Number Theory

vici

March 13, 2013

Contents

1 基本公理

1.1 良序原则(Well Ordering Principle)

每个自然数集合中都有一个最小值。

1.2 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：

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

那么$\mathbb{S}=\mathbb{N}$

2 整除性和约数

2.1 定义

$d \mid a$ 表示对某个整数k，有$a=kd$。
$d \nmid a$ 表示对任意整数k，无$a=kd$。
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**。

2.2 性质

1. 0可被任何（非0）整数整除。
2. 若$b \mid a$，则$\pm b \mid \pm a$。
3. 若$a \mid b, b \mid c$，则$a \mid c$。
4. 若$a \mid a_i, i=1,2,...,k$，则$a \mid (c_1a_1+c_2a_2+...+c_ka_k)$，$c_{1...k}$为任意整数。
5. 若p为素数且$p \mid ab$，则$p \mid a$或$p \mid b$。

2.3 举例

20的因子有2，4，5，10。

3 唯一分解定理

3.1 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**。

3.2 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。

3.3 举例

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

4 几个数论函数

4.1 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$\{x\}$。

4.1.1 性质

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

4.1.2 举例（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
$a = \left[\frac{100}{5}\right] + \left[\frac{100}{5^2}\right] + ... = 20 + 4 = 24$

4.2 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：$d\,(n) = (a_1 + 1)\,(a_2 + 1)\,...\,(a_n + 1)$

4.2.1 举例（72的因子个数）

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

4.3 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：
$\varphi(n)=p_1^{a_1-1}p_2^{a_2-1}...p_s^{a_s-1}(p_1-1)(p_2-1)...(p_s-1)$

4.3.1 举例（$1-1999$中与2000互素的数的个数）

$\varphi(2000)=\varphi\left(2^4\cdot5^3\right)=2^3\cdot5^2(2-1)(5-1)=800$

5 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

5.1 定义

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$a\equiv b\,(\mathrm{mod}m)$；否则称$a$与$b$关于模$m$**不同余**，记作$a\not\equiv b\,(\mathrm{mod}m)$。

5.2 举例

$34\equiv4\,(\mathrm{mod}15)$
$1000\equiv-1\,(\mathrm{mod}7)$
$34\not\equiv4\,(\mathrm{mod}8)$

5.3 性质1

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

5.3.1 举例：（将整除关系转变为同余式）

$a\equiv b\,(\mathrm{mod}m)\leftrightarrow a-b\equiv0\,(\mathrm{mod}m)\leftrightarrow m\mid a-b$
$7\equiv4\,(\mathrm{mod}3)\leftrightarrow3\mid(7-4)$

5.4 性质2

同余关系满足下列规律：

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

5.5 性质3

若$a_i \equiv b_i \,(\mathrm{mod} m)\,, i = 1, 2, ..., s$，则$a_1 + a_2 + ... + a_s \equiv b_1 + b_2 + ... + b_s \,(\mathrm{mod} m)$

5.5.1 推论

设k是整数，n是正整数

1. 若$a + b \equiv c \,(\mathrm{mod} m)$，则$a \equiv b - c \,(\mathrm{mod} m)$
2. 若$a \equiv b \,(\mathrm{mod} m)$，
   则$a + mk \equiv a \,(\mathrm{mod} m)\,, ak \equiv bk \,(\mathrm{mod} m)\,, a^n \equiv b^n \,(\mathrm{mod} m)$

5.5.2 结论

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

5.6 性质4

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

5.6.1 举例

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

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

5.7 性质5

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

5.8 性质6

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

5.9 性质7

若$a \equiv b \,(\mathrm{mod} m)$，且$m_1 \mid m$，则$a \equiv b \,(\mathrm{mod} m_1)$

5.10 性质8

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

6 公约数、公倍数及互素

6.1 定义

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）。
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**。
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）。

6.2 性质

1. 对任意的若干个正整数，1总是它们的公约数。
2. 对任意整数a，b和p，如果$\gcd(a, p) = 1$且$\gcd(b, p) = 1$，则$\gcd(ab, p) = 1$。
3. $\gcd(a, 0) = \gcd(a, ka) = |a|$
4. $\gcd(a, 1) = |1|$
5. $\gcd(a, b) = \gcd(b, a) = \gcd(-a, b)$
6. $\gcd(a, b) \cdot lcm(a, b) = ab$
7. 两个整数的最大公约数和最小公倍数中存在分配律：
   $\gcd(a, lcm(b, c)) = lcm(\gcd(a, b), \gcd(a, c))$
   $lcm(a, \gcd(b, c)) = \gcd(lcm(a, b), lcm(a, c))$

6.3 定理

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$d = ax + by$。

6.3.1 推论

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

6.4 最大公约数

1. 两数各分解质因子，然后取出相同的项乘起来
2. **辗转相除法**

6.4.1 GCD递归定理

对任意非负整数a和任意正整数b有$\gcd(a,b)=\gcd(b,a \bmod b)$

6.4.2 证明

1. $\gcd(a,b) \mid \gcd(b,a \bmod b)$
   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$d \mid \gcd(b,a \bmod b)$
2. $\gcd(b,a \bmod b) \mid \gcd(a,b)$
   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 $\gcd(a,b)=\gcd(b,a \bmod b)$

7 欧几里得算法

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$O(\log b)$

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

8 扩展欧几里得算法

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

```
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)
```

8.1 证明

1. 若$b = 0$
   令$x = 1, y = 0$，则满足$a = 1 \cdot a + 0 \cdot b$
2. 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$d = ax + by$

9 拉格朗日定理及子群

9.1 有限群

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

9.1.1 性质

1. **封闭性**：对所有$a, b \in S$，有$a \oplus b \in S$。
2. **单位元**：存在一个元素$e \in S$，称为群的单位元，满足对所有$a \in S$，$e \oplus a = a \oplus e = a$。
3. **结合律**：对所有$a, b, c \in S$，有$(a \oplus b) \oplus c = a \oplus (b \oplus c)$。
4. **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$a \oplus b = b \oplus a = e$。

9.2 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**。

9.3 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^*：
$Z_n^*=\left\{[a]_n\in Z_n:\gcd(a,n)=1\right\}$
Z_n与Z_n^*都是**有限可交换群**。

9.4 子群

一个有限群的非空封闭子集是一个**子群**。

9.4.1 性质

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。

9.5 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**。

9.5.1 推论

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

9.6 $a^{(k)}$运算

对$k\geq 1$定义$a^{(k)}$如下：
$a^{(k)}=\underbrace{a\oplus a\oplus ...\oplus a}_{k}$
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。

9.7 举例

- 在群$\{0, 2, 4, 6.....\}$中
  一个子群为$\{0, 4, ...\}$
- 在Z_6中
  $\langle 0\rangle = \{0\}$，$\langle 1\rangle = \{1, 2, 3, 4, 5\}$ ，$\langle 2\rangle = \{0, 2, 4\}$
- 在Z_7^*中
  $\langle 1\rangle = \{1\}$ ，$\langle 2\rangle = \{1, 2, 4\}$ ，$\langle 3\rangle = \{1, 2, 3, 4, 5, 6\}$

10 求解模线性方程

10.1 定义

考虑求解下列方程的问题：
$ax \equiv b \pmod{n}$ （其中$a > 0, n > 0$）

10.2 定理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$|\langle a\rangle| = \frac{n}{d}$。

10.2.1 举例

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

10.2.2 证明

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$\langle d\rangle \subseteq \langle a\rangle$
2. $\langle a\rangle \subseteq \langle d\rangle$
   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$\langle a\rangle \subseteq \langle d\rangle$

10.3 定理1 推论

1. 方程$ax \equiv b \pmod{n}$对于未知量x有解，当且仅当$\gcd(a,n) \mid b$。
2. 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。

10.3.1 证明

1. 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。

10.4 定理2

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

10.4.1 证明

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。

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

1. 对任意$n > 1$，如果$\gcd(a,n) = 1$，则方程$ax \equiv b \pmod{n}$有唯一解。
2. 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。

10.5.1 证明

因为x_0已经是方程的一个解，由定理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。

10.6 求解模线性方程

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。

```
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"
```

11 中国剩余定理

11.1 定义

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

11.2 求解思路

已知$a \equiv a_i \,(\mathrm{mod} n_i)\,, i = 0, 1, ..., k$

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

令$b_i m_i \equiv 1 \,(\mathrm{mod} n_i)$

解模线性方程，求得b_i

令$c_i = b_i m_i$，则

$a \equiv a_1 c_1 + a_2 c_2 + ... + a_k c_k \,(\mathrm{mod} n_1 \cdot n_2 \cdot ... \cdot n_k)$

11.3 举例

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？

此题可化为同余方程组

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

则进一步得

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

所以$70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 \equiv x\,(\mathrm{mod}\,(lcm\,(3,5,7)))$

$$233 \equiv x\,(\mathrm{mod}105)$$

得到$x = 23 + 105k\,(k \in \mathbb{Z})$

12 欧拉定理和费马定理

12.1 欧拉定理

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

12.1.1 举例

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

12.2 费马定理

如果p是素数，则$a^{p-1} \equiv 1\,(\mathrm{mod}p)$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。

13 反复平方法

13.1 定义

计算$a^b \bmod n$的值，其中a和b是非负整数，n是正整数。

13.2 求解

- 当用二进制表示b时，采用反复平方法，可以有效地解决这个问题。

```
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
```

14 素数的Eratosthenes筛法

	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

Primes:
2, 3, 5, 7,
11, 13, 17,
19, 23, 29,
31, 37, 41,
43, 47, 53,
59, 61

枚举所有整数$m = 2...n$

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

15 素数判定法

15.1 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）

15.1.1 素数判定

1. 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。
2. **Miller-Rabin随机性素数测试方法。**

```
WITNESS(a, n)
  let  n − 1 = 2^t u, where t ≥ 1 and u is odd
  x_0 = MODULAR − EXPONENTIATION(a, u, n)
  for  i = 1 to t
  do x_i = x_{i−1}^2 mod n
    if  x_i = 1 and x_{i−1} ≠ 1 and x_{i−1} ≠ n − 1
      then return true
  if  x_{i−1} ≠ 1
    then return true
  return  false
```

16 素数扩充知识

16.1 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。

16.1.1 举例

1. $(1+2i)$是高斯素数
2. 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$13=(3-2i)\cdot(3+2i)$

16.2 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**。

16.2.1 举例

$M_2=2^2-1=3$，$M_3=2^3-1=7$

References

[1] (美)Thomas H.Cormen, Charles E.Leiserson, Ronald L. Rivest, Clifford Stein 《Interoduction To Algorithms》

[2] (美)Ronald L.Graham, Donald E.Knuth, Oren Patashnik 《Concrete Mathematics》

[3] 裴定一，祝跃飞《算法数论》

[4] 李胜宏，李明德《高中数学竞赛培优教程》