整除性理论

袁平之

华南师范大学数学科学学院

July 11, 2009

主要内容

主要内容

研究的问题

问题1

研究两数做除法的全面情况。

问题2

研究两数是否整除，以及探讨由此而引伸出来的有关问题。

主要内容

带余除法

定理

带余除法：设a, b为两个整数，其中$b \neq 0$,则存在两个唯一的整数q和r,使得

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

成立.

整除的基本性质

线性性质；传递性和反对称性。

主要内容

Euclid 算法

定理

设a, b, c是任意三个不全为零的整数，且

$$a = bq + c,$$

其中q为整数，则$(a, b) = (a, c)$.

Euclid算法：

$$\begin{cases} n = q_1 m + r_1, & 0 < r_1 < m, \\ m = q_2 r_1 + r_2, & 0 < r_2 < r_1, \\ r_1 = k_3 r_2 + r_3, & 0 < r_3 < r_2, \\ \cdots & \\ r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}, & 0 < r_{k-1} < r_{k-2}, \\ r_{k-2} = q_k r_{k-1} + r_k, & r_{k-1} = q_{k+1} r_k. \end{cases} \tag{1}$$

Euclid 算法的应用

定理

如果给定整数a,b,则存在整数m,n使得(a, b)=ma+nb.

例子：

用辗转相除法求$a = 288, b = 158$的最大公因数和m, n使$ma + nb = (a, b)$. 由

$$288 = 158 \times 1 + 130, 158 = 130 \times 1 + 28,$$

$$130 = 28 \times 4 + 18, 28 = 18 \times 1 + 10,$$

$$18 = 10 \times 1 + 8, 8 = 2 \times 4$$

因此$(288, 158) = 2$.

Euclid 算法的应用

例子：

再由

$$2 = 10 - 8 = 10 - (18 - 10) = 10 \times 2 - 18$$

$$= (28 - 18)2 - 18 = 28 \times 2 - 18 \times 3 = 28 \times 2 - (130 - 28 \times 4) \times 3$$

$$= -130 \times 3 + 28 \times 14 = -130 \times 3 + (158 - 130) \times 14$$

$$= 14 \times 158 - 17 \times 130$$

$$= 14 \times 158 - 17(288 - 158) = 31 \times 158 - 17 \times 288$$

故$m = -17, n = 31.$

Euclid 算法的应用

Frobenius问题：

对s元($s \geq 2$)线性型$a_1x_1 + \cdots + a_sx_s, a_i > 0 (i = 1, \ldots, s), (a_1, \ldots, a_s) = 1$,存在一个仅与$a_1, \ldots, a_s$有关的整数$g(a_1, \ldots, a_s)$，凡大于$g(a_1, \ldots, a_s)$之数必可表为$a_1x_1 + \cdots a_sx_s (x_i \geq 0, i = 1, \ldots, s)$的形式，而$g(a_1, \ldots, a_s)$不能表为$a_1x_1 + \cdots a_sx_s (x_i \geq 0, i = 1, \ldots, s)$的形式。求出$g(a_1, \ldots, a_s)$的问题，即一次不定方程的Frobenius问题。

Euclid 算法的应用

线性联立方程的解：

设m, n为满足$1 \leq m < n$的整数，$a_{ij}, 1 \leq i \leq m, 1 \leq j \leq n$均为整数，求线性联立方程

$$\begin{cases} L_1 = a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ \qquad\qquad \ldots\ldots\ldots, \\ L_m = a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{cases} \tag{2}$$

的最小整数解。$\min(\max_{i=1,\ldots,n} |x_i|)$.

Euclid 算法可研究的问题

研究问题：

- 求最大公因子最好的算法；
- 求使得$ma + nb = (a, b)$的m, n的最好的算法；
- 求解Frobenius问题最好的算法；
- 求解线性联立方程最小解的上界和最好的算法。

主要内容

同余的定义

定义

对于固定的正整数m,若用m去除给定的整数a与b所得的余数相同，就称整数a与b对于模m同余，记为$a \equiv b \pmod{m}$.

同余的本质特征：

Z/mZ是一个由1生成的环，Z- 模。同余是局部性质。

同余的应用

应用

对于给定的整系数多项式$f(X)$,若$f(X) \equiv 0 \pmod{m}$没有解，则若$f(X) = 0$没有整数解。

孙子定理

Chinese remainder theorem：

Let $k \geq 2$. If $a_1, \ldots, a_k$ are integers and $m_1, \ldots, m_k$ are pairwise relatively prime positive integers, then there exists an integer x such that

$$x \equiv a_i \pmod{m_i} \quad \text{for all} \quad i = 1, \ldots, k.$$

If x is any solution of this set of congruences, then the integer y is also a solution if and only if

$$x \equiv y \pmod{m_1 \cdots m_k}.$$

研究问题

问题1

用局部方法求解一些特殊类型的不定方程的解。

孙子定理的应用和快速计算：

孙子定理的应用和求解孙子定理的解的快速算法。

主要内容

覆盖同余式组

定义

如果每一个整数都至少满足同余式组

$$x \equiv a_1 \pmod{n_1}, \ldots, x \equiv a_k \pmod{n_k},$$

$$1 < n_1 < \cdots < n_k, \quad 0 \leq a_i < n_i, i = 1, \ldots, k$$

中的一个，那就叫做一组覆盖同余式组。

著名猜测：

- 对任给$n_1 > 1$, 都存在覆盖同余式组。
- 不存在覆盖同余式组满足$2|n_1 \cdots n_k$.

主要内容

素数的定义与性质

素数的定义

A prime number is an integer p greater than 1 whose only positive divisors are 1 and p.

素数的性质：

1、If a prime number p divides a product of integers, then p divides one of the factors.

2、若p是一素数，a是任意整数，则有$p|a$或$(p, a) = 1$.

素数的判别

如何在多项式时间内判断给定的数是否是素数？AKS2002算法

主要内容

算术基本定理

Fundamental theorem of arithmetic

Every positive integer can be written uniquely (up to order) as the product of prime numbers.

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad , \alpha_i \geq 0, i = 1, \ldots, k, p_1 < \cdots < p_k.$$

$$n = \prod_{p|n} p^{v_p(n)},$$

$v_p(n)$ is the greatest integer r such that p^r divides n.

应用与问题

应用

可以用于求最大公因子和最小公倍数。

整数分解问题

如何在多项式时间内分解给定的正整数？目前还没有效算法，这是RSA算法的根基。

注解：

在自然数的子集

$$S = \{3k + 1 | k = 0, 1, 2, \ldots\}$$

中，如果定义其"素数"是恰有两个因子在S中，例如$4, 7, 10, 13, 19, 22, 25, 31, \ldots$都是$S$中的"素数"，那么$S$中的数100就有两种分解形式：

$$100 = 4 \times 25 = 10 \times 10.$$

这说明当素数的定义改变后，整数的唯一分解定理就不成立了。

问题1：整数唯一分解定理的本质是什么？

应用与问题

注解：

问题2： 对于一个数的集合，是否可以定义其中某些数为"素数"，使得在这个集合中数的唯一分解定理成立？

问题3： 如何判断给定一个正整数是否是素数？2002年AKS算法解决了这一问题：存在判断一个给定正整数为素数的多项式时间算法。

问题4： 分解给定的正整数n?目前还没有有效算法（大数分解问题,RSA算法的支柱）。

问题与结论

1、素数的个数是无穷的。
2、Dirichlet定理：设$k > 0, l > 0, (k, l) = 1$,那么形如$kn + l$的素数有无穷多个。
3、当$x = 0, 1, ,, 40$时，$x^2 - x + 41$都是素数。
4、不存在表示素数的多项式。
5、问题：形如$X^2 + 1$的素数是否无穷？
6、问题：是否存在多项式$f(x)$使得形如$f(x)$的素数无穷？

问题与结论

7、问题：寻找当$x = 1, 2, \ldots, N$时，$f(x)$都表示素数的二次或高次多项式$f(x)$。

8、问题：Mersenne素数$(2^p - 1)$的无穷性？Fermat 素数$(2^{2^n} + 1)$的无穷性？Fibonacci数列$(1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots)$ 中素数的无穷性?

主要内容

Euler定理

Euler函数的定义：

对任意正整数m，数列$0, 1, 2, \ldots, m-1$中与m互素的数的个数，称为Euler函数，记为$\varphi(m)$.

Euler函数的计算

设$n = \prod_{p|n} p^{v_p(n)}$，则$\varphi(n) = \prod_{p|n} p^{v_p(n)-1}(p-1)$.

Euler定理：

设m为一个正整数, a为与m互素的整数，则

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Euler定理的应用

数的整除特征：

- 一个整数被2（或5）整除当且仅当它的个位数字是2（或5）的倍数。
- 一个整数被4（或25）整除当且仅当它的末尾两位数字是4（或25）的倍数。
- 一个整数被8（或125）整除当且仅当它的末尾三位数字是8（或125）的倍数。
- 一个整数被3（或9）整除当且仅当它的各位数字之和是3（或9）的倍数。
- 一个整数$N = a_n \cdots a_1$被11当且仅当$a_n - a_{n-1} - \cdots + (-1)^{n-1} a_1$是11的倍数。

主要内容

二阶递归序列的的定义与性质

定义：

序列$u_n, v_n, n = 0, 1, 2, \ldots$定义为

$$u_{n+2} = Pu_{n+1} - Qu_n, \quad u_0 = 0, u_1 = 1,$$

$$u_{n+2} = Pv_{n+1} - Qv_n, \quad u_0 = 0, v_1 = P.$$

性质：

我们有：

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n = 0, 1, \ldots,$$

$$v_n = \alpha^n + \beta^n$$

α, β为二次方程$x^2 - Px + Q = 0, (P, Q) = 1$的两个根。

二阶递归序列的的定义与性质

定义:

Let $R > 0$, Q be nonzero coprime integers with $R - 4Q > 0$. Let α and β be the two roots of the trinomial $x^2 - \sqrt{R}x + Q$. The Lehmer sequence $\{P_n(R, Q)\}$ and the associated Lehmer sequence $\{Q_n(R, Q)\}$ with parameters R and Q are defined as follows:

$$P_n = P_n(R, Q) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & 2 \nmid n, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & 2|n \end{cases}$$

and

$$Q_n = Q_n(R, Q) = \begin{cases} (\alpha^n + \beta^n)/(\alpha + \beta), & 2 \nmid n, \\ \alpha^n + \beta^n, & 2|n \end{cases}$$

二阶递归序列的的定义与性质

性质：

Let $d = \gcd(m, n)$ for some integers m and n. We have

1. If $P_m \neq 1$, then $P_m | P_n$ if and only if $m | n$.
2. If $m \geq 1$, then $Q_m | Q_n$ if and only if n/m is an odd integer.
3. $\gcd(P_m, P_n) = U_d$.
4. $\gcd(Q_m, Q_n) = Q_d$ if m/d and n/d are odd, and 1 otherwise.
5. $\gcd(P_m, Q_n) = Q_d$ if m/d is even, and 1 otherwise.
6. $P_{2m} = 2P_mQ_m$.
7. For any prime p, $ord_p(P_{mp}/P_m) = 1$ or 0 which depends on $p | P_m a$ or not.

二阶递归序列的的定义与性质

性质：

1. $V_n^2 - \Delta U_n^2 = 4Q^n$.
2. If $m|n$, *then* $U_m|U_n$; if n/m is odd, then $V_m|V_n$。
3. $U_{2n} = U_n V_n$, $V_{2n} = V_n^2 - 2Q^n$.
4. If $d = \gcd(m, n)$, then $\gcd(U_m, U_n) = U_d$.
5. If $d = \gcd(m, n)$, then $\gcd(V_m, V_n) = V_d$ if m/d and n/d are odd, and 1, or 2 otherwise.
6. If p is a prime, and ω is the minimal positive integer with $p|U_\omega$ (defined ω to be the appearance of p in U_n), then for any positive integers k and λ, we have $p^{\lambda+1}|U_{k\omega p^\lambda}$.
7. If p is an odd prime with $p \nmid R\Delta$, $\varepsilon = (\frac{\Delta R}{p})$ is the Kronecker symbol, then $U_{p-\varepsilon} \equiv 0 \pmod{p}$.

二阶递归序列的的定义与性质

性质：

If p, q are odd primes, s and t are positive integers with $p^s||\Delta, q^t||R$, then

1. For $p^s > 3$, then $\mathrm{ord}_p U_m = \mathrm{ord}_p m, \mathrm{ord}_p V_m = 0$.
2. For $q^t > 3$, if m is odd, then $\mathrm{ord}_q U_m = 0$ and $\mathrm{ord}_q V_m / V_1 = \mathrm{ord}_q m$; if m is even, then $\mathrm{ord}_q V_m = 0$ and $\mathrm{ord}_q U_m = \mathrm{ord}_q m + t/2$.
3. Suppose $p^s = 3$ and λ is an integer with $3^\lambda||3R + \Delta$, then $\mathrm{ord}_3 V_m = 0$ and $\mathrm{ord}_3 U_{3m} = \lambda + \mathrm{ord}_3 m$, and if $3 \not| m$ then $\mathrm{ord}_3 U_m = 0$.
4. Suppose $q^t = 3$ and μ is an integer with $3^\mu||3\Delta + R$. If m is odd, then $\mathrm{ord}_3 U_m = 0$ and $\mathrm{ord}_3 V_{3m} / V_1 = \mathrm{ord}_3 m + \mu$, and $\mathrm{ord}_3 V_m / V_1 = 0$ with $3 \not| m$; if m is even, then $\mathrm{ord}_3 V_m = 0$ and $\mathrm{ord}_3 U_{3m} = \mathrm{ord}_3 m + \mu + 1/2$, and $\mathrm{ord}_3 U_m = 1/2$ with $3 \not| m$.

二阶递归序列的的定义与性质

性质：

1. Let $2||R$, if $2 \not| m$, then $\mathrm{ord}_2 U_m = \mathrm{ord}_2 V_m / V_1 = 0 (2 \not| m)$; if $2||m$, then $\mathrm{ord}_2 V_m = \mathrm{ord}_2 V_2$ and $\mathrm{ord}_2 U_m = 1/2$; if $4|m$, then $\mathrm{ord}_2 V_m = 1/2$ and $\mathrm{ord}_2 U_m = \mathrm{ord}_2 m - 1/2$.
2. Let $4|R$, if m is odd, then $\mathrm{ord}_2 U_m = 0$ and $\mathrm{ord}_2 V_m = \mathrm{ord}_2 V_1$; if m is even, then $\mathrm{ord}_2 U_m = \mathrm{ord}_2 m + \frac{1}{2}\mathrm{ord}_2 R - 1$ and $\mathrm{ord}_2 V_m = 1$.
3. 设p是一个素数，$p \not| 2Q$, 设u_l是序列$u_1, u_2, \ldots$中被p整除的下标最小的数，则$p|U_n \Longleftrightarrow l|n$.

主要内容

组合数$\binom{n}{k}$的整除性质

例1：

对任何正整数n，要使$n+1$个组合数$\binom{n}{0},\ldots,\binom{n}{n}$都为奇数当且仅当$n=2^k-1$.

例2：

对任何正整数$n,m>1,k\leq n+1$, 则$m^{n-k+1}|\binom{m^n}{k}$.

例3：初等数论100例21/100

设p 是一个素数, 则$\binom{n}{p}\equiv[\frac{n}{p}]\pmod p$；如果$p^s|[\frac{n}{p}]$，则$p^s|\binom{n}{p}$.

例4：初等数论100例36/100

对任何正整数n，求$\binom{2n}{1},\binom{2n}{3},\ldots,\binom{2n}{2n-1}$的最大公因子.

主要内容

一些例子

例1：初等数论100例3/100

设$n > 0, m > 0$，则和$S = \frac{1}{m} + \frac{1}{m+1} + \cdots + \frac{1}{m+n}$不是整数.

例2：初等数论100例4/100

设$m > n > 0, a_1 < a_2 < \ldots < a_s$是不超过$m$且与$n$互素的全部正整数，则和$S_m^n = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_s}$不是整数.

例3：初等数论100例15/100

证明对于$\leq 2n$的任何$n+1$个正整数中，至少有一个被另一个整除.

例4：初等数论100例16/100

设n 个整数$1 \leq a_1 < a_2 < \cdots < a_n \leq 2n$中任意两个整数$a_i, a_j$ 的最小公倍数$[a_i, a_j] > 2n$，则$a_1 > [\frac{2n}{3}]$.

一些例子

例5:

设$f(x) = a_0x^n + \cdots + a_{n-1}x + a_n$为整系数多项式，若$f(0), f(1)$都是奇数，那么$f(x) = 0$无整数解.

例6：

$2^p - 1, 2^q - 1$互素当且仅当p与q互素.

例7：

设a是正整数，则$\log_2 a$是有理数当且仅当$a = 2^m, m$ 为非负整数.

例8：$3x + 1$问题

一些例子

例9：初等数论100例59/100

设$n > 1, 2 \nmid n$，则对任意的$m, n \nmid m^{n-1} + 1$.

例10：初等数论100例70/100

设$p > 3$是一个素数，且设$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} + \frac{1}{p} = \frac{r}{ps}, (r, s) = 1$，则$p^3 | r - s$.

例11：

证明对任意$n \in \mathbb{N}$，$[(3 + \sqrt{5})^n]$是奇数.

例12：

求$[(\sqrt{3} + \sqrt{2})^{1998}]$ 的个位数字.

主要内容

数之谜

数的来源

我们知道数$\sqrt{2}$, π, $\sqrt{-1}$的来源，但我们并不知道数1和0的来源。

无理数与虚数

毕德哥拉斯学派的神秘的无理数，Gauss时期的$\sqrt{-1}$，等等。

正n边形

三等分角，直尺和圆规作图（正n 边形）（Galois理论）。

数之谜

超越数

神秘的超越数：1884年前后，我们有了π和e的超越性的证明。但我们不知道还有很多很多: Euler常数$\gamma = \lim_{n\to\infty}(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \ln n)$的无理性和超越性。Riemann-Zeta函数$\zeta(2n+1) = \sum_{k=1}^{\infty} \frac{1}{k^{2n+1}}$，我们仅知道$\zeta(3)$ 是无理数，$\zeta(5), \zeta(7), \zeta(9), \zeta(11)$中至少有一个是无理数。

孙子定理

韩信点兵：中国剩余定理(孙子定理).

主要内容

素数之谜

无穷性

素数的无穷性。

素数的判别

判断给定的一个正整数是否为素数，概率算法，2002年AKS算法。

算术级数中的素数

Dirichlet定理：$kn + l, \gcd(k, l) = 1, n = 1, 2, \ldots$中有无穷多个素数。

素数之谜

3个素数构成的等差数列

1939年，荷兰数学家Johannes van der Corput证明：有无穷多个由3个素数构成的等差数列。

Endre Szemeredi定理

1975年，匈牙利科学院的数学家施米列迪（Endre Szemeredi）证明了一个定理。如果简单地解释，这个定理的意思是在任何不会快速稀疏的整数子集中，肯定会有任意长度的等差数列。

格林和陶哲轩定理

2004年4月18日，格林和陶哲轩宣布：他们证明了"存在任意长度的素数等差数列"，也就是说，对于任意值K，存在K个成等差级数的素数。

Prime values of quadratic functions

Are there infinitely many primes of the form $a^2 + 1$?
Iwaniec has shown that there are infinitely many n for which $n^2 + 1$ is the product of at most two primes, and his results extend to other irreducible quadratics. With Friedlander he come close by shown that there are infinitely many primes of the form $x^2 + m^4$.

Primes of special forms

Primes of special form have been of perennial interest.
Mersenne primes $2^p - 1$, $p =$
$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217,$
Fermat numbers, $F_n = 2^{2^n} + 1$ are prime for $0 \leq n \leq 4$ and composite for $5 \leq n \leq 32$ and for many other values of n.
We are very unlikely to know for sure that the Fibonacci sequence

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots,$$

where $u_1 = u_2 = 1$ and $u_{r+1} = u_r + u_{r-1}$, contains infinitely many primes.

计算之谜

素数的多项式时间判定

给定一个正整数n, 是否存在多项式时间算法判定n 是素数？AKS算法。

RSA整数分解

给定一个正整数n, 是否存在多项式时间算法分解整数n？RSA算法的根基。

计算之谜

二次剩余的计算

给定一个素数p，是否存在多项式时间求解二次同余式

$$x^2 \equiv -1 \pmod{p}?$$

当假设GRH成立时，存在多项式时间算法。

二次非剩余的计算

给定一个素数p，是否存在多项式时间算法求出p的一个二次非剩余？
当假设GRH成立时，存在多项式时间算法。

主要内容

一次不定方程

Frobenius问题：

对s元($s \geq 2$)线性型$a_1x_1 + \cdots + a_sx_s, a_i > 0 (i = 1, \ldots, s), (a_1, \ldots, a_s) = 1$,存在一个仅与$a_1, \ldots, a_s$有关的整数$g(a_1, \ldots, a_s)$，凡大于$g(a_1, \ldots, a_s)$之数必可表为$a_1x_1 + \cdots a_sx_s (x_i \geq 0, i = 1, \ldots, s)$的形式，而$g(a_1, \ldots, a_s)$不能表为$a_1x_1 + \cdots a_sx_s (x_i \geq 0, i = 1, \ldots, s)$的形式。求出$g(a_1, \ldots, a_s)$的问题，即一次不定方程的Frobenius问题。

致谢

谢 谢 大 家!