

# Contents

I MISC	3
II 定理 Theorem	4
1 算术基本定理 (Fundamental theorem of arithmetic)	4
2 代数基本定理 (Fundamental theorem of algebra)	5
3 多项式除法、多项式余式定理 (Polynomial division, Polynomial remainder theorem)	6
4 因式定理 (Factor theorem)	6
5 因式分解定理	7
6 有理根定理 (Rational root theorem)	7
7 韦达定理 (Vieta's formulas)	9
7.1 Proof . . . . .	9
7.2 韦达定理的逆定理 . . . . .	9
7.3 Examples . . . . .	9
8 二项式定理 (Binomial theorem)	10
9 鸽巢原理 (Pigeonhole principle)	10
10 裴蜀定理 (Bézout's identity )	11

<b>III MISC</b>	<b>11</b>
<b>IV basics</b>	<b>13</b>
<b>11 反证法 (proof by contradiction)</b>	<b>13</b>
<b>12 素数、合数</b>	<b>14</b>
<b>13 排列组合 (permutation and combination)</b>	<b>15</b>
13.1 排列 (permutation) . . . . .	15
13.2 组合 (combination) . . . . .	16
<b>14 绝对值</b>	<b>16</b>
14.1 绝对值的意义 . . . . .	16
14.2 最值 . . . . .	16
14.3 推广 . . . . .	17
<b>15 整除规则 (divisibility rule)</b>	<b>17</b>
15.1 基本判别 (rules) . . . . .	17
15.2 proofs . . . . .	19
<b>16 MISC</b>	<b>20</b>
<b>17 todo</b>	<b>21</b>

## Part I

# MISC

数学基本思想：

抽象能力：会在错综复杂的事物中把握本质

推理能力：会在杂乱无章的事物中理清头绪

建模能力：会在千头万绪的事物中发现规律

数学四大基本思想：

函数与方程、数形结合、分类讨论和转化与化归（复杂或未知的问题，通过一定的变换，最终归结为已知或更容易解决的问题的思维方法）

数学基本方法：

数形结合、分类讨论、换元、数学归纳法、反证法、类比

数域（域：field）：指一个数集，它对加法、减法、乘法和除法（除数不为零）运算是封闭的，并且包含 0 和 1

换句话说，对数域中任意两个数进行这四种基本运算，其结果仍然属于这个数域。

常见的数域包括有理数域 (Q)、实数域 (R) 和复数域 (C)

一个集合成为数域，需满足以下条件：

1. 包含 0 和 1：数域中必须有加法单位元 0 和乘法单位元 1
2. 封闭性：加法和减法封闭；乘法封闭；除法封闭

非数域例子：自然数集和整数集，不构成数域，因为除法运算不封闭，例如  $2/3$  不属于自然数或者整数

丢番图方程，又称为不定方程 (Diophantine equation), Diophantus is a Greek mathematician

丢番图的研究在数论中占有重要地位，如丢番图方程、丢番图集合、丢番图逼近等都是数学的重要领域

最大公约数：GCD(Greatest Common Divisor) or HCF:(Highest Common Factor).

e.g.  $\gcd(3, 9) = 3$  ,  $\gcd(-3, 9) = 3$

$0!$  规定为 1

## Part II

# 定理 Theorem

## 1 算术基本定理 (Fundamental theorem of arithmetic)

算术基本定理, also called unique factorization theorem(正整数唯一分解定理) and prime factorization theorem, 即: 每个大于 1 的自然数, 要么本身就是素数, 要么可以写为 2 个或以上的素数的积, 而且这些素因子按大小排列之后, 写法仅有一种方式。例如:  $1200 = 2^4 \cdot 3 \cdot 5^2$

算术基本定理是初等数论中一个基本的定理, 也是许多其他定理的逻辑支撑点和出发点。

由两部分组成:

1. 分解的存在性
2. 分解的唯一性, 即若不考虑排列的顺序, 正整数分解为素数乘积的方式是唯一的

这个定理也是为什么 1 不是质数的主要原因, 如果 1 是 prime,  $2 = 2 \cdot 1 = 2 \cdot 1 \cdot 1 = \dots$

STATEMENT:

Every positive integer  $n > 1$  can be represented in exactly one way as a product of prime powers:

$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^k p_i^{n_i}$ , where  $p_1 < p_2 < p_3 \dots < p_k$  are primes, and  $n_i$  are positive integers.

Since  $a^0 = 1$ , any positive integer can be uniquely represented as an infinite product

taken over all the positive prime numbers, as

$$n = 2^{n_1} 3^{n_2} 5^{n_3} 7^{n_4} \dots = \prod_{i=1}^{\infty} P_i^{n_i}$$

等价命题：If a prime divides the product of two integers, then it must divide at least one of these integers. That is:

If Prime  $P|ab$ , then, either  $P|a$  or  $P|b$

Proof:

### 1. Existence

用反证法：假设存在大于 1 的自然数不能写为素数的乘积，把最小的那个称为  $n$ 。  
 $n$  不可为素数，因为  $n = n$ , 可以写成素数的成绩，因此  $n$  一定是合数，而每个合数都可以分解为两个严格小于自身而大于 1 的自然数的乘积。设  $n = a \times b$ , 根据假设,  $n$  是最小的不能写为素数乘积的自然数,  $a < n, b < n$ , 所以  $a = p_1 p_2 \times p_n, b = q_1 q_2 \dots q_n$ , and  $n = ab = p_1 p_2 \dots p_n q_1 q_2 \dots q_n$  可以写为素数的乘积，由此产生矛盾，故大于 1 的自然数必可以写为素数的乘积

### 2. Uniqueness

欧几里得引理：if  $p|ab$ , either  $p|a$  or  $p|b$

todo...

## 2 代数基本定理 (Fundamental theorem of algebra)

Also called "d'Alembert–Gauss theorem"

描述为：任何一个复系数的一元  $n$  次多项式方程 ( $n \geq 1$ ), 至少有一个复数根。

有时候这个定理描述为：任何一个非零的一元  $n$  次复系数多项式，都正好有  $n$  个复数根（重根视为多个根）。但实际上，是“至少有一个根的”直接结果，因为把多项式除以它的线性因子可以推出。也就是说，任何一个  $n$  次多项式，都可以因式分解为  $n$  个复系数一次多项式的乘积 (根据多项式除法)。

Proof?

推论：任何一个非零的一元  $n$  次复系数多项式，都正好有  $n$  个复数根（重根视为多个根）。

意义：复数域是代数封闭的；该定理是代数学和近世代数中的一个基础性结论

尽管这个定理被命名为“代数基本定理”，但它还没有纯粹的代数证明，许多数学家都相信这种证明不存在。另外，它也不是最基本的代数定理；因为在那个时候，代数基本上就是关于解实系数或复系数多项式方程，所以才被命名为代数基本定理。

所有的证明都包含了一些数学分析，至少是实数或复数函数的连续性概念。有些证明也用到了可微函数，甚至是解析函数。

### 3 多项式除法、多项式余式定理 (Polynomial division, Polynomial remainder theorem)

$$\frac{P(x)}{D(x)} = Q(x) + \frac{R(x)}{D(x)} \Rightarrow P(x) = D(x)Q(x) + R(x)$$

If  $D(x) = x - a$ , then  $P(x) = (x - a)Q(x) + R(x) = (x - a)Q(x) + r$

根据定义， $R(x)$  的次数小于 1, so  $R(x)$  只能为常数

$$\Rightarrow P(a) = (a - a)Q(x) + r = r$$

得到**多项式余式定理**：多项式  $P(x)$  除以  $x - a$  所得的余式  $= P(a)$

dividend = divisor x quotient + remainder

Examples:

Let  $f(x) = x^3 - 12x^2 - 42$ , divided by  $x - 3$ , gives the quotient  $x^2 - 9x - 27$ , and the remainder  $-123$ .

By the polynomial remainder theorem,  $f(3) = -123$

寻找多项式的切线？<https://zh.wikipedia.org/wiki/%E5%A4%9A%E9%A1%B9%E5%BC%8F%E9%99%A4%E6%B3%95>

? 直觉  
要用  
微积  
分, 但  
是这  
个是  
啥情  
况?

### 4 因式定理 (Factor theorem)

The Factor theorem connects polynomial factors with polynomial roots.(关于多项式的因式和零点的定理)

一个多项式  $f(x)$  有一个因式  $ax - b$  当且仅当  $f(\frac{b}{a}) = 0$

普遍应用于因式分解，利用长除法，除以零点  $(x - a)$

Example:

分解因式:  $(x - y)^3 + (y - z)^3 + (z - x)^3$

$x = y, y = x, x = z$  是 0 点, so  $k(x-y)(y-z)(x-z)$ , let  $x = 0, y = 1, z = 2 \Rightarrow k = 3$

## 5 因式分解定理

数域  $F$  上的每个次数  $\geq 1$  的多项式  $f(x)$  都可以分解为数域  $F$  上一些不可约多项式的乘积，并且是唯一的，即：

$f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)q_3(x)\cdots q_t(x)$ , 其中  $p_i(x)$  和  $q_j(x)$  都是数域  $F$  上的不可约多项式，那么必有  $s = t$ ，而且可以适当排列因式的次序，使得

$$p_i(x) = c_i q_i(x)$$

分解方法：公因式、公式法、分组分解、拆添项、十字交叉、一次因式检验法（有理根定理）

## 6 有理根定理 (Rational root theorem)

Also called rational root test, rational zero theorem, rational zero test or  $p/q$  theorem

描述：对于  $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$ , 系数  $a_i \in \mathbb{Z}$ , and  $a_0, a_n \neq 0$ .

该定理指出，如果存在有理根  $x = \frac{p}{q}$ , written in lowest term(that is  $p$  and  $q$  are relatively prime, 互质)，满足：

$p$  是  $a_0$  的整数因子, i.e.  $p|a_0$ . 整除符号, Tips<sup>1</sup>

$q$  是  $a_n$  的整数因子, i.e.  $q|a_n$ .

该定理是高斯定理关于多项式分解的一个特例

---

<sup>1</sup> $a|b$ :  $a$  整除  $b$ ,  $b$  能被  $a$  整除，也就是  $b$  除以非零  $a$ , 商是一个整数. i.e.  $2|6$

Proof:

Let  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$  with  $a_i \in \mathbb{Z}$ ,  $a_0, a_n \neq 0$

Suppose  $P(p/q) = 0$  for some coprime  $p, q \in \mathbb{Z}$ :

$$\begin{aligned} P\left(\frac{p}{q}\right) &= a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0 \\ \Rightarrow a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n &= 0 \\ \Rightarrow p(a_n p^{n-1} + a_{n-1} p q^{n-2} + \cdots + a_1 q^{n-1}) &= -a_0 q^n \Rightarrow () = -a_0 \frac{q^n}{p} \\ \Rightarrow q(a_{n-1} p^{n-1} + a_{n-2} p q^{n-2} + \cdots + a_0 q^{n-1}) &= -a_n p^n \Rightarrow () = -a_n \frac{p^n}{q} \end{aligned}$$

我们注意到，括弧内是整数，因为  $a_i$  是整数，所以这是关键

$p, q$  互质， $\frac{p}{q} = \pm \frac{a_0 \text{的因子}}{a_n \text{的因子}}$

注意  $p, q$  为 1 的特殊情况，显而易见 1 永远是第一个选择

关键点：

1. 系数是整数
2. 如果存在有理根，则必符合此定理，否则存在无理根（如  $\sqrt{89}$ ）亦或者复数根

Examples:

$$x^3 - 7x + 6 = 0:$$

有理根有可能是： $\pm \frac{\{1, 2, 3, 6\}}{1} = \pm 1, 2, 3, 6$ ，恰好  $1, 2, -3$ ，所以也恰好可以写为：

$$(x - 1)(x - 2)(x + 3) = 0$$

$3x^3 - 5x^2 + 5x - 2 = 0$ ，如果有有理根，则必在  $\pm \frac{1, 2}{1, 3} = \pm 1, 2, \frac{1}{3}, \frac{2}{3}$  中。8 个候选根，需要测试 8 次，最后才知道  $x = 2/3$  是唯一有理根。

很是繁琐不是？所以可以通过评估  $P(r)$  来测试缩小范围（比如使用秦九韶算法？）。

Firstly, if  $x < 0$ , the  $P$  will be negative, so every root is positive

$P(1) = 1$ , so 1 is not the root. Moreover, if one sets  $x = 1 + t$ , so  $Q(t) = P(1 + t)$ , 展开后，三次项是 3，一次项是 1，implies  $Q$  must belongs to  $\pm 1, \pm \frac{1}{3}$ , and  $P$  satisfy  $x = 1 + t \in 2, 0, 4/3, 2/3$ . 再次显示必须为正，两个候选项是  $2, 2/3$ , 将 2 带入，显然不是，最后测试  $2/3$

If  $a, b$  and  $\frac{a^2}{b} + \frac{b^2}{a}$  are integers, then both  $\frac{a^2}{b}$  and  $\frac{b^2}{a}$  must be integers.

## 7 韦达定理 (Vieta's formulas)

Any general polynomial of degree  $n$ ,  $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ , by the "fundamental theorem of algebra", roots are  $x_1, x_2, x_3 \dots$

$$\left\{ \begin{array}{l} x_1 + x_2 + x_3 + \cdots + x_{n-1} + x_n = -\frac{a_{n-1}}{a_n} \\ (x_1x_2 + x_1x_3 + x_1x_4 + \cdots + x_1x_n) + (x_2x_3 + x_2x_4 + \cdots + x_2x_n) + \cdots + x_{n-1}x_n = \frac{a_{n-2}}{a_n} \\ \vdots \\ x_1x_2x_3 \cdots x_n = (-1)^n \frac{a_0}{a_n} \end{array} \right.$$

### 7.1 Proof

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = a_n(x - x_1)(x - x_2) \cdots (x - x_n)$$

展开后比较系数

$$\left\{ \begin{array}{l} a_{n-1} = -a_n(x_1 + x_2 + \cdots + x_{n-1} + x_n) \\ a_{n-2} = a_n[(x_1x_2 + x_1x_3 + \cdots + x_1x_n) + (x_2x_3 + x_2x_4 + \cdots + x_2x_n) + \cdots + x_{n-1}x_n] \\ \vdots \\ a_0 = (-1)^n a_n x_1 x_2 \cdots x_n \end{array} \right.$$

### 7.2 韦达定理的逆定理

对于一元二次方程

利用圆来研究一元二次方程? <http://202.175.82.54/tplan/2006/intro/R027.pdf>

### 7.3 Examples

If  $n = 2$ (quadratic),  $ax^2 + bx + c = 0 = a(x - x_1)(x - x_2)$  展开比较即有, 也可以用求根公式

if  $n = 3$ ,  $x_1, x_2, x_3$  是  $ax^3 + bx^2 + cx + d = 0$  的三个根, then:

$ax^3 + bx^2 + cx + d = a(x - x_1)(x - x_2)(x - x_3) = a(x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_1x_3)x - x_1x_2x_3 = 0)$ , That is

$$x_1 + x_2 + x_3 = -\frac{b}{a}, x_1x_2 + x_1x_3 + x_2x_3 = \frac{c}{a}, x_1x_2x_3 = -\frac{d}{a}$$

## 8 二项式定理 (Binomial theorem)

$$(x + y)^n = C_n^0 x^n y^0 + C_n^1 x^{n-1} y^1 + C_n^2 x^{n-2} y^2 + \cdots + C_n^n x^0 y^n$$

Examples:

$$(x + y)^0 = 1$$

$$(x + y)^1 = x + y$$

$$(x + y)^2 = x^2 + 2xy + y^2$$

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

$$(x + y)^3 = xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy, \text{ total } 2^3 \text{ terms}$$

Let  $x = y = 1$ , we have  $2^n = C_n^0 + C_n^1 + \cdots + C_n^n$

Proof:

Method 1: 数学归纳法 (inductive proof)

Method 2: 组合方法

$(a + b)^n = \overbrace{(a + b)(a + b) \cdots (a + b)}^{\text{n terms}}$ ,  $n$  个括号相乘, 从  $n$  个选出  $k$  个括号中的  $a$ , 再从剩余的  $n - k$  个括号中选出  $(n - k)$  个  $b$ , 得到一组  $a^k b^{n-k}$ , 而这种选法共有  $C_n^k$  种, 故总共有  $C_n^k$  个  $a^k b^{n-k}$ ; 其他同理

More:

$$(1 + x)^{-1}$$

$$(1 + x)^{\frac{1}{2}}$$

$$(1 + \frac{1}{n})^n$$

Multinomial theorem:

$$(x_1 + x_2 + \cdots + x_m)^n$$

## 9 鸽巢原理 (Pigeonhole principle)

鸽笼原理, 又名狄利克雷抽屉原理、鸽巢原理。

表述 1：若有  $n$  个笼子和  $n + 1$  只鸽子，所有鸽子都被放在鸽笼里，那么至少有一只笼子有至少 2 只鸽子

表述 2：若有  $n$  个笼子和  $kn + 1$  只鸽子，所有鸽子都被放在鸽笼里，那么至少有一只笼子有至少  $k + 1$  只鸽子

集合论的表述：若  $A$  是  $n + 1$  个原色， $B$  是  $n$  元集，则不存在从  $A$  到  $B$  的单射

推广：如果把  $n$  个对象分配到  $m$  个容器中，必有一个容器容纳至少  $\frac{n}{m}$  个对象

反证法证明此原理

例子：

北京至少有两个人头发数是一样多。常人头发大概是 15 万左右，假定没有人的头发超过 100 万，北京人口大于 100 万。

有  $n$  个人（至少两人）互相握手（随意找人握），必有两人握过手的人数相同

这个原理经常在计算机中得到真正的应用，比如哈希表的重复问题是不可避免的，因为 keys 的数目总是比 indices 的数目多，什么算法都不可能解决

这个原理，还证明任何无损压缩算法，在把一些输入变小的同时，作为代价一定有其他的输入增大，否则对于长度为  $L$  的输入集合，该压缩算法总能将其映射到一个更小的长度小于  $L$  的输出集合，而这与鸽巢理论相悖

??....

## 10 裴蜀定理 (Bézout's identity )

**Bézout's identity(Bézout's lemma):** Let  $a$  and  $b$  be integers with greatest common divisor  $d$ , Then there exist integers  $x$  and  $y$  such that  $ax + by = d$ . Moreover, the integers of the form  $az + bt$  are exactly the multiples of  $d$

## Part III

# MISC

数学基本思想：

抽象能力：会在错综复杂的事物中把握本质

推理能力：会在杂乱无章的事物中理清头绪

建模能力：会在千头万绪的事物中发现规律

数学四大基本思想：

函数与方程、数形结合、分类讨论和转化与化归

数学基本方法：

数形结合、分类讨论、换元、数学归纳法、反证法、类比

数域 (域：field)：指一个数集，它对加法、减法、乘法和除法（除数不为零）运算是封闭的，并且包含 0 和 1

换句话说，对数域中任意两个数进行这四种基本运算，其结果仍然属于这个数域。

常见的数域包括有理数域 (Q)、实数域 (R) 和复数域 (C)

一个集合成为数域，需满足以下条件：

1. 包含 0 和 1：数域中必须有加法单位元 0 和乘法单位元 1
2. 封闭性：加法和减法封闭；乘法封闭；除法封闭

非数域例子：自然数集和整数集，不构成数域，因为除法运算不封闭，例如  $2/3$

不属于自然数或者整数

丢番图方程，又称为不定方程 (Diophantine equation), Diophantus is a Greek mathematician

丢番图的研究在数论中占有重要地位，如丢番图方程、丢番图集合、丢番图逼近等都是数学的重要领域

最大公约数: GCD(Greatest Common Divisor) or HCF:(Highest Common Factor).

e.g.  $\gcd(3, 9) = 3$  ,  $\gcd(-3, 9) = 3$

$0!$  规定为 1

## Part IV

# basics

### 11 反证法 (proof by contradiction)

英国数学家高德菲·哈罗德·哈代在他的文章《一个数学家的辩白》描述：“欧几里得最喜欢用的反证法，是数学家最精良的武器。它比起棋手所用的任何战术还要好：棋手可能需要牺牲一只兵甚至更多，但数学家却是牺牲整个棋局来获得胜利。”

反证法常用于“正面证明不容易或不能得出结果”的情况

Procedure:

1. The proposition to be proved is  $P$
2. We assume  $P$  to be false, i.e., we assume  $\neg P$
3. It is shown that  $\neg P$  implies falsehood. This is typically accomplished by deriving two mutually contradictory assertions.  $Q$  and  $\neg Q$  and appealing to the law of noncontradiction
4. Since assuming  $p$  to be false leads to a contradiction. It's concluded that  $p$  is in fact true

Example:  $\sqrt{2}$  是无理数的证明

假设  $\sqrt{2}$  是有理数，那么就可以写为  $\frac{p}{q}$ ，其中  $p, q$  为正整数且互质，那么有：  
 $p = \sqrt{2} \times q$ , then  $p^2 = 2 \times q^2$ , 很显然  $p^2$  是偶数，而只有偶数的平方才是偶数，  
所以  $p$  是偶数。假设  $p = 2s$ , then  $p^2 = 4s^2 = 2q^2 \Rightarrow q^2 = 2s^2$ , 从而  $q$  也是偶数，  
这与互质矛盾，假设不成立，从而得证。

## 12 素数、合数

素数 vs 质数

直到清末，prime number 一直被翻译为素数，素数、非素数、合成数都是日译名。汉语中的“素”有“根本”之义，有可能“素”与“数”读音接近，易混淆，用了“质”。但华罗庚的《堆垒素数》和陈景润研究的“哥德巴赫猜想”也是用的素数。现在的一些中小学教材，统一使用的是质数，但又标明了“质数，又叫素数”

为什么规定 1 不是素数？

1 既不是素数也不是合数。加入 1 是素数，那么一个数比如  $1 \times 2^2 \times 3^3$  也可以写为  $1^2 \times 2^2 \times 3^3$ ，这样分解就不唯一了

素数：大于 1 的自然数，如果只有 1 与自身两个因数，那么这个数就称为素数。如 2, 3, 5, 7, 11 etc。2 是最小的素数，也是素数中唯一的偶数

合数：大于 1 的自然数，如果除了 1 与自身以外，还有其他因数，则称此数为合数。如 4, 6, 8 etc.

根据定义，1 既不是素数，也不是合数。全体自然数分为：1、素数、合数。

互质 (互素, coprime)：两个或两个以上的整数的最大公约数是 1

如果数域是正整数，那么 1 与所有正整数互质

如果数域是整数，那么 1 and  $-1$  与所有整数互质，而且他们是仅有的与 0 互质的整数

两个整数  $(a, b)$  互质，记为： $a \perp b$

专门研究数学的人认为素数是最基本的数，因为任何大于 1 的整数要么是素数，要么是若干素数的积。德国的高斯曾经说过：“数学是科学的皇后，数论是数学的皇冠”。费马曾说过：“全部的数论问题就在于以何种方法来讲一个整数分解质因数”。

素数是有限的还是无限的？这被欧几里得证明了，有了欧几里得定理 (Euclid's theorem)，是数论中的基本定理。

欧几里得定理 (Euclid's theorem)：

《几何原本》第九卷中，有以下陈述：存在着比指定的任意多个素数更多的素数。

也即：素数的个数是无限的。

素数是无限的.

Proof1(欧几里得，不是反证法？):

1. 假设素数是有限的，那么可以假设素数只有一个有限的集合  $S$ , as  $\{p_1, p_2, \dots, p_n\}$
2. 构造一个新的数:  $Q = p_1 \times p_2 \times \dots \times p_n + 1$
3. 分析  $Q$ 
  - a,  $Q$  比  $S$  中的任意一个素数要大，它不在  $S$  内
  - b, 用集合  $S$  中的任何一个素数  $p_i$ 去除  $Q$ , 都会余 1
4. 得出矛盾
  - a, 意味着  $Q$  要么本身就是一个新的素数，它不在我们构造的集合  $S$  内
  - b, 要么  $Q$  是一个合数，它可以被一个比  $P_n$ (我们假设的最大的素数) 还要大的素数整除，根据算数基本定理，这意味着存在一个不在  $S$  内的素数，这个素数比
5. 这与我们最初假设的“素数是有限的”矛盾，因此素数一定有无限多个

Proof2(欧几里得):

考虑正整数  $n$  的阶乘  $n!$  可以被 2 到  $n$  的所有的整数整除， $n! + 1$  并不能被 2 到  $n$  的任何自然数所整除，因此  $n! + 1$  有两种可能性：是素数，或者能被大于  $n$  的素数 (素数基本定理) 整除，在任何一个 case 中，都表明至少存在一个比  $n$  大的素数

**素数定理**, 又称作质数定理, prime number theorem, 是素数分布理论的中心定理，是关于素数个数问题的一个命题：

## 13 排列组合 (permutation and combination)

### 13.1 排列 (permutation)

Permutaion(排列、变换、置换，比如古典密码里的置换) or Arrangement, 所以数学符合  $P$  和  $A$  都可以。

利用乘法原理:  $A_n^k = \overbrace{n(n-1)(n-2)\dots(n-k+1)}^{\text{k factors}} = \frac{n!}{(n-k)!}$

Also use:  $P_k^n$ ,  $P(n, k)$ ,  ${}_n P_k$ ,  ${}^n P_k$ ,  $P_{n,k}$ . Note the slight difference:  $P_k^n$  and  $A_n^k$

重复排列：从  $n$  个元素中取出  $k$  个元素， $k$  个元素可以重复： $U_k^n = n^k$

## 13.2 组合 (combination)

Combination just likes permutation, but the order doesn't matter

This formula can be derived from the fact that each  $k$ -combination of a set  $S$  of  $n$  members has permutations so

$P_n^k = C_n^k \times k!$  or  $C_n^k = P_n^k / k!$ . The  $C_n^k$  often denoted by  $\binom{n}{k}$

# 14 绝对值

## 14.1 绝对值的意义

本质是表示距离，比如数轴上的线段距离，差值的绝对值

第一要务一般是如何去绝对值，从代数上看就是要去讨论

不但要去绝对值，还要会用绝对值列出题目相应的等式或者不等式，然后去解

又比如  $|3 - 2x| + |x - 3|$  的最小值，要善于变换，以方便几何上的直观

## 14.2 最值

$f(x) = |x + 1| + |2 - x|$  的最值

$f(x) = |x + 1| + |2x - 1|$  的最值， Tips<sup>2</sup>

$f(x) = |x + 1| + |x| + |x - 2|$  的最值

$f(x) = |2x - 1| + |4x - 3|$

$f(x) = ||x - 1| - 3|$

---

<sup>2</sup> $|2x - 1| = 2|x - \frac{1}{2}|$

## 14.3 推广

$f(x) = |x - a_1| + |x - a_2| + |x - a_3| + \dots + |x - a_n|$   $f(x) = |x + 1| + |2x - 1|$  可以化简为:  $f(x) = |x + 1| + 2|x - \frac{1}{2}| = |x + 1| + |x - \frac{1}{2}| + |x - \frac{1}{2}|$

奇点偶段, 证明方法: 从 1 到 3 到 5, 从 2 到 4 到 6, 以至无穷

## 15 整除规则 (divisibility rule)

Let  $A = \overline{a_n a_{n-1} \dots a_2 a_1} = a_n \times 10^{n-1} + a_{n-1} \times 10^{n-2} \dots + a_2 \times 10 + a_1$

### 15.1 基本判别 (rules)

被 2 整除:

The last digit is even

被 3 整除和被 9 整除:

The sum of digits must be divisible by 3 or 9. Tips<sup>3</sup>

被 4 整除:

The last two digits must be divisible by 4. Tips<sup>4</sup>, 后者是关键

被 5 整除:

被 6 整除:

被 7 整除:

被 8 整除:

The last three digits must be divisible by 8

被 9 整除:

被 11 整除:

<sup>3</sup> $A = a_n \times (9+1)^{n-1} + a_{n-1} \times (9+1)^{n-2} \dots + a_2 \times (9+1) + a_1$   
 $= (a_n \times 9^{n-1} + a_{n-1} \times 9^{n-2} + \dots + a_2 \times 9) + (a_n + a_{n-1} + \dots + a_2 + a_1)$

<sup>4</sup> $A = \overline{a_n a_{n-1} \dots a_3} \times 100 + \overline{a_2 a_1}$

第一位数 - 第二位数 + 第三位数 - ...，最终值如果能被 11 整除，正负交替，从前往后和从后往前一样，负数也可以判定. Tips<sup>5</sup>

被 13 整除：

被 17 整除：

<sup>5</sup> $10 = 11 \times 1 - 1, 100 = 11 \times 9 + 1, 1000 = 11 \times 91 - 1$

## 15.2 proofs

被 7 整除

**方法 1:** 三位截断: if  $A = \overline{b_1 b_2 b_3 a_1 a_2 a_3}$  能被 7 整除, then:  $\overline{a_1 a_2 a_3} - \overline{b_1 b_2 b_3}$  可以被 7 整除

$$A/7 = (\overline{b_1 b_2 b_3} \times 10^3 + \overline{a_1 a_2 a_3})/7 = 143 \times \overline{b_1 b_2 b_3} + (\overline{a_1 a_2 a_3} - \overline{b_1 b_2 b_3})/7$$

**方法 2:** 降位, 如五位数变为四位, 再变为三位, 再两位。

Suppose we have a number  $A = \overline{a_1 a_2 a_3 a_4 b}$ , let  $A = \overline{ab}$ , while  $a = \overline{a_1 a_2 a_3 a_4}$ .

if 能化简为判断  $a + mb$  能否被 7 整除, 则简化成功:

$$\begin{cases} a + mb = 7n_1 \\ 10a + b = 7n_2 \end{cases} \Rightarrow (10m - 1)b = 7(n_1 - n_2)$$

That means  $10m - 1$  必须是 7 的倍数, 此时  $m$  可以为 5 or -2。那么我们就可  
以简化为判断  $a - 2b$  or  $a + 5b$ , -2 和 5 正好相差 7.

e.g.

$$329 \rightarrow 32 - 2 \times 9 = 14$$

$$4564 \rightarrow 456 - 2 \times 4 = 448 \rightarrow 44 + 8 \times 5 = 7 \times 12$$

推广:

被 11 整除:  $(10m - 1)|11$ ,  $m = -1$ 。当然, 被 11 整除还有一个更方便的方法,  
那就是依次加减

被 13 整除:  $(10m - 1)|13$ ,  $m = 4, -7$

被 17 整除:  $(10m - 1)|17$ ,  $m = -5$

我们可以看到,  $m$  是一个呈周期循环, 太大了就没有意义了, 如果一个三位数,  
最后化简还是三位数, 就没有了意义

这种方法用计算机编程来判断很方便

## 16 MISC

.....  
 $\frac{\sqrt{x^4+x^2+1}-\sqrt{x^4+1}}{x}$  的 max. tips<sup>6</sup>

.....  
 $x, y > 0$ , and  $x + 3y = x^3y^2$ , min of  $\frac{3}{x} + \frac{2}{y}$ , tips<sup>7</sup>

---

<sup>6</sup>1 讨论正负, 2 换元, 3 分子有理化

<sup>7</sup>把  $1/y$  带入

## 17 todo

生日问题 <https://zh.wikipedia.org/wiki/>