《密码学》

期末速成课

考点	重要程度	占分	题型人
1. 欧拉函数	***	0 - 6	选择 / 大题
2. 欧拉定理	**	0 - 3	选择 / 大题
3. 模运算	****	5 - 15	选择 填空
4. 欧几里得算法	***	5 - 8	选择 / 大题
5. 拓展欧几里得算法求逆	****	10 - 25	选择 / 大题

4.1 数论

一、欧拉函数

1、定义: 设m是一个正整数,则m个整数0, 1, 2..... m-1 中与m互素的整数的个数,记作 $\varphi(m)$,通常称为欧拉(Euler)函数

- $\Rightarrow \varphi(10) = 4$ [1, 3, 7, 9]

2、欧拉函数性质: 若gcd(m,n)=1, 则 $\varphi(mn)=\varphi(m)\varphi(n)$



扫码观看 视频讲解更清晰

二、欧拉定理

- 在数论中, 欧拉定理是一个关于同余的性质。
- 欧拉定理表明, 若n, a为正整数, 且互素 (即gcd (a, n) =1), 则:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

- 满足gcd(3,5)=1
- $\[\] \varphi(5) = 4 \]$

三、模运算

模运算基本四则运算:

$$(a + b) \% p \equiv (a\%p + b\%p) \% p$$

 $(a - b) \% p \equiv (a\%p - b\%p) \% p$
 $(a \times b) \% p \equiv (a\%p \times b\%p) \% p$
 $(a^b) \% p \equiv ((a\%p)^b) \% p$

· 三个横杠等价于左右两边相加减是P的倍数

核心: 换成余数代入 (相加减P的倍数)



三、模运算

求模/求余

- \triangleright 求余: 求整除后的余数 若 $a \mod b$ 是异号,结果与a同号【 $-4 \mod 3 = -1$ 】
- ▶ 求模: a mod b 不能为负数 【-3 mod 4 = 1】
- 当a、b全为正数时,求模和求余相同

解:

22003 mod 7

(1) 找7的倍数 → 21000

$$= (21000 + 1003) \mod 7$$

$$(a+b) \% p \equiv (a\%p + b\%p) \% p$$

= (21000 % 7 + 1003 % 7) mod 7

 $= 1003 \ mod \ 7$

(2) 找7的倍数 → 700

$$= (700 + 303) \, mod \, 7 \, = \, (700 \, \% \, 7 \, + 303 \, \% \, 7) mod \, 7$$

 $= 303 \mod 7$

(3) 找7的倍数 $= (280 + 23) \mod 7 = 23 \mod 7 = 2$

解:

4097 mod 13

(1) 找倍数 1300→2600 →3900

$$=$$
 (3900 + 197) $mod 13$

$$(a + b) \% p \equiv (a\%p + b\%p) \% p$$

$$= 197 \mod 13 = (130 + 67) \mod 13$$

$$= 67 \mod 13 = (65 + 2) \mod 13 = 2$$



方案1: 找倍数

解:

4097 mod 13

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$2^{\varphi(13)} \equiv 1 \pmod{13}$$

$$\therefore 2^{12} \equiv 1024 \times 4 \equiv 4096 \equiv 1 \pmod{13}$$

方案2: 欧拉定理找1

$$(a+b) \% p \equiv (a\%p + b\%p) \% p$$
原式 = (4096 + 1) mod 13 = (4096%13 + 1%13) mod 13 = (1+1) mod 13 = 2

四、欧几里得算法->拓展欧几里得算法

- 欧几里得算法=辗转相除法
- 欧几里得算法求最大公因数

定理:
$$gcd(a,b) = gcd(b,a \mod b)$$

 $a = bq+c$
 $(a,b)=(b,c)$

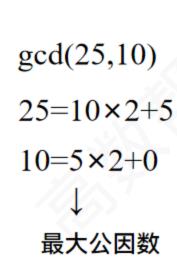


【題3】 gcd(55,22)=gcd(22,11)=gcd(11,0)=11

$$a = b q + c$$

eg gcd(26,7) $26 = 7 \times 3 + 5$
 $7 = 5 \times 1 + 2$
 $5 = 2 \times 2 + 1$
 $2 = 1 \times 2 + 0$
最大公约数 直到0结束

■ 最后等于0结束,等号后的数为最大公因数



拓展欧几里得算法求逆

当gcd(a,b)=1,即a,b互素时,ax+by=1中的解x是a模b的乘法逆元,即 $a \times x \equiv 1 \pmod{b}$

7mod26

$$26 = 7 \times 3 + 5$$

$$7 = 5 \times 1 + 2$$

$$5 = 2 \times 2 + 1$$

$$2 = 1 \times 2 + 0$$

往回带

$$1 = 5 - 2 \times 2$$

$$1 = 5 - (7 - 5) \times 2$$

$$= 5 \times 3 - 7 \times 2$$

$$=(26 - 7 \times 3) \times 3 - 7 \times 2$$

$$= 26 \times 3 - 7 \times 11$$