4-4 Number Theory

Jun Ma

majun@nju.edu.cn

2021 年 3 月 31 日

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

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

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

(f) -4357 and 3754

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

$$r = 1463, s = 1698$$

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.

- Suppose that $\gcd(a, b) = t$, then $a = k_1 t$, $b = k_2 t$, $k_1, k_2 \neq 0$, then

$$ar + bs = t(k_1 r + k_2 s) = 1$$

- Suppose that $\gcd(a, b) = t$, then $a = k_1 t$, $b = k_2 t$, $k_1, k_2 \neq 0$, then

$$ar + bs = t(k_1 r + k_2 s) = 1$$

- $k_1 r + k_2 s \neq 0$, so $t|1$; therefore, $t = 1$

TJ 2-19

Let $x, y \in \mathbb{N}$ be relatively prime. If xy is a perfect square, prove that x and y must both be perfect squares.

Assume

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

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

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

Assume

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

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

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

So,

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

Assume

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

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

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

So,

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

Therefore,

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

So, x, y are both perfect squares.

TJ 2-29

Prove that there are an infinite number of primes of the form $6n + 5$.

- Suppose there are finite number of primes $p_0 = 5, p_1, p_2, \cdots, p_k$ of form $6n+5$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 6p_1p_2\cdots p_k + 5$$

- Suppose there are finite number of primes $p_0 = 5, p_1, p_2, \cdots, p_k$ of form $6n + 5$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 6p_1p_2 \cdots p_k + 5$$

- **Case 1 :** P is prime. Contradiction!

- Suppose there are finite number of primes $p_0 = 5, p_1, p_2, \cdots, p_k$ of form $6n+5$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 6p_1p_2\cdots p_k + 5$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.

- Suppose there are finite number of primes $p_0 = 5, p_1, p_2, \cdots, p_k$ of form $6n+5$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 6p_1p_2\cdots p_k + 5$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
    - Obviously, $q_i \neq 0, 2, 3, 4 \pmod 6$

- Suppose there are finite number of primes $p_0 = 5, p_1, p_2, \cdots, p_k$ of form $6n + 5$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 6p_1p_2 \cdots p_k + 5$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2 \cdots q_s$, where each q_i is a prime.
  - Obviously, $q_i \neq 0, 2, 3, 4 \pmod 6$
  - **Case 2.1:** $\forall q_i, q_i = 1 \pmod 6$. Then, $P = q_1q_2 \cdots q_s = 1 \pmod 6$, which is contradict to $P = 5 \pmod 6$

- Suppose there are finite number of primes $p_0 = 5, p_1, p_2, \cdots, p_k$ of form $6n+5$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 6p_1p_2\cdots p_k + 5$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
  - Obviously, $q_i \neq 0, 2, 3, 4 \pmod 6$
  - **Case 2.1:** $\forall q_i, q_i = 1 \pmod 6$. Then, $P = q_1q_2\cdots q_s = 1 \pmod 6$, which is contradict to $P = 5 \pmod 6$
  - **Case 2.2:** $\exists q_i = p_t = 5 \pmod 6 \in S$. Then,

$$q_i|P \Rightarrow p_t|P \Rightarrow p_t|6p_1p_2\cdots p_k + 5 \Rightarrow p_t|5$$

- Suppose there are finite number of primes $p_0 = 5, p_1, p_2, \cdots, p_k$ of form $6n+5$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 6p_1p_2\cdots p_k + 5$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
  - Obviously, $q_i \neq 0, 2, 3, 4 \pmod 6$
  - **Case 2.1:** $\forall q_i, q_i = 1 \pmod 6$. Then, $P = q_1q_2\cdots q_s = 1 \pmod 6$, which is contradict to $P = 5 \pmod 6$
  - **Case 2.2:** $\exists q_i = p_t = 5 \pmod 6 \in S$. Then,

$$q_i | P \Rightarrow p_t | P \Rightarrow p_t | 6p_1p_2\cdots p_k + 5 \Rightarrow p_t | 5$$

However $\forall p_t \in S, p_t > 5$. Contradiction!

- Suppose there are finite number of primes $p_0 = 5, p_1, p_2, \cdots, p_k$ of form $6n + 5$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 6p_1p_2\cdots p_k + 5$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
  - Obviously, $q_i \neq 0, 2, 3, 4 \pmod 6$
  - **Case 2.1:** $\forall q_i, q_i = 1 \pmod 6$. Then, $P = q_1q_2\cdots q_s = 1 \pmod 6$, which is contradict to $P = 5 \pmod 6$
  - **Case 2.2:** $\exists q_i = p_t = 5 \pmod 6 \in S$. Then,

    $$q_i|P \Rightarrow p_t|P \Rightarrow p_t|6p_1p_2\cdots p_k + 5 \Rightarrow p_t|5$$

    However $\forall p_t \in S, p_t > 5$. Contradiction!
  - **Case 2.3:** $\exists q_i = 5$. Then

    $$q_i|P \Rightarrow 5|6p_1p_2\cdots p_k + 5 \Rightarrow 5|6p_1p_2\cdots p_k \Rightarrow \exists p_t \in S, 5|p_t$$

    Which is impossible, as p_t is a prime.Contradiction!

TJ 2-30

Prove that there are an infinite number of primes of the form $4n-1$.

- Suppose there are finite number of primes $p_0 = 3, p_1, p_2, \cdots, p_k$ of form $4n - 1$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 4p_1p_2 \cdots p_k + 3$$

- Suppose there are finite number of primes $p_0 = 3, p_1, p_2, \cdots, p_k$ of form $4n-1$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 4p_1p_2\cdots p_k + 3$$

- **Case 1 :** P is prime. Contradiction!

- Suppose there are finite number of primes $p_0 = 3, p_1, p_2, \cdots, p_k$ of form $4n-1$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 4p_1p_2\cdots p_k + 3$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.

- Suppose there are finite number of primes $p_0 = 3, p_1, p_2, \cdots, p_k$ of form $4n-1$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 4p_1p_2\cdots p_k + 3$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
  - Obviously, $q_i \neq 0, 2 \pmod 4$

- Suppose there are finite number of primes $p_0 = 3, p_1, p_2, \cdots, p_k$ of form $4n-1$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 4p_1p_2\cdots p_k + 3$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
  - Obviously, $q_i \neq 0, 2 \pmod 4$
  - **Case 2.1:** $\forall q_i, q_i = 1 \pmod 4$. Then, $P = q_1q_2\cdots q_s = 1 \pmod 4$, which is contradict to $P = 3 \pmod 4$

- Suppose there are finite number of primes $p_0 = 3, p_1, p_2, \cdots, p_k$ of form $4n-1$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 4p_1p_2\cdots p_k + 3$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
  - Obviously, $q_i \neq 0, 2 \pmod 4$
  - **Case 2.1:** $\forall q_i, q_i = 1 \pmod 4$. Then, $P = q_1q_2\cdots q_s = 1 \pmod 4$, which is contradict to $P = 3 \pmod 4$
  - **Case 2.2:** $\exists q_i = p_t \in S$. Then,

$$q_i|P \Rightarrow p_t|P \Rightarrow p_t|4p_1p_2\cdots p_k - 1 \Rightarrow p_t|3$$

- Suppose there are finite number of primes $p_0 = 3, p_1, p_2, \cdots, p_k$ of form $4n-1$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 4p_1p_2\cdots p_k + 3$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
  - Obviously, $q_i \neq 0, 2 \pmod 4$
  - **Case 2.1:** $\forall q_i, q_i = 1 \pmod 4$. Then, $P = q_1q_2\cdots q_s = 1 \pmod 4$, which is contradict to $P = 3 \pmod 4$
  - **Case 2.2:** $\exists q_i = p_t \in S$. Then,

$$q_i|P \Rightarrow p_t|P \Rightarrow p_t|4p_1p_2\cdots p_k - 1 \Rightarrow p_t|3$$

However $\forall p_t \in S, p_t > 3$. Contradiction!

- Suppose there are finite number of primes $p_0 = 3, p_1, p_2, \cdots, p_k$ of form $4n-1$. Denote $S = \{p_1, p_2, \cdots, p_k\}$. Let

$$P = 4p_1p_2\cdots p_k + 3$$

- **Case 1 :** P is prime. Contradiction!
- **Case 2 :** $P = q_1q_2\cdots q_s$, where each q_i is a prime.
    - Obviously, $q_i \neq 0, 2 \pmod 4$
    - **Case 2.1:** $\forall q_i, q_i = 1 \pmod 4$. Then, $P = q_1q_2\cdots q_s = 1 \pmod 4$, which is contradict to $P = 3 \pmod 4$
    - **Case 2.2:** $\exists q_i = p_t \in S$. Then,

    $$q_i|P \Rightarrow p_t|P \Rightarrow p_t|4p_1p_2\cdots p_k - 1 \Rightarrow p_t|3$$

    However $\forall p_t \in S, p_t > 3$. Contradiction!
    - **Case 2.3:** $\exists q_i = 3$. Then

    $$q_i|P \Rightarrow 3|4p_1p_2\cdots p_k + 3 \Rightarrow 3|4p_1p_2\cdots p_k \Rightarrow \exists p_t \in S, 3|p_t$$

    Which is impossible, as p_t is a prime.Contradiction!

CS 2.2-2

If $a \cdot 133 - 2m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

CS 2.2-2

If $a \cdot 133 - 2m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

Lemma 2.8 The equation

$$a \cdot_n x = 1$$

has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1. \quad (2.6)$$

CS 2.2-2

If $a \cdot 133 - 2m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

Lemma 2.8

The equation

$$a \cdot_n x = 1$$

has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1. \quad (2.6)$$

Precondition : $n \geq 2$

CS 2.2-2

If $a \cdot 133 - 2m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

Lemma 2.8

The equation

$$a \cdot_n x = 1$$

has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1. \quad (2.6)$$

$$\text{Precondition}: n \geq 2$$

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

CS 2.2-2

If $a \cdot 133 - 2m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

Lemma 2.8

The equation

$$a \cdot_n x = 1$$

has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1. \tag{2.6}$$

$$\text{Precondition}: n \geq 2$$

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

$$m = 1?$$

CS 2.2-2

If $a \cdot 133 - 2m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

Lemma 2.8

The equation

$$a \cdot_n x = 1$$

has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1. \tag{2.6}$$

$$\text{Precondition}: n \geq 2$$

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

$$m = 1?a^{-1} = 0$$

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 $a \cdot_{10} 2 = 1$?

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 $a \cdot_{10} 2 = 1$?

Corollary 2.16 For any positive integer n, an element a of Z_n has a multiplicative inverse if and only if $\gcd(a, n) = 1$.

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 $a \cdot_{10} 2 = 1$?

Corollary 2.16 For any positive integer n, an element a of Z_n has a multiplicative inverse if and only if $\gcd(a, n) = 1$.

- $\gcd(31, 22) = 1$, 22 has one inverse in Z_{31}

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 $a \cdot_{10} 2 = 1$?

Corollary 2.16 For any positive integer n, an element a of Z_n has a multiplicative inverse if and only if $\gcd(a, n) = 1$.

- $\gcd(31, 22) = 1$, 22 has one inverse in Z_{31}
- $\gcd(10, 2) = 2$, 2 has no inverse in Z_{10}

CS 2.2-6

If $a \cdot 133 - m \cdot 277 = 1$, what can you say about all possible common divisors of a and m?

CS 2.2-6

If $a \cdot 133 - m \cdot 277 = 1$, what can you say about all possible common divisors of a and m?

Theorem 2.15

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 $jx + ky = 1$.

CS 2.2-6

If $a \cdot 133 - m \cdot 277 = 1$, what can you say about all possible common divisors of a and m?

Theorem 2.15 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 $jx + ky = 1$.

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

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?

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?

Theorem 2.1 **(Euclid's Division Theorem)** Let n be a positive integer. Then for every integer m, there exist unique integers q and r such that $m = nq + r$ and $0 \leq r < n$.

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

$$\gcd(j, k) = \gcd(r, j). \tag{2.7}$$

CS 2.2-16

Notice that if m is negative, then $-m$ is positive. Thus, by Theorem 2.12, $-m = qn + r$ for $0 \leq r < n$. This gives $m = -qn - r$. If $r = 0$, then $m = q'n + r'$ for $0 \leq r' \leq n$ and $q' = -q$. However, if $r > 0$, then you cannot take $r' = -r$ and have $0 \leq r' < n$. Notice, though, that because you have already finished the case in which $r = 0$, you may assume that $0 \leq n - r < n$. This suggests that if you were to take r' to be $n - r$, you might be able to find a q' so that $m = q'n + r'$, with $0 \leq r' \leq n$, which would let you conclude that Euclid's division theorem is valid for negative values m as well as for nonnegative values m. Find a q' that works, and explain how you have extended Euclid's division theorem from the version in Theorem 2.12 to the version in Theorem 2.1.

Theorem 2.12 **(Euclid's Division Theorem, Restricted Version)** Let n be a positive integer. Then for every nonnegative integer m, there exist unique integers q and r such that $m = nq + r$ and $0 \le r < n$.

$$\Downarrow$$

Theorem 2.1 **(Euclid's Division Theorem)** Let n be a positive integer. Then for every integer m, there exist unique integers q and r such that $m = nq + r$ and $0 \le r < n$.

If $m < 0, -m = qn + r, r = 0$, then

$$m = -qn$$

Let $q' = -q, r' = 0$.
If $m < 0, -m = qn + r, r > 0$, then

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

Let $q' = -(q+1), r' = n - r$.

CS 2.2-19

The least common multiple (LCM) of two positive integers x and y is the smallest positive integer z such that z is an integer multiple of both x and y. Give a formula for the least common multiple that involves the GCD.

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

- Assume

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

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

- Assume

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

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

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

- Assume

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

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

- Then

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

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

- Assume

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

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

- Then

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

- So

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


Thank
You!