第 4-4 讲: 数论初步

姓名: 林凡琪 **学号:** 211240042

评分: ______ **评阅:** ______

2023 年 3 月 21 日

请独立完成作业，不得抄袭。
若得到他人帮助, 请致谢。
若参考了其它资料，请给出引用。
鼓励讨论，但需独立书写解题过程。

1 作业 (必做部分)

题目 1 (TJ 2-15(b,f))

解答:
(b) 234 and 165

$$gcd(234, 165) = 3$$

$$r = 12, s = -17$$

(f)-4357 and 3754

$$gcd(-4357, 3754) = 1$$

$$r = 1463, s = 1698$$

题目 2 (TJ 2-16)

证明:
令 $gcd(a, b) = t$, 那么 $a = k_1t, b = k_2t, k_1, k_2 \neq 0$, 可知

$$ar + bs = t(k_1r + k_2s) = 1$$

因为 $k_1r + k_2s \neq 0$, 所以 $t|1$
可知 $t = 1$ □

题目 3 (TJ 2-19)

证明:
令

$$xy = p_1^{2k_1} p_2^{2k_2} ... p_t^{2k_t}, k_i \geq 0$$

$$x = p_1^{a_1} p_2^{a_2} ... p_t^{a_t}, a_i \geq 0$$

$$y = p_1^{b_1} p_2^{b_2} ... p_t^{b_t}, b_i \geq 0$$

所以

$$gcd(x, y) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} ... p_t^{min(a_t,b_t)} = 1$$

所以

$$min(a_i, b_i) = 0 \Rightarrow a_i = 0, b_i = 2k_i \text{ or } a_i = 2k_i, b_i = 0$$

所以 x,y 都是 perfect squares.

题目 4 (TJ 2-29)

证明:
反证法:

假设有有限的质数 $p_0 = 5, p_1, p_2, ..., p_k$ 可以用 $6n + 5$ 的形式表示.

令 $S = \{p_1, p_2, ..., p_k\}$.

令 $P = 6p_1p_2...p_k + 5$

当 P 是质数, 与假设矛盾.

当 $P = q_1q_2...q_s$(其中 q_i 是质数), 显然 $q_i \neq 0, 2, 3, 4 (\mod 6)$

如果 $\forall q_i, q_i = 1(\mod 6)$. 那么, $P = q_1q_2...q_s = 1(\mod 6)$, 这和 $P = 5(\mod 6)$ 矛盾

如果 $\exists q_i = p_t = 5(\mod 6) \in S$, 那么 $q_i|P \Rightarrow p_t|P \Rightarrow p_t|6p_1p_2...p_k + 5 \Rightarrow p_t|5$. 但是与 $\forall p_t \in S, p_t > 5$ 矛盾

如果 $\exists q_i = 5$. 那么 $q_i|P \Rightarrow 5|6p_1p_2...p_k + 5 \Rightarrow 5|6p_1p_2...p_k \Rightarrow \exists p_t \in S, 5|p_t$

但这和 p_t 是质数矛盾。

综上得证。

题目 5 (TJ 2-30)

证明:
反证法:

假设有有限的质数 $p_0 = 3, p_1, p_2, ..., p_k$ 可以用 $4n - 1$ 的形式表示.

令 $S = \{p_1, p_2, ..., p_k\}$.

令 $P = 4p_1p_2...p_k + 3$

当 P 是质数, 与假设矛盾.

当 $P = q_1q_2...q_s$(其中 q_i 是质数), 显然 $q_i \neq 0, 2(\mod 4)$

如果 $\forall q_i, q_i = 1(\mod 4)$. 那么, $P = q_1q_2...q_s = 1(\mod 4)$, 这和 $P = 3(\mod 4)$ 矛盾

如果 $\exists q_i = p_t \in S$, 那么 $q_i|P \Rightarrow p_t|P \Rightarrow p_t|4p_1p_2...p_k - 1 \Rightarrow p_t|3$. 但是与 $\forall p_t \in S, p_t > 3$ 矛盾

如果 $\exists q_i = 3$. 那么 $q_i|P \Rightarrow 3|4p_1p_2...p_k + 3 \Rightarrow 3|4p_1p_2...p_k \Rightarrow \exists p_t \in S, 3|p_t$

但这和 p_t 是质数矛盾。

综上得证。 $\square$

题目 6 (CS 2.2-2)

解答:
能保证 a 有模 m 的逆

根据 Lemma 2.8，a 有模 m 的逆的充要条件是 a 和 m 互质。

而在题目中 $a \cdot 133{-}2m \cdot 277 = 1.$

前提条件有 $n\ geq 2$

可知

$$n = m \geq 2, y = -544, a^{-1} = 133$$

说明 $gcd(a, m) = 1$，所以 a 有模 m 的逆。

题目 7 (CS 2.2-4)

解答:
根据 Corallary 2.16 可知,

$gcd(31, 32) = 1, 22$ 在 Z_{31} 里有一个逆

$gcd(10, 2) = 2, 2$ 在 Z_{10} 里没有逆

题目 8 (CS 2.2-6)

解答:
根据 TH 2.15 可知，two positive integers j and k have greatest common divisor 1 (and thus are relatively prime) if and only if there are integers x and y such that $jx + ky = 1$

所以

$$gcd(a, m) = 1$$

题目 9 (CS 2.2-8)

解答:
According to TH 2.1, which is exactly Euclid's Division Theorem. Let j be a positive integer. Then for every integer k, there exists unique integers q and r and $0 \leq r < n$

According to Lemma 2.13, if j, k, q and r are positive integers such that $k = jq + r$, then

$$gcd(j, k) = gcd(r, j)$$

This means that the greatest common divisor of q and k is equal to the greatest common divisor of r and q.

题目 10 (CS 2.2-16)

解答:
如果 $m < 0, -m = qn + r, r = 0$, 那么

$$m = -qn$$

令 $q' = -q, r' = 0$. 如果 $m < 0, -m = qn + r, r > 0$, 那么

$$m = -qn - r = -(q+1)n + (n-r)$$

令 $q' = -(q+1), r' = n - r$.

题目 11 (CS 2.2-19)

解答:

$$xy = gcd(x, y) \cdot lcm(x, y)$$

令

$$x = p_1^{a_1} p_2^{a_2} ... p_t^{a_t}, a_i \geq 0$$

$$y = p_1^{b_1} p_2^{b_2} ... p_t^{b_t}, b_i \geq 0$$

然后

$$gcd(x, y) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} ... p_t^{min(a_t,b_t)}$$
$$lcm(x, y) = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} ... p_t^{max(a_t,b_t)}$$

所以

$$\begin{aligned} xy &= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_t^{a_t+b_t} \\ &= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} p_2^{\min(a_2,b_2)+\max(a_2,b_2)} \cdots p_t^{\min(a_t,b_t)+\max(a_t,b_t)} \\ &= \gcd(x, y) \cdot \operatorname{lcm}(x, y) \end{aligned}$$

---

2 作业 (选做部分)

3 Open Topics

Open Topics 1 (Lucas 定理)

- 参考资料：https://brilliant.org/wiki/lucas-theorem/

Open Topics 2 (Miller-Rabin Algorithm)

4 反馈