代基期末试题(回忆版)

1、(1) 设 $d=(1859,1573)$，求 d，并将 d 写成 $1859a+1573b$ 的形式$(a,b$为整数)，一组(a,b)即可

(2) 对任意正整数 n，证明 $n\mid\varphi(2^n-1)$，这里 $\varphi(\cdot)$ 为欧拉函数

2、(1)设 $\sigma_1=(135)(2467)$，$\sigma_2=(145)(2367)$，$\sigma=\sigma_1\sigma_2$，试求 σ，并求出 σ_1 和σ 的阶

(2) 试将$(123\cdots n)(123\cdots n-1)\cdots(123)(12)$ 写成不交轮换之积，并说明其奇偶性

3、设 p,q 为不同的素数

(1) 求 pq 阶循环群中生成元的个数

(2) 证明 pq 阶 $Abel$ 群必为循环群

4、(1) 求出所有素数使得 $x^2\equiv 10(mod\, p)$ 有解

(2) 设素数 $p\equiv 7\, mod\, 40$，证明 p 不能表示成 x^2-10y^2 的形式$(x,y$ 为整数)

5、(1) 若素数 p 为 a^4+1 的奇因子，证明 $p\equiv 1 \mod 8$

(2) 证明形如 $8m+1$ 的素数有无穷多个

6、(1) 证明 $f(x)=x^4+1$ 在 $\mathbb{Z}[x]$ 上不可约

(2) p 为素数 记 $\overline{f}(x)$ 为 $f(x)$ 在 $\mathbb{F}_p[x]$上的约化多项式，证明 $\overline{f}(x)$ 在 $\mathbb{F}_p[x]$ 上可约

7、设 $p=2^{4n}+1$ 为素数，证明 7 为模 p 的原根