

Contents

I	MISC	4
II	Part1	4
1	算术基本定理	5
2	代数基本定理	6
3	多项式除法、多项式余式定理	7
4	因式定理 (Factor theorem)	7
5	多项式因式分解唯一定理	8
6	有理根定理 (Rational root theorem)	9
7	韦达定理 (Vieta's formulas)	10
7.1	Proof	10
7.2	韦达定理的逆定理	10
7.3	Examples	10
8	二项式定理 (Binomial theorem)	11
9	鸽巢原理 (Pigeonhole principle)	12
10	裴蜀 (贝祖) 定理 (Bézout's identity)	12
11	欧几里得算法、更相减损术	13
11.1	欧几里得算法	13
11.2	更相减损术	14
12	反证法 (proof by contradiction)	15

13 牛顿法 (Newton's method, or Newton-Raphson method)	15
III Part2 - basics	15
14 数学符号	16
15 环 (Ring)、域 (Field)	16
16 素数、合数	16
17 排列组合 (permutation and combination)	18
17.1 排列 (permutation)	18
17.2 组合 (combination)	18
18 绝对值	18
18.1 绝对值的意义	18
18.2 最值	19
18.3 推广	19
19 整除规则 (divisibility rule)	19
19.1 基本判别 (rules)	19
19.2 proofs	21
20 恒等式 Identity	21
20.1 等幂和差	22
21 不等式 inequalities	22
22 指数与对数	22
23 三角形	23
24 三角函数	23

25 todo

24

26 MISC

24

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：

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

Part 1

1 算术基本定理

Fundamental theorem of arithmetic, also called unique factorization theorem(正整数唯一分解定理), or prime factorization theorem.

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 $p_1 < p_2 < p_3 \cdots < p_k$ 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

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

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： $1200 = 2^4 \cdot 3 \cdot 5^2$

此定理是初等数论中一个基本定理，也是许多其他定理的逻辑支撑点和出发点。
它把对自然数的研究转化为对其最基本的元素——素数的研究

由两部分组成：

1. 分解存在性
2. 分解唯一性，即若不考虑排列顺序，正整数分解为素数乘积的方式是唯一的

这个定理也是 1 不是质数的主要原因, if 1 is prime, $2 = 2 \cdot 1 = 2 \cdot 1 \cdot 1 = \dots$

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 $n = n$ ，可以写成素数的乘积，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 $a = p_1 p_2 \cdots p_n, b = q_1 q_2 \cdots q_n$ ，and $n = ab = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_n$ 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"

STATEMENT:

Every non-constant single-variable polynomial with complex coefficients has at least one complex root. 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。

COROLLARY:

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）。

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?

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）；保证了任何复系数多项式方程在复数域内总有解，并能完全因式分解为一次因式（即 n 次多项式有 n 个复数根）；It's the basic connection between algebra and geometry

?

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

So, $P(a) = (a - a)Q(a) + r = r$

得到**多项式余式定理**的定义: 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, 但是这个是个啥情况?

4 因式定理 (Factor theorem)

STATEMENT:

Univariate polynomial $f(x)$ has a factor $(x - a)$, iff $f(a) = 0$

COROLLARY:

$f(x)$ has a factor $(ax - b)$, iff $f(\frac{b}{a}) = 0$

That is:

If $f(x)$ has a factor $(x - a)$, then $f(a) = 0$.

If $f(a) = 0$, then $f(x)$ has a factor $(x - a)$

The Factor theorem **connects polynomial factors with polynomial roots**.

关于多项式的因式和零点的定理, 是多项式余式定理的推论

此定理普遍应用于因式分解, 利用长除法, 除以零点 $(x - a)$

思考: 为什么不可以是 $(2x - 2a)$ 之类的呢?

If 我们用长除法, 那么其它项会出现分数, 更复杂了不是

Proofs:

If $(x - a)$ is a factor of $f(x)$, obviously, $f(a) = 0$. So, we only need to prove the converse.

Proof1:

First, we begin with $a = 0$, We write $f(x) = c_0 + c_1x^1 + \cdots + c_nx^n$, since $f(a) = 0$, so $c_0 = 0$, $f(x) = x(c_1x + \cdots + c_nx^{n-1})$, Thus...

Then, we prove the theorem for general a by reducing to the $a = 0$ case.

We observe that $f(x + a)$ is a polynomial with a root at $x = 0$, it follows that $f(x + a) = x \cdot g(x)$ (This is the key step) for certain polynomial $g(x)$ (this one is different with the former $g(x)$).

So, $f(x) = f((x - a) + a) = (x - a)g(x - a)$, thus...

Proof2:

We use the equation: $x^n - y^n$

Since $f(a) = 0$, so we can write $f(x) = \sum_i^n x^i = c_1x^1 + c_2x^2 + \cdots + c_nx^n$

$f(x) = f(x) - f(a) = \sum_i^n (x^i - a^i)$, Observe that every summand had $(x - a)$ as a factor. Thus...

Proof3:

Using Euclidean division of polynomials: Perform a Euclidean division of $f(x)$ by $(x - a)$, $f(x) = (x - a)Q(x) + R(x)$, where $\deg(R) < \deg(x - a)$. So R is constant.

We know that $f(a) = 0 = R$, so $f(x) = (x - a)Q(x)$

5 多项式因式分解唯一定理

STATEMENT:

数域 F 上的每个次数 ≥ 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:

$f(x) = p_1(x)p_2(x)p_3(x) \cdots p_s(x) = q_1(x)q_2(x)q_3(x) \cdots q_t(x)$, 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 $p_i(x) = c_iq_i(x)$

实数域 (Real Field, $\mathbb{R}[x]$): 都可以唯一的分解为一次因式和不可约二次因式 ($\Delta < 0$) 的乘积

有理数域 (Rational Field, $\mathbb{Q}[x]$): 分解成的不可约多项式可能是一次、二次或更高次, 但要求它们在有理数域内不可再分

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 test or p/q theorem. 该定理是高斯定理关于多项式分解的一个特例

STATEMENT:

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 $a_0, a_n \neq 0$.

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^a

q 是 a_n 的整数因子, i.e. $q|a_n$.

^a $a|b$: 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. $2|6$

How to memory: Use the simplest way: $2x + 1 = 0$

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 $p, q \in \mathbb{Z}$:

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

$$\Rightarrow a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

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

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 永远是第一优选择

关键点:

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

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 , $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, by the "fundamental theorem of algebra", roots are $x_1, x_2, x_3 \cdots$

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_{n-1} + x_n = -\frac{a_{n-1}}{a_n} \\ (x_1 x_2 + x_1 x_3 + x_1 x_4 + \cdots + x_1 x_n) + (x_2 x_3 + x_2 x_4 + \cdots + x_2 x_n) + \cdots + x_{n-1} x_n = \frac{a_{n-2}}{a_n} \\ \vdots \\ x_1 x_2 x_3 \cdots x_n = (-1)^n \frac{a_0}{a_n} \end{cases}$$

7.1 Proof

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = a_n (x - x_1)(x - x_2) \cdots (x - x_n)$$

展开后比较系数:

$$\begin{cases} a_{n-1} = -a_n(x_1 + x_2 + \cdots + x_{n-1} + x_n) \\ a_{n-2} = a_n[(x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n) + (x_2 x_3 + x_2 x_4 + \cdots + x_2 x_n) + \cdots + x_{n-1} x_n] \\ \vdots \\ a_0 = (-1)^n a_n x_1 x_2 \cdots x_n \end{cases}$$

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:

$$\begin{aligned} ax^3 + bx^2 + cx + d &= a(x - x_1)(x - x_2)(x - x_3) \\ &= a[x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_1x_3)x - x_1x_2x_3] \end{aligned}$$

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

$(a + b)^n = \overbrace{(a + b)(a + b) \cdots (a + b)}^{n \text{ terms}}$, 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)

鸽巢原理，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 (贝祖) 定理 (Bézout's identity)

Bézout's identity(lemma): $\forall a, b \in \mathbb{Z}, \exists x, y \in \mathbb{Z}, \text{ s.t. } ax + by = \gcd(a, b)$

关于未知数 x, y 的线性不定方程: $ax + by = m, a, b, m \in \mathbb{Z}$, 有整数解, 当且仅当 m 是 a, b 的最大公约数 d 的倍数。

特别的, $ax + by = 1$ 有整数解, iff(if and only if) a, b 互素

e.g. $2x + 3y = 1$ and $2x + 4y = 1$, $\gcd(15, 69) = 3, 3 = 15 \times (-9) + 69 \times 2$

等式也可用来给最大公约数定义: d 就是最小的可以写为 $ax + by$ 的正整数

多个整数间的裴蜀定理:

if $\gcd(a_1, a_2, \dots, a_n) = d$, then there are integers $x_1, x_2 \dots x_n$,

such that $d = a_1x_1 + a_2x_2 + \dots + a_nx_n$ has the following properties:

1. d is the smallest positive integer of this form

2. every form of this form is a multiple of d

Proof:

如果 a, b 中有一个是 0, 很容易得证, 以下假设 a, b 都不为 0。

Let $A = \{xa + yb; (x; y) \in \mathbb{Z}^2\}$

首先, $A \cap \mathbb{N}^*$ 不是空集 (至少包含 $|a| |b|$), 由于自然数集合是良序的 (??), A 中存在最小正元素 $d_0 = x_0a + y_0b$ 。考虑 A 中任意一个正元素 $p (= x_1a + y_1b)$ 对 d_0 的带余除法: let $p = qd_0 + r, q \in \mathbb{Z}^+, 0 \leq r < d_0$

$r = p - qd_0 = x_1a + y_1b - q(x_0a + y_0b) = (x_1 - qx_0)a + (y_1 - qy_0)b \in A$

so, $r = 0, d_0 | p$. 也就是说 p 都是 d_0 的倍数, 特别的: $d_0 | a, d_0 | b$, 因此 d_0 是 a, b 的公约数

另一方面: 对于 a, b 的任意公约数 d , let $a = md, b = nd$, so:

$d_0 = x_0a + y_0b = (x_0m + y_0n)d$

so $d | d_0$, 所以 d_0 是 a, b 的最大公约数

Proof???

11 欧几里得算法、更相减损术

11.1 欧几里得算法

辗转相除法 (Euclidean algorithm), 是已知最古老的算法, 可追溯至公元前 300 年前。

$\gcd(a, b) = \gcd(b, a \bmod b)$

$$a = q_0b + r_0 (0 < r_0 < b)$$

$$b = q_1r_0 + r_1 (0 < r_1 < r_0)$$

$$r_0 = q_2r_1 + r_2 (0 < r_2 < r_1)$$

$$r_1 = q_3r_2 + r_3 (0 < r_3 < r_2)$$

\vdots

这里 $b > r_0 > r_1 > r_2 > \dots \geq 0$, 在足够的步之后, 必然会出现余数为 0。(最大公约数有时候也可以去掉括弧, 比如 $\gcd(a, b)$ 也可以表示为 (a, b) , 但是后者与坐标重复, 所以……)

So, $(a, b) = (b, r_0) = (r_0, r_1) = (r_1, r_2) = \dots (r_{n-1}, r_n) = (r_n, 0) = r_n$

e.g.

$$2419 = 2183 \times 1 + 236,$$

$$\gcd(2419, 2183) = \gcd(2183, 236)$$

$$2183 = 236 \times 9 + 59,$$

$$\gcd(2183, 236) = \gcd(236, 59)$$

$$236 = 59 \times 4,$$

$$\gcd(236, 59) = 59$$

关键点在于: $a = qb + r$, $\gcd(a, b) = \gcd(b, r)$. Proof:

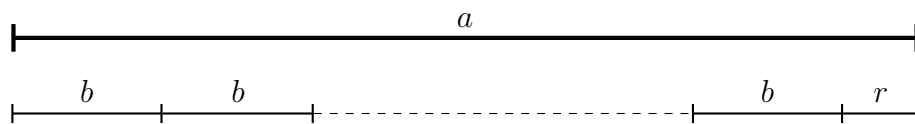
Let t 为 a, b 的一个公因数, then $t|a$, $t|b$, $t|qb$, $r = a - qb$

$\therefore t|(a - qb)$, i.e. $t|r$, $\therefore t$ 也是 b, r 的一个公因数

反之, Let s 为 b, r 的一个公因数, 则 $s|b$, $s|r$

$\therefore s|(qb + r)$, i.e. $s|a$, $\therefore s$ 也是 a, b 的公因数

So a, b 的全体公因数和 b, r 的全体公因数是一致的, 故它们有共同的最大公因数



上图, 我们从丈量的角度也理解。能同时丈量 a, b 的线段, 都能够量尽 b, r , 反之亦然

带余除法 (除法原理)(欧几里得除法 Euclidean division)(division with remainder).

$a = qb + r$, $0 \leq r < |b|$, 可用数学归纳法证明

多项式的带余除法 (多项式长除法): $A = QB + R$, R 是零多项式, 或者它的次数严格小于 B 的次数

辗转相除法是基于带余除法, 进而定义了欧几里得整环

11.2 更相减损术

更相减损术, 出自《九章算术》

e.g. $\gcd(126, 98)$, 写成分数 $\frac{126}{98}$

第一步: 可半者半之。分子分母约去 2, 得 $\frac{63}{49}$

第二步: 副置分母、子之数, 以少减多, 更相减损, 求其等也。

$(63, 49) \rightarrow (14, 49) \rightarrow (14, 21) \rightarrow (14, 7) \rightarrow (7, 7)$

稍加改进, 便可以直接计算最大公约数:

$(126, 98) \rightarrow (28, 98) \rightarrow (28, 70) \rightarrow (28, 42) \rightarrow (28, 14) \rightarrow (14, 14)$

与欧几里得的辗转相除相比较, 可以把除法看作连续的减法。对于求多个数的最大公因数, 更相减损更具优势:

$$\begin{aligned}\gcd(623, 1424, 801, 1513) &= (623, 1424 - 801, 801 - 623, 1513 - 1424) \\ &= (623, 623, 178, 89) \\ &= (623 - 6 \times 89, 623 - 6 \times 89, 178 - 89, 89) \\ &= (89, 89, 89, 89) \\ &= 89\end{aligned}$$

12 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。

13 牛顿法 (Newton's method, or Newton-Raphson method)

它是一种在实数域和复数域上近似求解方程的方法

Part III

Part2 - basics

14 数学符号

乘号曾经用过十几种，现在通用的有两种： \times and \cdot 。前者是英国数学家 William Oughtred 在 1631 年出版的《数学之论》提出的。莱布尼茨认为 \times 和拉丁字母 x 很像，赞成用 \cdot 。

平方根号曾经用拉丁文“Radix”的首尾两个字母合并起来使用， $\sqrt{}$ 是笛卡尔在他的《几何学》中第一次使用的，由拉丁字母“r”变化而来。

15 环 (Ring)、域 (Field)

自然数 (natural numbers)(\mathbb{N}): $1, 2, 3 \dots$ or $0, 1, 2, 3 \dots$

整数 (integer)(\mathbb{Z}): $\dots, -2, -1, 0, 1, 2, \dots$

有理数 (rational number)(\mathbb{Q}): 可表示为分数的数

实数 (real number)(\mathbb{R}): 所有有理数和无理数的集合，数轴上的所有点

复数 (complex number)(\mathbb{C})

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

环的具体定义并没有完全统一。一般定义：

给定一个集合 \mathbb{R} 以及定义在 \mathbb{R} 上的二元运算 $+$ and \times 。如果满足八个性质，则称 $(\mathbb{R}, +, \times)$ 构成了一个环。

交换环：如果一个环 \mathbb{R} 还额外满足乘法的交换律

域是环的一种，区别在于域还要求它的非零元素可以做除法，且域的乘法有交换律。比如：有理数域、实数域、复数域等等。

案例： $(x - 2)$ 是不是 $(x - 2)(x - 3)$ 和 $x^2 - 4$ 的最大公因式？那 $(\frac{x}{2} - 1)$ 呢？

分析：在整数环中， $(x - 2)$ 是它们的一个公因式，同时也是最大公因式，但 $(\frac{x}{2} - 1)$ 就不是，因为 $\frac{1}{2} \notin \mathbb{Z}$ 。但如果在有理数域或者实数域， $(\frac{x}{2} - 1)$ 则是它们的一个公因式，事实上，它们的公因式可以有无数个，可以写为 $k(x - 2)$ ，其中 $k \neq 0$, and $k \in \mathbb{Q}$ or $k \in \mathbb{R}$ 。

16 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： $a \perp b$

任何有理数都可以表示为连个互质的整数之比，也就是一个最简分数。根据有理数定义，有理数是指可以表示成两个整数之比的数，而分数的可以通过不断约分最终得到一个分子和分母互质的最简分数

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: ...

17 排列组合 (permutation and combination)

17.1 排列 (permutation)

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

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

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: $U_k^n = n^k$

17.2 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

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

18 绝对值

18.1 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

第一要务一般是如果去绝对值，从代数上看就是要去讨论
不但要会去绝对值，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

18.2 最值

$$\begin{aligned} f(x) &= |x + 1| + |2 - x| \text{ 的最值} \\ f(x) &= |x + 1| + |2x - 1| \text{ 的最值, Tips}^1 \\ f(x) &= |x + 1| + |x| + |x - 2| \text{ 的最值} \\ f(x) &= |2x - 1| + |4x - 3| \\ f(x) &= ||x - 1| - 3| \end{aligned}$$

18.3 推广

$$f(x) = |x - a_1| + |x - a_2| + |x - a_3| + \dots + |x - a_n| \quad f(x) = |x + 1| + |2x - 1| \text{ 可以}$$

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

19 整除规则 (divisibility rule)

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

19.1 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. Tips²

被 4 整除:

The last two digits must be divisible by 4. Tips³, 后者是关键

被 5 整除:

$$\begin{aligned} {}^1 |2x - 1| &= 2|x - \frac{1}{2}| \\ {}^2 A &= a_n \times (9 + 1)^{n-1} + a_{n-1} \times (9 + 1)^{n-2} \dots + a_2 \times (9 + 1) + a_1 \\ &= (a_n \times 9^{n-1} + a_{n-1} \times 9^{n-2} + \dots + a_2 \times 9) + (a_n + a_{n-1} + \dots + a_2 + a_1) \\ {}^3 A &= \overline{a_n a_{n-1} \dots a_3} \times 100 + \overline{a_2 a_1} \end{aligned}$$

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：

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. Tips⁴

被 13 整除：

被 17 整除：

⁴ $10 = 11 \times 1 - 1, 100 = 11 \times 9 + 1, 1000 = 11 \times 91 - 1$

19.2 proofs

被 7 整除

方法 1: 三位截断: if $A = \overline{b_1b_2b_3a_1a_2a_3}$ 能被 7 整除, then: $\overline{a_1a_2a_3} - \overline{b_1b_2b_3}$ 可以被 7 整除

$$A/7 = (\overline{b_1b_2b_3} \times 10^3 + \overline{a_1a_2a_3})/7 = 143 \times \overline{b_1b_2b_3} + (\overline{a_1a_2a_3} - \overline{b_1b_2b_3})/7$$

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 $A = \overline{a_1a_2a_3a_4b}$, let $A = \overline{ab}$, while $a = \overline{a_1a_2a_3a_4}$.

如果能简化为判断 $a + mb$ 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

20 恒等式 Identity

The basic ones like: $(a + b)(c + d) = ac + ad + bc + bd$

$$(a + b)^2 = a^2 + 2ab + b^2$$

$$(a - b)^2 = a^2 - 2ab + b^2$$

$$(a + b + c)^2 = a^2 + b^2 + c^2 + 2ab + 2bc + 2ac$$

$$(a - b - c)^2 = \dots$$

$$(a + b + c + d)^2 = a^2 + b^2 + c^2 + d^2 + 2ab + 2ac + 2ad + 2bc + 2bd + 2cd$$

$$a^3 - b^3 = (a + b)(a^2 - ab + b^2) = (a - b)^3 + 3ab(a + b)$$

$$a^3 + b^3 = (a - b)(a^2 + ab + b^2) = (a + b)^3 - 3ab(a + b)$$

$$(a+b+c)^3 = a^3 + b^3 + c^3 + 3(a+b)(b+c)(a+c)$$

$$a^3 + b^3 + c^3 = (a+b+c)^3 + 3(a+b+c)(-ab-ac-bc) + 3abc, \text{ 对称多项式}$$

$$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2 + b^2 + c^2 - ab - bc - ac)$$

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ab - cd)^2$$

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k = x^n + C_n^1 x^1 y^{n-1} + C_n^2 x^2 y^{n-2} + \dots + C_n^{n-2} x^{n-2} y^2 + C_{n-1}^1 x^{n-1} y^1 + y^n$$

$$y^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + x^2y^{n-3} + xy^{n-2} + y^{n-1})$$

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \dots + x^2y^{n-3} - xy^{n-2} + y^{n-1}y) \dots n \text{ is odd}$$

$$x^4 + y^4 = (x^2 + y^2)^2 - 2(xy)^2$$

$$x^4 + 4y^4 = x^4 + 4x^2y^2 + 4y^2 - 4x^2y^2, \text{ named as "Sophie Germain's identity"}$$

$$a^4 + a^2b^2 + b^4 = a^4 + 2a^2b^2 + b^4 - a^2b^2$$

20.1 等幂和差

$$y^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + x^2y^{n-3} + xy^{n-2} + y^{n-1})$$

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \dots + x^2y^{n-3} - xy^{n-2} + y^{n-1}y) \dots n \text{ is odd}$$

Proof1: 多项式长除法

Proof2: 等比数列: $1 + q + q^2 + \dots + q^n = \frac{q^{n+1}-1}{q-1}$, Let $q = \frac{a}{b}$

等幂和差逆定理:

$$a^4 + a^2b^2 + b^4 = (a^2 + b^2 - ab)(a^2 + b^2 + ab)$$

21 不等式 inequalities

22 指数与对数

指数的定义涉及定义上的扩展, 这是数学最常见的思维方式: a^n 就是 a 自乘 n 次, 故 $a^0 (a \neq 0)$ 没有定义。虽然理论上没有定义, 但是我们可以加以定义, 仍希望保持指数的定律, 因此 a^0 别无选择, 只可能是 1 ($a^0 = a^{n-n} = a^n/a^n = 1, n \in \mathbb{Z}^+$) ($a^m \cdot a^n = a^{m+n}$ when $n = 0, m \in \mathbb{Z}^+, a^m \cdot a^0 = a^{m+0} = a^m$).

Let $n = -m, a^m \cdot a^n = a^m \cdot a^{-m} = a^0 = 1 \Rightarrow a^{-m} = 1/a^m$

当指数推广到有理数时，为能使 $a^{\frac{p}{q}} = a^{\frac{2p}{2q}}, p, q \in \mathbb{Z}$ ，就限定了 $a > 0$ ，当 $a < 0$ 情况就变得复杂。

$$-2 = \sqrt[3]{-8} = (-8)^{\frac{1}{3}} = (-8)^{\frac{2}{6}} = [(-8)^2]^{\frac{1}{6}} = 64^{\frac{1}{6}} = 2$$

23 三角形

24 三角函数

25 todo

生日问题 <https://zh.wikipedia.org/wiki/>

26 MISC

.....
 $\frac{\sqrt{x^4+x^2+1}-\sqrt{x^4+1}}{x}$ 的 max. tips⁵

.....
 $x, y > 0$, and $x + 3y = x^3y^2$, min of $\frac{3}{x} + \frac{2}{y}$, tips⁶
.....

⁵1 讨论正负, 2 换元, 3 分子有理化

⁶把 $1/y$ 带入