

1. 证明：任意  $n$  个连续的整数中( $n \geq 1$ )，有且仅有一个数被  $n$  整除。
2. 设  $n, k$  是正整数，证明： $n^k, n^{k+4}$  的 10 进制展开的个位数相同。
3. 证明：若  $(a, b) = 1$ ，则  $(a+b, a-b) = 1$  或 2
4. 用辗转相除法求  $a = 288, b = 158$  的最大公因数和  $m, n$  使  $ma + nb = (a, b)$

思考题：

1. 调研扩展欧几里得除法
2. 编程实现欧几里得除法和扩展欧几里得除法

1. 设  $a, b$  是正整数, 证明:  $(a+b)[a, b] = a[b, a+b]$
2. 证明: 若  $n > 0, a^n | b^n$  则  $a | b$
3. 设  $n > 2$ , 证明在  $n$  和  $n!$  之间一定有一个素数。
4. 证明: 形如  $6n + 5$  的素数有无穷多。

思考题:

1. 求第 1000000 个素数
2. 求  $n!+1$  的最小素因子,  $n$  为整数且  $n \leq 20$

1. 设 $m > 1, m|(m-1)! + 1$ , 证明:  $m$  是素数.
2. 求 $176x - 162y = 2$ 的所有整数解.
3. 求 $2x + 3y + 4z = 5$ 的所有整数解.

1. 若 $n$ 是整数, 证明 $13|4^{2n+1} + 3^{n+2}$
2. 证明: 对于任意整数 $x$ ,  $\frac{1}{5}x^5 + \frac{1}{3}x^3 + \frac{7}{15}x$ 为整数

### 思考题

1. 寻找一个合数 $n$ , 和一个整数 $b$ , 满足 $b^n \equiv b \pmod{n}$
2. 寻找一个合数 $n$ , 对所有与之互素的整数 $b$ , 满足 $b^{n-1} \equiv 1 \pmod{n}$
3. 调研素性判定方法

1. 求解同余式  $111x \equiv 75 \pmod{321}$
2. 解同余方程  $58x \equiv 87 \pmod{47}$
3. 求解同余式  $256x \equiv 179 \pmod{337}$
4. 设整数  $n \geq 2$ , 证明:  $\sum_{\substack{1 \leq i \leq n \\ (i,n)=1}} i \equiv 0 \pmod{n}$
5. 证明 Wilson 定理的逆命题成立。
6. 证明: 若  $p$  是奇素数,  $N = 1 + 2 + \cdots + (p-1)$ , 则

$$(p-1)! \equiv p-1 \pmod{N}。$$

1. 设整数  $n \geq 2$ , 证明:  $\sum_{\substack{1 \leq i \leq n \\ (i,n)=1}} i = \frac{1}{2} n \varphi(n)$ , 即在数列  $1, 2, \dots, n$  中与  $n$  互素的整数之

和是  $\frac{1}{2} n \varphi(n)$

2. 证明: 若  $2p+1$  是奇素数, 则  $(p!)^2 + (-1)^p \equiv 0 \pmod{2p+1}$ .

3. 解同余式组

$$x \equiv 1 \pmod{7}, x \equiv 3 \pmod{5}, x \equiv 5 \pmod{9}$$

4. 解同余式组

$$4x \equiv 3 \pmod{25} \quad 3x \equiv 8 \pmod{20}$$

5. 解同余式组:  $x \equiv 8 \pmod{15}, x \equiv 5 \pmod{8}, x \equiv 13 \pmod{25}$ .

1. 证明:  $61! + 1 \equiv 0 \pmod{71}$
2. 证明: 对任意给定的  $n > 1$ , 存在  $m > 0$ , 使得同余式
$$x^2 \equiv 1 \pmod{m}$$
的解的个数大于  $n$

1、设  $p$  是奇素数，证明：模  $p$  的两个二次剩余的乘积是二次剩余；两个二次非剩余的乘积是二次剩余；一个二次剩余和一个二次非剩余的乘积是二次非剩余。

2、设  $p$  是奇素数，证明：模  $p$  的所有二次剩余的乘积与  $(-1)^{\frac{p+1}{2}}$  对模  $p$  同余。



1、 设素数  $p \equiv 3 \pmod{4}$ ,  $\left(\frac{n}{p}\right) = 1$ , 证明:  $x \equiv \pm n^{\frac{p+1}{4}} \pmod{p}$  是同余方程  $x^2 \equiv n \pmod{p}$

的解。

2、 证明: 对于任意的奇素数  $p$ , 总存在整数  $n$ , 使得

$$p \mid (n^2 + 1)(n^2 + 2)(n^2 - 2)$$

3、 求  $\left(\frac{323}{41}\right)$  的值

1. 已知 563 是素数，判定方程  $x^2 \equiv 429 \pmod{563}$  是否有解
2. 证明：3 是所有大于 3 的梅森素数（形如  $2^q - 1$ ， $q$  是素数）的一个非平方剩余。
3. 利用雅可比符号性质计算  $\left(\frac{51}{71}\right)$

1. 证明：如果正整数  $n$  满足  $n = 2\varphi(n)$ ，那么存在一个正整数  $j$ ，使得  $n = 2^j$
2. 证明：正整数  $n$  是合数当且仅当  $\sigma(n) > n + \sqrt{n}$
3. 设  $n$  为任给的正整数，求  $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)$  的值。

1. 证明：如果  $a$  对奇素数  $p$  的阶是奇数，则同余式  $a^x + 1 \equiv 0 \pmod{p}$  没有解.
2. 设  $m$  为正整数，若对模  $m$  存在某个整数  $a$  次数为  $m-1$ ，则  $m$  为素数.
3. 若  $x$  模  $m$  的次数为  $a$ ， $y$  模  $m$  的次数为  $b$ ，并且  $(a, b) = 1$ ，则  $xy$  对模  $m$  的次数为  $ab$ .

1. 设  $m \geq 3$ ,  $g_1$  和  $g_2$  都是模  $m$  的原根, 则  $g = g_1 g_2$  不是模  $m$  的原根。
2. 设  $g$  是奇素数  $p$  的一个原根, 证明: 当  $p \equiv 1 \pmod{4}$  时,  $-g$  也是  $p$  的一个原根; 当  $p \equiv 3 \pmod{4}$  时,  $-g$  对  $p$  的次数为  $\frac{p-1}{2}$ .
3. 素数 71 有一个原根 7, 求出 71 的所有原根以及求出  $71^2$  和  $2 \times 71^2$  的一个原根。

1、设  $p$  是奇素数，证明：当且仅当  $p-1$  不整除  $n$  时，有

$$1^n + 2^n + \cdots + (p-1)^n \equiv 0 \pmod{p}$$

2、计算 2 模 465 的次数；5 模  $2^{15}$  的次数.

- 1、已知 3 是模 17 的原根，构造指数表，解同余式  $6x^{12} \equiv 11 \pmod{17}$
2. 假设  $p$  是一个奇素数，证明同余方程  $x^4 \equiv -1 \pmod{p}$  有解当且仅当  $p$  形如  $8k+1$