《CSP-J 初级组算法中数学》

Day01-初等数论(上)

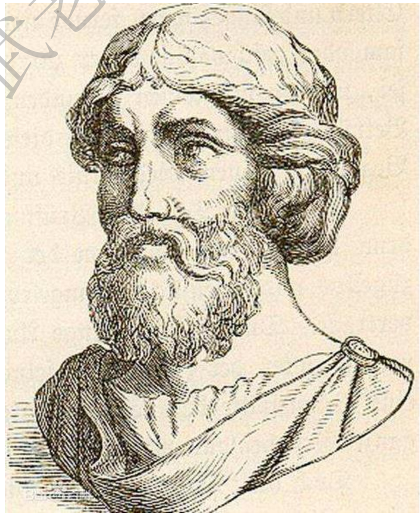
主讲人：小武老师

初等数论

初等数论是研究数的规律，特别是整数性质的数学分支。它是数论的一个最古老的分支。

可达信奥-小武老师-keda.ac

初等数论发展历史



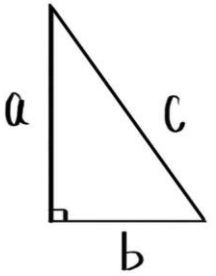
毕达哥拉斯
古希腊数学家、哲学家

第一个注重“数”的人

老毕，辈分高，水平也高，
所以，他创立的**毕达哥拉斯学派**，
门徒众多，是古希腊四大门派之一。

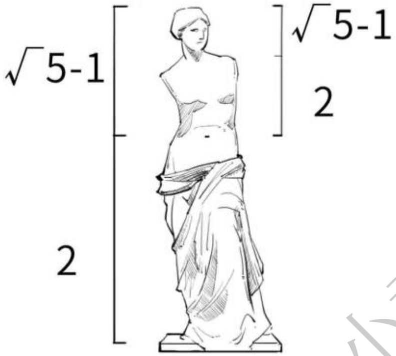
老毕作为数学的宗师，搞出过许多高冷的数学理论，

比如他证明了：



$a^2+b^2=c^2$

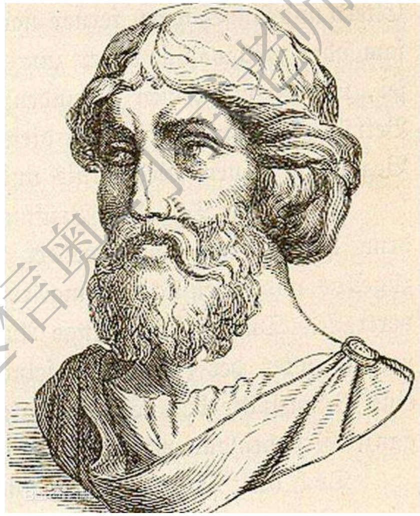
勾股定理



黄金分割

因此，勾股定理在西方也叫做：**毕达哥拉斯定理。**

初等数论发展历史



毕达哥拉斯

(公元前580—公元前590)

古希腊数学家、哲学家

“富二代”

证明了正多面体的个数

毕达哥拉斯定理（勾股定理）

欧几里得

(公元前330—公元前275)

古希腊数学家、哲学家

“几何之父”

《几何原本》

初步建立了整数的整除理论

费马（1601-1665）

法国律师和业余数学家

“业余数学家之王”

费马大定理

$$x^n + y^n = z^n$$

欧拉（1707-1783）

瑞士数学家、自然科学家

13岁时入读巴塞尔大学

“所有人的老师”

数学史上最多产的数学家

各种欧拉公式

高斯（1777-1855）

德国数学家、物理学家

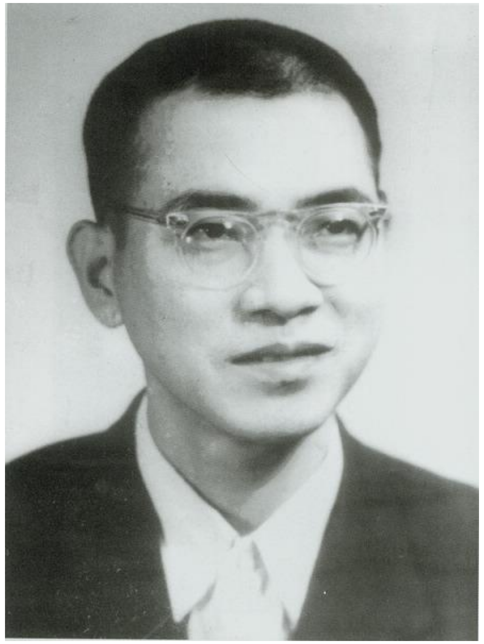
正十七边形的尺规作图法

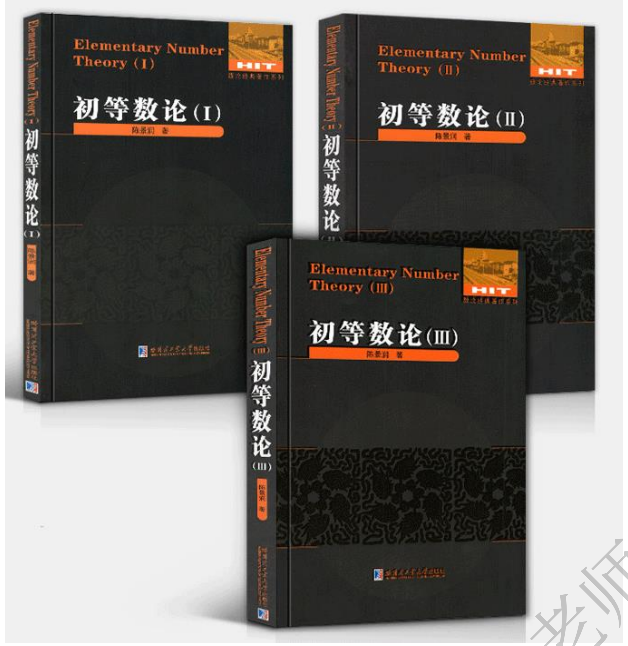
二项式定理的一般形式

“数学王子”

世界上第一张地球磁场图

参考教材





陈景润（1933年5月22日－1996年3月19日），福建福州人，中国数学家，华罗庚数学奖得主。“1+2”是哥德巴赫猜想研究的丰碑。

1+2：表达偶数为一个素数及一个不超过两个素数的乘积之和。

课程大纲

1 初等数论 (上)
奇数、偶数、质数、合数、约数、倍数、因数、最小公倍数、最大公约数、欧几里得算法等

2 初等数论 (中)
算术基本定理、同余关系、孙子定理等

3 初等数论 (下)
质数判定、质数筛、埃氏筛法、线性筛法等

4 函数 (上)
坐标、函数图像、一次函数、变量与函数等

5 函数 (下)
二次函数、指数函数、对数函数、根式与指数幂、幂运算等

6 数列基础
等差数列、等比数列、递推公式、通项公式等

7 矩阵基础
一维矩阵、二维矩阵、矩阵的运算、转置、杨辉三角等

8 数及其运算
数的进制、二进制、八进制、十六进制、编码（ASCII）等

9 计数原理与排列组合 (上)
加法原理、乘法原理、排列与组合、再看杨辉三角等

10 计数原理与排列组合 (下)
捆绑法、插空法、CSP真题训练等

整数的整除性

$0,1,2,3,4\cdots,n\cdots$ 这些数叫做正整数，又叫做自然数(非负整数)

$1,3,5,7,9\cdots$ 这些数叫做奇数

$2,4,6,8,10\cdots$ 这些数叫做偶数

正整数+正整数=正整数

正整数×正整数=正整数

$\cdots,-4,-3,-2,-1,0,1,2,3,4,\cdots$ 这些数叫做整数（正整数、负整数、0）

整数+整数=整数

整数-整数=整数

整数×整数=整数

Q1: 如何判定一个数是偶数还是奇数?

Q2: 什么样的整数除什么样的整数才能得到整数呢?

因数和倍数

定义1：设a,b是整数， b≠0. 如果有一个整数c,它使得 a=bc，则a叫做b的倍数，b叫做a的因数。我们有时说，b能整除a 或a能被b整除；

$$12 = 3 \times 4$$

12 是 3 的倍数，3 是 12 的因数。3能整除12，或12能被3整除

如果b能整除a，我们可以用 b|a这个符号来表示。如：

$$2|4, 3|6, 6|(-30), (-5)|20$$

$$2|4, 3|6, 6|(-30), (-5)|20$$

$$|a| = \begin{cases} a & \text{if} \quad a \geq 0 \\ -a & \text{if} \quad a < 0 \end{cases}$$

素数和复合数

引理1：设a,b是两个整数， b≠0. 则一定有并且只有两个整数q,r，可使以下表达式成立：

$$a = bq + r, 0 \leq r < |b|$$

$eg.12 = 3 \times 4 + 0$

$eg.23 = 3 \times 7 + 2$

$eg.27 = 3 \times 9 + 0$

$eg.100 = 33 \times 3 + 1$

素数和复合数

定义2：一个大于1的正整数，只能被1和它本身整除，不能被其它正整除整除，这样的正整数叫做素数（也叫做质数）。

eg. $2, 3, 5, 7, 11, 13, 17, 19$ 都是质数

Q3: 如何判定一个数是质数?

定义3：一个正整数除了能被1和它本身整除以外，还能被另外的正整数整除，这样的正整数叫做复合数（也叫做合数）。

eg. $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20$ 都是合数

Q4: 如何判定一个数是合数?

素数和复合数

由素数和复合数的定义，可知，全体正整数可分为三类：

(1) 1这个数

(2) 全体素数（质数）

(3) 全体复合数（合数）

Q5：合数由多少个?

定义4： 如果一个正整数a由一个因数b，而b又是素数，则b就叫做a的素因数（质因数）。例如，12 = 3 × 4，3是素数，而4不是素数，所以3是12的素因数（质因数）。而4不是12的素因数。

可达信奥—小武老师—keda.ac

素数和复合数

引理1：如果a是一个大于1的整数，则a的大于1的最小因数一定是素数。（可以分素数和合数讨论证明）

这个引理说明了：任何大于1的整数都至少有一个素因数。

$$12 = 2 \times 6 \qquad 23 = 1 \times 23 \qquad 27 = 3 \times 9$$

素数和复合数

引理2：如果a是一个大于1的整数，而所有≤$\sqrt{a}$的素数都除不尽a，则a是素数。

Step 1：证明（1）：如果a被 > 1 而 ≤ $\sqrt{a}$的整数都除不尽，则a是素数

假设a是合数，则 a=bc，而a被> 1 而 ≤ $\sqrt{a}$的整数都除不尽，则 b> $\sqrt{a}$，c> $\sqrt{a}$，则bc>a，这与 bc=a 是矛盾的。

```cpp
bool isPrime(int n){
    if (n == 0 || n == 1) return false;
    for (int i = 2; i <= sqrt(n); i++){
            if( n%i == 0){
                return false;
            }
        }
    return true;
}
```

开根号法判定质数

素数和复合数

引理2：如果a是一个大于1的整数，而所有≤$\sqrt{a}$的素数都除不尽a，则a是素数。

Step 2：证明（2）：所有的素数除不尽即可

假设a是合数，则a一定有> 1而≤ $\sqrt{a}$的因数，有引理1可知大于1的最小因数一定是素数。

```
bool isPrime(int n){
    if (n == 0 || n == 1) return false;
    for (int i = 2; i <= sqrt(n); i++){
            if( n%i == 0){
                return false;
            }
        }
    return true;
}
```

开根号法判定质数（如何优化？）

素数的分布

在1到100中间有25个素数,

在1到1000中间有168个素数,

在1000 到2000中间有135个素数,

在2000到3000中间有127个素数,

在3000到4000中间有120个素数,

在4000到5000中间有119个素数,

在5000 到10000中间有560个素数.

到目前为止所知道的最大素数是:

$$2^{19937}-1$$

Q6: 如何编程验证哥德巴赫猜想?

哥德巴赫猜想: 凡是大于4的偶数都是两个奇素数之和! 如:

6 = 3 + 3,	8 = 3 + 5,	10 = 5 + 5,
12 = 5 + 7,	14 = 7 + 7,	16 = 3 + 13,
18 = 5 + 13,	20 = 7 + 13,	22 = 3 + 19

最大公约(因)数

最大公约数(greatest common divisor,简写为gcd)

$$10 = 1 \times 10 = 2 \times 5$$

10有因数1, 2, 5, 10

$$15 = 1 \times 15 = 3 \times 5$$

15有因数1, 3, 5, 15

1, 5都是10和15的公因数

定义5: 如果n≥2是整数, 而a1,a2,···,an和d都是正整数。又设

d|a1, d|a2, ···, d|an

则d叫做a1,a2,···,an的公因数, 公因数中的最大的那一个数叫做a1,a2,···,an的最大公因数。

记作:

(a1,a2,···,an) = d

可达信奥—小武老师—keda.ac

最大公约(因)数

例1 求36和24的最大公因数.

$$36 = 2 \times 2 \times 3 \times 3$$

$$24 = 2 \times 2 \times 2 \times 3$$

素因数2,2,3是这两个数所共有的，它们的乘积就是这两个数的最大公因数。

$$2 \times 2 \times 3 = 12$$

例2 求48，60和72的最大公因数.

$$48 = 2 \times 2 \times \boxed{2 \times 2 \times 3} = 2^4 \times 3$$

$$60 = \boxed{2 \times 2 \times 3} \times 5 = 2^2 \times 3 \times 5$$

$$72 = 2 \times \boxed{2 \times 2 \times 3} \times 3 = 2^3 \times 3^2$$

$$2 \times 2 \times 3 = 12$$

求几个数的最大公因数，先把这些数分别分解素因数，然后在各个公有的素因数里，取出公共的部分相乘即可。

辗转相除法（欧几里得算法）

引理：假设a和b都是正整数，且 a>b，

a=bq+r，0<r<b

其中q和r都是正整数，则a和b的最大公因数等于b和r的最大公因数。即

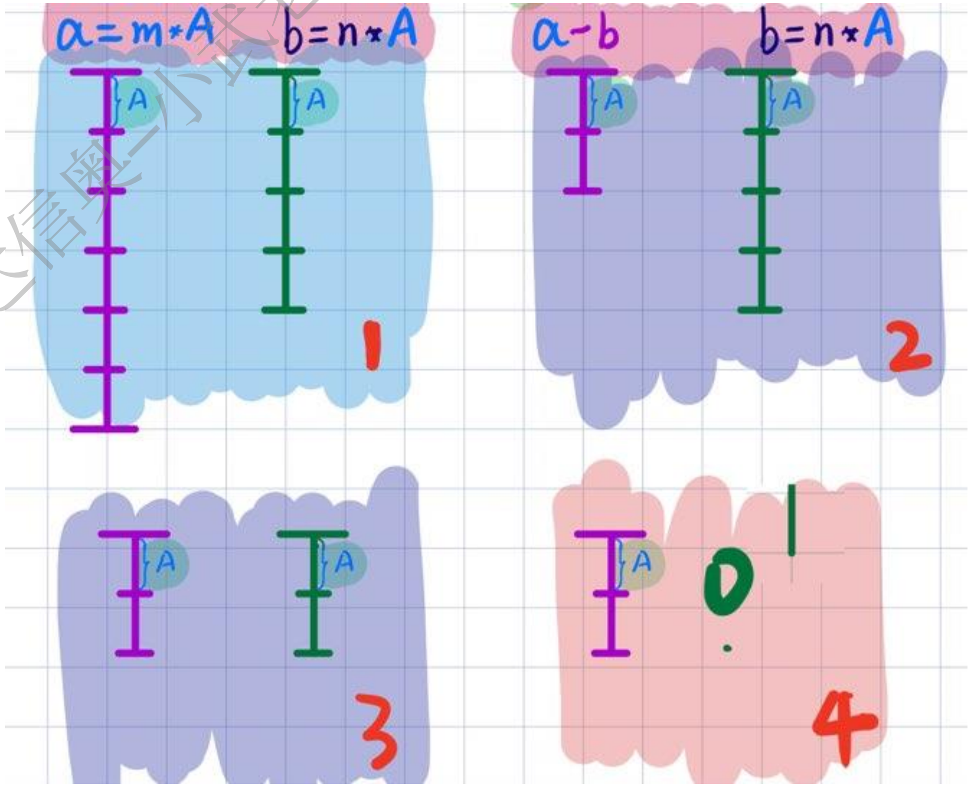
(a,b) = (b,r)

$$124 = 20 \times 6 + 4$$

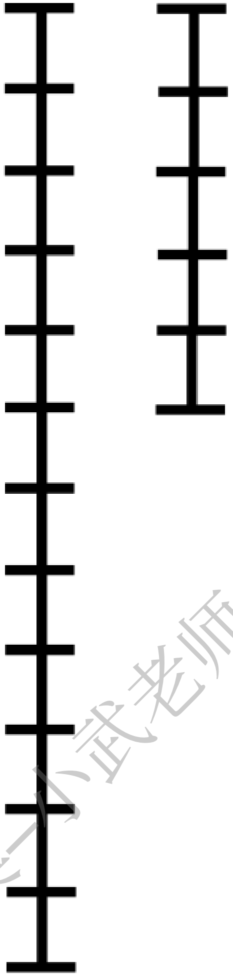
证明：设（a,b）= d，a=dm， b=dn，由 r=a-bq=(m-qn)d，所以 d|r.
由d|r,d|b,所以 d|(b,r),即(b,r)≥d. 假设(b,r) = D > d，则 D|b，D|r，由a=bq+r，所以D|a. 由D|a，D|b所以，D|(a,b),即(a,b)=d≥D,此与假设(b,r)=D>d矛盾，所以(b,r)=d.因此，(a,b) = d =(b,r).

辗转相除法（欧几里得算法）

最大公约数(greatest common divisor,简写为gcd)



$$gcd(a,b)=\begin{cases} a & b=0 \\ gcd(b,a\%b) & \end{cases}$$



辗转相除（减）法

辗转相除法（欧几里得算法）

例3 求6731和2809的最大公因数

$$6371 = 2809 \times 2 + 1113$$
$$2809 = 1113 \times 2 + 583$$
$$1113 = 583 \times 1 + 530$$
$$583 = 530 \times 1 + 53$$
$$530 = 53 \times 10 + 0$$

$$(6371, 2809) = (2809, 1113)$$
$$(2809, 1113) = (1113, 583)$$
$$(1113, 583) = (583, 530)$$
$$(583, 530) = (530, 53) = 53$$

$$(6371, 2809) = 53$$

例4 求5767，4453最大公因数

$$(5767, 4453) = 73$$

$$gcd(a,b) = \begin{cases} a & b=0 \\ gcd(b, a\%b) & \end{cases}$$

辗转相除法（欧几里得算法）

$$(6371, 2809) = (2809, 1113)$$

$$(2809, 1113) = (1113, 583)$$

$$(1113, 583) = (583, 530)$$

$$(583, 530) = (530, 53) = 53$$

$$(6371, 2809) = 53$$

$$gcd(a,b) = \begin{cases} a & b=0 \\ gcd(b, a\%b) & \end{cases}$$

```
int gcd(int m, int n){//辗转相除法
    if(n == 0) return m;
    else return gcd(n, m%n);
}
```

最小公倍数

最小公倍数(leatest Common Mutiple, LCM)

定义6：如果 n≥2是整数，而a1,a2,···,an和m都是正整数，又

a1|m, a2|m,···,an|m

则m叫做a1,a2,···,an的公倍数。如果m是a1,a2,···,an的最小的公倍数，我们就写作：

{a1,a2,···,an} = m

$$\{4,6\} = 12$$

求解方法： 分解质因数法。最小公倍数等于它们所有的质因数的乘积（如果有几个质因数相同，则比较两数中哪个数有该质因数的个数较多，乘较多的次数。

可达信奥-小武老师-keda.ac

最小公倍数

最小公倍数(leatest Common Mutiple, LCM)

求解方法： 分解质因数法。最小公倍数等于它们所有的质因数的乘积（如果有几个质因数相同，则比较两数中哪个数有该质因数的个数较多，乘较多的次数。

例5 求36和24的最小公倍数

$$36 = 2 \times 2 \times 3 \times 3$$

$$24 = 2 \times 2 \times 2 \times 3$$

$$lcm(36, 24) = 3^2 \times 2^3 = 72$$

例6 求108，28和42的最小公倍数

$$108 = 2^2 \times 3^3$$

$$28 = 2^2 \times 7$$

$$42 = 2 \times 3 \times 7$$

$$lcm(108, 28, 42) = 2^2 \times 3^3 \times 7 = 756$$

最小公倍数

最小公倍数(leatest Common Mutiple, LCM)

求解方法: 公式法。假设a和b都是正整数，a和b的最大公因数是d,而a和b的最小公倍数是m,即(a,b)=d,而{a,b} = m，则:

$$ab = dm$$

例5 求36和24的最小公倍数

$$36 = 2 \times 2 \times 3 \times 3$$

$$24 = 2 \times 2 \times 2 \times 3$$

$$lcm(36, 24) = 36 \times 24/12 = 72$$

例6 求108，28和42的最小公倍数

$$108 = 2^2 \times 3^3$$

$$28 = 2^2 \times 7$$

$$42 = 2 \times 3 \times 7$$

$$lcm(28, 42) = 28 \times 42/14 = 84$$

$$lcm(84, 108) = 84 \times 108/12 = 756$$

可达信奥—小武老师—keda.ac

总结

- **初等数论**
  - 偶数与奇数
    - 如何判定
  - 质数与合数
    - 普通判定方法
    - 开根号法
  - 质因数分解
    - 求最大公约数
    - 求最小公倍数
  - 最大公约数
    - 普通方法
    - 辗转相除法
  - 最小公倍数
    - 分解质因数法
    - 公式法

课后习题与实验

Talk is cheap, show me the code !

下节课见啦！

可达信奥-小武老师-keda.ac