Number Theory

vici

Northeast Normal University

March 13, 2013

基本公理

Theorem (良序原则(Well Ordering Principle))

每个自然数集合中都有一个最小值。

Theorem (有限归纳原则(Finite Induction))

$\mathbb{N}$是自然数集合，设$\mathbb{S}$为$\mathbb{N}$的一个子集合。

如果$\mathbb{S}$符合以下两点：

- $\mathbb{S}$中包含0。
- 如果数字k属于$\mathbb{S}$，那么$k+1$也属于$\mathbb{S}$。

那么$\mathbb{S} = \mathbb{N}$

整除性和约数

Definition

$d \mid a$ 表示对某个整数k，有$a = kd$。

$d \nmid a$ 表示对任意整数k，无$a = kd$。

Property

- 0可被任何（非0）整数整除。
- 若$b \mid a$，则$\pm b \mid \pm a$。
- 若$a \mid b, b \mid c$，则$a \mid c$。
- 若$a \mid a_i, i = 1, 2, 3, ..., k$，则$a \mid (c_1 a_1 + c_2 a_2 + ... + c_k a_k)$，这里$c_{1...k}$为任意整数。
- 若p为素数且$p \mid ab$，则$p \mid a$或$p \mid b$。

整除性和约数

Definition

如果$d \mid a$并且$d \geq 0$，则我们说d是a的**约数**。

每个整数a都可以被其**平凡约数**1和a整除，a的**非平凡约数**也称为a的**因子**。

Example

20的因子有2，4，5，10。

唯一分解定理

Theorem (带余除法定理)

设$a, b \in Z, b \neq 0$，则存在唯一的整数对q和r，使$a = qb + r$，$0 \leq r < |b|$，r称为b除a所得的**最小剩余**。

Theorem (唯一分解定理)

任一自然数n皆可唯一表为素数之积

$$n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$$

$p_1 < p_2 < ... < p_k$为素数，$a_1, a_2, \ldots, a_k$为自然数。

Example

$1620 = 2^2 \cdot 3^4 \cdot 5$

几个数论函数

Definition (函数$[x]$)

设x是实数，不大于x的最大整数称为x的整数部分，记为$[x]$；

$x-[x]$称为x的小数部分，记为$\{x\}$。

Property

- 若$p^a \parallel n!$，则$a=[\frac{n}{p}]+[\frac{n}{p^2}]+[\frac{n}{p^3}]+\ldots$

Example (求100!最后连续0的个数)

由于100!中2的个数大于5的个数，所以100!中5的次数即为结果

$a=[\frac{100}{5}]+[\frac{100}{5^2}]+\ldots=20+4=24$

几个数论函数

Definition (函数$d(n)$)

正整数n的正因数个数称为**除法函数**。若n的标准分解式为$n=p_1^{a_1}p_2^{a_2}...p_s^{a_s}$，则利用乘法原理得：

$$d(n)=(a_1+1)(a_2+1)...(a_n+1)$$

Example (72的因子个数)

$d(72)=d\left(2^3\cdot 3^2\right)=(3+1)(2+1)=12$

几个数论函数

Definition (欧拉函数$\varphi(n)$)

正整数n与$1, ..., n-1$互素的数的个数称为n的**欧拉函数**，记为$\varphi(n)$。若n的标准分解式为$n = p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$，则$\varphi(n)$的计算公式为：

$$\varphi(n) = p_1^{a_1-1} p_2^{a_2-1} ... p_s^{a_s-1} (p_1 - 1)(p_2 - 1)...(p_s - 1)$$

Example ($1 - 1999$中与2000互素的数的个数)

$$\varphi(2000) = \varphi\left(2^4 \cdot 5^3\right) = 2^3 \cdot 5^2 (2-1)(5-1) = 800$$

同余及其基本性质

同余的概念是高斯（Gauss）在1800年左右给出的

Definition

设m是正整数，若用m去除整数a，b，所得余数相同，则称a与b关于模m**同余**，记作$a \equiv b \pmod{m}$；否则称a与b关于模m**不同余**，记作$a \not\equiv b \pmod{m}$。

Example

$34 \equiv 4 \pmod{15}$

$1000 \equiv -1 \pmod{7}$

$34 \not\equiv 4 \pmod{8}$

同余及其基本性质

Property 1

$a \equiv b\,(\mathrm{mod}\, m)$的充要条件是$a = b + mt, t \in \mathbb{Z}$，也即$m \mid a - b$

Example (将整除关系转变为同余式)

$a \equiv b\,(\mathrm{mod}\, m) \leftrightarrow a - b \equiv 0\,(\mathrm{mod}\, m) \leftrightarrow m \mid a - b$

- $7 \equiv 4\,(\mathrm{mod} 3) \leftrightarrow 3 \mid (7 - 4)$

Property 2

同余关系满足下列规律：

- **自反律**：对任何模m都有$a \equiv a\,(\mathrm{mod}\, m)$
- **对称律**：若$a \equiv b\,(\mathrm{mod}\, m)$，则$b \equiv a\,(\mathrm{mod}\, m)$
- **传递律**：若$a \equiv b\,(\mathrm{mod}\, m)$，$b \equiv c\,(\mathrm{mod}\, m)$，则$a \equiv c\,(\mathrm{mod}\, m)$

同余及其基本性质

Property 3

若$a_i \equiv b_i \pmod{m}, i = 1, 2, ..., s$，则

$$a_1 + a_2 + ... + a_s \equiv b_1 + b_2 + ... + b_s \pmod{m}$$

推论：设k是整数，n是正整数

- 若$a + b \equiv c \pmod{m}$，则$a \equiv b - c \pmod{m}$
- 若$a \equiv b \pmod{m}$，
  则$a + mk \equiv a \pmod{m}, ak \equiv bk \pmod{m}, a^n \equiv b^n \pmod{m}$

Conclusion

性质3及推论表明，对于加、减、乘及乘方而言，同余式与等式的运算规律是一致的：可以移项，可以同乘一整数，也可以乘方

Property 4

设$f(x)$是系数全为整数的多项式，若$a+b\equiv c\,(\mathrm{mod}\,m)$，则

$$f(a)\equiv f(b)\,(\mathrm{mod}\,m)$$

Example (试求$\left(257^{33}+46\right)^{26}$被50除所得的余数)

- $\left(257^{33}+46\right)^{26}\equiv\left(7^{33}+46\right)^{26}(\mathrm{mod}\,50)$
- $\left(7^{33}+46\right)^{26}\equiv\left(\left(7^{2}\right)^{16}\times 7+46\right)^{26}(\mathrm{mod}\,50)\equiv$ $\left(\left(-1\right)^{16}\times 7+46\right)^{26}(\mathrm{mod}\,50)\equiv 3^{26}\,(\mathrm{mod}\,50)$
- $3^{26}\equiv\left(3^{5}\right)^{5}\times 3\equiv\left(-7^{5}\right)\times 3\equiv$ $-\left(7^{2}\right)^{2}\times 7\times 3\equiv -21\equiv 29\,(\mathrm{mod}\,50)$
- 注意到$0\leq 29<50$，所以29就是所求余数

同余及其基本性质

Property 5

若$ad \equiv bd \pmod{m}$，且$(d, m) = 1$，则$a \equiv b \pmod{m}$

Property 6

若$a \equiv b \pmod{m}$，且$d \mid a$，$d \mid b$，$d \mid m$，则$\frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{m}{d}\right)$

Property 7

若$a \equiv b \pmod{m}$，且$m_1 \mid m$，则$a \equiv b \pmod{m_1}$

Property 8

若$a \equiv b \pmod{m_i}, i = 1, 2, ..., s$，则$a \equiv b(\bmod\ [m_1, m_2, ..., m_s])$

公约数、公倍数及互素

Definition

公约数，亦称“公因数”。如果一个整数同时是几个整数的约数，称这个整数为它们的**公约数**。

公约数中最大的称为**最大公约数**（Greatest Common Divisor，GCD）。

Property

对任意的若干个正整数，1总是它们的公约数。

Definition

如果两个整数a与b仅有公约数1，即如果$\gcd(a,b)=1$，则a与b称为**互质数**。

Property

对任意整数a，b和p，如果$\gcd(a,p)=1$且$\gcd(b,p)=1$，则$\gcd(ab,p)=1$。

公约数、公倍数及互素

Property

- $\gcd(a, 0) = \gcd(a, ka) = |a|$
- $\gcd(a, 1) = |1|$
- $\gcd(a, b) = \gcd(b, a) = \gcd(-a, b)$

Theorem

如果a和b是不都为0的任意整数，则$d = \gcd(a, b)$是a与b的线性组合集合$\{ax + by : x, y \in \mathbb{Z}\}$，有$d = ax + by$。

Inference

- 对任意整数a和b，如果$d \mid a$并且$d \mid b$，则$d \mid \gcd(a, b)$。
- 对所有整数a和b以及任意非负整数n，$\gcd(an, bn) = n \cdot \gcd(a, b)$。
- 对所有正整数n，a和b，如果$n \mid ab$并且$\gcd(a, n) = 1$，则$n \mid b$。

公约数、公倍数及互素

Definition

两个或两个以上的数公有的倍数叫做这几个数的**公倍数**，其中最小的一个叫做这几个数的**最小公倍数**（Least Common Multiple，LCM）。

Property

- $\gcd(a,b)\cdot lcm(a,b)=ab$
- 两个整数的最大公约数和最小公倍数中存在分配律：

  $\gcd(a, lcm(b,c)) = lcm(\gcd(a,b), \gcd(a,c))$

  $lcm(a, \gcd(b,c)) = \gcd(lcm(a,b), lcm(a,c))$

最大公约数

Methods

- 两数各分解质因子，然后取出相同的项乘起来
- **辗转相除法**

Theorem (GCD递归定理)

对任意非负整数a和任意正整数b有

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

最大公约数

Proof (GCD递归定理).

- $\gcd(a,b) \mid \gcd(b, a \bmod b)$

  设$d = \gcd(a,b)$，则$d \mid a$且$d \mid b$

  设$q = \left[\frac{a}{b}\right]$，则$a \bmod b = a - qb$

  由$d \mid ax + by$，得$d \mid (a \bmod b)$

  所以$d \mid \gcd(b, a \bmod b)$

- $\gcd(b, a \bmod b) \mid \gcd(a,b)$

  设$d = \gcd(b, a \bmod b)$

  则$d \mid b$且$d \mid (a \bmod b)$

  设$q = \left[\frac{a}{b}\right]$，则$a = qb + (a \bmod b)$

  得$d \mid a$

  所以$d \mid \gcd(b, a \bmod b)$

因此 $\gcd(a,b) = \gcd(b, a \bmod b)$ □

欧几里得算法

Definition

欧几里德（约公元前300年古希腊著名数学家）的《几何原本》描述了下列GCD算法。

- 复杂度约$O(\log b)$)

Algorithm

```
EUCLID (a, b)
  if  b = 0
  then  return  a
  else  return  EUCLID (b, a mod b)
```

扩展欧几里得算法

Definition

根据$d = \gcd(a, b) = ax + by$，那么Extended-Euclid算法将通过一对非负整数返回一个三元式(d, x, y)。

- (复杂度与ECULID基本相同)

Algorithm

```
EXTENDED−EUCLID(a, b)
  if b = 0
    then return (a, 1, 0)
    (d′, x′, y′) = EXTENDED−EUCLID(b, a mod b)
    (d, x, y) = (d′, y′, x′ − [a / b] · y′)
  return (d, x, y)
```

扩展欧几里得算法

Proof ($d = ax + by$).

- 若$b = 0$

  令$x = 1, y = 0$，则满足$a = 1 \cdot a + 0 \cdot b$

- 若$b \neq 0$

  则$\begin{cases} d' = \gcd(b, a \bmod b) \\ d' = bx' + (a \bmod b)\, y' \end{cases}$

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

  $d = bx' + (a - [a/b]\, b)\, y' = a\, y' + b(x' - [a/b]\, y')$

  令$\begin{cases} x = y' \\ y = x' - [a/b]\, y' \end{cases}$

  则满足$d = ax + by$

$\square$

模运算

Definition (有限群)

群$(S, \oplus)$是一个集合S和定义在S上的二进制运算$\oplus$。

Property

- **封闭性**：对所有$a, b \in S$，有$a \oplus b \in S$。
- **单位元**：存在一个元素$e \in S$，称为群的单位元，满足对所有$a \in S$，$e \oplus a = a \oplus e = a$。
- **结合律**：对所有$a, b, c \in S$，有$(a \oplus b) \oplus c = a \oplus (b \oplus c)$。
- **逆元**： 对每个$a \in S$，存在唯一的元素$b \in S$，称为a的逆元，满足$a \oplus b = b \oplus a = e$。

Definition (交换群)

如果群$(S, \oplus)$满足交换律，对所有$a, b \in S$，有$a \oplus b = b \oplus a$，则它是一个**交换群**。

拉格朗日定理及子群

Definition (有限可交换群)

定义**模加法群**$(Z_n, +n)$，规模为$|Z_n| = n$。

定义**模乘法群**$(Z_n^*, \cdot n)$，该群元素为Z_n中与n互素的元素组成的集合Z_n^*：

$$Z_n^* = \{[a]_n \in Z_n : \gcd(a, n) = 1\}$$

Z_n与Z_n^*都是**有限可交换群**。

Definition (子群)

一个有限群的非空封闭子集是一个**子群**。

Property

如果$(S, \oplus)$是一个有限群，S'是S的一个任意非空子集，并满足对所有$a, b \in S$，有$a \oplus b \in S'$，则$(S', \oplus)$是$(S, \oplus)$的一个子群。

拉格朗日定理及子群

Definition (拉格朗日定理)

如果$(S, \oplus)$是一个有限群，$(S', \oplus)$是$(S, \oplus)$的一个子群，
则$|S'|$是$|S|$的一个约数。

- 对一个群S的子群S'，如果$S' \neq S$，则子群S'称为群S的**真子群**。

Inference

如果$S.$是有限群S的真子群，则$|S'| \leq \frac{|S|}{2}$。

Definition

对$k \geq 1$定义$a^{(k)}$如下：
$a^{(k)} = a \oplus a \oplus ... \oplus a$ （k个a）
在群Z_n中，有$a^{(k)} = ka \bmod n$；在群Z_n^*中，有$a^{(k)} = a^k \bmod n$。
由a生成的子群用$\langle a \rangle$或$(\langle a \rangle, \oplus)$表示，其定义如下：

$$\langle a \rangle = \left\{ a^{(k)} : k \geq 1 \right\}$$

群S中a的价用$ord(a)$表示，定义为满足$a^{(t)} \equiv e$的最小整数t。

拉格朗日定理及子群

Example (在群$\{0, 2, 4, 6......\}$中)

一个子群为$\{0, 4, ...\}$。

Example (在Z_6中)

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{1, 2, 3, 4, 5\}$

$\langle 2 \rangle = \{0, 2, 4\}$

Example (Z_7^*)

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{1, 2, 4\}$

$\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\}$

求解模线性方程

Definition (考虑求解下列方程的问题：)

$ax \equiv b\,(\bmod n)$ （其中$a > 0, n > 0$）

Theorem 1

对任意正整数a和n，如果$d = \gcd(a, n)$，则

在Z_n中$\langle a \rangle = \langle d \rangle = \left\{0, d, 2d, ..., \left(\frac{n}{d} - 1\right) d\right\}$，因此有$|\langle a \rangle| = \frac{n}{d}$。

Example (3 mod 5)

$\langle 3 \rangle = \langle \gcd(3,5) \rangle = \langle 1 \rangle$

$\langle 1 \rangle = 1^{(x)} \bmod 5\,(x = 0,1,2,3,4) = \{0,1,2,3,4\}$

求解模线性方程

Proof (Theorem 1).

- $\langle d \rangle \subseteq \langle a \rangle$

  因为$ax' + ny' = d$

  则$ax' \equiv d \pmod{n}$

  所以$d \in \langle a \rangle$，同时$(kd \bmod n) \in \langle a \rangle$。

  即$\langle d \rangle \subseteq \langle a \rangle$

- $\langle a \rangle \subseteq \langle d \rangle$

  设$m \in \langle a \rangle$

  $m = ax \bmod n$

  则有$m = ax + ny$

  因为$d \mid a$且$d \mid n$，则有$d \mid m$

  所以$m \in \langle d \rangle$，进而$\langle a \rangle \subseteq \langle d \rangle$

$\square$

求解模线性方程

Theorem 1. Inference

- 方程$ax \equiv b \pmod{n}$对于未知量x有解，当且仅当$\gcd(a,n) \mid b$。
- 方程$ax \equiv b \pmod{n}$或者有d个不同的解，其中$d = \gcd(a,n)$；或者无解。

Proof (Theorem 1 Inference).

- 对于$ax \equiv b \pmod{n}$若有解，则$b \in \langle a \rangle$
  序列$a_i \bmod n$具有周期性，周期为$|\langle a \rangle| = \frac{n}{d}$
  则b在$a_i \bmod n$中出现d次。

□

求解模线性方程

Theorem 2

设$d = \gcd(a, n)$，假定对整数x'和y'，有$d = ax' + ny'$。如果$d \mid b$，则$ax_0 \equiv ax' \left[\frac{b}{d}\right] (\bmod n) \equiv d \left[\frac{b}{d}\right] (\bmod n) \equiv b (\bmod n)$。

Proof (Theorem 2).

对于$x_0 = x' \left(\frac{b}{d}\right) \bmod n$，$d = \gcd(a, n)$

则有$d \mid b, d = ax' + ny'$

令$x_0 = x' \left[\frac{b}{d}\right] \bmod n$

$ax_0 \equiv ax' \left[\frac{b}{d}\right] \bmod n \equiv d \left[\frac{b}{d}\right] \bmod n \equiv b \bmod n$

则x_0为方程的一个解。 □

求解模线性方程

Theorem 3

假设方程$ax \equiv b \pmod{n}$有解（即有$d \mid b, d = \gcd(a, b)$），x_0是该方程的任意一个解，则该方程对模n恰有d个不同的解，分别为：

$x_i = x_0 + i \cdot \left(\frac{n}{d}\right) \, (i = 0, 1, 2, ..., d-1)$

Inference

- 对任意$n > 1$，如果$\gcd(a, n) = 1$，则方程$ax \equiv b \pmod{n}$有唯一解。
- 对任意$n > 1$，如果$\gcd(a, n) = 1$，则方程$ax \equiv 1 \pmod{n}$有唯一解或无解。

Proof (Theorem 3).

因为x_0已经是方程的一个解，由Theorem 1推论，那么其他解都在$\langle a \rangle$中，所以通过加周期后去模依次寻找即可。 □

求解模线性方程

Definition

下列算法可以输出该方程的所有解。输入a和n为任意正整数，b为任意整数。

Algorithm

```
MODULAR−LINEAR−EQUATION−SOLVER(a, b, n)
  (d, x', y') = EXTENDED−EUCLID(a, n)
  if d | b
    then x0 = x' · (b / d) mod n
    for i = 0 to d − 1
      do print (x0 + i · (n / d)) mod n
      else print "no solution"
```

中国剩余定理

Definition

设$n = n_1 \cdot n_2 \cdot ... \cdot n_k$，其中因子$n_i$两两互质。有以下对应关系：

$$a \leftrightarrow (a_1, a_2, ..., a_k)$$

其中$a \in Z_n, a_i \cdot n \in Z_{n_i}$，而且对$i = 1, 2, ..., k$：

$$a_i = a \bmod n_i$$

对Z_n中元素所执行的运算可以等价的作用于对应的k元组，即在适当的系统中独立的对每个坐标的位置执行所需的运算。

如果$\begin{cases} a \leftrightarrow (a_1, a_2, ..., a_k) \\ b \leftrightarrow (b_1, b_2, ..., b_k) \end{cases}$

则$\begin{cases} (a+b) \bmod n \leftrightarrow ((a_1+b_1) \bmod n_1, ..., (a_k+b_k) \bmod n_k) \\ (a-b) \bmod n \leftrightarrow ((a_1-b_1) \bmod n_1, ..., (a_k-b_k) \bmod n_k) \\ (a \cdot b) \bmod n \leftrightarrow ((a_1 \cdot b_1) \bmod n_1, ..., (a_k \cdot b_k) \bmod n_k) \end{cases}$

中国剩余定理

Methods

已知$a \equiv a_i \pmod{n_i}, i = 0, 1, ..., k$

求得$m_i = n_1 \cdot n_2 \cdot ... \cdot n_{i-1} \cdot n_{i+1} \cdot ... \cdot n_k$

令$b_i m_i \equiv 1 \pmod{n_i}$

解模线性方程，求得b_i

令$c_i = b_i m_i$，则

$a \equiv a_1 c_1 + a_2 c_2 + ... + a_k c_k \pmod{n_1 \cdot n_2 \cdot ... \cdot n_k}$

Example:

今有物，不知其数，三三数之，剩二；五五数之，剩三；七七数之，剩二。问物几何？ —《孙子算经》

此题可化为同余方程组

$$\begin{cases} x \equiv 2\,(\bmod 3) \\ x \equiv 3\,(\bmod 5) \\ x \equiv 2\,(\bmod 7) \end{cases}$$

则进一步得

$$\begin{cases} lcm\,(5,7)\cdot k \equiv 1\,(\bmod 3) \rightarrow 70 \equiv 1\,(\bmod 3) \\ lcm\,(3,7)\cdot k \equiv 1\,(\bmod 5) \rightarrow 21 \equiv 1\,(\bmod 5) \\ lcm\,(3,5)\cdot k \equiv 1\,(\bmod 7) \rightarrow 15 \equiv 1\,(\bmod 7) \end{cases}$$

所以$70\cdot 2 + 21\cdot 3 + 15\cdot 2 \equiv x\,(\bmod\,(lcm\,(3,5,7)))$

$$233 \equiv x\,(\bmod 105)$$

得到$x = 23 + 105k\,(k \in \mathbb{Z})$

欧拉定理和费马定理

Theorem (欧拉定理)

对于任意整数$n > 1$，$a^{\varphi(n)} \equiv 1 \pmod{n}$对所有$a \in Z_n^*$都成立。

Example

因为$4 \in Z_9^*$，所以$4^{\varphi(9)} \equiv 1 \pmod{9}$

Theorem (费马定理)

如果p是素数，则$a^{p-1} \equiv 1 \pmod{p}$对所有$a \in Z_p^*$都成立。

- 当p为素数时，有$\varphi(p) = p - 1$，所以费马定理是欧拉定理的特殊情况。

反复平方法

Definition

计算$a^b \bmod n$的值，其中a和b是非负整数，n是正整数。

Algorithm(反复平方法)

```
MODULAR−EXPONENTIATION(a, b, n)
  c = 0, d = 1
  let ⟨b_k, b_{k−1}, ..., b_0⟩ be the binary representation of b
  for i = k downto 0
    do c = 2c
       d = (d · d) mod n
       if b_i = 1
         then c = c + 1
              d = (d · a) mod n
  return d
```

素数的Eratosthenes筛法

Methods

枚举所有整数$m = 2...n$

- 如果m未被标记
  1. 将m加入素数表
  2. 将所有m的倍数（小于等于n）标记
- 如果m已被标记，则m为合数

Sieve of Eratosthenes (8×8)

Step 1: Numbers from $2 \ldots 64$

	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

素数判定法

Theorem (素数定理)

$$\lim_{n\to\infty}\frac{\pi(n)}{n/\ln n}=1$$ （$\pi(n)$为不大于x的素数个数）

Methods

- 试除法：将该数N用小于等于它的所有素数去试除，若均无法整除，则N为素数。
- **Miller-Rabin随机性素数测试方法。**

素数判定法

Algorithm(Miller-Rabin)

WITNESS(a, n)

let $n-1=2^t u$, where $t \geq 1$ and u is odd

$x_0 = \text{MODULAR} - \text{EXPONENTIATION}(a, u, n)$

for i = 1 to t

do $x_i = x_{i-1}^2 \bmod n$

if $x_i = 1$ and $x_{i-1} \neq 1$ and $x_{i-1} \neq n-1$

then return true

if $x_{i-1} \neq 1$

then return true

return false

素数扩充知识

Definition (高斯素数)

高斯素数是不能表现为1、i或本身除外的两个复整数的乘积的复整数。 高斯素数是把素数在复数范围内的扩展。

Example

- $(1+2i)$是高斯素数
- 有的数在实数范围内是素数，但在复数范围内不是素数。例如$13=(3-2i)\cdot(3+2i)$

Definition (梅森素数)

梅森数是指形如2^n-1的数，记为M_n。 如果一个梅森数是素数，那么称它为**梅森素数**。

Example

$M_2=2^2-1=3$，$M_3=2^3-1=7$

参考资料

- (美)Thomas H.Cormen, Charles E.Leiserson, Ronald L. Rivest, Clifford Stein

  《Interoduction To Algorithms》
- (美)Ronald L.Graham, Donald E.Knuth, Oren Patashnik

  《Concrete Mathematics》
- 裴定一，祝跃飞

  《算法数论》
- 李胜宏，李明德

  《高中数学竞赛培优教程》