初等数论，群

参考答案

1. (10 分) (1) 求 $\gcd(10^6-1, 10^{15}-1)$.

   (2) 设自然数 $n, m \geq 1$，证明：$\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)}-1$.

解 两道题的做法是一样的，我们证明对自然数 $a, n, m \geq 1$，$\gcd(a^n-1, a^m-1) = a^{\gcd(n,m)}-1$. 于是 $\gcd(10^6-1, 10^{15}-1) = 10^3-1$.

不妨设 $m \geq n$，$\gcd(a^n-1, a^m-1) = \gcd(a^n-1, a^m-a^n) = \gcd(a^n-1, a^n(a^{m-n}-1))$. 显然 $\gcd(a^n-1, a^n) = \gcd(a^n-1, a^n-(a^n-1)) = \gcd(a^n-1, 1) = 1$. 根据互素的性质，$\gcd(a^n-1, a^n(a^{m-n}-1)) = \gcd(a^n-1, a^{m-n}-1)$. 根据带余除法，$m = qn+r$，$0 \leq r < n$，重复上面的减法，我们得到 $\gcd(a^n-1, a^m-1) = \gcd(a^n-1, a^r-1)$，这一过程与 Euclid 辗转相除算法相同，所以用同样的论证可以得到 $\gcd(a^n-1, a^m-1) = a^{\gcd(n,m)}-1$.

2. (10 分) 对实数 $x \in \mathbb{R}$，定义

$$\mu(x) = \inf\left\{\alpha \in \mathbb{R} : \left|x - \frac{p}{q}\right| \leq \frac{1}{q^\alpha} \text{ 仅有有限组互素整数解 } (p,q), q > 0\right\}.$$

证明：对 $x \in \mathbb{Q}$，$\mu(x) = 1$.

提示：首先证明 $\mu(x) \geq 1$，然后考虑 $|x - p/q| \leq 1/q^{1+\epsilon}$ 的解个数，进而证明 $\mu(x) < 1+\epsilon$.

解 将 x 写作 a/b，这里 a, b 互素，$b > 0$.

首先证明方程 $|x-p/q| \leq 1/q$ 有无穷组解. 取任意一个素数 $q > b$，$x - p/q = (aq-pb)/(bq)$，根据带余除法，存在 p 使得 $aq = bp + r$，这里 $0 \leq r < b$，于是 $0 \leq aq - pb < b$，所以 $|x-p/q| < 1/q$. 再验证 p, q 互素，$\gcd(p,q) \leq \gcd(bp, q) = \gcd(aq-r, q) = \gcd(-r, q)$，因为 q 是素数，$q > b > r$，所以 $\gcd(-r, q) = 1$. 于是 $\gcd(p,q) = 1$. 因为素数有无穷多，所以互素的解也是无穷多组.

然后再证明对任意 $\epsilon > 0$，$|x - p/q| \leq 1/q^{1+\epsilon}$ 只有有限个互素解，因而 $\mu(x) < 1+\epsilon$. 假设 $|x-p/q| = |(aq-pb)/(bq)| \leq 1/q^{1+\epsilon}$，那么 $|aq-pb|/b \leq 1/q^\epsilon$. 如果 $x \neq p/q$，那么 $b \geq q^\epsilon$. 如果有无穷组互素解，那么 q 可以任意大，不可能有 $b \geq q^\epsilon$，因而只有有限组互素解. 如果 $x = p/q$，那么 $p = a$，$q = b$，因此只有一组解.

3. (10 分) 如果 $p = 2p'+1$，其中 p, p' 都是素数，那么 p 被称作“安全素数”. 考虑两个安全素数 $p = 2p'+1, q = 2q'+1$，其中 p, p', q, q' 两两不同且均大于 2. 记 $n = pq$.

证明：$\mathbb{Z}_{n^2}^* \cong \mathbb{Z}_n^* \times \mathbb{Z}_n$.

提示：考虑如下三个映射，$\pi_1 : \mathbb{Z}_p^* \to \mathbb{Z}_{p^2}^*$，$\pi_2 : \mathbb{Z}_p \to \mathbb{Z}_{p^2}^*$ 和 $\pi : \mathbb{Z}_p^* \times \mathbb{Z}_p \to \mathbb{Z}_{p^2}^*$

$$\pi_1(a) = a^p, \qquad \pi_2(t) = (1+p)^t, \qquad \pi(a,t) = a^p(1+p)^t.$$

解　我们给两种解法.

解法一:

由中国剩余定理,

$$\mathbb{Z}_{p^2q^2} \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{q^2}.$$

两边同时取单位群，得到

$$\mathbb{Z}^*_{p^2q^2} \cong \mathbb{Z}^*_{p^2} \times \mathbb{Z}^*_{q^2}.$$

注意到 $|\mathbb{Z}^*_{p^2}| = \phi(p^2) = p(p-1) = 2pp'$，因此

$$\mathbb{Z}^*_{p^2} \cong \mathbb{Z}_p \times \mathbb{Z}_{p'} \times \mathbb{Z}_2 \cong \mathbb{Z}_p \times \mathbb{Z}_{2p'} \cong \mathbb{Z}_p \times \mathbb{Z}^*_p.$$

其中每一个同构都是因为有限 Abel 群分类定理（他们都是有限 Abel 群）. 于是,

$$\mathbb{Z}_{p^2q^2} \cong \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}^*_p \times \mathbb{Z}^*_q. \tag{1}$$

根据中国剩余定理,

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q,$$

两边同时取单位群，得到

$$\mathbb{Z}^*_{pq} \cong \mathbb{Z}^*_p \times \mathbb{Z}^*_q.$$

因此，结合 (1)，我们有

$$\mathbb{Z}_{p^2q^2} \cong \mathbb{Z}_{pq} \times \mathbb{Z}^*_{pq}.$$

解法二:

考虑 $\pi : \mathbb{Z}^*_p \times \mathbb{Z}_p \to \mathbb{Z}^*_{p^2}$，$\pi(a,t) = a^p(1+p)^t$. 我们先验证这是一个同态.

$$\begin{aligned}
\pi(a_1a_2, t_1+t_2) &= (a_1a_2)^p(1+p)^{t_1+t_2} \\
&= a_1^p(1+p)^{t_1} \cdot a_2^p(1+p)^{t_2} \\
&= \pi(a_1,t_1)\pi(a_2,t_2).
\end{aligned}$$

这就完成了验证.

其次，我们来证明这是一个单射. 根据二项式定理，$(1+p)^t = 1 + pt + p^2(\dots) \equiv 1 + pt \pmod{p^2}$. 考虑 $\pi(a,t) = a^p(1+p)^t \equiv 1 \pmod{p^2}$，对两边同时取 $2p'$ 次幂，因为 $\phi(p^2) = 2pp'$，由 Euler 定理，我们有

$$a^{\phi(p^2)}(1+p)^{2p't} \equiv 1 \pmod{p^2} \iff a(1+2pp't) \equiv 1 \pmod{p^2}.$$

因此，$a + 2app't = a(1+2pp't) \equiv 1 \pmod{p}$，注意到 $p \mid 2pp't$，所以 $a \equiv 1 \pmod{p}$. 于是 $1 + 2pp't \equiv 1 \pmod{p^2} \iff p \mid 2p't$，因为 $p, 2p'$ 互素，所以 $p \mid t \implies t \equiv 0 \pmod{p}$.

最后，因为 $|\mathbb{Z}^*_p \times \mathbb{Z}_p| = |\mathbb{Z}^*_p| \cdot |\mathbb{Z}_p| = \phi(p)p = 2pp'$，同时 $|\mathbb{Z}^*_{p^2}| = \phi(p^2) = 2pp' = |\mathbb{Z}^*_p \times \mathbb{Z}_p|$，所以 π 是一个双射，于是

$$\mathbb{Z}^*_{p^2} \cong \mathbb{Z}^*_p \times \mathbb{Z}_p.$$

剩下的证明和法一是一样的.

4. (5 分) 已知群 G 满足 $\forall g \in G, g^2 = e$. 证明 G 是阿贝尔群.

解　对任意两个元素 $a, b \in G$，为证明 $ab = ba$，只需证明它们的交换子 $(ab)(ba)^{-1}$ 等于 e.

$$(ab)(ba)^{-1} = (ab)(ba) = abba = aa = e$$

5. (5 分) 证明或证伪以下命题:

(1) 单同态 $\varphi : G \to G$ 一定是自同构.

(2) 满同态 $\varphi : G \to G$ 一定是自同构.

解

(1) 反例：$\mathbb{Z}$ 上的同态 $x \mapsto 2x$.

(2) 反例：$\mathbb{R}/\mathbb{Z}$ 上的同态 $x \mapsto 2x$.

6. (10 分) 设 G 是一个有限阿贝尔群，证明以下命题

(1) $\prod_{g\in G} g$ 的平方等于单位元 e.

(2) 如果 G 中没有阶（order）为 2 的元素，或 G 中有超过一个阶为 2 的元素，那么 $\prod_{g\in G} g = e$.

(3) 如果 G 中唯一的阶（order）为 2 的元素 y，那么 $\prod_{g\in G} g = y$.

(4) (Wilson's theorem) 如果 p 是素数，$(p-1)! \equiv -1 \mod p$.

解

(1) $\left(\prod_{g\in G} g\right)^2 = \prod_{g\in G} g \prod_{g\in G} g^{-1} = \prod_{g\in G} gg^{-1} = e$.

(2) 定义 $H := \{g \in G \mid g^2 = e\}$ 为所有阶不超过 2 的元素. 将 $G \setminus H$ 中的元素两两配对，每个元素与它的逆配对，可以将 $G \setminus H$ 写成

$$G \setminus H = \{g_1, g_1^{-1}, g_2, g_2^{-1}, \dots\}.$$

因此 $\prod_{g\in G\setminus H} = e$. 剩下只需证明 $\prod_{g\in H} = e$.

不难验证 H 是 G 的子群.

若 G 中没有阶为 2 的元素：$H = \{e\}$，符合要求.

若 G 中有超过一个阶为 2 的元素：(有限生成阿贝尔群的基本定理可以带来更简短的证明) 令 $K_0 = \{e\}$. 只要 $K_i \subsetneq H$，任选 $h_i \in H \setminus K_i$，递归地定义 $K_{i+1} = K_i \cup h_i K_i$. 不难说明 a) $|K_i| = 2^i$，b) 每个 K_i 都是 H 的子群，c) 特别地，$H = K_t$ 其中 $t \geq 2$.

$$\prod_{g\in H} g = \prod_{g\in K_{t-1}} g \prod_{g\in K_{t-1}} h_{t-1}g = \prod_{g\in K_{t-1}} gh_{t-1}g = \prod_{g\in K_{t-1}} h_{t-1} = h_{t-1}^{|K_{t-1}|} = h_{t-1}^{2^{t-1}} = e.$$

(3) 类似地定义 H，可知 $H = \{e, y\}$. 因此 $\sum_{g\in G} g = \sum_{g\in H} g = y$.

(4) 当 $p > 2$ 时，在群 $\mathbb{Z}_p^*$ 中，-1 是唯一的阶为 2 的元素，因而 $\sum_{a\in\mathbb{Z}_p^*} a = -1$。