

4. 设 a, b, c, d 均为正整数, 下列叙述是否正确? 若正确, 请给出证明; 否则, 请给出反例.

- (1) 若 $a \mid c, b \mid c$, 则 $ab \mid c$.
- (2) 若 $a \mid c, b \mid d$, 则 $ab \mid cd$.
- (3) 若 $ab \mid c$, 则 $a \mid c$.
- (4) 若 $a \mid bc$, 则 $a \mid b$ 或 $a \mid c$.

(1) 不正确, $a=2, b=4, c=4$

(2) 正确. 因为 $a \mid c, b \mid d$,

$$\text{设 } c=ma, d=nb, \text{ 则 } cd=mnab$$

$$\text{即 } ab \mid cd.$$

(3) 正确. 因为 $ab \mid c$, 设 $c=kab$

$$\text{则 } c=(kb)a, \text{ 即 } a \mid c.$$

(4) 不正确, $a=b, b=2, c=3$.

16. 证明: 对任意的整数 x, y, u, v , 有 $\gcd(a, b) \leq \gcd(xa + yb, ua + vb)$.

证明: 记 $\gcd(a, b) = d, d \mid a, d \mid b$

$$\text{则 } d \mid xa + yb, d \mid ua + vb,$$

$$\text{则 } d \mid \gcd(xa + yb, ua + vb)$$

$$\text{则 } \gcd(a, b) \leq \gcd(xa + yb, ua + vb)$$

34. 下列叙述是否正确? 若正确, 试证明之; 否则, 试给出反例.

- (1) 若 $a^2 \equiv b^2 \pmod{m}$, 则 $a \equiv b \pmod{m}$ 或 $a \equiv -b \pmod{m}$.
- (2) 若 $a \equiv b \pmod{m}$, 则 $a^2 \equiv b^2 \pmod{m}$.
- (3) 若 $a^2 \equiv b^2 \pmod{m^2}$, 则 $a \equiv b \pmod{m}$.
- (4) 若 $a \equiv b \pmod{mn}$, 则 $a \equiv b \pmod{m}$ 且 $a \equiv b \pmod{n}$.
- (5) 若 $a \equiv b \pmod{m}$ 且 $a \equiv b \pmod{n}$, 则 $a \equiv b \pmod{mn}$.

(1) 不正确, $m=4, a=4, b=2$

(2) 正确. 因为 $a \equiv b \pmod{m}$, 设 $a-b=km$

$$\text{则 } a^2 - b^2 = (a+b)(a-b) = k(a+b)m$$

$$\text{即 } a^2 \equiv b^2 \pmod{m}.$$

(3) 不正确, $m=2, a=\frac{5}{2}, b=\frac{3}{2}$.

(4) 正确. $a-b=kmn$ 则 $a-b=(kn)m=(kn)n$

$$\text{即 } a \equiv b \pmod{m} \text{ 且 } a \equiv b \pmod{n}$$

(5) 不正确, $m=n=2, a=4, b=2$.

35. 下列一次同余方程是否有解? 若有解, 试给出它的全部解.

(1) $9x \equiv 3 \pmod{6}$.

(2) $4x \equiv 3 \pmod{6}$.

(3) $3x \equiv -1 \pmod{5}$.

(4) $8x \equiv 2 \pmod{4}$.

(5) $20x \equiv 12 \pmod{8}$.

(1) $\gcd(9, 6) = 3$ 有解

$$9 \times 1 \equiv 9 \times 3 \equiv 9 \times 5 \equiv 3 \pmod{6}$$

$$9 \times 2 \equiv 9 \times 4 \equiv 9 \times 6 \equiv 0 \pmod{6}$$

$$x = 2i + 1, i \in \mathbb{Z}$$

(2) $\gcd(4, 6) = 2, 2 \nmid 3$, 无解

(3) $\gcd(3, 5) = 1$, 有解

$$3 \times 1 \equiv -2 \pmod{5}, 3 \times 2 \equiv 1 \pmod{5},$$

$$3 \times 3 \equiv -1 \pmod{5}, 3 \times 4 \equiv 2 \pmod{5}$$

$$x = 3 + 5i, i \in \mathbb{Z}$$

(4) $\gcd(4, 8) = 4, 4 \nmid 2$, 无解

(5) $\gcd(20, 8) = 4, 4 \mid 12$, 有解

$$20 \times 1 \equiv 4 \pmod{8}, 20 \times 2 \equiv 0 \pmod{8}, 20 \times 3 \equiv 4 \pmod{8}$$

$$20 \times 4 \equiv 0 \pmod{8}, 20 \times 5 \equiv 4 \pmod{8}, 20 \times 6 \equiv 0 \pmod{8}$$

$$20 \times 7 \equiv 4 \pmod{8}$$

$$x = 2i + 1, i \in \mathbb{Z}$$

37. 对下列每一组数 a 和 m , 是否有 a 的模 m 逆? 若有, 试给出.

(1) 2, 3.

(2) 8, 12.

(3) 18, 7.

(4) 12, 21.

(5) 5, 9.

(6) -1, 9.

(1) $\gcd(2, 3) = 1$, 有

$$2 \times 2 - 1 \times 3 = 1 \Rightarrow 2 \times 2 \equiv 1 \pmod{3} \Rightarrow a^{-1} = 2$$

(2) $\gcd(8, 12) = 4 \neq 1$, 无

(3) $\gcd(18, 7) = 1$, 有

$$18 = 2 \times 7 + 4, 7 = 4 + 3, 4 = 3 + 1$$

$$2 \times 18 - 5 \times 7 = 1 \Rightarrow 2 \times 18 \equiv 1 \pmod{7} \Rightarrow a^{-1} = 2$$

$$(4) \gcd(12, 21) = 3 \neq 1, \text{无}$$

$$(5) \gcd(5, 9) = 1, \text{有}$$

$$2 \times 5 - 1 \times 9 = 1 \Rightarrow 2 \times 5 \equiv 1 \pmod{9} \Rightarrow a^{-1} = 2$$

$$(6) \gcd(-1, 9) = 1, \text{有}$$

$$8 \times (-1) + 9 \times 1 = 1 \Rightarrow 8 \times (-1) \equiv 1 \pmod{9} \Rightarrow a^{-1} = 8$$

45. 利用费马小定理计算.

$$(1) 2^{325} \pmod{5}.$$

$$(2) 3^{516} \pmod{7}.$$

$$(3) 8^{1003} \pmod{11}.$$

(1) 因为5是素数且 $(2, 5) = 1$,

$$\text{故 } 2^4 \equiv 1 \pmod{5}$$

$$\Rightarrow 2^{325} \equiv 2^{81 \times 4 + 1} \equiv 2 \pmod{5}$$

$$(2) 3^6 \equiv 1 \pmod{7}$$

$$\Rightarrow 3^{516} \equiv 3^{86 \times 6} \equiv 1 \pmod{7}$$

$$(3) 8^{10} \equiv 1 \pmod{11}$$

$$\Rightarrow 8^{1003} \equiv 8^3 \equiv 512 \equiv 6 \pmod{11}$$