原根和阶

1. 什么是阶

假设 a，m 为整数，m > 1， （a，m）= 1，则使得 $a^e \equiv 1(modm)$ 成立的最小正整数 e 称之为 a 对模m的阶，记做 ordm(a)

2. 什么是原根

若 a 的阶 $e = \varphi(m)$ ，则称 a 为 模m 的原根

3. 小例题

模数 m 为7，求对模7而言，它的阶和原根是什么?

> 解答: m 是素数，所以7的缩系有 {1, 2, 3, 4, 5, 6}，一个一个分析
>
> $1^1 \equiv 1(mod7)$ 所以 1 对模7的阶是1
>
> $2^1 \equiv 2(mod7); 2^2 \equiv 4(mod7); 2^3 \equiv 1(mod7)$ 所以 2 对模7的阶是3
>
> $3^1 \equiv 3(mod7); 3^2 \equiv 2(mod7); 3^3 \equiv 6(mod7); 3^4 \equiv 4(mod7); 3^5 \equiv 5(mod7); 3^6 \equiv 1(mod7)$
>
> 所以 3 对模7的阶是6
>
> 以此类推......
>
> 对模7而言，「1，2，3，4，5，6」的阶为「1，3，6，3，6，2」，由于 $\varphi(7) = 6$ ，所以原根是3，5

4. 做题小技巧

当求得某个数 $a^b \equiv -1(modm)$ 时，那么 2*b 就是a 模 m 的阶，例如:

> $5^3 \equiv -1(mod14)$，那么6就是5对模14的阶

5. 一些性质

- 假设 a，m 为整数，m > 1， （a，m）= 1， 则 $ordm(a)|\varphi(m)$

- 假设 a，m 为整数，m > 1，（a，m）= 1，d为正整数，则 $a^d \equiv 1(mod m)$ 的充分必要条件是 ordm(a)|d

> 其实这两条定理都挺容易理解的：
> 1. 由欧拉定理我们可以知道 $a^{\varphi(m)} \equiv 1(mod m)$ ，而ordm(a)是阶，即满足式子的最小整数，所以ordm(a) <= $\varphi(m)$，且$\varphi(m) = ordm(a) + 2k(k \in Z)$
> 2. 第二条性质和第一条本质一样...

6. 小例题2（利用👆性质较快算阶）

例: 求ord17(5)

解：由于$\varphi(17) = 16$，由性质1可知，$ord17(5)|16$，所以$ord17(5)$的可能取值有1，2，4，8，16，依次代入：

$5^8 \equiv -1(mod17)$，所以16是5模17的阶，即$ord17(5) = 16$

7. 又一些性质

设a，b，$m \in Z$，$(a，m) = 1$

- 若b ≡ a (mod m)，则 ordm(a) = ordm(b)
- $ordm(a^{-1}) = ordm(a)$

8. 小例题3（利用👆性质较快算阶）

已知ord17(5)为16，求ord17(7)?

解: 由于 $5 \equiv 7^{-1}$（$mod17$），所以，$ord17(5) = ord17(7^{-1}) = ord17(7)$

所以ord17(7)=16

9. 简化剩余系

若 m > 1，且(a, m)=1，则:

$a^0, a^1, a^2....a^{ordm(a)-1}$两两互素，且当$a$为原根时，👈的$\varphi(m)$个元素构成一个缩系

打个比方，由小例题2可知，5是模17的一个原根，则 $\{a^k(mod17)|k \in [0, 15]\}$ 组成一个缩系

> 下面是对于求逆元的某些应用（个人觉得意义不大，除非它把表格给你，欧几里得他不香吗）

有了【例5.1.4】中的表格，求逆元也变得更简单. 例如，如果求$11^{-1}(\bmod 17)$，常规的方法是有欧几里德算法求解. 实际上，$11^{-1} \equiv (5^{11})^{-1} \equiv 1 \times 5^{-11} \equiv 5^{16} \times 5^{-11} \equiv 5^5 \equiv 14(\bmod 17)$. 由$11 \times 14 = 154 \equiv 1(\bmod 17)$知，结果正确.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
5^k	1	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7

《信息安全数学基础》 第5章

10. 双一些性质

设a，b，$m \in Z$，$(a，m) = 1$ ，则：

- 若$a^d \equiv a^k(modm)$，则$d \equiv k(mod(ordm(a)))$
- $a^n \equiv a^{n(mod(ordm(a)))}(modm)$

11. 小例题4

已知ord7(2)=3， 求$2^{2002}(mod7)$

> 解法1：$2^3 \equiv 1(mod7)$，所以$2^{2002} \equiv (2^3)^{667} * 2^1(mod7) \equiv 2(mod7)$
>
> 解法2：由👆的性质(2)得$2^{2002} \equiv 2^{2002(mod(ord7(2)))}(mod7) \equiv 2^{2002(mod3)}(mod7) \equiv 2(mod7)$

~~吐槽一下，性质可用性/意义还是不大，除非题目明示你~~

12. 叒一些性质

假设 a，m 为整数，m > 1，（a，m）= 1，d>=0，则：

$ordm(a^d) \equiv \frac{ordm(a)}{(ordm(a),d)}$

> 推论: 假如 g 是模 m 的原根，整数 d >=1，则 g^d是模m的原根的充要条件是$(d，\varphi(m)) = 1$

13. 例题5

- (1)

【例5.1.10】 已知$\text{ord}_{17}(5)=16$，$5^2=8(\text{mod } 17)$, 所以

$$\text{ord}_{17}(8)=\text{ord}_{17}(5^2)=\frac{\text{ord}_{17}(5)}{(\text{ord}_{17}(5),2)}=\frac{16}{(16,2)}=8.$$

$$\text{ord}_{17}(6)=\text{ord}_{17}(5^3)=\frac{\text{ord}_{17}(5)}{(\text{ord}_{17}(5),3)}=\frac{16}{(16,3)}=16.$$

- (2)利用推论“g^d是模m的原根的充要条件是$(d，\varphi(m))=1$”

【例5.1.11】 由$\text{ord}_{17}(5)=16$可知5是模17的原根, 由原根5就可以求出17的所有原根.

解: 模17的所有原根为5^1, 5^3, 5^5, 5^7, 5^9, 5^{11}, 5^{13}, 5^{15}. 即

$5^1\equiv5(\text{mod } 17)$, $5^3\equiv6(\text{mod } 17)$, $5^5\equiv14(\text{mod } 17)$,

$5^7\equiv10(\text{mod } 17)$, $5^9\equiv12(\text{mod } 17)$, $5^{11}\equiv11(\text{mod } 17)$,

$5^{13}\equiv13(\text{mod } 17)$, $5^{15}\equiv6(\text{mod } 17)$.

14. 叕一些性质

若 m > 1且m有原根，则原根个数为 $\varphi(\varphi(m))$ 个

15. 小例题6

【例5.1.12】 求出模25的所有原根.

解: $\varphi(25)=20$, $\varphi(\varphi(25))=\varphi(20)=8$. 故25若有原根, 则其必有8个原根.然后寻找模25的一个原根. 通过计算可得,

$2^5 \equiv 7 \pmod{25}$, $2^{10} \equiv 24 \equiv -1 \pmod{25}$.

所以2是模25的一个原根.

因为模20的简化剩余系为{1, 3, 7, 9, 11, 13, 17, 19}, 故模25的所有原根为: $2^1\equiv 2$, $2^3\equiv 8$, $2^7\equiv 3$, $2^9\equiv 12$, $2^{11}\equiv 23$,

$2^{13}\equiv 17$, $2^{17}\equiv 22$, $2^{19}\equiv 13 \pmod{17}$.

即模25的原根为: 2, 3, 8, 12, 13, 17, 22, 23.

16. 素数的原根性质

- 素数的原根存在，因为模 m 的原根存在的充要条件是m = 2，4，p^a，2p^a
- ordp(g) = d，d < p-1， 则$g^t(t=1,2,3...d)$都不是模p的原根
- 设 p 是素数:

  $\varphi(p)$的素因数为$q1$，$q2$，$q3...qk$，则g是模p的一个原根的充要条件是$g^{\varphi(p)/qi}(!\equiv)1(modm)$

> ~~说实话，这个死🐎定理太抽象了~~

17. 对应👆上述性质的例题

【例5.1.12】 求$p=17$的原根.

解 先求$g=2$模17的阶. 由于$\varphi(17)=16$. $16=2^4$的素因数只有$q=2$,

$$\frac{\varphi(p)}{q}=8$$

故只需计算g^8模$p=17$是否同余1.

因$2^8 \pmod{17} \equiv 1$. 所以2模17的阶为8. 即2不是模17的原根.

由【定理5.1.7】, $2^1 \pmod{17} \equiv 2$, $2^2 \pmod{17} \equiv 4$, $2^3 \pmod{17} \equiv 8$, $2^4 \pmod{17} \equiv 16$, $2^5 \pmod{17} \equiv 15$, $2^6 \pmod{17} \equiv 13$, $2^7 \pmod{17} \equiv 9$, $2^8 \pmod{17} \equiv 1$. 都不是模17的原根.

> ~~说真的，太抽象了~~