Divisibility and division algorithm

1. If a and b are integers with $a \neq 0$, we say a *divides* b if there is an integer k such that $b = ak$. a is called a *factor* of b and b is a *multiple* of a.

   Notation: $a \mid b$ when a divides b. $a \nmid b$ when a does not divide b.

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

2. Essential properties: Let a, b, c be integers, then
   - if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$
   - if $a \mid b$, then $a \mid bc$ for all integers c
   - if $a \mid b$ and $b \mid c$, then $a \mid c$

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

   $$a = b \cdot q + r \quad \text{and} \quad 0 \leq r < |b|.$$

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

   Proof: Problems 11.17 and 11.18

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

The Fundamental Theorem of Arithmetic

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

   Examples: 2, 3, 5, 7, 11, 13 are primes.

2. The Fundamental Theorem of Arithmetic ("prime factorization"): Every integer $n > 1$ can be written as a product of primes.

   Proof by induction: see the class website, click "more examples on mathematical 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) $1024 = 2^{10}$

Greatest common divisor and Euclidean algorithm

1. 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* (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 $\pm 1, \pm 2, \pm 3, \pm 6$.

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

   1. compute the prime factorization $a = 2^{n_1}3^{n_2}5^{n_3}\cdots$
   2. compute the prime factorization $b = 2^{m_1}3^{m_2}5^{m_3}\cdots$
   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 $500 = 2^2 \cdot 5^3$,

$$\gcd(120,500) = 2^{\min\{3,2\}}3^{\min\{1,0\}}5^{\min\{1,3\}} = 2^2 3^0 5^1 = 20$$

3. **Euclidean theorem**: Let $a = bq + r$. Then $\gcd(a,b) = \gcd(b,r)$.

   Proof: Let

$$A = \text{set of common divisors of } a \text{ and } b$$
$$B = \text{set of common divisors of } b \text{ and } r.$$

   Then if we can show the following set identity:

$$A = B \tag{1}$$

   we have shown that $\gcd(a,b) = \gcd(b,r)$, since both pairs must have the same greatest common divisor.

   - Show that $A \subseteq B$: let $d \mid a$ and $d \mid b$, then $d \mid bq$. It follows that $d \mid a - bq$. Therefore $d \mid b$ and $d \mid r$.
   - Show that $B \subseteq A$: let $d \mid b$ and $d \mid r$, then $d \mid bq$. It follows that $d \mid bq + r$. Therefore, $d \mid a$ and $d \mid b$.

   Since $A \subseteq B$ and $B \subseteq A$, the set identity (1) is true! $\square$.

4. Euclidean algorithm for computing $\gcd(a,b)$.

   Let $r_0 = a$ and $r_1 = b$. By successively applying the division algorithm, we obtain

$$\begin{aligned}
a = r_0 &= r_1 \cdot q_1 + r_2, & 0 \le r_2 < r_1 = b,\\
r_1 &= r_2 \cdot q_2 + r_3, & 0 \le r_3 < r_2,\\
&\cdots\\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n, & 0 \le r_n < r_{n-1},\\
r_{n-1} &= r_n \cdot q_n + 0.
\end{aligned}$$

   Eventually, a remainder of zero must occur, since the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \ge 0$ cannot contain more than a terms. As a result, by Euclidean theorem, it follows that

$$\gcd(a,b) = \gcd(r_0,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n$$

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

5. Example: Compute $\gcd(414, 662)$

   By Euclidean algorithm, we have

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

   Hence $\gcd(414, 662) = 2$.

6. The Euclidean algorithm – pseudocode

```
procedure gcd(a,b: positive integers)
x := a
y := b
while y /= 0
   r := x mod y
   x := y
   y := r
end while
return x      % x is the gcd(a,b)
```

7. By reversing the steps of Euclidean algorithm, we can find x and y such that $\gcd(a, b) = a \cdot x + b \cdot y$.

   Example: $\gcd(414, 662) = 2 = 414 \cdot 8 + 662 \cdot (-5)$.

Modular arithmetic.

1. **Modular operation:** $a(\text{mod} m) = r =$ the remainder after dividing a by $m > 0$. (note, $0 \leq r < m$).

   Examples: (a) $7(\text{mod}3) = 1$, since $7 = 3 \cdot 2 + 1$.

   (b) $3(\text{mod}7) = 3$, since $3 = 7 \cdot 0 + 3$

   (c) $-133 \bmod 9 = 2$, since $-133 = 9 \cdot (-15) + 2$.

2. 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: $a \equiv b \pmod{m}$:

   Examples: (a) $17 \equiv 5 (\text{mod } 6)$,

   (b) $24 \not\equiv 14 (\text{mod } 6)$.

3. By the definition, we know that $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$. Using this fact, we can prove the following properties of mudular arithmetic:

   If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

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

   (b) $ac \equiv bd \pmod{m}$

4. Applications of congruences in Hashing function, random number generation, cryptology, ...