初等数论 第2讲

孙智伟

南京大学数学学院

邮箱：zwsun@nju.edu.cn

个人主页：http://maths.nju.edu.cn/~zwsun

2024年8月7日

第二讲内容

第二讲　同余式、抽屉原理及其他

§2.1 同余式

§2.2 抽屉原理及其他技巧

§2.3 二次剩余理论

§2.4 a模m的次数

§2.5 一些著名的猜想或定理

同余式基本性质

设m为正整数。对于整数a, b, 如果$a - b$为m的倍数，则称a与b模m同余(a is congruent to b modulo m)，记为$a \equiv b \pmod{m}$, m叫做这个同余式的**模**(modulus).

模m同余关系是$\mathbb{Z}$上的等价关系，即它满足自反性、对称性与传递性:

$$a \equiv a \pmod{m};\ a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m};$$

$$a \equiv b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}.$$

模m同余式还可象等式那样左右两边分别相加减或相乘。

$$a \equiv b \pmod{m} \text{ 且 } c \equiv d \pmod{m}$$

$$\Rightarrow a \pm c \equiv b \pm d \pmod{m},\ ac \equiv bd \pmod{m},$$

这是因为

$$(a \pm c) - (b \pm d) = (a - b) \pm (c - d),\ ac - bd = (a - b)c + b(c - d).$$

十进制数模9的特点

例题： 设$n \in \mathbb{N}$的十进制表示为$a_k a_{k-1} \cdots a_0$ (其中$a_0, \ldots, a_k \in \{0, \ldots, 9\}$), 则

$$n \equiv \sum_{i=0}^{k} a_i \pmod 9.$$

特别地, $9 \mid n \iff 9 \mid \sum_{i=0}^{k} a_i$, 也有$3 \mid n \iff 3 \mid \sum_{i=0}^{k} a_i$.

证明：$10 \equiv 1 \pmod 9$, 两边自乘i次得

$$10^i \equiv 1^i = 1 \pmod 9.$$

因此

$$n = \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i \pmod 9.$$

费马小定理

定理1.1 (费马小定理, Fermat's little theorem). 设p为素数，a为整数。则$a^p \equiv a \pmod{p}$, 亦即$p \nmid a$ 时$a^{p-1} \equiv 1 \pmod{p}$.

证明 (Euler): p整除$a^p - a = a(a^{p-1} - 1)$但$p \nmid a$时必$a^{p-1} \equiv 1 \pmod{p}$. 故只要证$a^p \equiv a \pmod{p}$. 如果$n^p \equiv n \pmod{p}$, 则$(-n)^p = (-1)^p n^p \equiv -n \pmod{p}$.

下面只要对$n = 0, 1, 2, \ldots$证明$n^p \equiv n \pmod{p}$. 显然$0^p \equiv 0 \pmod{p}$. 假如$n^p \equiv n \pmod{p}$, 则

$$(n+1)^p = n^p + \sum_{k=1}^{p-1} \binom{p}{k} n^k + 1^p \equiv n + 1 \pmod{p},$$

因为$1 \leqslant k \leqslant p-1$时$p$整除$k!\binom{p}{k} = p(p-1)\ldots(p-k+1)$从而$p \mid \binom{p}{k}$.

Fermat商

例题. 求2^{2024}模37的最小非负余数。

解： 依Fermat小定理, $2^{36} \equiv 1 \pmod{37}$. 作带余除法$2024 = 36 \times 56 + 8$, 于是

$$2^{2024} = (2^{36})^{56} \times 2^8 \equiv 2^8 = 2^5 \times 2^3 \equiv -5 \times 2^3 \equiv -3 \equiv 34 \pmod{37}.$$

设素数p不整除整数a, 我们把$q_p(a) = (a^{p-1} - 1)/p \in \mathbb{Z}$ 叫做以a为底的Fermat商. 如果整数a与b都不被p整除, 则

$$q_p(ab) = b^{p-1}\frac{a^{p-1} - 1}{p} + \frac{b^{p-1} - 1}{p} \equiv q_p(a) + q_p(b) \pmod{p}.$$

Lucas同余式

定理1.2 [E. Lucas, 1878]. 设p为素数. 对于$k, n \in \mathbb{N}$与$s, t \in \{0, \ldots, p-1\}$, 我们有

$$\binom{pn+s}{pk+t} \equiv \binom{n}{k}\binom{s}{t} \pmod{p}.$$

等价地, 如果$a_i, b_i \in \{0, \ldots, p-1\}$ $(i = 0, \ldots, k)$, 则

$$\binom{\sum_{i=0}^{k} a_i p^i}{\sum_{i=0}^{k} b_i p^i} \equiv \prod_{i=0}^{k} \binom{a_i}{b_i} \pmod{p}.$$

证明: $(1+x)^p = 1 + x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k \equiv 1 + x^p \pmod{p}$.

因此

$$(1+x)^{pn+s} \equiv (1+x)^s (1+x^p)^n \pmod{p}.$$

比较这个等式两边展开式中x^{pk+t}中系数, 我们得到

$$\binom{pn+s}{pk+t} \equiv \binom{s}{t}\binom{n}{k} \pmod{p}.$$

Euler函数与简化剩余系

对于正整数m, $1, \ldots, m$中与m互素的数个数记为$\varphi(m)$. φ叫做Euler函数(Euler's totient function).

例如：$\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = \varphi(6) = 2$.

$m > 2$时$\varphi(m)$为偶数，因为$m/2$不是与m互素的整数，且$(a, m) = 1 \iff (m - a, m) = 1$.

对于素数p及正整数n,

$$\varphi(p^n) = |\{1 \leqslant a \leqslant p^n : \ p \nmid a\}| = p^n - |\{1 \leqslant a \leqslant p^n : \ p \mid a\}| = p^n - p^{n-1}.$$

对于$a, q \in \mathbb{Z}$, 显然$(a + mq, m) = 1 \iff (a, m) = 1$.

如果整数$a_1, \ldots, a_m$模正整数m两两不同余，则称$\{a_1, \ldots, a_m\}$为**模m的完全剩余系**.

如果整数$a_1, \ldots, a_{\varphi(m)}$都与正整数$m$互素且模$m$两两不同余，则称$\{a_1, \ldots, a_m\}$为**模$m$的简化剩余系**.

关于Euler函数的例题

例题：对于正整数n证明

$$\sum_{d|n}\varphi(d)=n \text{ 且 } \sum_{d=1}^{n}\varphi(d)\left\lfloor\frac{n}{d}\right\rfloor=\frac{n(n+1)}{2}.$$

证明：每个m/n $(1\leqslant m\leqslant n)$可唯一地表成既约分数$c/d$ $(1\leqslant c\leqslant d$且$(c,d)=1)$的形式，这儿$d\mid n$. 因此

$$\bigcup_{d|n}\left\{\frac{c}{d}:\ 1\leqslant c\leqslant d\ \&\ (c,d)=1\right\}=\left\{\frac{m}{n}:\ m=1,\ldots,n\right\}.$$

两边计算基数得$\sum_{d|n}\varphi(d)=n$.

$$\sum_{d=1}^{n}\varphi(d)\left\lfloor\frac{n}{d}\right\rfloor=\sum_{d=1}^{n}\varphi(d)\sum_{\substack{k=1\\ d|k}}^{n}1=\sum_{k=1}^{n}\sum_{d|k}\varphi(d)=\sum_{k=1}^{n}k=\frac{n(n+1)}{2}.$$

Euler推广Fermat小定理

定理1.3 (Euler定理). 设整数a与正整数m互素，则

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

证明：设$\{a_1, \ldots, a_{\varphi(m)}\}$为模$m$的一个简化剩余系。对于$1 \leqslant i \leqslant m$, aa_i也与m互素。注意

$$aa_i \equiv aa_j \pmod{m} \iff m \mid a(a_i - a_j) \iff m \mid a_i - a_j \iff i = j.$$

因此$\{aa_i : i = 1, \ldots, \varphi(m)\}$也是模$m$的简化剩余系。于是

$$\prod_{i=1}^{\varphi(m)} aa_i \equiv \prod_{\substack{x=1 \\ (x,m)=1}}^{m} x \equiv \prod_{i=1}^{\varphi(m)} a_i \pmod{m},$$

从而m整除$(a^{\varphi(m)} - 1)a_1 \cdots a_{\varphi(m)}$. 而$a_1 \cdots a_{\varphi(m)}$与$m$互素，故$m \mid a^{\varphi(m)} - 1$.

线性同余方程

对于正整数m与整系数多项式$P(x_1,\ldots,x_n)$, $q_1,\ldots,q_n\in\mathbb{Z}$时

$$P(x_1+mq_1,\ldots,x_n+mq_n)\equiv P(x_1,\ldots,x_n)\pmod m.$$

同余方程$P(x_1,\ldots,x_n)\equiv 0\pmod m$的解数指

$$|\{\langle x_1,\ldots,x_n\rangle : 0\leqslant x_1,\ldots,x_n\leqslant m-1 \text{ 且 } P(x_1,\ldots,x_n)\equiv 0\pmod m\}|.$$

任给$a_1,\ldots,a_n,b\in\mathbb{Z}$,

$$\begin{aligned}
& a_1x_1+\cdots a_nx_n\equiv b\pmod m\text{有整数解}\\
\iff\ & a_1x_1+\cdots+a_nx_n+mx_{n+1}=b\text{有整数解}\\
\iff\ & b\in a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}+m\mathbb{Z}=(a_1,\ldots,a_n,m)\mathbb{Z}\\
\iff\ & (a_1,\ldots,a_n,m)\mid b.
\end{aligned}$$

$(a,m)=1$且$b\in\mathbb{Z}$时,

$$ax\equiv b\pmod m\iff x\equiv a^{\varphi(m)-1}b\pmod m.$$

线性同余方程组

同余方程组起源于中国南北朝时期（公元五世纪）的著作《孙子算经》中一道名题：“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。”此题相当于要求解同余方程组

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

在西方，同余的概念直到17世纪才在Fermat小定理(参看第一章第5讲)中出现，现在流行的同余式记号是Gauss在19世纪引入的。

中国剩余定理

定理1.4 (中国剩余定理, Chinese Remainder Theorem). 设正整数$m_1, \ldots, m_n$两两互素。任给$a_1, \ldots, a_n \in \mathbb{Z}$, 同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \cdots\cdots\cdots\cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

的整数通解为

$$x \equiv \sum_{i=1}^{n} a_i M_i M_i^* \pmod{M},$$

这儿$M = \prod_{i=1}^{n} m_i$, $M_i = \frac{M}{m_i}$, $M_i^* \in \mathbb{Z}$且$M_i M_i^* \equiv 1 \pmod{m_i}$.

中国剩余定理现在这个一般形式及其证明首次出现于南宋数学家秦九韶(1202-1261)的名著《数书九章》(1247年出版)，在西方这结果直到十九世纪才由Gauss等人发现。

利用中国剩余定理的例题

例题： 求解同余式组

$$\begin{cases} x \equiv 3 \pmod 5, \\ x \equiv 4 \pmod 7, \\ x \equiv 5 \pmod 9. \end{cases}$$

解：$5, 7, 9$两两互素，$M = 5 \times 7 \times 9 = 315$.

$M_1 = 7 \times 9 = 63 \equiv 3 \pmod 5$，$M_1 x \equiv 1 \pmod 5$有解$x = 2$，可取$M_1^* = 2$. $M_2 = 5 \times 9 = 45 \equiv 3 \pmod 7$，$M_2 x \equiv 1 \pmod 7$有解$x = -2$，故可取$M_2^* = -2$. $M_3 = 5 \times 7 = 35 \equiv -1 \pmod 9$，$M_3 x \equiv 1 \pmod 9$有解$x = -1$，故可取$M_3^* = -1$. 所求通解为

$$\begin{aligned} x &\equiv 3M_1M_1^* + 4M_2M_2^* + 5M_3M_3^* \\ &\equiv 3 \times 63 \times 2 + 4 \times 45 \times (-2) + 5 \times 35 \times (-1) \\ &\equiv 63 - 45 + 4 \times 35 = 158 \pmod{315}. \end{aligned}$$

Wilson定理

定理1.5 (Wilson定理). 对于整数$p > 1$,

$$p\text{为素数} \iff (p-1)! \equiv -1 \pmod{p}.$$

证明：$\Leftarrow$: 设$(p-1)! \equiv -1 \pmod{p}$, 则$((p-1)!, p) = (-1, p) = 1$, 于是$1 < d < p$时$(d, p) = 1$从而$d \nmid p$. 因此$p$无真因子, 即$p$为素数。

$\Rightarrow$: $p = 2$为素数且$(2-1)! = 1 \equiv -1 \pmod{2}$.

下设p为奇素数。对于$a \in \{1, \ldots, p-1\}$, 有唯一的$1 \leqslant x \leqslant p-1$使得$ax \equiv 1 \pmod{p}$, 把这个$x$记为$a^*$, 叫做$a$模$p$的（乘法）逆元。注意

$$a^* = a \iff a^2 \equiv 1 \pmod{p} \iff p \mid (a-1)(a+1) \iff a \in \{1, p-1\}.$$

因此可把$\{2, \ldots, p-2\}$分成$(p-3)/2$个互逆对$\{x_i, x_i^*\}$ $(i = 1 \ldots, \frac{p-3}{2})$. 于是

$$(p-1)! = 1 \times (p-1) \prod_{i=1}^{(p-3)/2} x_i x_i^* \equiv -1 \pmod{p}.$$

一个推论

推论1.1. 设p为奇素数, 则

$$\left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

证明：

$$(p-1)! = \prod_{k=1}^{(p-1)/2} k(p-k)$$

$$\equiv \prod_{k=1}^{(p-1)/2} (-k^2) = (-1)^{(p-1)/2} \left(\frac{p-1}{2}!\right)^2 \pmod{p}.$$

再结合Wilson定理即得所要结果。

§2.2. 抽屉原理及其他技巧

组合中的抽屉原理(又称鸽笼原理)断言把$n+1$个物体放入n个抽屉中后必有一个抽屉包含至少两个物体. 此原理在数学上的首次使用出现于Dirichlet下述结果的证明中.

定理2.1 (Dirichlet) 任给无理数θ, 有无穷多个既约有理数$\frac{x}{y}$(其中$x \in \mathbb{Z},\ y \in \mathbb{Z}_+$ 且$(x,y)=1$) 使得

$$\left|\theta - \frac{x}{y}\right| < \frac{1}{y^2}.$$

证明：任给一个正整数n_0, 区间$[0,1)$是n_0个两两不相交的长为$\frac{1}{n_0}$的小区间

$$\left[0, \frac{1}{n_0}\right),\ \left[\frac{1}{n_0}, \frac{2}{n_0}\right),\ \cdots,\ \left[\frac{n_0-1}{n_0}, 1\right)$$

的并. 对实数α, 称$\{\alpha\} = \alpha - \lfloor\alpha\rfloor$为$\alpha$的小数部分. $0, \{\theta\}, \cdots, \{n_0\theta\}$落入上述$n_0$个小区间中, 依抽屉原理有$0 \leqslant k < l \leqslant n_0$ 使得$\{k\theta\}$与$\{l\theta\}$落入同一个小区间中.

继续证明

于是

$$|l\theta - \lfloor l\theta \rfloor - (k\theta - \lfloor k\theta \rfloor)| = |\{l\theta\} - \{k\theta\}| < \frac{1}{n_0},$$

亦即

$$\left|\theta - \frac{\lfloor l\theta \rfloor - \lfloor k\theta \rfloor}{l-k}\right| < \frac{1}{n_0(l-k)}.$$

令

$$x_0 = \frac{\lfloor l\theta \rfloor - \lfloor k\theta \rfloor}{(l-k, \lfloor l\theta \rfloor - \lfloor k\theta \rfloor)},\ y_0 = \frac{l-k}{(l-k, \lfloor l\theta \rfloor - \lfloor k\theta \rfloor)}.$$

则$(x_0, y_0) = 1$, $0 < y_0 \leqslant l-k \leqslant n_0$, 而且

$$\left|\theta - \frac{x_0}{y_0}\right| < \frac{1}{n_0(l-k)} \leqslant \frac{1}{n_0 y_0} \leqslant \frac{1}{y_0^2}.$$

继续证明

取正整数$n_1 > 1/|\theta - \frac{x_0}{y_0}|$. 依上法, 又有既约有理数$\frac{x_1}{y_1}$ (其中$x_1 \in \mathbb{Z}$, $y_1 \in \mathbb{Z}^+$且$(x_1, y_1) = 1$), 使得

$$\left|\theta - \frac{x_1}{y_1}\right| < \frac{1}{n_1 y_1} \leqslant \frac{1}{y_1^2}.$$

再取正整数$n_2 > 1/|\theta - \frac{x_1}{y_1}|$ 与既约有理数$\frac{x_2}{y_2}$ (其中$x_2 \in \mathbb{Z}$, $y_2 \in \mathbb{Z}^+$且$(x_2, y_2) = 1$), 使得

$$\left|\theta - \frac{x_2}{y_2}\right| < \frac{1}{n_2 y_2} \leqslant \frac{1}{y_2^2}.$$

注意

$$\left|\theta - \frac{x_0}{y_0}\right| > \frac{1}{n_1} > \left|\theta - \frac{x_1}{y_1}\right| > \frac{1}{n_2} > \left|\theta - \frac{x_2}{y_2}\right|.$$

继续进行下去, 我们就找到了无穷多对既约有理数$\frac{x_0}{y_0}$, $\frac{x_1}{y_1}$, $\frac{x_2}{y_2}$, $\cdots$ 使得对$i = 0, 1, 2, \cdots$都有

$$\left|\theta - \frac{x_i}{y_i}\right| < \frac{1}{y_i^2} \text{ 且 } \left|\theta - \frac{x_i}{y_i}\right| > \left|\theta - \frac{x_{i+1}}{y_{i+1}}\right|.$$

Pell方程

推论2.1. 设$d \in \mathbb{Z}^+$不是完全平方，则有非零整数m使得程$x^2 - dy^2 = m$有无穷多组整数解.

证明：$\sqrt{d}$为无理数。依定理2.1, 有无穷多个有序对$(x, y) \in \mathbb{Z} \times \mathbb{Z}^+$ 使得

$$\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{y^2}, \quad \text{即 } |x - \sqrt{d}\, y| < \frac{1}{y},$$

于是

$$\begin{aligned} |x^2 - dy^2| &= |x - \sqrt{d}\, y| \cdot |(x - \sqrt{d}\, y) + 2\sqrt{d}\, y| \\ &< \frac{1}{y}\left(\frac{1}{y} + 2\sqrt{d}\, y\right) \leqslant 2\sqrt{d} + 1. \end{aligned}$$

因此有整数m使得$|m| < 2\sqrt{d} + 1$且方程$x^2 - dy^2 = m$有无穷多组整数解. 由于$\sqrt{d}$不是有理数, m不等于0.

注：$d \in \mathbb{Z}^+$不是平方数时Pell方程$x^2 - dy^2 = 1$有无穷多组整数解. 如果(x_0, y_0)为解，则由$(x_0 + y_0\sqrt{d})^m = x_m + y_m\sqrt{d}$给出的$(x_m, y_m)$也是.

Erdős-Szekeres定理

定理2.2 (Erdős-Sekeres, 1935). 实数列$a_1, \ldots, a_{n^2+1}$必含长为$n+1$的单调子序列。

证明：假设$a_1, \ldots, a_{n^2+1}$不含长为$n+1$的单调不减子序列，对$1 \leqslant i \leqslant n^2+1$让$\ell_i$表示起始相为$a_i$的最长的单调不减子序列长度, 则$1 \leqslant \ell_i \leqslant n$. 注意$\{\ell_1, \ldots, \ell_{n^2+1}\} \subseteq \{1, \ldots, n\}$. 必有$1 \leqslant k \leqslant n$使得它在$\ell_1, \ldots, \ell_{n^2+1}$中出现次数对于$n$. 设

$$\ell_{i_1} = \ell_{i_2} = \cdots = \ell_{i_{n+1}} = k \ (1 \leqslant i_1 < i_2 < \cdots < i_{n+1} \leqslant n^2+1).$$

如果$a_{i_j} < a_{i_{j+1}}$, 则应有$\ell_{i_j} \geqslant \ell_{i_{j+1}} + 1$. 因此

$$a_{i_1} \geqslant a_{i_2} \geqslant \cdots \geqslant a_{i_{n+1}},$$

这是$\{a_i\}_{i=1}^{n^2+1}$的单调不增子序列.

两整数平方和

两个整数平方和对乘法封闭，因为

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

定理2.3 (由Fermat猜出，Euler首先证明). 素数$p \equiv 1 \pmod 4$可表成两个整数的平方和。

证明 (Hermite): 令$q = \frac{p-1}{2}!$. 依Wilson定理的推论, $q^2 \equiv (-1)^{(p+1)/2} = -1 \pmod p$. 考察诸$x + qy$ $(0 \leqslant x, y \leqslant \lfloor\sqrt{p}\rfloor)$. 由于$(\lfloor\sqrt{p}\rfloor + 1)^2 > \sqrt{p}^2 = p$, 依抽屉原理上述数中必有两个模$p$同余。假设$x_1 + qy_1 \equiv x_2 + qy_2 \pmod p$, 这儿$0 \leqslant x_1, y_1, x_2, y_2 \leqslant \lfloor\sqrt{p}\rfloor$, 且$(x_1, y_1)$与$(x_2, y_2)$是不同的有序对. 令$x = |x_1 - x_2|$, $y = |y_1 - y_2$, 则$x^2 + y^2 > 0$, 而且

$$x^2+y^2 = (x_1-x_2)^2+(y_1-y_2)^2 = q^2(y_2-y_1)^2+(y_1-y_2)^2 \equiv 0 \pmod p.$$

注意$0 < x^2 + y^2 < \sqrt{p}^2 + \sqrt{p}^2 = 2p$, 故必定$x^2 + y^2 = p$.

其他应用抽屉原理的例子

例2.1. 任给n个正整数$a_1, \ldots, a_n$, 其中必有若干个之和为n倍数。

证明：模n的最小非负余数只能是$0, 1, \ldots, n-1$之一，故$n+1$个部分和

$$s_0 = 0,\ s_1 = a_1,\ s_2 = a_1 + a_2,\ s_n = a_1 + a_2 + \cdots + a_n$$

中必有两个模n同余。设$s_j \equiv s_k \pmod{n}$, 这里$0 \leqslant j < k \leqslant n$. 则

$$a_{j+1} + \cdots + a_k = s_k - s_j \equiv 0 \pmod{n}.$$

例2.2. 不超过$2n$的正整数$a_1, \ldots, a_{n+1}$中必有一个整除另一个。

证明：不妨设$a_1 = 2^{\alpha_1} q_1 \leqslant \cdots \leqslant a_{n+1} = 2^{\alpha_{n+1}} q_{n+1}$, 其中诸$\alpha_i$为自然数，诸$q_i$为正奇数。考虑到$q_1, \ldots, q_{n+1}$都属于$\{1, 3, \ldots, 2n-1\}$, 必有$1 \leqslant i < j \leqslant n+1$使得$q_i = q_j$. 于是$\alpha_i \leqslant \alpha_j$且$a_i \mid a_j$.

$\frac{1}{m}+\frac{1}{m+1}+\cdots+\frac{1}{m+n}\notin\mathbb{Z}$

例2.3. 任给正整数m与n, 证明$\frac{1}{m}+\frac{1}{m+1}+\cdots+\frac{1}{m+n}\notin\mathbb{Z}$.

证明：对$0=1,\ldots,n$, 写$m+i=2^{a_i}q_i$, 其中$a_i\in\mathbb{N}$, q_i为正奇数. 由于$m,m+1,\ldots,m+n$中有偶数，$a=\max\{a_0,\ldots,a_n\}$是个正整数。假如$0\leqslant i<j\leqslant n$且$a_i=a_j=a$, 则因$m+i<m+j$有$q_i<q_j$. 而$q_i,q_j$均为奇数，故有偶数$q$使得$q_i<q<q_j$, 从而

$$m+i=2^aq_i<2^aq<2^aq_j=m+j.$$

写$2^aq=m+k$, 则$i<k<j$且$a_k\geqslant a+1$. 这与a的定义矛盾。

由上，有唯一的$0\leqslant j\leqslant n$使得$a_j=a$. 于是有$x\in\mathbb{Z}$使得

$$S:=\sum_{i=0}^{n}\frac{1}{m+i}=\sum_{i=0}^{n}\frac{1}{2^{a_i}q_i}=\frac{1}{2^aq_j}+\frac{x}{2^{a-1}\prod_{i\neq j}q_i},$$

从而$S\times2^a\prod_{i=0}^{n}q_i=2xq_j+\prod_{i\neq j}q_i$, 如果$S\in\mathbb{Z}$, 则上述等式左边为偶数，右边为奇数，可得矛盾。因此S不是整数.

埃及分数

形如 $\frac{1}{n}$ （其中n为正整数）的分数叫单位分数。古埃及人考虑把正有理数表成不同单位分数之和（这样的有理数叫埃及分数），例如：他们注意到

$$\frac{2}{35}=\frac{1}{30}+\frac{1}{42},\quad \frac{10}{73}=\frac{1}{11}+\frac{1}{22}+\frac{1}{1606}.$$

1202年Fibonacci证明每个正有理数都可表成不同的单位分数之和，这是因为

$$\frac{1}{n}-\frac{1}{n+1}=\frac{(n+1)-n}{n(n+1)}=\frac{1}{n(n+1)}.$$

由此结论知调和级数$\sum_{n=1}^{\infty}\frac{1}{n}$发散.

例2.4. 把3/5表成不同单位分数之和。

$$\frac{3}{5}=\frac{1}{5}+\frac{2}{5}=\frac{1}{5}+2\left(\frac{1}{6}+\frac{1}{30}\right)=\frac{1}{5}+\frac{1}{3}+\frac{1}{15}.$$

§2.3. 二次剩余理论

对于奇素数p及不被p整除的整数a, 如果$x^2 \equiv a \pmod{p}$有整数解，则称a为模p的**平方剩余**，否则称a为模p的**平方非剩余**.

任何整数x可写成$pq + r$的形式，这儿$q, r \in \mathbb{Z}$且$|r| \leqslant \frac{p-1}{2}$. 于是

$$x^2 = (pq + r)^2 \equiv |r|^2 \pmod{p}.$$

另一方面，$0 \leqslant k < l \leqslant (p-1)/2$时

$$l^2 - k^2 = (l-k)(l+k) \not\equiv 0 \pmod{p}.$$

因此，任何平方数与

$$0^2,\ 1^2,\ \cdots,\ \left(\frac{p-1}{2}\right)^2$$

中恰好一个同余。模p的一个简化剩余系中平方剩余与平方非剩余各有$\frac{p-1}{2}$个.

例如: $1, 2, 3, 4$中1与4为模5的平方剩余, 2与3为模5的平方非剩余。

Euler的一个引理

引理3.1 (Euler) 设p为奇素数, 则有正整数$m < p$使得pm可表示成$x^2 + y^2 + 1$, 其中$x, y \in \mathbb{Z}$.

证明：由于模p的一个简化剩余系中恰有$(p-1)/2$个平方非剩余，$\frac{p+1}{2}$个数

$$-1 - 0^2, -1 - 1^2, \cdots, -1 - \left(\frac{p-1}{2}\right)^2$$

中必有一个与某平方数模p同余, 即有$x, y \in \{0, 1, \cdots, \frac{p-1}{2}\}$使得$-1 - x^2 \equiv y^2 \pmod{p}$. 写$x^2 + y^2 + 1 = pm$, 这里$m \in \mathbb{Z}_+$. 由于

$$pm = x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2,$$

必定$m < p$.

四平方和定理

定理3.1 (Lagrange四平方和定理). 每个$n \in \mathbb{N} = \{0, 1, 2, \ldots\}$可表成四个自然数的平方和。

A. Diophantus (丢番图，公元前299-215或285-201) 首先意识到这个结果并在其著作《Arithmetica(算术)》中给了及几个例子。1621年，法国人Bachet把Diophantus著作译成拉丁文时加注释陈述出四平方和定理（只是个猜想）。

1748年，Euler（欧拉）发现四平方和恒等式

$$\begin{aligned}&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ =&(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3)^2\\ &+ (x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)^2 + (x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2)^2,\end{aligned}$$

从而把问题归结为素数表成四平方和。Euler还证明了上述引理3.1.

1770年，Lagrange在Euler多年工作基础上证明了每个自然数可表成四个整数的平方和。

1-3-5猜想

1-3-5猜想(悬赏1350美元) (孙智伟, 2016年4月9日): 任何$n \in \mathbb{N}$可表成$x^2+y^2+z^2+w^2$(其中$x,y,z,w \in \mathbb{N}$)使得$x+3y+5z$为平方数。

有唯一表示的几个例子:

$$\begin{aligned} 7 &= 1^2+1^2+1^2+2^2 \text{ 且 } 1+3\times 1+5\times 1 = 3^2,\\ 8 &= 0^2+2^2+2^2+0^2 \text{ 且 } 0+3\times 2+5\times 2 = 4^2,\\ 31 &= 5^2+2^2+1^2+1^2 \text{ 且 } 5+3\times 2+5\times 1 = 4^2,\\ 43 &= 1^2+5^2+4^2+1^2 \text{ 且 } 1+3\times 5+5\times 4 = 6^2. \end{aligned}$$

2020年，1-3-5猜想被葡萄牙Porto大学António Machiavelo和他的博士生Nikolaos Tsopanidis所证明。他们的论文*"Zhi-Wei Sun's 1-3-5 Conjecture and Variations"*发表于J. Number Theory 222(2021), 1-20.

24-猜想与四平方猜想

24-猜想 (孙智伟，2016). 每个$n \in \mathbb{N}$可表示成

$$x^2 + y^2 + z^2 + w^2 \ (x, y, z, w \in \mathbb{N})$$

使得x与$x + 24y$都是平方数。

我为此猜想的证明悬赏2400美元。

四平方猜想 (孙智伟，2019). 每个整数$n > 1$可表示成

$$x^2 + y^2 + (2^a 3^b)^2 + (2^c 5^d)^2,$$

其中$x, y, a, b, c, d \in \mathbb{N}$.

我为此猜想的证明悬赏2500美元。

悬赏3500美元的猜想

三幂五幂猜想 (孙智伟, 2018年4月28日). 任何整数$n > 1$可表成$a^2 + b^2 + 3^c + 5^d$, 其中$a, b, c, d \in \mathbb{N} = \{0, 1, 2, \ldots\}$.

注记. 我将此猜想验证到2×10^{10}, 并宣布为此猜想的第一个证明悬赏3500美元。

三个有唯一表示法的例子：

$$\begin{aligned} 2 &= 0^2 + 0^2 + 3^0 + 5^0, \\ 5 &= 0^2 + 1^2 + 3^1 + 5^0, \\ 25 &= 1^2 + 4^2 + 3^1 + 5^1. \end{aligned}$$

Legendre符号

设p为奇素数，整数a对p的Legendre符号如下定义：

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{如果}a\text{为模}p\text{的平方剩余,} \\ -1 & \text{如果}a\text{为模}p\text{的平方非剩余,} \\ 0 & \text{如果 } p \mid a. \end{cases}$$

显然

$$a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Euler判别条件

定理3.2 (Euler判别条件). 设p为奇素数，$a \in \mathbb{Z}$. 则

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

证明：如果$p \mid a$, 则$a^{(p-1)/2} \equiv 0 = (\frac{a}{p}) \pmod{p}$. 下设$p \nmid a$. 如果$x^2 \equiv a \pmod{p}$, 则

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 = \left(\frac{a}{p}\right) \pmod{p}.$$

如果a为模p的平方非剩余，则$1 \leqslant k \leqslant (p-1)/2$时$ak^2 \equiv x^2 \pmod{p}$无解(不然, $a \equiv a(kk^*)^2 \equiv (k^*x)^2 \pmod{p}$, 矛盾)。因此

$$\{1^2, \ldots, ((p-1)/2)^2, a1^2, \ldots, a((p-1)/2)^2\}$$

为模p的一个简化剩余系，从而

$$a^{(p-1)/2}(p-1)!^2 \equiv \prod_{k=1}^{(p-1)/2} k(-k) \times ak(-k) \equiv (p-1)! \pmod{p}.$$

再利用Wilson定理得到$a^{(p-1)/2} \equiv -1 = (\frac{a}{p}) \pmod{p}$.

推论

推论3.1 设p为奇素数。

(i) 对任何$a, b \in \mathbb{Z}$有$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(ii) 我们有

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{如果 } p \equiv 1 \pmod 4, \\ -1 & \text{如果 } p \equiv 3 \pmod 4. \end{cases}$$

证明：(i) 由Euler判别条件知

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p.$$

而$\left|\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right| \leqslant 2 < p$, 故有$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(ii) 由Euler判别条件知

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p,$$

从而$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Gauss引理

引理3.2 (Gauss引理). 设奇素数p不整除整数a, 则

$$\left(\frac{a}{p}\right) = (-1)^{|\{1\leqslant k\leqslant \frac{p-1}{2}:\ \{\frac{ka}{p}\}>\frac{1}{2}\}|}. \qquad (*)$$

证明: 对每个$1 \leqslant k \leqslant (p-1)/2$ 有唯一的$k' \in \mathbb{Z}$使得$ka \equiv k' \pmod p$且$|k'| \leqslant (p-1)/2$. $1 \leqslant k < l \leqslant (p-1)/2$时$ka \not\equiv \pm la \pmod p$, 从而$|k'| \neq |l'|$. 因此

$$\{|k'|:\ k = 1, \ldots, (p-1)/2\} = \{1, \ldots, (p-1)/2\}.$$

显然$\{\frac{ka}{p}\} > \frac{1}{2}$当且仅当$k' < 0$. 故有

$$\left(\frac{a}{p}\right)\frac{p-1}{2}! \equiv \prod_{k=1}^{(p-1)/2} ka \equiv (-1)^{|\{1\leqslant k\leqslant \frac{p-1}{2}:\ k'<0\}|}\prod_{k=1}^{(p-1)/2} |k'|$$

$$\equiv (-1)^{|\{1\leqslant k\leqslant \frac{p-1}{2}:\ \frac{ka}{p}>\frac{1}{2}\}|}\frac{p-1}{2}! \pmod p.$$

从而$(*)$成立。

$(\frac{2}{p})$的确定

定理3.3. 任给奇素数p, 我们有

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{若} p \equiv \pm 1 \pmod 8, \\ -1 & \text{若} p \equiv \pm 3 \pmod 8. \end{cases}$$

证明: $p = 8q \pm 1$时,

$$\frac{p^2-1}{8} = \frac{(8q \pm 1)^2 - 1}{8} = 8q^2 \pm 2q \equiv 0 \pmod 2.$$

$p = 8q \pm 3$时,

$$\frac{p^2-1}{8} = \frac{(8q \pm 3)^2 - 1}{8} = 8q^2 \pm 6q + 1 \equiv 1 \pmod 2.$$

$1 \leqslant k \leqslant (p-1)/2$时$\{\frac{2k}{p}\} > \frac{1}{2} \iff k > \frac{p}{4}$. 利用Gauss引理可得

$$\begin{aligned} \left(\frac{2}{p}\right) &= (-1)^{\frac{p-1}{2} - |\{1 \leqslant k \leqslant \frac{p-1}{2} : k \leqslant \frac{p-1}{4}\}|} \\ &= (-1)^{\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor} = (-1)^{\lfloor \frac{p+1}{4} \rfloor} = (-1)^{(p^2-1)/8}. \end{aligned}$$

在Mersenne数上的应用

例题： 设$p > 3$为素数且$p \equiv 3 \pmod 4$. 如果$q = 2p + 1$为素数, 则$M_p = 2^p - 1$为合数。

证明：$q = 2p + 1 \equiv 2 \times 3 + 1 = 7 \pmod 8$, 因而

$$M_p = 2^{(q-1)/2} \equiv \left(\frac{2}{q}\right) - 1 = 1 - 1 \equiv 0 \pmod q.$$

注意

$$M_p = (1+1)^p - 1 = 1 + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} \geqslant 1 + p + \frac{p(p-1)}{2} + p > q.$$

因此q为M_p的真因子，M_p为合数。

二次互反律

下述结果由Euler首先猜出其等价形式，并由Gauss首先严格证明。

定理3.4 (二次互反律). 对于不同的奇素数p与q, 我们有

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

利用$(\frac{-1}{p}),(\frac{2}{p})$的公式以及二次互反律，可方便地计算出具体的Legendre符号。

例题：判断同余式$x^2\equiv 79 \pmod{113}$是否有解。

解：79与113为素数，利用二次互反律得

$$\left(\frac{79}{113}\right)=\left(\frac{113}{79}\right)=\left(\frac{34}{79}\right)=\left(\frac{2}{79}\right)\left(\frac{17}{79}\right)=\left(\frac{17}{79}\right)=\left(\frac{79}{17}\right)=\left(\frac{11}{17}\right)$$
$$=\left(\frac{17}{11}\right)=\left(\frac{6}{11}\right)=\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)=-\left(\frac{3}{11}\right)=\left(\frac{11}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

因此$x^2\equiv 79 \pmod{113}$无整数解。

又一道例题

例题：对于正整数n及n^2+n-1的素因子p，证明p的十进制表示中个位数为$1,5,9$之一。

证明：由于n^2+n-1为奇数，p是奇素数。注意

$$n^2+n-1 \equiv 0 \pmod{p}, \text{ 从而 } (2n+1)^2 \equiv 5 \pmod{p}.$$

因此$(\frac{5}{p}) \neq -1$. $p \neq 5$时,

$$\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) = 1,$$

从而$p \equiv \pm 1 \pmod 5$. 故$p \equiv 1,5,9 \pmod{10}$.

在Fibonacci数列上的应用

Fibonacci数列如下给出：

$$F_0 = 0,\ F_1 = 1,\ F_{n+1} = F_n + F_{n-1}\ (n = 1, 2, 3, \ldots).$$

例题：对于奇素数p, 证明

$$F_p \equiv \begin{cases} 1 \pmod{p} & \text{如果 } p \equiv \pm 1 \pmod{5}, \\ -1 \pmod{p} & \text{如果 } p \equiv \pm 2 \pmod{5}. \end{cases}$$

证明：

$$\begin{aligned} \sqrt{5}F_p &= \left(\frac{1+\sqrt{5}}{2}\right)^p - \left(\frac{1-\sqrt{5}}{2}\right)^p \\ &= \frac{1}{2^p} \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} \left((\sqrt{5})^{2k+1} - (-\sqrt{5})^{2k+1}\right). \end{aligned}$$

继续证明

于是

$$2^{p-1}F_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} 5^k \equiv 5^{(p-1)/2} \equiv \left(\frac{5}{p}\right) \pmod{p},$$

从而

$$F_p \equiv \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \pmod{p}.$$

注意

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & \text{如果} p \equiv \pm 1 \pmod 5, \\ -1 & \text{如果} p \equiv \pm 2 \pmod 5. \end{cases}$$

故有所要结果.

在Lucas数上的应用

作为Fibonacci数对偶的Lucas数如下给出：

$$L_0 = 2,\ L_1 = 1,\ L_{n+1} = L_n + L_{n-1}\ (n = 1, 2, 3, \ldots).$$

例题：对于奇素数p, 证明

$$L_p \equiv 1 \pmod{p}.$$

证明：

$$L_p = \left(\frac{1+\sqrt{5}}{2}\right)^p + \left(\frac{1-\sqrt{5}}{2}\right)^p$$

$$= \frac{1}{2^p}\sum_{k=0}^{(p-1)/2}\binom{p}{2k}\left((\sqrt{5})^{2k} + (-\sqrt{5})^{2k}\right) = \frac{1}{2^{p-1}}\sum_{k=0}^{(p-1)/2}\binom{p}{2k}5^k,$$

从而

$$L_p \equiv 2^{p-1}L_p \equiv 5^0 = 1 \pmod{p}.$$

$F_{p-(\frac{p}{5})} \equiv 0 \pmod{p}$

容易证明

$$L_n = 2F_{n+1} - F_n = F_n + 2F_{n-1} \ (n = 1, 2, 3, \ldots).$$

定理3.5 (D. D. Wall, 1960). 对任何奇素数p有

$$F_{p-(\frac{p}{5})} \equiv 0 \pmod{p}.$$

证明：$p = 5$时$F_{p-(\frac{p}{5})} = F_5 = 5 \equiv 0 \pmod{p}$. 如果$p \equiv \pm 1 \pmod 5$, 则

$$2F_{p-1} = L_p - F_p \equiv 1 - \left(\frac{p}{5}\right) = 0 \pmod{p},$$

从而$F_{p-(\frac{p}{5})} \equiv 0 \pmod{p}$. 如果$p \equiv \pm 2 \pmod 5$, 则

$$2F_{p+1} = L_p + F_p \equiv 1 + \left(\frac{p}{5}\right) = 0 \pmod{p},$$

从而$F_{p-(\frac{p}{5})} = F_{p+1} \equiv 0 \pmod{p}$.

Wall-Sun-Sun素数

对于奇素数p, 孙智宏与孙智伟[Acta Arith. 60 (1992)]证明了

$$p^2 \nmid F_{p-(\frac{p}{5})}$$

$\Longrightarrow$ Fermat方程$x^p + y^p = z^p$ 没有适合 $p \nmid xyz$ 的整数解.

使得$F_{p-(\frac{p}{5})} \equiv 0 \pmod{p^2}$的奇素数$p$后来被命名为Wall-Sun-Sun素数。出于粗略的概率上的考虑, 人们倾向于认为应该有无穷多个Wall-Sun-Sun素数.

目前尚未发现任何Wall-Sun-Sun素数, 已有的搜索表明第一个Wall-Sun-Sun素数要大于$2^{64} \approx 1.84 \times 10^{19}$.

§2.4 a模m的次数

设整数a与正整数m互素。使得$a^d \equiv 1 \pmod{m}$的最小正整数d叫做a**模**m**的次数**（或**阶**）. $0 \leqslant k < l \leqslant d-1$时$a^{l-k} \not\equiv 1 \pmod{m}$, 从而$a^0, a^1, \ldots, a^{d-1}$模$m$两两不同. 对于正整数$n = dq + r$ $(0 \leqslant r < d)$,

$$\begin{aligned} a^n \equiv 1 \pmod{m} &\iff (a^d)^q a^r \equiv 1 \pmod{m} \\ &\iff a^r \equiv 1 \pmod{m} \\ &\iff r = 0 \iff d \mid m. \end{aligned}$$

特别地，利用Euler定理得$d \mid \varphi(m)$.

如果$g \in \mathbb{Z}$模m的次数为$\varphi(m)$, 即$\{g^k : k = 0, \ldots, \varphi(m)-1\}$为模$m$的简化剩余系，则称$g$为模$m$的**原根**(primitive root).

已知模正整数m的原根存在当且仅当m形如$1, 2, 4, p^a, 2p^a$(其中p为奇素数, $a \in \mathbb{Z}^+$).

关于Fermat数

定理4.1 (Euler, Lucas). 设$n > 1$为整数，p为Fermat数$F_n = 2^{2^n} + 1$的素因子，则$p \equiv 1 \pmod{2^{n+2}}$.

证明：设2模p的阶为d. 由于

$$2^{2^n} \equiv -1 \not\equiv 1 \pmod{p} \text{ 但 } 2^{2^{n+1}} \equiv (-1)^2 = 1 \pmod{p},$$

我们有$d \nmid 2^n$但$d \mid 2^{n+1}$. 因此$2^{n+1} = d$整除$\varphi(p) = p - 1$.

由于$n \geqslant 2$, 2^{n+1}为8倍数，从而$p \equiv 1 \pmod{8}$. 注意

$$(-1)^{\frac{p-1}{2^{n+1}}} \equiv (2^{2^n})^{\frac{p-1}{2^{n+1}}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) = 1 \pmod{p}.$$

因此$(p-1)/2^{n+1}$为偶数，从而$p \equiv 1 \pmod{2^{n+2}}$.

Euler发现F_5有素因子$p = 641 = 2^7 \times 5 + 1$.

关于$1^k + \cdots + (p-1)^k$模p

定理4.2. 设p为素数，$k \in \mathbb{Z}^+$. 则

$$1^k + \cdots + (p-1)^k \equiv \begin{cases} -1 \pmod{p} & \text{如果} p-1 \mid k, \\ 0 \pmod{p} & \text{如果} p-1 \nmid k. \end{cases}$$

证明：令$S = \sum_{r=1}^{p-1} r^k$. 如果$p-1 \mid k$, 则依Fermat小定理有

$$S \equiv \sum_{r=1}^{p-1} 1 = p-1 \equiv -1 \pmod{p}.$$

现在假设$p-1 \nmid k$. 设g为模p的一个原根, 则$g^k \not\equiv 1 \pmod{p}$(因为$p-1 \nmid k$). 注意

$$g^k S = \sum_{r=1}^{p-1} (gr)^k \equiv \sum_{s=1}^{p-1} s^k = S \pmod{p},$$

从而$p \mid (g^k - 1)S$. 因$p \nmid g^k - 1$, 必有$p \mid S$.

最后一道例题

例题：设p与$q = 4p + 1$都是素数，证明2是模q的一个原根。

证明：设2模q的阶为d, 则d整除$\varphi(q) = q - 1 = 4p$. 如果$2^4 \equiv 1 \mod q$, 则$q = 5$, 此不可能. 因此$d \nmid 4$. 注意$q = 4p + 1 \equiv 4 \times 1 + 1 = 5 \pmod 8$且

$$2^{2p} = 2^{(q-1)/2} \equiv \left(\frac{2}{q}\right) = -1 \pmod q.$$

因此$d \nmid 2p$. 而d为$4p$的因子，只能$d = 4p = \varphi(q)$, 从而2为模q的原根。

猜想 (孙智伟，2013). 任给素数p, 有$g \in \{1, \ldots, p-1\}$使得g为模p的原根且$g - 1$为平方数。

§2.5 一些著名的猜想或定理

数论是研究整数（及有理数）性质的一个传统数学分支，其中绝大部分属于纯粹数学。Gauss称“数论是数学的女王”。Kronecker 说：“上帝创造了自然数，其它数学都是人造的。”

哥德巴赫（Goldbach）猜想（简称为命题“1+1”）：大于2的的偶数可表成两个素数之和。

例如：

$$4 = 2+2,\ 6 = 3+3,\ 8 = 5+3,\ 10 = 5+5,\ 12 = 7+5,\ 14 = 11+3.$$

哥德巴赫猜想因其高难度被誉为“数论皇冠上的明珠”，这一猜想至今仍未解决，目前这方面最好的结果仍是陈景润的“1+2”（充分大的偶数可写成一个素数与不超过两个素数乘积的和，例如：$22 = 17 + 5 = 7 + 3 \times 5$）。最近有人证明陈景润定理中的“充分大”可明确为大于$10^{1872344071119349}$.

陈景润

陈景润（1933-1996）呕心沥血探素多年，付出了青春和健康才换来“1+2”。1999年我国发行纪念陈景润在哥德巴赫猜想上最佳结果的80分邮票。1996年发现的编号为7681的小行星后来被命名为“陈景润星”。

Goldbach猜想似乎没有实际用途，但最近有人指出它与晶体学约束以及对称群的阶密切相关。

孪生素数

对于素数$p > 2$, $p + 1$为偶数因而不是素数。如果p与$p + 2$都是素数，则说它们是一对孪生素数。例如：

$$\{3, 5\},\ \{5, 7\},\ \{11, 13\},\ \{17, 19\},\ \{29, 31\},\ \{41,\ 43\}$$

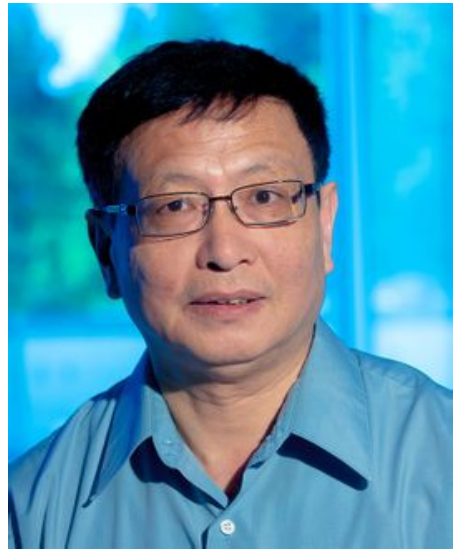
都是孪生素数对。

孪生素数猜想:有无穷多对孪生素数。

这个猜测或许古希腊数学家就意识到了，1849年法国数学家de Polignac甚至猜测每个正偶数可表成相邻素数差无穷多次。

网上有人把Goldbach猜想与孪生素数猜想这两大名题比作“倚天剑”与“屠龙刀”，得其一便为数论世界的“武林至尊”（即便获得者不在乎名利也会是这样的结局）。

张益唐



2013年4月，名不见经传的华人数学家张益唐（58岁，1985年出国前是我国解析数论学家潘承彪教授的硕士生，美国New Hampshire（新罕布什尔）大学临时讲师）写出“Bounded gaps between primes”这一惊世骇俗的杰作（后发表于Annals of Math.），用精巧的解析数论方法成功地证明有无穷多对素数p与$q < p$使得$p - q \leqslant 7 \times 10^7$, 亦即存在小于7千万的正偶数d使有无穷多对相邻素数差为d.

张益唐工作后续发展

张益唐的重大突破震撼了整个数论界（甚至数学界），毕竟孪生素数这一古老难题连Euler, Gauss, Dirichlet, Riemann, Hilbert, Hardy, Selberg, Tao等数学大家都无可奈何啊！关于张益唐事迹的各种报道铺天盖地，国际上著名解析数论专家Andrew Granville认为这是数论史上伟大的成果之一（“One of the great results in the history of number theory”），这里我再引用一位网友的评论：“张益唐的定理无疑雄居当代数学的一个制高点，是属于给这个星球上的人们增加光辉的作品”。

后来青年数学家James Marynard用更为简洁的方法把7千万降到600，现在最好的上界是246.

孪生素数猜想目前也无实际用途，人们探讨它纯粹出于理论上的兴趣。张于1992年在Purdue大学博士毕业后找不到工作，在快餐店打工多年，1999年才获得新罕布什尔大学临时讲师教职。

Collatz猜想

Collatz在1937年还是大学生时提出了下述著名的猜测。

Collatz猜想（也称“$3x+1$猜想”）：任给正整数a_1 ,如定义好$a_1, \ldots, a_n$, 则在a_n 为奇数时让$a_{n+1} = 3a_n + 1$, 在a_n为偶数时让$a_{n+1} = a_n/2$. 那么必有正整数N使得$a_N = 1$.

例如：

$$7 \to 22 \to 11 \to 34 \to 17 \to 52 \to 26 \to 13$$

$$\to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1.$$

数学家已对$a_1 \leqslant 2^{60}$验证了Collatz猜想。

据认为数学家在五十至一百年内对这猜测无能为力，这一问题目前也看不出有何用途。Terence Tao(陶哲轩)最近在此问题的概率版本上取得重要突破。

Dirichlet定理与van der Waerden定理

长为k的公差为n的等差数列（又称算术级数）如下：

$$a,\ a+n,\ a+2n,\ \ldots,\ a+(k-1)n.$$

Dirichlet定理 (1837). 设整数a与正整数n互素，则无穷等差数列

$$a,\ a+n,\ a+2n,\ a+3n,\ \ldots$$

中包含无穷多个素数.

van der Waerden定理 （1927）：把全体正整数随意地放入n个抽屉中后，对任给的正整数k都有个抽屉包含长为k的等差数列。

例如：把素数放入第一个抽屉中而把合数放入第二个抽屉中，那么素数或者合数中含有指定长度的等差数列。注意5, 11, 17, 23, 29是长为5的素数等差数列。

Green-Tao定理

2004年青年数学家Ben Green（英国人）与Terence Tao（陶哲轩，澳籍华裔, 2006年的Fields奖获得者）将解析数论、组合数学与动力系统相结合成功地证明了著名的Green–Tao定理。

Green-Tao定理 （2004）：任给正整数$k \geqslant 3$, 有k个素数成等差数列。

注：目前已发现的最长的素数等差数列只有26项。

Waring问题

Lagrange在Euler多年工作基础上证明了每个自然数可表成4个整数的平方和。

1770年Waring在他的《代数沉思录》中写道：“每个自然数都是4个自然数的平方和，9个自然数的立方和，19个自然数的4次方和，37 个自然数的5次方和。一般地，对整数$k > 1$存在取值尽可能小的整数$g(k)$使得每个自然数都可表示成$g(k)$个自然数的k次方和。”

如何确定$g(k)$便是著名的Waring问题，1940年Hilbert对一般的$k > 1$确立了$g(k)$ 的存在性。已知$g(2) = 4$, $g(3) = 9$,

$g(4) = 19$ (1986年), $g(5) = 37$ (1964年陈景润), $g(6) = 73$ (1940年).

还可证明k充分大时$g(k) = 2^k + \lfloor \left(\frac{3}{2}\right)^k \rfloor - 2$, 其中地板函数$\lfloor x \rfloor$表示$x$的整数部分.

Gibreath猜想(1958)

在由小到大排的素数序列基础上计算相邻两项差的绝对值得到一个新的序列，再计算这序列相邻两项差的绝对值又得一个序列，如此进行下去。在素数列之后得到的序列左边第一项总为1.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

$$1, \ 2, \ 2, \ 4, \ 2, \ 4, \ 2, \ 4, \ \ldots$$

$$1, \ 0, \ 2, \ 2, \ 2, \ 2, \ 2, \ \ldots$$

$$1, \ 2, \ 0, \ 0, \ 0, \ 0, \ \ldots$$

$$1, \ 2, \ 0, \ 0, \ 0, \ \ldots$$

$$1, \ 2, \ 0, \ 0, \ \ldots$$

$$1, 2, 0, \ldots$$

$$1, 2, \ldots$$

$$1, \ldots$$

参考书

1. 孙智伟，基础数论入门，哈尔滨工业大学出版社，2014.

2. 孙智伟，Fibonacci数与Hilbert第十问题，哈尔滨工业大学出版社，2024.

谢谢!