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 $p = a$，$q = b$，这种情况下只有一组解.

3. (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.

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

4. (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 $\sum_{a\in\mathbb{Z}_p^*} a = -1$。

5. (10 分) 形如 $aba^{-1}b^{-1}$ 被称作 a, b 的换位子. 给定群 G, 定义它的换位子群（commutator subgroup）$G' = \langle aba^{-1}b^{-1} : a, b \in G\rangle$ 为所有换位子生成的群.

(1) 证明：$G' \trianglelefteq G$.

(2) 考虑 $N \trianglelefteq G$，证明：G/N 是 Abel 群当且仅当 $G' \leq N$.

(3) 考虑 Sym(4)，即 $\{1, 2, 3, 4\}$ 上的对称群，请给出一个序列：

$$S_4 = G^0 \triangleright G^1 \triangleright \cdots \triangleright G^n = \{1\},$$

满足 G^i/G^{i+1}（$i = 0, \dots, n-1$）是 Abel 群.

解

(1) G' 是 G 的子群显然，下证正规性：对于任意 $a \in G, b \in G'$, $aba^{-1}b^{-1} \in G'$，故 $aba^{-1} \in G'$，正规性得证.

(2) G/N 是 Abel 群 $\iff$ 任意 $a, b \in G, aN \cdot bN = bN \cdot aN \iff$ 任意 $a, b \in G, abN = baN \iff$ 任意 $a, b \in G$，$a^{-1}b^{-1}ab \in N \iff G' \leq N$.

(3) 考虑不断取前面一个群的换位子群. Sym(4) 的换位子群是 Alt(4). Alt(4) 的换位子群是

$$\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

这个群被称为 Klein 四元数群，记为 V. V 的换位子群为 $\{1\}$.

故可以构造序列：$\mathrm{Sym}(4) \triangleright \mathrm{Alt}(4) \triangleright V \triangleright \{1\}$.

注. 存在上面序列的群被称为**可解群**，$\mathrm{Sym}(n)$ 是可解群当且仅当 $n \leq 4$，特别地，Sym(5) 的正规子群 Alt(5) 是单群，因而不可解. 一个群是否可解对应了一个代数方程是否可以根式求解，这是 *Galois* 理论的重要内容.

关于四元数群：我们知道，虚数单位 i 是满足 $i^2 = -1$ 的人造数. 然而，我们完全不需要限制只有一个 i 和一个 $-i$ 满足这一方程，我们还可以给出别的不同的虚数单位 $j, k, \ldots$. 但是，并不是任意个数的虚数单位都可以得到我们想要的代数系统，实际上，类似 $\mathbb{R}$ 和 $\mathbb{C}$ 的数域（即带单位元的赋范可除代数）只有四元数（三个虚数单位）和八元数（七个虚数单位）*(Hurwitz* 定理）. 四元数的虚数单位连同 1 构成了四元数群.

6. (5 分) 考虑集合 S 与 S 上的二元运算 $\cdot$. 如果 $\cdot$ 满足结合律, 那么 $(S, \cdot)$ 构成半群 (semigroup). 如果还存在单位元, 那么称作幺半群 (monid). 如果还存在逆元, 那么就是群.

假设半群 $(S, \cdot)$ 额外满足

- 对称性 $\forall a \forall b\ a \cdot b = b \cdot a$
- 消去律 $\forall a \forall b \forall c\ a \cdot b = a \cdot c \to b = c$

证明, 可以将 S 嵌入一个群 G 中. 也就是存在群 $(G, \star)$, 满足 $S \subseteq G$ 且 $\forall a \forall b\ a \cdot b = a \star b$.

解 不失一般性, 假设 S 非空. 题目等价于构造一个单射 $\pi : S \to G$, 满足 $\pi(a \cdot b) = \pi(a)\pi(b)$.

定义 $S \times S$ 上的关系 $\sim$ 为 $(a, b) \sim (c, d) \iff ad = bc$. 不难验证 $\sim$ 是一个等价关系：自反性和对称性是显然的, 对于传递性:

$$(a, b) \sim (c, d) \ \wedge\ (c, d) \sim (e, f) \implies ad = bc \ \wedge\ cf = de$$
$$\implies adcf = bcde \implies af = be \implies (a, b) \sim (e, f).$$

定义 $G = S/\sim$. 定义 G 上的二元运算 $\overline{(a, b)} \star \overline{(c, d)} = \overline{(ac, bd)}$. 这里用上横线表示所在的等价类.

需要说明这个二元运算是良定义的, 其输出不依赖于代表元的选取:

$$(a',b') \in \overline{(a,b)}, (c',d') \in \overline{(c,d)} \implies a'b = b'a, c'd = d'c \implies a'c'bd = b'd'ac$$
$$\implies (a'c', b'd') \sim (ac, bd) \implies \overline{(a'c', b'd')} = \overline{(ac, bd)}.$$

任意选定 $u \in S$, 将嵌入 $\pi : S \to G$ 定义为 $\pi(a) = \overline{(au, u)}$.