- **Example:** Calculate **gcd(119,544)**and find the values of ***x*** and ***y*** that satisfy the equation **119*x*+544*y*=gcd(119,544)** through the backward substitution process.
- **Solve:** ①Apply the Euclidean algorithm.

We begin by performing the division steps of the Euclidean algorithm:

$544=119\times4+68$

$119=68\times1+51$

$68=51\times1+17$

$51=17\times3+0$

- **Solve:** ②Use backward substitution to find x and y.

  Now, we work backwards to express 17 as a linear combination of 119 and 544. From the last division:

  $119x+544y=\gcd(119,544)=17$

  $17=68-51\times1$

  $17=68-(119-68\times1)\times1$

  $17=68\times2-119$

  $17=(544-119\times4)\times2-119$

  $17=544\times2-119\times8-119$

  $17=544\times2-119\times9$

- The GCD of **119** and **544** is **17**, which can be expressed as a linear combination: $119\times(-9)+544\times2=17$

The Necessary and Sufficient Condition for Coprimality

- Two integers a and b are *coprime* if $\gcd(a,b)=1$.
- A set of integers $a_1, a_2, \ldots, a_n$ is *pairwise coprime* if every pair of distinct elements is coprime, i.e., $\gcd(a_i, a_j)=1$ for all $i \neq j$.
- **For example**, 8 and 15 are coprime, while 8 and 12 are not coprime.The numbers 4, 9, 11, and 35 are pairwise coprime.
- **Theorem 8.10:** The necessary and sufficient condition for two integers a **and** b **to be coprime** is that there exist integers x and y such that $xa+yb=1$.

The Necessary and Sufficient Condition for Coprimality

- **Necessity:** If integers a and b are coprime, then there exist integers x and y such that the equation $ax + by = 1$ holds.
- **Proof:**

  ①By the definition of coprimeness, $\gcd(a,b)=1$.

  ②By Bézout's Theorem, since $\gcd(a,b)=1$, there must exist integers x and y such the $ax+by=gcd(a,b)$.

  ③Substituting $\gcd(a,b)=1$, we get $ax+by=1$, thus finding the values of x and y that satisfy the condition.

- **Sufficiency:** Proving that the equation $ax + by = 1$ holds is a sufficient condition for a and b to be coprime.

- **Proof:**

①Suppose there exist integers x and y such that the equation $ax + by=1$ holds, meaning a and b can be expressed as a linear combination to generate the smallest positive integer 1.

②Let d be a common divisor of a and b , so $a=d\cdot m$ and $b=d\cdot n$, where m and n are integers. The equation $ax + by=1$ can be rewritten as $d\cdot(mx+ny)=1$.

③Since only 1 multiplied by 1 results in 1 among positive integers, d must be 1.

④Therefore, since a and b have no common divisors greater than 1, we have $\gcd(a,b)=1$, and by the definition of coprimeness, a and b are coprime.

↳ Coprime Divisibility Transfer Theorem

- **Theorem 8.11**: Let $a|c$, $b|c$, a and b be coprime. Then, $ab|c$.
- **Proof:**

①By the necessary and sufficient condition for coprimeness, there exist integers x and y such tha $xa+yb=1$.

②Multiplying both sides by c, we get $cxa+cyb=c$. Since $a|xa$ and $b|c$, we have $ab|cxa$.

③Similarly, since $b|yb$ and $a|c$, we have $ab|cyb$. Thus, we have $ab|cxa+cyb$, which simplifies to $ab|c$.

8.2 Greatest Common Divisor and Least Common Multiple

- Brief summary

Objective :

Key Concepts :

Discrete Mathematics 2025 Spring

同济经管 TONGJI SEM

魏可佶 kejiwei@tongji.edu.cn

CAMEA 中国高质量MBA教育认证 AACSB ACCREDITED EQUIS ACCREDITED

- 8.1 Prime Numbers
- 8.2 Greatest Common Divisor and Least Common Multiple
- 8.3 Congruence
- 8.4 Linear Congruence Equations and the Chinese Remainder Theorem
- 8.5 Euler's Theorem and Fermat's Little Theorem

8.3 Congruence

- Congruence
- Modular Arithmetic
- Equivalence Class modulo m

- **Definition 8.5 :** Let ***m*** be a positive integer, and ***a*** and ***b*** be integers.
  - If $m|(a-b)$, then ***a*** is said to be ***congruent*** to ***b*** modulo ***m***, or ***a*** is congruent to ***b*** modulo ***m***, denoted as $a \equiv b \pmod{m}$.
  - If ***a*** is ***not congruent*** to ***b*** modulo ***m***, we write $a \not\equiv b \pmod{m}$.
- The ***necessary and sufficient conditions*** for $a \equiv b \pmod{m}$. :

  (1) $a \bmod m = b \bmod m$.

  (2) $a \equiv b \pmod{m}$ if and only if $a-b$ is a multiple of ***m***, i.e., $a=b+km$, where ***k*** is an integer.
- **Example：** $5 \equiv 17 \pmod 6$, $264 \equiv 249 \pmod 5$, $24 \not\equiv 16 \pmod 6$.

- Congruence modulo m satisfies the properties of an *equivalence relation*.

  That is, for all integers $a,b,c \in Z$, the following hold:

  ① **Reflexivity:** $a \equiv a \pmod{m}$

  ② **Transitivity:** $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

  ③ **Symmetry:** $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

  - Shorthand notation for the equivalence relation modulo m:

    $a_1 \equiv a_2 \equiv \ldots \equiv a_k \pmod{m}$.

- *Closure of Algebraic Operations* under Congruence Modulo m

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

  ① $a \pm c \equiv b \pm d \pmod{m}$ (Additive and subtractive property)

  ② $ac \equiv bd \pmod{m}$ (Multiplicative property)

  ③ $a^k \equiv b^k \pmod{m}$, where k is a non-negative integer (Exponentiation property)