}$ is an integer) a / b $a \mid b \rightarrow \frac{b}{a} = c$ integer

we say that a is a *factor* of b and that b is a *multiple* of a.

notation $a \mid b$ denotes that a divides b. $3 \quad 12$ $3 \mid 12$ $\overset{b}{12} = \overset{a}{3} \times \overset{c}{4}$

We write $a \nmid b$ when a does not divide b.

Division

Example 1

Determine whether $3 \mid 7$ and whether $3 \mid 12$.

$3 \mid 7$

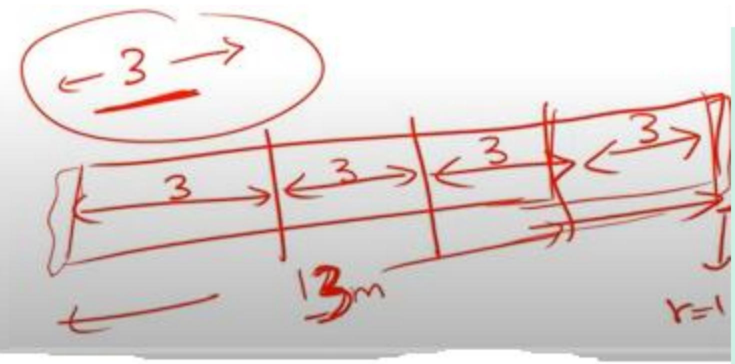
$a \mid b$

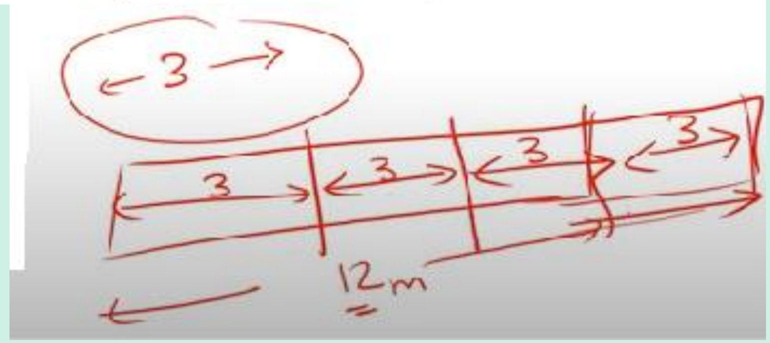
It follows that $3 \nmid 7$, because $7/3$ is not an integer.

$3 \mid 12$ because $12/3 = 4$. which is an integer.

$r = 0$

$\frac{13}{3}$ $\quad 3 \nmid 13$





Division

Theorem

Let a, b, and c be integers, where $a \neq 0$. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

(ii) if $a \mid b$, then $a \mid bc$ for all integers c

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$

$\overset{a}{3} \mid \overset{b}{6}$, $\overset{a}{3} \mid \overset{c}{9}$

$3 \mid (6+9)$

<u>As a result:</u>

If $a \mid b$ and $a \mid c$, then $a \mid \boldsymbol{m}b + \boldsymbol{n}c$ whenever $\boldsymbol{m}$ and $\boldsymbol{n}$ are integers

3 | 12 and 3 | 15, then 3 | 12m + 15n for all integers m and n.

Division

Examples

1)Does 2 divdes 4?

2)Does 2 divdes 8?

3) 2 divdes 4 + 8 ?

4)Does 2 divdes 4?

5)Does 2 divdes 4 * 5?

6)Does 2 divdes 4 * 4?

7)Does 2 divdes 4?

8)Does 4 divdes 16?

9)Does 2 divdes 16?

2 | 4 → 4/2 = 2   r = 0

2 | 4 × 2

Division

The Division Algorithm

$\frac{1}{-2} = \frac{-1}{2}$

Let $\boldsymbol{a}$ be an integer and $\boldsymbol{d}$ a positive integer. Then

$$\frac{a}{d} = \boxed{\text{quotient } (q)} \quad , \quad \boxed{\text{remainder } (r)}$$

dividend → a, divisor → d

$$\text{with}, \quad \boxed{0 \le r < d}$$

The remainder r cannot be negative!

$$a = dq + \mathbf{r}$$

$$q = a \textbf{ div } d$$
$$r = a \textbf{ mod } d$$

$\overset{a}{12} = \overset{d}{3} \times \overset{q}{4} + \overset{r}{0}$

$\overset{a}{10} = \overset{d}{3} \times \overset{q}{3} + \overset{r}{1}$

$$q = \left\lfloor \frac{a}{d} \right\rfloor$$

$$r = a - qd$$

Division

Example 1

What are the quotient and remainder when 101 is divided by 11?

$$q = \lfloor 101/11 \rfloor = \lfloor 9.18 \rfloor = 9,$$

$$r = 101 - (9)(11) = 2$$

$$\underline{r} = \overset{a}{101} - \underline{(\overset{q}{9})(\overset{d}{11})} = \boxed{2}$$

Solution: We have

$$\underline{r} = \underline{a} - \underline{dq}$$

$$\boxed{a = dq + r}$$

$$101 = 11 \cdot 9 + 2.$$

Hence, the quotient when 101 is divided by 11 is $\overset{q}{9} = 101$ **div** 11, and the remainder is $\underset{r}{2} = 101$ **mod** 11.

Division

Example 2

What are the quotient and remainder when -11 is divided by 3?

$-11-(-9) = -2$

$r = -2$

!!

$$q = \lfloor -11/3 \rfloor = \lfloor -3.6 \rfloor = -4,$$

$$r = -11 - (3)(-4) = 1$$

$0 \leq r < 3$

$= r = \underbrace{(-11)}_{a} - \underbrace{(3)}_{d}\underbrace{(-4)}_{q} = \boxed{1}$

Solution: We have

$$-11 = 3(-4) + 1.$$

$a = dq + r$

Hence, the quotient when -11 is divided by 3 is $-4 = -11$ **div** 3, and the remainder is $1 = -11$ **mod** 3.

Division

Example 3

Evaluate:

- $11 \bmod 2 = 1$

$$q = \lfloor 11/2 \rfloor = 5,$$
$$r = 11 - (2)(5) = 1$$

- $-11 \bmod 2 = 1$

$$q = \lfloor -11/2 \rfloor = -6,$$
$$r = -11 - (2)(-6) = 1$$

Primes

Definition

A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p.

A positive integer that is greater than 1 and is not prime is called *composite*.

Ex: The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

Primes

Theorem 1

The Fundamental Theorem OF Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes.

2, 3, 4, 5, 6 - -

$4 \rightarrow 2 \times 2$, $6 \rightarrow 2 \times 3$

Theorem 2

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Primes

<u>Example 1:</u> The integer 100 is prime or not ?

The prime numbers $\leq \sqrt{100}$ are 2, 3, 5, and 7

$$2|100, \qquad \text{and} \qquad 5|100$$

So, 100 is not a prime integer. 100 is a composite integer.

Example 2

2, 3, 4, ---, 101

The integer 101 is prime or not ?

$\leq \sqrt{101}$

The prime numbers $\leq \sqrt{101}$ are 2, 3, 5, and 7

$$2 \nmid 101, \qquad 3 \nmid 101, \qquad 5 \nmid 101, \qquad \text{and} \qquad 7 \nmid 101$$

So, 101 is a prime integer.

Primes

Example 3

Find the prime factorization of 100?

The prime numbers $\leq \sqrt{100}$ are 2, 3, 5, and 7

$$\left(\begin{array}{r|r} 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}\right)$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5$$
$$= 2^2 \cdot 5^2$$

$$\left(\begin{array}{r|r} 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}\right)$$

$\sqrt{50}$

$\leq 2, 3,$

Primes

Primes

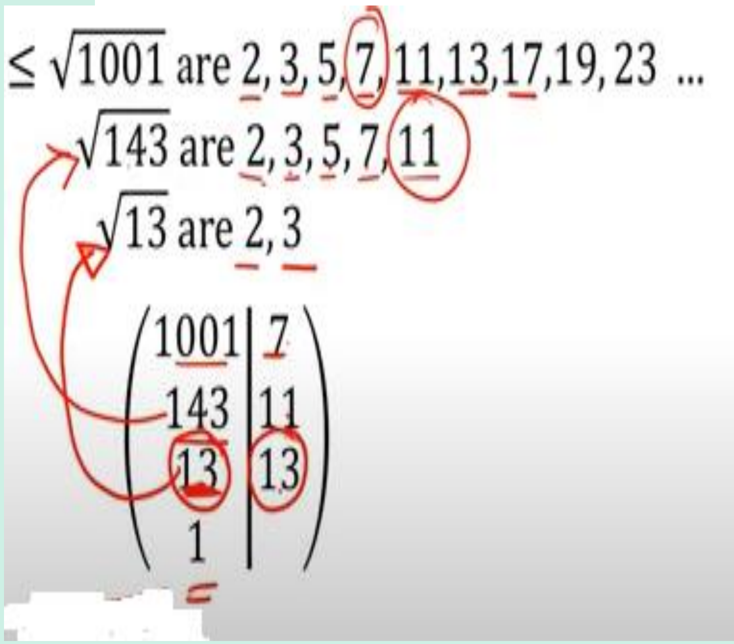
Example 4

Find the prime factorization of 1001?

The prime numbers $\leq \sqrt{1001}$ are $2, 3, 5, 7, 11, 13, 17, 19, 23$ ...

$\sqrt{143}$ are $2, 3, 5, 7, 11$

$\sqrt{13}$ are $2, 3$



$$\left(\begin{array}{c|c} 1001 & 7 \\ 143 & 11 \\ 13 & 13 \\ 1 & \end{array}\right)$$

$$1001 = 7 \cdot 11 \cdot 13$$

Primes

Example 5

Find the prime factorization of 999?

3	999
3	333
3	111
37	37
	1

~~2~~, 3, 5, 7 →

$999 = 3 \times 3 \times 3 \times 37$

- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

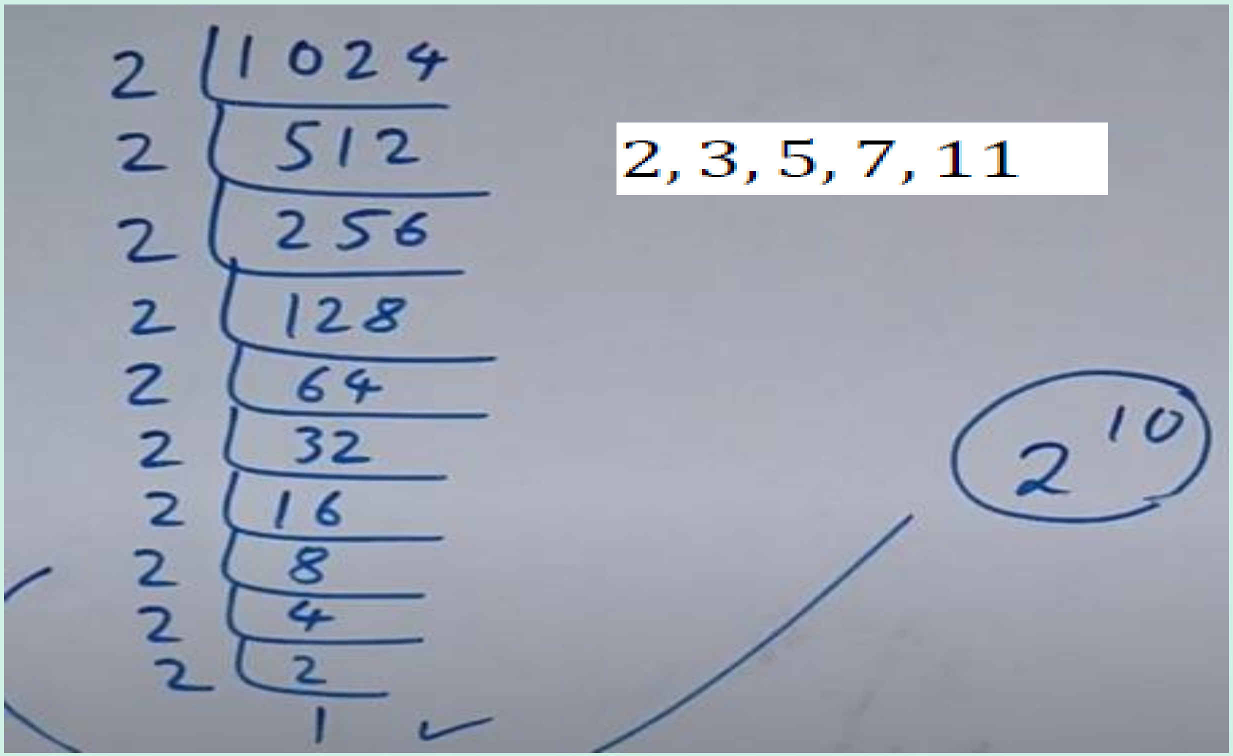
Example

$641 = 641$

Primes

Example 6

Find the prime factorization of 1024?



- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Greatest Common Divisors

Definition "gcd"

Let a and b be integers, not both zero.

The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b.

is denoted by $\gcd(a, b)$.

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

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

$$\underset{2^3}{} \quad \underset{5^2}{}$$

$$a = \overset{2^3}{p_1^{a_1}} \overset{5^2}{p_2^{a_2}} \cdots p_n^{a_n}, \ b = \overset{2^2}{p_1^{b_1}} \overset{5^0}{p_2^{b_2}} \cdots p_n^{b_n},$$

$$\gcd(a, b) = \underset{2^2}{p_1^{\min(a_1, b_1)}} \underset{5^0}{p_2^{\min(a_2, b_2)}} \cdots p_n^{\min(a_n, b_n)},$$

Greatest Common Divisors

Definition "gcd"

For 12 and 18, what is the greatest common factor?

We have four common factors $\{1, 2, 3, 6\}$
The greatest one is $\{6\}$.

Example 1

What is the greatest common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, $\gcd(24, 36) = 12$.

Greatest Common Divisors

Example 1

What is the greatest common divisor of 24 and 36?

$\sqrt{24}$ are 2, 3

$\sqrt{36}$ are 2, 3, 5

$$\left(\begin{array}{c|c} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}\right) = 2^3 \cdot 3$$

$$\left(\begin{array}{c|c} 36 & 2 \\ 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array}\right) = 2^2 \cdot 3^2$$

$$\gcd(24,36) = 2^2 \cdot 3 = 12$$

Greatest Common Divisors

Example 2

What is the gcd(120, 500) ?

$\sqrt{120}$ are 2, 3,5,7

$\sqrt{500}$ are 2, 3, 5,7,11,13,17,19

$$\left(\begin{array}{r|r} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}\right) = 2^3 \cdot 3 \cdot 5$$

$\underline{2}^{3} \cdot \underline{3}^{0} \cdot \underline{5}^{1}$

$$\left(\begin{array}{r|r} 500 & 2 \\ 250 & 2 \\ 125 & 5 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}\right) = 2^2 \cdot 5^3$$

$\underline{2}^{2} \cdot \underline{5}^{3} \cdot 3^{0}$

$\underline{2}^{2} \cdot \underline{3}^{0} \cdot \underline{5}^{1} = 20$

$$\gcd(120, 500) = 2^2 \cdot 3^0 \cdot 5 = 20$$

Greatest Common Divisors

Definition 1

The integers a and b are $\boxed{\textit{relatively prime}}$ if their $\boxed{\text{greatest common divisor is 1}}$.

Is 17 and 22 are relatively prime? (Yes)

gcd 17, 22 = 1

$1 = 2^0 \times 11^0 \times 17^0$

$17 = 17^1 \cdot 2^0 \cdot 11^0 \qquad 22 = 2^1 \times 11^1 \times 17^0$

Greatest Common Divisors

Definition 2

The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

Example:

Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution:

Because $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, and $\gcd(17, 21) = 1$, we conclude that 10, 17, and 21 are pairwise relatively prime.

Because $\gcd(10, 24) = 2 > 1$, we see that 10, 19, and 24 are not pairwise relatively prime.

Least Common Multiple

Definition "lcm"

The *least common multiple* of the positive integers a and b

is the smallest positive integer that

is divisible by both a and b.

The least common multiple of a and b is denoted by $\text{lcm}(a, b)$.

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

Least Common Multiple

Example 1

What is the lcm 24, 36 ?

$\sqrt{24}$ are 2, 3

$\sqrt{36}$ are 2, 3, 5

$$\left(\begin{array}{c|c} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}\right) = 2^3 \cdot 3$$

$$\left(\begin{array}{c|c} 36 & 2 \\ 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array}\right) = 2^2 \cdot 3^2$$

$$\mathrm{lcm}(24,36) = 2^3 \cdot 3^2 = 72$$

Least Common Multiple

Example 2

What is the lcm 120, 500 ?

$\sqrt{120}$ are 2, 3,5,7

$\sqrt{500}$ are 2, 3, 5,7,11,13,17,19

$$\left(\begin{array}{c|c} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}\right) = 2^3 \cdot 3 \cdot 5$$

$$\left(\begin{array}{c|c} 500 & 2 \\ 250 & 2 \\ 125 & 5 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}\right) = 2^2 \cdot 5^3$$

$$\operatorname{lcm}(120, 500) = 2^3 \cdot 3^1 \cdot 5^3 = 3000$$

Questions?