- 教材讨论
  - TJ第2章
  - CS第2章第2节

问题1：数学归纳法和良序原理

- 什么是良序原理？
- 你有哪些手段证明“对于任意自然数n，某命题都成立”？

- 你能用其中某种方法证明莱曼引理吗？
  $8a^4+4b^4+2c^4=d^4$没有正整数解

问题1：数学归纳法和良序原理

- 什么是良序原理？
- 你有哪些手段证明“对于任意自然数n，某命题都成立”？
  - 数学归纳法
  - 良序原理（反证法：不成立的那些自然数的集合没有最小元）
- 你能用其中某种方法证明莱曼引理吗？
  $8a^4+4b^4+2c^4=d^4$没有正整数解

问题1：数学归纳法和良序原理

- 什么是良序原理？
- 你有哪些手段证明“对于任意自然数n，某命题都成立”？
  - 数学归纳法
  - 良序原理（反证法：不成立的那些自然数的集合没有最小元）
- 你能用其中某种方法证明莱曼引理吗？
  $8a^4+4b^4+2c^4=d^4$没有正整数解

假设所有解中，(a,b,c,d)使abcd最小
发现d是偶数，将$d=2d'$代入：$4a^4+2b^4+c^4=8d'^4$
发现c是偶数，将$c=2c'$代入：$2a^4+b^4+8c'^4=4d'^4$
发现b是偶数，将$b=2b'$代入：$a^4+8b'^4+4c'^4=2d'^4$
发现a是偶数，将$a=2a'$代入：$8a'^4+4b'^4+2c'^4=d'^4$
找到了新的解(a',b',c',d')且$a'b'c'd'<abcd$，矛盾

问题2：逆元、最大公约数、质数

Given an element b in Z_n, what can you say in general about the possible number of elements a such that $a \cdot_n b = 1$ in Z_n?

为什么？你用到了哪些定理得出了你的结论？

问题2：逆元、最大公约数、质数

Given an element b in Z_n, what can you say in general about the possible number of elements a such that $a \cdot_n b = 1$ in Z_n?

为什么？你用到了哪些定理得出了你的结论？

- 如果gcd(b,n)>1：找不到a
- 如果gcd(b,n)=1：有且只有一个a

Theorem 2.7 *If an element of Z_n has a multiplicative inverse, then it has exactly one inverse.*

Theorem 2.9 *A number a has a multiplicative inverse in Z_n if and only if there are integers x and y such that $ax + ny = 1$.*

Lemma 2.11 *Given a and n, if there exist integers x and y such that $ax + ny = 1$ then* $\gcd(a, n) = 1$.

问题2：逆元、最大公约数、质数 (续)

Either find an equation of the form $a \cdot_n x = b$ in Z_n that has a unique solution even though a and n are not relatively prime, or prove that no such equation exists. In other words, you are either to prove the statement that if $a \cdot_n x = b$ has a unique solution in Z_n, then a and n are relatively prime or to find a counter example.

问题2：逆元、最大公约数、质数 (续)

Either find an equation of the form $a \cdot_n x = b$ in Z_n that has a unique solution even though a and n are not relatively prime, or prove that no such equation exists. In other words, you are either to prove the statement that if $a \cdot_n x = b$ has a unique solution in Z_n, then a and n are relatively prime or to find a counter example.

- 反证：假设gcd(a,n)=g>1
  - 如果g|b
    - $a \cdot_n x = b$有g个解α、α+n/g、α+2n/g……
      其中，α是$(a/g) \cdot_{n/g} x = (b/g)$的唯一解
      因为$(a/g) \cdot_{n/g} x = (b/g)$的解也是原方程的解
  - 否则
    - 很容易证明无解

问题3：欧氏算法

- 辗转相除法和这个引理之间有什么关系？

Lemma 2.13 *If j, k, q, and r are positive integers such that $k = jq + r$ then* $\gcd(j,k) = \gcd(r,j)$

- 辗转相除法的迭代计算到什么时候终止？
- 请使用辗转相除法计算gcd(210,126)，并求出一组r和s使得210r+126s=gcd(210,126)

问题3：欧氏算法

- 辗转相除法和这个引理之间有什么关系？

Lemma 2.13 *If j, k, q, and r are positive integers such that $k = jq + r$ then* $\gcd(j,k) = \gcd(r,j)$

- 辗转相除法的迭代计算到什么时候终止？
- 请使用辗转相除法计算gcd(210,126)，并求出一组r和s使得210r+126s=gcd(210,126)

$$
\begin{aligned}
2415 &= 945 \cdot 2 + 525 \\
945 &= 525 \cdot 1 + 420 \\
525 &= 420 \cdot 1 + 105 \\
420 &= 105 \cdot 4 + 0.
\end{aligned}
$$

$$
\begin{aligned}
105 &= 525 + (-1) \cdot 420 \\
&= 525 + (-1) \cdot [945 + (-1) \cdot 525] \\
&= 2 \cdot 525 + (-1) \cdot 945 \\
&= 2 \cdot [2415 + (-2) \cdot 945] + (-1) \cdot 945 \\
&= 2 \cdot 2415 + (-5) \cdot 945.
\end{aligned}
$$

问题3：欧氏算法(续)

Bob and Alice want to choose a key they can use for cryptography, but all they have to communicate is a bugged phone line. Bob proposes that they each choose a secret number, a for Alice and b for Bob. They also choose, over the phone, a prime number p with more digits than any key they want to use, and one more number q. Bob will send Alice bq mod p, and Alice will send Bob aq mod p. Their key (which they will keep secret) will then be abq mod p. (Here we don't worry about the details of how they use their key, only with how they choose it.) As Bob explains, their wire tapper will know p, q, aq mod p, and bq mod p, but will not know a or b, so their key should be safe.

Is this scheme safe, that is can the wiretapper compute abq mod p? If so, how does she do it?