初等数论

吴 伊 涛

2022 年春

课程特点和设置

- 课程特点：双语教学
- 参考教材：Kenneth H.Rosen著，夏鸿刚译，《初等数论及其应用》（第6版）

其它推荐阅读：

- 见习题课文件最后的“Suggest Reading”

教学内容、授课方式

1. 数学证明的基本方法：反证法和数学归纳法（1周）

2. 整数理论（进制表示、整除和素数、算术基本定理、素数的分布、算术函数）（4周+1习题课）

3. 丢番图方程（组）理论（约3周+1习题课）

4. 同余理论（约5周+1习题课）

分数计算

1. 平时成绩= 签到考勤分（10分）+上课纪律分（30分）+作业分数（20分）+讲题分+期中考试成绩×40%，大于100按100计算。

2. 作业分数：第1、3部分结束后各有一次大作业，会用大写字母评定等级。**注意：这个等级评定是对你每次作业的评价，和平时成绩中的作业分数无关。**具体参见每个作业文件附的说明

3. 期中考试成绩：第2部分结束后有一次期中考试，满分100分。

4. 讲题分：第1、2、3部分结束后有习题课，习题课文件的题目会在每一部分开始时发给大家，需要大家习题课时上台讲解。每题讲解正确的话会有讲题分（具体分数已经注明在习题课文件中），此外，平时上课时也时常会请同学们上台解题，每次也有2分的讲题分。

5. 总评成绩= 平时成绩$\times 40\%+$ 期末考试卷面成绩$\times 60\%$。

6. 申请免听的同学需要做一下上学期的初等数论期末考试卷，*80*分以上才可以申请免听。

Proof by Contradiction(反证法)

Example 1： Prove $\sqrt{2}$ is an irrational number.

Proof: Assume not, then $\sqrt{2}$ is an rational number.

Then we can write $\sqrt{2} = \frac{p}{q}$, where p, q both are integers, with $q \neq 0$ and at least one of p, q is odd(Why?).

Now, we have

$$\sqrt{2} = \frac{p}{q} \qquad (*)$$

Squaring both sides of (*), we then get:

$$2q^2 = p^2 \qquad (**)$$

Since the left hand side(LHS for short) of (**) is an even number, thus p^2 is also even, which leads to p is also even(Why?). So $p = 2p_1$ for some integer p_1.

Now, apply $p = 2p_1$ to (**), we then get:

$$q^2 = 2p_1^2 \qquad (***)$$

The right hand side(RHS for short) of (***) is an even number, thus q^2 is also even, which leads to q is also even. Thus p, q both even, a contradiction to the assumption that at least one of p, q is odd. $\square$

Explanations of red sentence.

The 1st red sentence can be deduced from the following fact: Every fractional(rational number) can be written in a form $\frac{a}{b}$ such that at least one of a, b is odd.

Reason: Given a fractional $\frac{x}{y}$, if one of x, y is odd, then nothing to do. If x, y are both even, then we can divide x, y by 2. Repeated this procedure, we get the required form. e.g.

$$\frac{3}{15} = \frac{3}{15}$$

$$\frac{6}{24} = \frac{3}{12}$$

$$\frac{8}{48} = \frac{4}{24} = \frac{2}{12} = \frac{1}{6}$$

Explanations of red sentence.

The 2nd red sentence can be deduced from the following fact: The square of odd is odd, the square of even is even.

square of even:

$$(2k)^2 = 4k^2 = 2(2k^2)$$

square of odd:

$$(2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Exercise 1: Prove $\sqrt{3}$ is an irrational number.

Proof: Assume not, then $\sqrt{3}$ is an rational number.

Then we can write $\sqrt{3} = \frac{p}{q}$, where p, q both are integers, with $q \neq 0$ and at least one of p, q is not a multiple of 3(Why?).

Now, we have

$$\sqrt{3} = \frac{p}{q} \qquad (*)$$

Squaring both sides of (*), we then get:

$$3q^2 = p^2 \qquad (**)$$

Since the LHS of (**) is a multiple of 3, thus p^2 is also a multiple of 3, which leads to p is also a multiple of 3(Why?). So $p = 3p_1$ for some integer p_1.

Now, apply $p = 3p_1$ to (**), we then get:

$$q^2 = 3p_1^2 \qquad (***)$$

The RHS of (***) is a multiple of 3, thus q^2 is also a multiple of 3, which leads to q is also a multiple of 3.

Thus p, q both are multiple of 3, a contradiction to the assumption that at least one of p, q is not a multiple of 3. $\square$

Explanations of blue sentence.

The 1st blue sentence can be deduced from the following fact: Every fractional(rational number) can be written in a form $\frac{a}{b}$ such that at least one of a, b is not a multiple of 3.

Reason: Given a fractional $\frac{x}{y}$, if one of x, y is not a multiple of 3, then nothing to do. If x, y are both multiples of 3, then we can divide x, y by 3. Repeated this procedure, we get the required form. e.g.

$$\frac{3}{15} = \frac{1}{5}$$

$$\frac{6}{24} = \frac{2}{8}$$

$$\frac{8}{48} = \frac{8}{48}$$

Explanations of blue sentence.

The 2nd blue sentence can be deduced from the following (stronger) fact: The square of a 3k-type integer is still a 3k-type integer, the square of a 3k+1-type or 3k+2 type integer is a 3k+1 type integer.

square of a 3k-type integer:

$$(3k)^2 = 9k^2 = 3(3k^2)$$

square of a 3k+1-type or 3k+2 type integer:

$$(3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$$

$$(3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$$

Exercise 2: Prove $\sqrt{8}$ is an irrational number.

Proof: Assume not, then $\sqrt{8}$ is an rational number.

Then we can write $\sqrt{8} = \frac{p}{q}$, where p, q both are integers, with $q \neq 0$ and at least one of p, q is not a multiple of 8(Is this correct?).

Now, we have

$$\sqrt{8} = \frac{p}{q} \qquad (*)$$

Squaring both sides of (*), we then get:

$$8q^2 = p^2 \qquad (**)$$

Since the LHS of (**) is a multiple of 8, thus p^2 is also a multiple of 8, which leads to p is also a multiple of 8(Is this correct?). So $p = 8p_1$ for some integer p_1.

Now, apply $p = 8p_1$ to (**), we then get:

$$q^2 = 8p_1^2 \qquad (***)$$

The RHS of (***) is a multiple of 8, thus q^2 is also a multiple of 8, which leads to q is also a multiple of 8(Is this correct?).

Thus p, q both are multiple of 8, a contradiction to the assumption that at least one of p, q is not a multiple of 8. $\square$

The 1st red sentence is correct from a similar argument as before.

The 2nd red sentence is wrong:

e.g. $m = 8$, $4^2 = 16$ is a multiple of 8, but 4 is NOT a multiple of 8!

Thus the above proof of $\sqrt{8}$ is an irrational number is **wrong**.

Note: For general m, x^2 is a multiple of m doesn't imply that x is also a multiple of m!

Question 1

Q: For what m? x^2 is a multiple of m implies that x is also a multiple of m?

A: m is square free, i.e. m is not a multiple of any square except 1.

(So 2 is square free, 3 is square free, but 8 is NOT square free since 8 is a multiple of $4 = 2^2$. Similarly, 12 is not square free, 500 is not square free...)

Note: $\sqrt{8} = 2\sqrt{2}$, thus $\sqrt{8} = 2\sqrt{2}$ is irrational.

Similarly, one can get $\sqrt{12} = 2\sqrt{3}$, $\sqrt{500} = 10\sqrt{5}$ are irrational...

Question 2

Q: In case it is hard to get the factorization of m, e.g. $m = 1000009$.

Can we say something about $\sqrt{1000009}$?

Question 3

Q: Let m be a positive integer, prove that $\sqrt{m}$ is irrational if and only if m is not a square.

Notations

$\mathbb{N}$: natural numbers

$\mathbb{Z}$: integers ($\mathbb{Z}^+$: positive integers, $\mathbb{Z}^-$: negative integers)

$\mathbb{Q}$: rational numbers

$\mathbb{R}$: real numbers

$\mathbb{C}$: complex numbers

Example 2: Prove $\sqrt{2} \in \mathbb{R} \backslash \mathbb{Q}$.

Proof: Assume not, then $\sqrt{2} \in \mathbb{Q}$.

Then we can write $\sqrt{2} = \frac{p}{q}$, where $p, q \in \mathbb{Z}$, with $q \neq 0$ and at least one of p, q is odd.

Now, we have

$$\sqrt{2} = \frac{p}{q} \qquad (*)$$

Squaring both sides of (*), we then get:

$$2q^2 = p^2 \qquad (**)$$

The LHS of (**) is an even number $\Rightarrow p^2$ is even $\Rightarrow p$ is also even $\Rightarrow p = 2p_1$ for some integer p_1.

Now, apply $p = 2p_1$ to (**), we then get:

$$q^2 = 2p_1^2 \qquad (***)$$

The RHS of (***) is an even number $\Rightarrow q^2$ is also even $\Rightarrow q$ is also even.

Thus p, q both even, a contradiction to the assumption that at least one of p, q is odd. $\square$

Example 3: Prove $\sqrt{2}+\sqrt{3} \in \mathbb{R}\backslash\mathbb{Q}$.

Proof: Assume not, then $\sqrt{2}+\sqrt{3} \in \mathbb{Q}$.

Then we can write $\sqrt{2}+\sqrt{3} = \frac{p}{q}$, where $p, q \in \mathbb{Z}$, with $q \neq 0$. Now, we have

$$\sqrt{2}+\sqrt{3} = \frac{p}{q} \qquad (*)$$

Squaring both sides of (1), we then get:

$$5 + 2\sqrt{6} = \frac{p^2}{q^2}$$

which equivalents to

$$\sqrt{6} = \frac{p^2 - 5q^2}{2q^2} \qquad (**)$$

Claim: $\sqrt{6} \in \mathbb{R} \backslash \mathbb{Q}$

Assume not, then $\sqrt{6} \in \mathbb{Q}$.

Then we can write $\sqrt{6} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, with $b \neq 0$ and at least one of a, b is odd.

Now, we have

$$\sqrt{6} = \frac{a}{b} \qquad (1)$$

Squaring both sides of (1), we then get:

$$6b^2 = a^2 \qquad (2)$$

The LHS of (2) is an even number $\Rightarrow a^2$ is even $\Rightarrow a$ is also even $\Rightarrow a = 2a_1$ for some integer p_1.

Now, apply $p = 2p_1$ to (2), we then get:

$$3b^2 = 2a_1^2 \qquad (3)$$

The RHS of (3) is an even number $\Rightarrow 3b^2$ is also even $\Rightarrow b^2$ is also even $\Rightarrow b$ is also even. Thus a, b both even, a contradiction to the assumption that at least one of a, b is odd. So, $\sqrt{6} \in \mathbb{R}\backslash\mathbb{Q}$, we get the claim.

Now, the LHS of (**) is irrational, but the RHS of (**) is rational, a contradiction. Thus $\sqrt{2} + \sqrt{3} \in \mathbb{R}\backslash\mathbb{Q}$. $\square$

Question 4

*Q: Prove $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}+\sqrt{11} \in \mathbb{R}\backslash\mathbb{Q}$?

Question 5

Q: Let m, n be positive integers, prove that $\sqrt{m} + \sqrt{n}$ is irrational if and only if at least one of m, n is not a square.

Math Induction(数学归纳法)

1. 1st math induction(第一数学归纳法).

Aim: Want to prove statement P(n) holds for any positive integer $n \geq n_0$, where n_0 is a fixed integer.

Step 1: Prove $\mathrm{P}(n_0)$.(Be careful here!)

Step 2: Assume when $n = k(k \geq n_0)$, P(n) holds.

Step 3: Prove $\mathrm{P}(k+1)$.

Example 4: Use induction to prove: for any positive integer n,

$$1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$$

Proof:

Denote the equality in the statement as (*).

Use induction on n.

When $n=1$, the LHS of (*) $=1^2=1$, the RHS of (*) $=\frac{1\times2\times3}{6}=1$. The equality (*) holds.

Assume when $n=k(k\geq1)$, (*) holds, i.e. $1^2+2^2+\cdots+k^2=\frac{k(k+1)(2k+1)}{6}$

When $n=k+1$, we need to prove (*) also holds.

The LHS of (*) $=1^2+2^2+\cdots+k^2+(k+1)^2=(1^2+2^2+\cdots+k^2)+(k+1)^2=\frac{k(k+1)(2k+1)}{6}+(k+1)^2=\frac{k+1}{6}(2k^2+7k+6)$(By induction hypothesis).

The RHS of (*) $= \frac{(k+1)(k+2)(2k+3)}{6} = \frac{k+1}{6}(2k^2 + 7k + 6) =$ The LHS of (*).

So (*) also holds when $n = k + 1$.

By Math induction, the equality holds for any positive integer n. $\square$

Example 5: Use induction to prove: for any integer n greater than 2, $n < 2^{n-1}$. (i.e. $\forall n \in \mathbb{Z}^{>2}, n < 2^{n-1}$.)

Proof:

Use induction on n.

When $n = 3$, $3 < 2^{3-1} = 4$, the inequality holds.

Assume when $n = k (k \geq 3)$, $n < 2^{n-1}$.

When $n = k + 1$, we need to prove $k + 1 < 2^k$.

By induction hypothesis, $k < 2^{k-1}$, thus $k + 1 < 2k < 2 \cdot 2^{k-1} = 2^k$.

So the inequality also holds when $n = k + 1$. By Math induction, the inequality holds for all integers greater than 2. $\square$

Exercise 3: Use induction to prove: for any positive integer n, $n! > 3^{n-2}$.

Proof:

Use induction on n.

When $n = 1$, $1! = 1 > 3^{1-2} = \frac{1}{3}$, the inequality holds.

When $n = 2$, $2! = 1 \times 2 = 2 > 3^{2-2} = 1$, the inequality still holds.

Assume when $n = k (k \geq 2)$, $n! > 3^{n-2}$.

When $n = k + 1$, we need to prove $(k + 1)! > 3^{k+1-2} = 3^{k-1}$.

By induction hypothesis, $k! > 3^{k-2}$. So

$$(k + 1)! = k! \cdot (k + 1) > 3^{k-2} \cdot (k + 1) \geq 3^{k-1}$$

So the inequality also holds when $n = k + 1$. By Math induction, the inequality holds for all positive integers. $\square$

2. 2nd math induction(第二数学归纳法).

Aim: Want to prove statement P(n) holds for any positive integer $n \geq n_0$, where n_0 is a fixed integer.

Step 1: Prove P(n_0).(Be careful here!)

Step 2: Assume when $n \leq k (k \geq n_0)$, P(n) holds.

Step 3: Prove P($k+1$).

Example 6: Use induction to prove: for any integer n greater than 1, there exist natural numbers x, y, such that $n = 2x + 3y$.

(i.e. $\forall n \in \mathbb{Z}^{>1}, \quad \exists x, y \in \mathbb{N}, \quad s.t. n = 2x + 3y.$)

Proof:

Use induction on n.

When $n = 2$, $2 = 2 \times 1 + 3 \times 0$, the statement holds.

When $n = 3$, $3 = 2 \times 0 + 3 \times 1$, the statement also holds. (Why this step?)

Assume when $n \leq k (k \geq 3)$, the statement holds, i.e. $\forall 2 \leq n \leq k (k \geq 3)$,there exist natural numbers x, y(depends on n), such that $n = 2x + 3y$.

When $n = k+1$, we need to find natural numbers x, y, such that $k+1 = 2x + 3y$.

By induction hypothesis, there exist natural numbers s, t, such that $k - 1 = 2s + 3t$, then $k + 1 = k - 1 + 2 = 2(s + 1) + 3t$, thus the statement also holds when $n = k + 1$. By Math induction, the statement holds for all positive integer greater than 1. $\square$

Example 7: Consider the Fibonacci sequence f_n:

$$1, 1, 2, 3, 5, 8, 13, 21, \cdots$$

(i.e. $f_1 = 1, f_2 = 1, f_{n+2} = f_n + f_{n+1} \quad (n \geq 1)$)

Use induction to prove: for any positive integer n,

$$f_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$$

Proof:

Denote the equality $f_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$ as (*).

Use induction on n.

When $n = 1$, the LHS of (*) $= f_1 = 1$

the RHS of (*) $= \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^1 - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^1 = 1$

(*) holds.

When $n = 2$, the LHS of (*) $= f_2 = 1$

the RHS of (*) $= \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^2 - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^2 = \frac{1}{\sqrt{5}}(\frac{6+2\sqrt{5}}{4}) - \frac{1}{\sqrt{5}}(\frac{6-2\sqrt{5}}{4}) = 1$

(*) holds.

(Why this step?)

Assume when $n \leq k (k \geq 2)$, (*) holds.

When $n = k + 1$,

The LHS of (*) $= f_{k+1} = f_{k-1} + f_k$.

By induction hypothesis,

$$f_{k-1} = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{k-1} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{k-1}$$

$$f_k = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{k} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{k}$$

Thus the LHS of (*) $= f_{k+1} = f_{k-1} + f_k = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{k-1} + \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{k} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{k-1} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{k} = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{k-1}(\frac{1+\sqrt{5}}{2} + 1) - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{k-1}(\frac{1-\sqrt{5}}{2} + 1) = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{k-1}(\frac{1+\sqrt{5}}{2})^{2} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{k-1}(\frac{1-\sqrt{5}}{2})^{2} = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{k+1} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{k+1} =$ the RHS of (*)

By Math induction, (*) holds for all positive integers. $\square$

Exercise: The Lucas numbers are defined recursively by

$$1, 3, 4, 7, 11, 18, 29, 47, \cdots$$

$(L_1 = 1, L_2 = 3, L_{n+2} = L_n + L_{n+1} \quad (n \geq 1))$

Use induction to prove: for any positive integer n,

$$L_n = (\frac{1+\sqrt{5}}{2})^n + (\frac{1-\sqrt{5}}{2})^n$$

谢谢！