初等数论

请在 10 月 19 日课前提交纸质作业.

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

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

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 $\mu(x) < 1 + \epsilon$.

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：（这里 $\cong$ 是同构的记号）

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

   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 $\pi : \mathbb{Z}_p^* \times \mathbb{Z}_p \to \mathbb{Z}_{p^2}^*$

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