2006-2007 学年第二学期数论与代数结构考试题

1．(20) 设 $a>2$ 是奇数．证明

(1) 一定存在正整数 $d \le a-1$，使得 $a \mid 2^d-1$；

(2) 设 d_0 是满足（1）的最小正整数. 那么 $a \mid 2^h-1(h \in N)$ 的充要条件是 $d_0 \mid h$.

2．（10 分）给定模 m，及 $0 \le a < m$， $0 \le x < \phi(m)$，试估计计算 $a^x \pmod m$ 的复杂度。

3．（20）给出一种由群 Z_p^*，Z_q^* 构造群 Z_{pq}^* 的方法， 其中 p, q 是素数，如果 p, q 是强素数，即存在 p', q' 使得 $p=2p'+1,\ \ q=2q'+1$。试求出在群 Z_{pq}^* 中阶是 $2p'q'$ 的元素的个数。

4．（20）设 p 是奇素数，证明：模 p 必有原根。

5．（20） 若 ϕ 是群 G 到群 G' 的同态满射，证明 $G/Ker\phi \cong G'$。

6．（10）证明： p 是奇素数， $p-1$ 的所有不同的素因数是 $q_1, q_2, \cdots q_s$，那么 g 为模 p 原根的充要条件是 $g^{(p-1)/q_j} \ne 1 \pmod p,\ \ j=1,2,\cdots s$.