原根和阶（2）

1. 离散对数

- 设 g 是模 m 的一个原根，若 a 是一个与 m 互素的整数，则存在一个唯一的整数 r $(r <= \varphi(m))$，使得 $g^r \equiv a(mod m)$（*）
- 若 * 号式子成立，则称 r 为以 g 为底的 a 对模 m 的一个离散对数，写作 r = inda

2. 例题

【例5.2.1】 已知5是模17的原根. 求10对模17的离散对数.

解: 先构造以5为底的阶函数表.再构造离散对数表. 可得, 10对模17的离散对数为7.

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$a \equiv 5^r$	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$r=\log_g a$	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

3. 性质

设 m > 1，g 是模 m 的一个原根，(a, m) = 1， $g^r \equiv a(mod m)$ ，则 r 满足 $r \equiv inda(mod \varphi(m))$

4. 离散对数的密码学应用（看PPT）