1. If \( a \) and \( b \) are integers with \( a \neq 0 \), we say \( a \text{ divides } b \) if there is an integer \( k \) such that \( b = ak \). \( a \) is called a \textit{factor} of \( b \) and \( b \) is a \textit{multiple} of \( a \).

Notation: \( a \mid b \) when \( a \text{ divides } b \). \( a \notmid b \) when \( a \text{ does not divide } b \).

Examples: (a) \( 3 \mid 12 \). (b) \( 3 \notmid 7 \).

Essential properties: Let \( a, b, c \) be integers, then

- if \( a \mid b \) and \( a \mid c \), then \( a \mid (b + c) \) and \( a \mid (b - c) \) and
- if \( a \mid b \), then \( a \mid bc \) for all integers \( c \)
- if \( a \mid b \) and \( b \mid c \), then \( a \mid c \)

2. Theorem (Division Algorithm): Let \( a \) and \( b \) be integers with \( b \neq 0 \). Then there exist unique integers \( q \) and \( r \), such that

\[
a = b \cdot q + r, \quad 0 \leq r < |b|.
\]

The number \( b \) is called the \textit{divisor}, \( q \) is called the \textit{quotient} and \( r \) is called the \textit{remainder} (Note that \( r \) must be non-negative.)

Example: (a) \( 101 = 11 \cdot 9 + 2 \). (b) \( -11 = 3 \cdot (-4) + 1 \).

3. A positive integer \( p \) greater than 1 is called \textit{prime} if the only positive factors of \( p \) are 1 and \( p \). Otherwise, it is called \textit{composite}.

E.g.: \( 2, 3, 5, 7, 11, 13, \ldots \) are primes.

4. The Fundamental Theorem of Arithmetic (“prime factorization”): Every integer \( n > 1 \) can be written as a product of primes. (Proof by induction)

Examples: (a) \( 100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2 \). (b) \( 999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37 \). (c) \( 1024 = 2^{10} \)

5. Let \( a \) and \( b \) be integers, not both zero. The \textit{largest} integer \( d \) such that \( d \mid a \) and \( d \mid b \) is called the \textit{greatest common divisor} (gcd) of \( a \) and \( b \). notation: \( \gcd(a, b) = d \).

Examples:

(a) \( \gcd(24, 36) = 12 \), note that the common divisors of 24 and 36 are 1, 2, 3, 4, 6, 12.

(b) \( \gcd(17, 22) = 1 \), note that 17 is a prime.

(c) \( \gcd(1, 123) = 1 \) and \( \gcd(0, 321) = 321 \)

(d) \( \gcd(12, -18) = 6 \), note that the common divisors of 12 and \( -18 \) are \( \pm 1, \pm 2, \pm 3, \pm 6 \).

6. Prime factorization based algorithm for computing \( \gcd(a, b) \):

1. compute the prime factorization \( a = 2^{n_1}3^{n_2}5^{n_3}\ldots \)

2. compute the prime factorization \( b = 2^{m_1}3^{m_2}5^{m_3}\ldots \)

3. \( \gcd(a, b) = 2^{\min(n_1, m_1)}3^{\min(n_2, m_2)}5^{\min(n_3, m_3)}\ldots \)

Example: By the prime factorizations of \( 120 = 2^3 \cdot 3 \cdot 5 \) and \( 500 = 2^2 \cdot 5^3 \),

\[
\gcd(120, 500) = 2^{\min(3, 2)}3^{\min(1, 0)}5^{\min(1, 3)} = 2^23^05^1 = 20
\]
7. Euclidean algorithm for computing \( \text{gcd}(a, b) \).

- **Theorem:** Let \( a = bq + r \). Then \( \text{gcd}(a, b) = \text{gcd}(b, r) \).

  **Proof:** If we can show the following set identity:
  
  \[ (*) \text{ "Set of common divisors of } a \text{ and } b\" = \text{"Set of common divisors of } b \text{ and } r\"
  
  Then we will have shown that \( \text{gcd}(a, b) = \text{gcd}(b, r) \), since both pairs must have the same greatest common divisor. To show \((*)\),
  
  "\( \rightarrow\)" let \( d | a \) and \( d | b \), then \( d | bq \). It follows that \( d | a - bq \). Therefore \( d | b \) and \( d | r \).
  
  "\( \leftarrow\)" let \( d | b \) and \( d | r \), then \( d | bq \). It follows that \( d | bq + r \). Therefore, \( d | a \) and \( d | b \).

- **Algorithm:** let \( r_0 = a \) and \( r_1 = b \). By successively applying “the division algorithm”, we obtain

  \[
  \begin{align*}
  a &= r_0 = r_1 \cdot q_1 + r_2, \quad &0 \leq r_2 < r_1 = b, \\
  r_1 &= r_2 \cdot q_2 + r_3, \quad &0 \leq r_3 < r_2, \\
  &\vdots \\
  r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n, \quad &0 \leq r_n < r_{n-1}, \\
  r_{n-1} &= r_n \cdot q_n + 0.
  \end{align*}
  \]

  Eventually, a remainder of zero must occur, since the sequence of remainders \( a = r_0 > r_1 > r_2 > \cdots \geq 0 \) cannot contain more than \( a \) terms. As a result, by the theorem, it follows that
  
  \[ \text{gcd}(a, b) = \text{gcd}(r_0, r_1) = \text{gcd}(r_1, r_2) = \cdots = \text{gcd}(r_{n-1}, r_n) = \text{gcd}(r_n, 0) = r_n \]

  Note: it can be shown that the number of divisions required by the Euclidean algorithm is \( O(\log b) \), where assuming \( a \geq b > 0 \)

- **Example:** \( \text{gcd}(414, 662) = ? \)

  \[
  \begin{align*}
  662 &= 414 \cdot 1 + 248 \\
  414 &= 248 \cdot 1 + 166 \\
  248 &= 166 \cdot 1 + 82 \\
  166 &= 82 \cdot 2 + 0 \\
  82 &= 0 \cdot 41 + 0
  \end{align*}
  \]

  Hence \( \text{gcd}(414, 662) = 2 \).

8. Modular operation: \( a \mod m = r \) = the remainder after dividing \( a \) by \( m \) > 0. (note, \( 0 \leq r < m \)).

- Examples:
  
  (a) \( 7 \mod 3 = 1 \), since \( 7 = 3 \cdot 2 + 1 \).  \( \text{ (b) } 3 \mod 7 = 3, \text{ since } 3 = 7 \cdot 0 + 3 \)
  
  (c) \( -133 \mod 9 = 2, \text{ since } -133 = 9 \cdot (-15) + 2 \).

9. If \( a \) and \( b \) are integers, and \( m \) is a positive integer, then \( a \) is congruent to \( b \) modulo \( m \) if \( m | (a - b) \).

- notation: \( a \equiv b \mod m \)

- Examples: \( (a) 17 \equiv 5 \mod 6 \), \( (b) 24 \not\equiv 14 \mod 6 \).

10. By the definition, we know that \( a \equiv b \mod m \) if and only if there is an integer \( k \) such that \( a = b + km \). Using this fact, we can prove the following.

- Basic properties of modular arithmetic: If \( a \equiv b \mod m \) and \( c \equiv d \mod m \), then
  
  (a) \( a + c \equiv b + d \mod m \).
  
  (b) \( ac \equiv bd \mod m \).

11. Applications of congruences: Hashing function, random number generation, cryptology, ....