第 4-4 讲: 数论初步

姓名： 朱宇博　　**学号：** 191220186

评分： ______　　**评阅：** ______

2021 年 3 月 22 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))
For each of the following pairs of numbers a and b, calculate gcd(a,b) and find integers r and s such that gcd(a, b) = ra + sb.
(b)234 and 165
(f)−4357 and 3754

解答:
(b)

$$
\begin{aligned}
234 &= 165 \times 1 + 69 \\
165 &= 69 \times 2 + 27 \\
69 &= 27 \times 2 + 15 \\
27 &= 15 \times 1 + 12 \\
15 &= 12 \times 1 + 3 \\
12 &= 3 \times 4 + 0
\end{aligned}
$$

Therefore gcd(234, 165) = 3

$$
\begin{aligned}
3 &= 1 \times 15 + (-1) \times 12 \\
&= (-1) \times 27 + 2 \times 15 \\
&= 2 \times 69 + (-5) \times 27 \\
&= 12 \times 69 + (-5) \times 165 \\
&= 2 \times 69 + (-5) \times 27 \\
&= 12 \times 234 + (-17) \times 165
\end{aligned}
$$

So $r = 12, s = -17$

(f)

$$
\begin{aligned}
-4357 &= 3754 \times (-1) + (-603) \\
3754 &= (-603) \times (-6) + 136 \\
-603 &= 136 \times (-4) + (-59) \\
136 &= (-59) \times (-2) + 18 \\
-59 &= 18 \times (-3) + (-5) \\
18 &= (-5) \times (-3) + (-3) \\
-5 &= (-3) \times 1 + (-2) \\
(-3) &= (-2) \times 1 + (-1) \\
(-2) &= (-1) \times 2 + 0
\end{aligned}
$$

Therefore gcd(−4357, 3754) = 1

```
-4357 3754
1 *1 +0 *0 =1
-2 *0 +1 *1 =1
3 *1 +-2 *1 =1
-5 *1 +3 *2 =1
18 *2 +-5 *7 =1
-59 *7 +18 *23 =1
136 *23 +-59 *53 =1
-603 *53 +136 *235 =1
3754 *235 +-603 *1463 =1
-4357 *1463 +3754 *1698 =1
zhuyubo@zhuyubodeMacBook-Pro code %
```

So $r = 1463, s = 1698$

题目 2 (TJ 2-16)
Let a and b be nonzero integers. If there exist integers r and s such that $ar + bs = 1$, show that a and b are relatively prime.

解答:
由 Theorem 2.10 的证明过程可知，$S = \{am + bn : m, n \in \mathbb{Z} \wedge am + bn > 0\}$ 中的最小元是 gcd(a,b)。
由集合 S 的性质，显然有：若 $1 \in S$, 则 1 为 S 中最小元，即为 gcd(a,b)
由题设可知 1 在集合 S 中。故 gcd(a,b)=1, a 和 b 互质

题目 3 (TJ 2-19)
Let $x, y \in N$ be relatively prime. If xy is a perfect square, prove that x and y must both be perfect squares.

解答:
反证法。假设 x 不为完全平方数，则 x 存在一个质因子 a，在 x 的质数乘积分解中，出现奇数次。
由于 x, y 互质，则在 y 的质数乘积分解中，不会出现质因子 a。
故在 xy 的的质数乘积分解中，质因子 a 出现的次数仍为奇数次，故 xy 不为完全平

方数，与题设矛盾。
得证

题目 4 (TJ 2-29)
Prove that there are an infinite number of primes of the form 6n + 5.

解答:
反证。假设 $S = \{x|x \quad is \quad prime \wedge \exists p, 6p + 5 = x\}$ 为有限集，记 $|S| = N$
令 $T = \prod_{i=1}^{N} x_i$, $x_i \in S$。
当 N 为奇数时，T 模 6 为 5，故 $T + 6$ 模 6 为 5。
在 $T + 6$ 的所有质因子中，一定存在形如 $6n + 5$ 的质因子。否则，$T + 6$ 模 6 不为 5。由于 $x_i(x_i \in S)$ 都不为 $T + 6$ 的因子，则存在一个形如 $6n + 5$ 的质数，不在集合 S 中，与假设矛盾。
当 N 为偶数时，T 模 6 为 1，故 $T + 4$ 模 6 为 5。
在 $T + 4$ 的所有质因子中，一定存在形如 $6n + 5$ 的质因子。否则，$T + 4$ 模 6 不为 5。由于 $x_i(x_i \in S)$ 都不为 $T + 4$ 的因子，则存在一个形如 $6n + 5$ 的质数，不在集合 S 中，与假设矛盾。
故形如 $6n + 5$ 的质数有无穷多个。

题目 5 (TJ 2-30)
Prove that there are an infinite number of primes of the form 4n − 1.

解答:
反证。假设 $S = \{x|x \quad is \quad prime \wedge \exists p, 4n - 1 = x\}$ 为有限集，记 $|S| = N$
令 $T = \prod_{i=1}^{N} x_i$, $x_i \in S$。
当 N 为奇数时，T 模 4 为 3，故 $T + 4$ 模 4 为 3。
在 $T + 4$ 的所有质因子中，一定存在形如 $4n - 1$ 的质因子。否则，$T + 4$ 模 4 不为 3。由于 $x_i(x_i \in S)$ 都不为 $T + 4$ 的因子，则存在一个形如 $4n - 1$ 的质数，不在集合 S 中，与假设矛盾。
当 N 为偶数时，T 模 4 为 1，故 $T + 2$ 模 4 为 3。
在 $T + 2$ 的所有质因子中，一定存在形如 $4n - 1$ 的质因子。否则，$T + 2$ 模 4 不为 3。由于 $x_i(x_i \in S)$ 都不为 $T + 2$ 的因子，则存在一个形如 $4n - 1$ 的质数，不在集合 S 中，与假设矛盾。
故形如 $4n - 1$ 的质数有无穷多个。

题目 6 (CS 2.2-2)
If a · 133−m · 277 = 1, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

解答:
存在逆，由 a · 133−m · 277 = 1，我们可知 gcd(a,m)=1，且 $133a \equiv 1 \pmod{m}$，故 a 的逆为 $133 \mod m$

题目 7 (CS 2.2-4)
How many elements a are there such that a $\cdot_{31}$ 22 = 1? How many elements a are there such that a $\cdot_{10}$ 2 = 1?

解答:
(1)
因为 gcd(31,22)=1, 故 22 存在一个在模 31 意义下的逆。数量为 1
(2)
因为 $gcd(10, 2) \neq 1$, 故 2 不存在一个在模 10 意义下的逆。数量为 0

题目 8 (CS 2.2-6)
If a · 133−m · 277 = 1, what can you say about all possible common divisors of a and m?

解答:
若满足上述等式，则 a 与 m 互质，其公因数只有 1 和-1

题目 9 (CS 2.2-8)
If k = jq +r, as in Euclid’ s division theorem, is there a relationship between gcd(q, k) and gcd(r, q)? If so, what is it?

解答:
gcd(q, k) =gcd(r, q).
其中 j 和 q 是等同地位的，可相互替换。
由欧几里得定理可得两者最大公因数相同

题目 10 (CS 2.2-16)

解答:
若 m 为负数，则存在唯一的 q 和 r，使得 $-m = nq + r$，其中 $0 \leq r < n$
若 r 为 0，则显然有 m=n(-q)+r 满足该形式。
若 r 大于 0，因为 $-m = nq + r$，则有 $m = -nq - r$，令 $q' = -q - 1$，则 $m = n(q' + 1) - r = nq' + (n - r)$
此式满足上述形式。
以下证明唯一性。假设存在 q 和 r，q' 和 r' 满足 $m = nq + r$, $m = nq' + r'$, 其中 $0 \leq r < n$，$0 \leq r' < n$
因此有 $n(q - q') = r' - r$，即 $n|r' - r$, 由于 $0 \leq r < n$，$0 \leq r' < n$，故 $|r' - r| < n$。
因此可推得 $r = r'$。
所以 $n(q - q') = 0$，得 $q - q'$
故唯一性可证

题目 11 (CS 2.2-19)

解答:
$lcm(x, y) = \frac{xy}{gcd(x,y)}$

---

2 作业 (选做部分)

3 Open Topics

Open Topics 1 (介绍皮亚诺公理)

Open Topics 2 (Miller-Rabin Algorithm)

4 反馈