2007-2008 学年第二学期数论与代数结构考试题答案

1.（20）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 $n = x^k$ 。

证明：很明显这里 k 不超过 $\log_2 n$，对于 $[2, \log_2 n]$ 中的每一个整数 k，对于区间 $[1, n]$ 利用两分法，先取中间一个整数做 k 次方与 n 比较大小，如果相等结束。如果比 n 大则取前面的半区间，如果比 n 小则取后面的半区间，再继续进行同样的步骤直到所剩区间中只有一个整数为止，验证这个数的 k 次方是否与 n 相等。相等说明 n 是一个整数 k 次方，如果不等则对下面的 k 进行相同的步骤。可以看出这里 k 的个数不超过 $\log_2 n$，对于每一个 k 两分法进行的次数为 $\log_2 n$，每一次两分法比较大小的运算次数为 $(\log_2 n)^2$，所以 验证一个整数 n 是否是一个整数的幂需要的计算复杂度是 $(\log_2 n)^4$ 。故命题成立。

2.（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。

(i) 证明：因为方程

$$x^{p-1} = 1 (\mathrm{mod}\ p)$$

有 $p-1$ 个解，而方程

$$\frac{x^{p-1}-1}{x^{q_j^{\beta_j}}-1} = 0 (\mathrm{mod}\ p)$$

最多有 $p-1-d$ 个解。所以方程

$$x^{q_j^{\beta_j}} = 1 (\mathrm{mod}\ p)$$

恰好有 $q_j^{\beta_j}$ 个解，同样方程

$$x^{q_j^{\beta_j - 1}} = 1 (\mathrm{mod}\ p)$$

恰好有 $q_j^{\beta_j - 1}$ 个解，故必存在 a_j 是方程 $x^{q_j^{\beta_j}} = 1 (\mathrm{mod}\ p)$ 的解，而不是方程

$x^{q_j^{\beta_j-1}} = 1 (\mathrm{mod}\ p)$ 的解。容易验证满足这样条件的 a_j 的阶是 $q_j^{\beta_j}$。

(ii) 证明：由于是 $q_1^{\beta_1}, \cdots, q_r^{\beta_r}$ 两两互质，所以 $a_1 \cdots a_r$ 的阶 $[q_1^{\beta_1}, \cdots, q_r^{\beta_r}] = p-1$，故 $a_1 \cdots a_r$ 是模 p 的原根，结论成立。

3.（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 $ax + by = (a, b)$。

证明：设 a, b 是给定的两个整数，$b \neq 0$，b 不能整除 a，重复应用带余除法得到的下面 k 个等式：

$a = q_0 b + r_0$， $0 < r_0 < |b|$，

$b = q_1 r_0 + r_1$， $0 < r_1 < r_0$，

$r_0 = q_2 r_1 + r_2$， $0 < r_2 < r_1$，

… … … … … … … …

$r_{k-5} = q_{k-3} r_{k-4} + r_{k-3}$， $0 < r_{k-3} < r_{k-4}$，

$r_{k-4} = q_{k-2} r_{k-3} + r_{k-2}$， $0 < r_{k-2} < r_{k-3}$ ，

$r_{k-3} = q_{k-1} r_{k-2}$.

依次往上推，可得

$$r_{k-2} = (r_{k-2}, r_{k-3}) = \ldots\ldots = (r_1, r_0) = (r_0, b) = (a, b)$$

由 Euclid 算法中的第 k 式 (a, b) 可表成 r_{k-3} 和 r_{k-4} 的整系数线性组合，利用第 $k-1$ 式可消去通过消除 r_{k-3}，得到 (a, b) 的关于 r_{k-4} 和 r_{k-5} 的整系数线性组合．这样依次利用第 $k-2, k-3, \cdots, 2, 1$ 式，就得到 (a, b) 表为 a 和 b 的整系数线性组合．故结论成立．

4.（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 $G/H \cong G'/H'$。

证明： 由同态基本定理，$G' \sim G'/H'$，ϕ 是自然同态，又因为 $f: G \sim G'$，

故$\varphi: G \sim G' \sim G'/H'$是$G$到$G'/H'$的满同态．若能证明$\ker\varphi = H$，则由同态基本定理就可推出所要结论．

$\forall a \in G$，$\varphi(a) = (\phi \circ f)(a) = \phi(f(a)) = f(a)H'$，设$a \in f^{-1}(H')$，则$f(a) \in H' \Rightarrow f(a)H' = H' \Rightarrow \varphi(a) = H'$，即$a \in \ker\varphi$，亦即$f^{-1}(H') \subseteq \ker\varphi$．

反之，设$a \in \ker\varphi$，则

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

即$f^{-1}(H') \supseteq \ker\varphi$，从而$\ker\varphi = H$为$G$的不变子群．由同态基本定理得证$G/H \cong G'/H'$．

5.（20） 设U表示一切单位根作成的乘群，证明：Q/Z与U同构。

证明：容易知道$U = \left\{ e(\frac{a}{b}) \mid a, b \in Z, b \neq 0, a < b \right\}$，

作影射 φ：$Q/Z \rightarrow U$

$\frac{a}{b} \rightarrow e(\frac{a}{b})$

容易验证φ是一个即单且满的影射，并且保持同态（这两点需要具体验证）。