四次多项式模素数的不同取值个数

淮阴师范学院　孙智宏

1. 两种不同的数学传统

计算传统: 运用高超的计算技巧得出深刻的数学定理或公式

例: Euler, Gauss, Cauchy, Jacobi, Kummer, Ramanujan

Riemann的直觉也是依赖于大量的计算

数学就是计算的学问.

M.F.Atiyah（阿提雅）: 历史上的许多大数学家，比如Euler和Gauss，为了给自己找到素材而不得不靠自己的双手进行冗长的数值计算，他们正是借助这些素材才推测出了具有普遍性的定律或者是发现了著名的模式。

抽象传统: 通过抽象和概念化的理解和证明导出数学发现

例: Dedekind, Hilbert, Galois, Grothendieck

Apery关于$\zeta(3)$无理性的证明是Euler应该能够想到的,喜欢抽象的数学家对此无能为力.

Galois之前就没有数学?

2.三次多项式模素数的不同取值个数

设p为自然数, $f(x)$为整系数多项式,我们定义

$$V_p(f(x)) = \Big|\Big\{c \in \{0,1,\ldots,p-1\} : f(x) \equiv c \pmod{p} \text{ is solvable}\Big\}\Big|.$$

p为奇素数时$V_p(x^2) = (p+1)/2$.

$\mathbb{Z}$表示整数集合, $(\frac{a}{p})$为Jacobi符号.

定理1 (von Sterneck, 1908) 设$p > 3$为素数, $a_1, a_2, a_3 \in \mathbb{Z}$, $p \nmid a_1^2 - 3a_2$, 则

$$V_p(x^3 + a_1x^2 + a_2x + a_3) = (2p + (\frac{p}{3}))/3.$$

3. 关于$V_p(x^4+bx)$的一个猜想

猜想1(1999.6.25) 设p为$3k+2$形奇素数, $b\in\mathbb{Z}$, $p\nmid b$,则

$$V_p(x^4+bx)=\left[\frac{5p+7}{8}\right].$$

4. 四次同余式与三次同余式的联系

一般的四次同余式: $x^4+ax^2+bx+c\equiv 0\pmod p$

预解方程: $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\pmod p$

它们有相同的判别式$D(a,b,c)$

猜想2(1999.3.28) 设$p > 3$为素数, $a, b, c \in \mathbb{Z}$, $p \nmid bD(a, b, c)$, 方程$y^3 + 2ay^2 + (a^2 - 4c)y - b^2 \equiv 0 \pmod{p}$的所有解为$y_1, \ldots, y_n$, 则同余式$x^4 + ax^2 + bx + c \equiv 0 \pmod{p}$ 的解数为$1 + \sum_{i=1}^{n} (\frac{y_i}{p})$.

猜想3 设$p > 3$为素数, $a, b, c \in \mathbb{Z}$, 则同余式$x^4 + ax^2 + bx + c \equiv 0 \pmod{p}$ 有唯一解当且仅当同余式$y^3 + 2ay^2 + (a^2 - 4c)y - b^2 \equiv 0 \pmod{p}$无解.

猜想2本质上由T.Skolem在1952年证明.

1999.4.1: 如果猜想3正确,则猜想2可得到证明.

1999.7.1: 如果猜想2正确,则猜想1可得到证明.

5. 四次同余式唯一解的构造

设$a,b,c\in\mathbb{Z}$, 定义三元递归序列$\{S_n\}$如下:

$$S_0=3,\ S_1=-2a,\ S_2=2a^2+8c,$$
$$S_{n+3}+2aS_{n+2}+(a^2-4c)S_{n+1}-b^2S_n=0\ (n\geq 0).$$

若$y^3+2ay^2+(a^2-4c)y-b^2=(y-y_1)(y-y_2)(y-y_3)$,则$S_n=y_1^n+y_2^n+y_3^n$.

猜想4(1999.8.21) 设$p>5$为素数,$a,b,c\in\mathbb{Z}$,同余式$y^3+2ay^2+(a^2-4c)y-b^2\equiv 0\pmod p$无解,则同余式$x^4+ax^2+bx+c\equiv 0\pmod p$的唯一解$x_0$满足:

$$x_0^2\equiv\frac{1}{2}(S_{(p+1)/2}-a)\pmod p,$$
$$x_0\equiv\frac{a^2-4c-S_{(p+1)/2}^2}{4b}\pmod p.$$

猜想4$\Rightarrow$猜想3$\Rightarrow$猜想2$\Rightarrow$猜想1

6. 三次同余式

猜想5(1999.8.22) 设$p > 3$为素数,$a_1, a_2, a_3 \in \mathbb{Z}$,$p \nmid a_1^2 - 3a_2$, 则同余式$x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}$无解当且仅当$s_{p+1} \equiv a_2 \pmod{p}$,其中$\{s_n\}$如下定义: ‘

$$s_0 = 3,\ s_1 = -a_1,\ s_2 = a_1^2 - 2a_2,$$
$$s_{n+3} + a_1s_{n+2} + a_2s_{n+1} + a_3s_n = 0\ (n \geq 0).$$

猜想5⇒猜想4⇒猜想3⇒猜想2⇒猜想1

利用三次方程求根公式导出$s_{p+1} \pmod{p}$与Lucas序列$V_{(p-(\frac{p}{3}))/3} \pmod{p}$的关系,再利用三次剩余理论确定$V_{(p-(\frac{p}{3}))/3} \pmod{p}$与三次同余式可解性的关系,从而解决猜想5.

定理2.(1999.8.23) 设$p > 3$为素数,$a_1, a_2, a_3 \in \mathbb{Z}$,$p \nmid a_1^2 - 3a_2$, 则同余式$x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}$之解数

$$N = \begin{cases} 3 & \text{if } s_{p+1} \equiv a_1^2 - 2a_2 \pmod{p}, \\ 0 & \text{if } s_{p+1} \equiv a_2 \pmod{p}, \\ 1 & \text{if } s_{p+1} \not\equiv a_2, a_1^2 - 2a_2 \pmod{p}. \end{cases}$$

7. 当$p \equiv 1 \pmod 3$时$V_p(x^4+bx)$的值

利用四次同余式与预解同余式解数的关系及6阶分圆数可证明

定理3(1999.7.2) 设$p \equiv 7 \pmod{12}$为素数, $b \in \mathbb{Z}$, $p \nmid b$, $p = A^2+3B^2 (A, B \in \mathbb{Z})$, $A \equiv 1 \pmod 3$,则

$$V_p(x^4+bx) = \begin{cases} \frac{1}{8}(5p+7+6(-1)^{\frac{p-7}{12}}-4A) \\ \quad \text{if } 2b \text{ is a cubic residue of } p, \\ \frac{1}{8}(5p+1+2A) \\ \quad \text{if } 2b \text{ is a cubic nonresidue of } p. \end{cases}$$

利用12阶分圆数可证明

定理4 设$p \equiv 1 \pmod{12}$为素数, $b \in \mathbb{Z}$, $p \nmid b$, $p = A^2+3B^2 (A, B \in \mathbb{Z})$, $A \equiv 1 \pmod 3$,则

$$V_p(x^4+bx) = \begin{cases} \frac{1}{8}(5p+9-6(-1)^{\frac{p-1}{12}}) \\ \quad \text{if } 2b \text{ is a cubic residue of } p, \\ \frac{1}{8}(5p+3 \pm 6B) \\ \quad \text{if } (2b)^{\frac{p-1}{3}} \equiv \frac{1}{2}(-1 \mp \frac{A}{B} \pmod p). \end{cases}$$

8. 与F_p上椭圆曲线点数的联系

定理5 设$p>3$为素数, $k\in\mathbb{Z}$, $p\nmid k$,

$$\delta(k,p)=\Big|\Big\{x\in\{1,2,\ldots,p-1\}:\\ x^3+4kx+8k^2\equiv 0\ (\mathrm{mod}\ p),\ (\frac{x}{p})=-1\Big\}\Big|,$$

则

$$8V_p(x^4+2kx^2+4k^2x)=5p+2+(-1)^{\frac{p-1}{2}}+4\delta(k,p)\\ +(\frac{p}{3})(\#E_p(x^3-(18k+3)x-27k^2-18k-2)\\ -\#E_p(x^3-3k^2x+k^3(27k+2)).$$

9. $V_p(x^4-3x^2+2x)$的值

定理6 设$p>3$为素数, 则

(1) 当$p\equiv 11\ (\mathrm{mod}\ 12)$时

$$V_p(x^4-3x^2+2x)\\ =\begin{cases}\dfrac{5p+1}{8}+\dfrac{1}{2}(1-(\dfrac{3^{\frac{p+1}{4}}+1}{p})) & \text{if } 24\mid p-11,\\ \dfrac{5}{8}(p+1) & \text{if } 24\mid p-23.\end{cases}$$

(2) 当$p \equiv 7 \pmod{12}$, $p = A^2 + 3B^2$, $A \equiv 1 \pmod 3$时

$$V_p(x^4 - 3x^2 + 2x) = \frac{1}{8}(5p + 1 - 2A).$$

(3) 当$p \equiv 5 \pmod{12}$, $p = c^2 + d^2$, $2 \mid d$, $c + d \equiv 1 \pmod 4$, $c \equiv d \pmod 3$ 时

$$V_p(x^4 - 3x^2 + 2x) = \frac{1}{8}(5p + 3 - 2d).$$

(4) 当$p \equiv 1 \pmod{12}$, $p = c^2 + d^2 = A^2 + 3B^2$, $2 \mid d$, $c + d \equiv 1 \pmod 4$, $A \equiv 1 \pmod 3$ 时

$$V_p(x^4 - 3x^2 + 2x)$$
$$= \begin{cases} \frac{1}{8}(5p + 3 + 4\delta(p) - 2A - 2c) & \text{if } 3 \mid c, \\ \frac{1}{8}(5p + 3 + 4\delta(p) - 2A + 2c) & \text{if } 3 \mid d, \end{cases}$$

其中

$$\delta(p) = \begin{cases} 1 & \text{if } 24 \mid p - 13, \\ 0 & \text{if } 24 \mid p - 1 \text{ and } 8 \mid B - d, \\ 2 & \text{if } 24 \mid p - 1 \text{ and } 8 \nmid B - d. \end{cases}$$

10. $V_p(x^4+ax^2+bx)$的估计

定理7 设$p>3$为素数, $a,b\in\mathbb{Z}$, $p\nmid b$, 则

$$\left|V_p(x^4+ax^2+bx)-\frac{5p}{8}\right|\le\frac{1}{2}\sqrt{p}+\frac{15}{8}.$$

Birch and Swinnerton-Dyer(1959)运用Weil结果对几乎所有的多项式$f(x)$证明

$$V_p(f(x))=p\left(1-\frac{1}{2!}+\frac{1}{3!}-\cdots-(-1)^d\frac{1}{d!}\right)+O(\sqrt{p}),$$

其中d为$f(x)$的次数.

1967年K. McCann and K.S.Williams运用Skolem结果证明

$$V_p(x^4+ax^2+bx)=\frac{5p}{8}+O(\sqrt{p}).$$

11. 什么是好的数学?

唯有普遍的真理才是科学的唯一目标

例: Newton, Leibniz, Cauchy, Weierstrass

Chasles: 总有一个主要的真理,人们会认出它来,因为别的定理都将通过简单的变换或作为容易的推论而从它得出. 作为知识基础的伟大的真理总具有简单和直观的特色.

C.Segre（塞格雷）: 一般来讲，我们可以把具有下述性质的所有研究工作都称做重要的：同本身就很重要的事物有关；具有很大的一般性；把表面上不同的学科统一在单一的观点之下，使之简化并得到阐明；其结果有可能产生许许多多的推论。

中学教师中的研究者,几何定理的新证明,Ramsey数的研究与猜想

Gowers,Tao的观点和见解