2007-2008 学年第二学期数论与代数结构考试题

1.（10）证明：存在多项式时间算法验证一个整数 n 是否是一个整数的幂。也就是对于整数 n 是否存在整数 x, k 使得 $n = x^k$.

2. （10）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）设 p 是奇素数，$p-1$ 的标准素因子分解式是 $q_1^{\beta_1} \cdots q_r^{\beta_r}$ 。 证明：

（i） 对于任一 $j(1 \le j \le r)$，存在 a_j 对模 p 的指数是 $q_j^{\beta_j}$（不能利用模 p 存在原根证明）；

（ii） $a_1 \cdots a_r$ 是模 p 的原根。

4.（20） 设 a, b 是两个不全为零的整数， 证明：存在两个整数 x, y 使得 $ax + by = (a, b)$.

5.（20）设 f 是 G 到 G' 的满同态，H' 是 G' 的不变子群，

$$H = f^{-1}(H') = \{a \mid a \in G,\ f(a) \in H'\},$$

证明： H 是 G 的不变子群，且 $G/H \cong G'/H'$.

6.（20） 设 U 表示一切单位根作成的乘群，证明：Q/Z 与 U 同构。