

三次型： p 进问题

Cubic forms: the p -adic problem

断言"对任何 p 都存在某个 ℓ , 使 $C(\mathbf{x})$ 具有性质 $\mathcal{A}(p^\ell)$ ", 等价于断言"方程 $C(\mathbf{x}) = 0$ 在 p 进数域中有非奇异解"。我们将证明: 当 $n \geq 10$ 时这是成立的。若干位数学家各自独立地证明了: 方程 $C(\mathbf{x}) = 0$ 在 $n \geq 10$ 时总有非平凡的 p 进解, 并且他们的任何一个证明都能服务于我们的目的, 因为 (如 Lewis 教授向我指出的) 从任何一个非平凡解都可以推出一个非奇异解。然而, 我更愿意采用我自己的证明, 因为它就是为了直接导向性质 $\mathcal{A}(p^\ell)$ 而设计的。

设 $N = \frac{1}{2}n(n+1)$ 。设 $\mathcal{C}$ 表示一个有 n 行 N 列的矩阵, 其一般元素为 c_{ijk} , 其中 i 指明行, 而数对 j, k (满足 $j \leq k$) 指明列, 约定这些数对按某种固定次序排列。设 Δ 表示由 $\mathcal{C}$ 的任意 n 列所构成的一个典型的 n 阶行列式, 可能的行列式个数为 $\binom{N}{n}$ 。我们可以假定 (必要时给 $C(\mathbf{x})$ 乘上因子 6) 诸 c_{ijk} 都是整数, 从而各个 Δ 都是整数。

定义. 设 $h(C)$ 表示所有行列式 Δ (若它们不全为 0) 的最大公因数; 在它们全为 0 的情形, 令 $h(C) = 0$ 。

引理 18.1. 设

$$x'_i = \sum_{r=1}^n q_{ir} x_r, \quad (1 \leq i \leq n),$$

为一个具有整系数 q_{ir} 、行列式 $q \neq 0$ 的线性变换, 并设

$$C(x_1, \dots, x_n) = C'(x'_1, \dots, x'_n)$$

恒等地成立。那么 $h(C)$ 能被 $qh(C')$ 整除。

证. 两个型 C 与 C' 中的系数由下式相联系:

$$c_{rst} = \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n q_{ir} q_{js} q_{kt} c'_{ijk}.$$

在上面定义矩阵 C 时, 我们在满足 $1 \leq j \leq k \leq n$ 的数对 j, k 与整数 $1 \leq \mu \leq N$ 之间选定了一个一一对应。于是 C' 的一般元素是 $c'_{ijk} = c'_{i\mu}$, 其中 $i = 1, 2, \dots, n$ 且

$\mu = 1, 2, \dots, N$, 这里 μ 表示数对 j, k 。类似地, 把满足 $s \leq t$ 的数对 s, t 用 ν 表示, 则 $\mathcal{C}$ 的一般元素是 $c_{rst} = c_{r\nu}$ 。令

$$u_{\mu\nu} = \begin{cases} q_{js}q_{kt}, & j = k, \\ q_{js}q_{kt} + q_{ks}q_{jt}, & j < k, \end{cases}$$

其中 μ 表示数对 j, k , ν 表示数对 s, t 。则两组系数之间的关系可写成

$$c_{r\nu} = \sum_{i=1}^n \sum_{\mu=1}^N q_{ir} c'_{i\mu} u_{\mu\nu},$$

其中 $r = 1, 2, \dots, n$ 且 $\nu = 1, 2, \dots, N$ 。用矩阵记号即为

$$\mathcal{C} = \mathcal{Q}^T \mathcal{C}' \mathcal{U},$$

其中 $\mathcal{Q} = (q_{ir})$ 是一个 $n \times n$ 矩阵, $\mathcal{U} = (u_{\mu\nu})$ 是一个 $N \times N$ 矩阵, T 表示转置。

设 Δ 为由 $\mathcal{C}$ 的第 $\nu_1, \dots, \nu_n$ 列所构成的行列式, 符号地记为:

$$\Delta = (\det \mathcal{C})_{\nu_1, \dots, \nu_n}^{1, \dots, n}.$$

由于矩阵 $\mathcal{Q}$ 的行列式为 q , 故有

$$\pm \Delta = q (\det \mathcal{C}' \mathcal{U})_{\nu_1, \dots, \nu_n}^{1, \dots, n}.$$

由一个熟知的结果有

$$(\det \mathcal{C}' \mathcal{U})_{\nu_1, \dots, \nu_n}^{1, \dots, n} = \sum_{\rho_1, \dots, \rho_n} (\det \mathcal{C}')_{\rho_1, \dots, \rho_n}^{1, \dots, n} (\det \mathcal{U})_{\nu_1, \dots, \nu_n}^{\rho_1, \dots, \rho_n},$$

其中求和遍及从 $1, \dots, N$ 中选取 $\rho_1, \dots, \rho_n$ 的全部 $\binom{N}{n}$ 种选法 (不计次序)。

在和式的每一项中, 第一个因子是由 $\mathcal{C}'$ 所能构成的某个 n 阶行列式 Δ' , 而第二个因子是一个整数。因此该和能被 $h(\mathcal{C}')$ 整除, 从而 Δ 能被 $qh(\mathcal{C}')$ 整除。这就证明了结论。 ■

推论. $h(\mathcal{C})$ 是 $\mathcal{C}$ 的一个算术不变量。也就是说, 对于任意两个等价的型, 它取相同的值。

证. 若 $\mathcal{C}$ 与 $\mathcal{C}'$ 是等价的型, 则该引理对 $q = 1$ 适用, 于是表明 $h(\mathcal{C})$ 能被 $h(\mathcal{C}')$ 整除。同理 $h(\mathcal{C}')$ 能被 $h(\mathcal{C})$ 整除, 由此即得结论。 ■

引理 18.2. 若 $\mathcal{C}(\mathbf{x})$ 是非退化的, 则 $h(\mathcal{C}) \neq 0$ 。

证. 若 $h(C) = 0$, 则由 C 所构成的全部 n 阶行列式都为零, 即 C 的 n 行线性相关。于是存在不全为零的 $p_1, \dots, p_n$, 使得

$$\sum_{i=1}^n p_i c_{ijk} = 0$$

对一切 j, k 成立; 并且我们可以取 $p_1, \dots, p_n$ 为最大公因数为 1 的整数。由于

$$\frac{1}{3} \frac{\partial C}{\partial x_i} = \sum_j \sum_k c_{ijk} x_j x_k,$$

故有

$$p_1 \frac{\partial C}{\partial x_1} + \dots + p_n \frac{\partial C}{\partial x_n} = 0$$

关于 $x_1, \dots, x_n$ 恒等地成立。众所周知, 存在一个整数元素的 $n \times n$ 矩阵 p_{ir} , 其行列式为 ± 1 , 使得对 $i = 1, 2, \dots, n$ 有 $p_{in} = p_i$ 。令

$$x_i = \sum_{r=1}^n p_{ir} y_r,$$

则有

$$\frac{\partial C}{\partial y_n} = 0$$

恒等地成立, 从而 $C(\mathbf{x})$ 等价于一个仅含 $y_1, \dots, y_{n-1}$ 的型, 因而是退化的。■

这个引理的逆命题也成立, 因为上述论证是可逆的, 但我们将不需要它。

引理 18.3. 若 $n \geq 4$ 且 $C(\mathbf{x})$ 不具有性质 $\mathcal{A}(p)$, 则 $C(\mathbf{x})$ 等价于一个如下类型的型

$$C'(x_1, x_2, x_3) + pC''(x_1, \dots, x_n). \quad (18.1)$$

证. 由 Chevalley 的一条定理¹, 方程 $C(\mathbf{x}) \equiv 0 \pmod{p}$ 有异于 $\mathbf{x} = \mathbf{0}$ 的解, 因为变量个数超过该同余式的次数。由于 $C(\mathbf{x})$ 不具有性质 $\mathcal{A}(p)$, 我们必有

$$\frac{\partial C}{\partial x_i} \equiv 0 \pmod{p}$$

对一切 i 成立。经过一个适当的整系数么模变换, 我们可以把所考虑的解取为

$$x_1 = 1, \quad x_2 = x_3 = \dots = x_n = 0.$$

那么 $C(\mathbf{x})$ 具有如下形式

$$apx_1^3 + px_1^2(b_2x_2 + \cdots + b_nx_n) + x_1B(x_2, \dots, x_n) + C_{n-1}(x_2, \dots, x_n),$$

其中 B 与 C_{n-1} 分别为二次型与三次型。事实上，诸 $x_1^2x_j$ 的系数都能被 p 整除，因为它们正是

$$\frac{\partial C}{\partial x_2}, \dots, \frac{\partial C}{\partial x_n}$$

在该解处的值。

若 B 的某些系数不能被 p 整除，我们可以选取 $x_2, \dots, x_n$ 使得

$$B(x_2, \dots, x_n) \not\equiv 0 \pmod{p},$$

办法是取形如 $1, 0, \dots, 0$ 或形如 $1, 1, 0, \dots, 0$ 的值。然后我们可以选取 x_1 使得

$$x_1B(x_2, \dots, x_n) + C_{n-1}(x_2, \dots, x_n) \equiv 0 \pmod{p},$$

这就给出 $C(\mathbf{x}) \equiv 0 \pmod{p}$ 的一个满足 $\partial C / \partial x_1 \not\equiv 0 \pmod{p}$ 的解，与假设矛盾。

因此我们可以假定 B 的全部系数都能被 p 整除。于是 $C(\mathbf{x})$ 等价于

$$px_1Q_n(x_1, x_2, \dots, x_n) + C_{n-1}(x_2, \dots, x_n),$$

其中 Q_n 是一个二次型。

若 $n \geq 5$ ，我们可以令 $x_1 = 0$ ，并对 $C_{n-1}(x_2, \dots, x_n)$ 应用上述论证，因为这个型同样不能具有性质 $\mathcal{A}(p)$ 。于是 C_{n-1} 等价于

$$px_2Q_{n-1}(x_2, \dots, x_n) + C_{n-2}(x_3, \dots, x_n).$$

这一过程继续下去，直到我们达到 $C_3(x_{n-2}, x_{n-1}, x_n)$ ，此时 Chevalley 定理不再适用。因此 $C(\mathbf{x})$ 等价于一个如下类型的型

$$p(x_1Q_n + \cdots + x_{n-3}Q_4) + C_3(x_{n-2}, x_{n-1}, x_n).$$

把变量的书写次序颠倒过来，我们便得到一个类型 (18.1) 的型。 ■

引理 18.4. 若在引理 18.3 的结果中，那个关于 $x_4, \dots, x_n$ 的型

$$C''(0, 0, 0, x_4, \dots, x_n)$$

具有性质 $\mathcal{A}(p^\lambda)$ ，则 $C(\mathbf{x})$ 对某个 $\ell \leq \lambda + 1$ 具有性质 $\mathcal{A}(p^\ell)$ 。

证. 在引理 17.1 的证明中我们看到, 若一个型 C^* 具有性质 $\mathcal{A}(p^\lambda)$, 则对每个 $\nu \geq 0$, 同余式

$$C^*(\mathbf{x}) \equiv 0 \pmod{p^{2\lambda-1+\nu}} \quad (18.2)$$

$$\frac{\partial C^*}{\partial x_i} \equiv 0 \pmod{p^{\lambda-1}} \quad (18.3)$$

对一切 i 可解, 并且此外对某个 j 有

$$\frac{\partial C^*}{\partial x_j} \not\equiv 0 \pmod{p^\lambda}. \quad (18.4)$$

为简便起见, 我们把 (18.3) 与 (18.4) 表述为

$$p^{\lambda-1} \parallel \left(\frac{\partial C^*}{\partial x_1}, \dots, \frac{\partial C^*}{\partial x_n} \right).$$

" $C''(0, 0, 0, x_4, \dots, x_n)$ 具有性质 $\mathcal{A}(p^\lambda)$ " 这一假设蕴含着 (取 $\nu = 1$) 存在整数 $x_4, \dots, x_n$, 使得

$$C''(0, 0, 0, x_4, \dots, x_n) \equiv 0 \pmod{p^{2\lambda}}, \quad p^\lambda \parallel \left(\frac{\partial C''}{\partial x_4}, \dots, \frac{\partial C''}{\partial x_n} \right).$$

因此

$$C(0, 0, 0, x_4, \dots, x_n) \equiv 0 \pmod{p^{2\lambda+1}}, \quad p^\lambda \parallel \left(\frac{\partial C}{\partial x_4}, \dots, \frac{\partial C}{\partial x_n} \right).$$

若对这些 $x_1, x_2, \dots, x_n$ 的值, 我们用

$$p^{\ell-1} \parallel \left(\frac{\partial C}{\partial x_1}, \dots, \frac{\partial C}{\partial x_n} \right)$$

来定义 ℓ , 则 $\ell \leq \lambda + 1$, 且 $C(\mathbf{x})$ 具有性质 $\mathcal{A}(p^\ell)$. ■

引理 18.5. 若 $n \geq 10$ 且 $C(\mathbf{x})$ 不具有性质 $\mathcal{A}(p)$ 、 $\mathcal{A}(p^2)$ 、 $\mathcal{A}(p^3)$ 中的任何一个, 则它等价于一个如下类型的型

$$C^*(x_1, x_2, \dots, x_9, px_{10}, \dots, px_n). \quad (18.5)$$

证. 在等价于 C (我们仍记之为 C) 的型的表达式 (18.1) 中, 对 $i = 1, 2, 3$ 令 $x_i = py_i$. 这给出

$$C(py_1, py_2, py_3, x_4, \dots, x_n) \equiv p^3 C'(y_1, y_2, y_3) + p C''(py_1, py_2, py_3, x_4, \dots, x_n).$$

忽略 p^3 的倍数, 我们有

$$\begin{aligned} C(py_1, py_2, py_3, x_4, \dots, x_n) \\ \equiv p^2 C_{1,2}(y_1, y_2, y_3 \mid x_4, \dots, x_n) + pC''(0, 0, 0, x_4, \dots, x_n) \pmod{p^3}, \end{aligned} \quad (18.6)$$

其中 $C_{1,2}$ 表示一个关于 y_1, y_2, y_3 是一次、关于 $x_4, \dots, x_n$ 是二次的型。

由引理 18.4, 型 $C''(0, 0, 0, x_4, \dots, x_n)$ 不具有性质 $\mathcal{A}(p)$ 或 $\mathcal{A}(p^2)$ 中的任何一个。我们对这个型应用引理 18.3, 并在结果中对 $i = 4, 5, 6$ 令 $x_i = py_i$ 。略去 p^2 的倍数, 我们得到

$$C''(0, 0, 0, py_4, py_5, py_6, x_7, \dots, x_n) \equiv pC^{(3)}(0, \dots, 0, x_7, \dots, x_n) \pmod{p^2}. \quad (18.7)$$

进一步地, 由引理 18.4, 关于 $x_7, \dots, x_n$ 的型 $C^{(3)}(0, \dots, 0, x_7, \dots, x_n)$ 不具有性质 $\mathcal{A}(p)$ 。

在 (18.6) 中对 $i = 4, 5, 6$ 令 $x_i = py_i$, 并利用 (18.7), 我们得到一个可写为如下形式的结果

$$\begin{aligned} C(py_1, \dots, py_6, x_7, \dots, x_n) \\ \equiv p^2(y_1Q_1 + y_2Q_2 + y_3Q_3) + p^2C^{(3)}(0, \dots, 0, x_7, \dots, x_n) \pmod{p^3}, \end{aligned} \quad (18.8)$$

其中 Q_1, Q_2, Q_3 是关于 $x_7, \dots, x_n$ 的二次型。应当注意, y_4, y_5, y_6 不出现在 (18.8) 的右端。

假设这些二次型之一, 比如说 Q_1 , 不恒 $\equiv 0 \pmod{p}$ 。那么存在使 $Q_1 \not\equiv 0 \pmod{p}$ 的 $x_7, \dots, x_n$, 并且我们可以选取 y_1, y_2, y_3 使得

$$y_1Q_1 + y_2Q_2 + y_3Q_3 + C^{(3)}(0, \dots, 0, x_7, \dots, x_n) \equiv 0 \pmod{p}.$$

这给出

$$C(py_1, \dots, py_6, x_7, \dots, x_n) \equiv 0 \pmod{p^3},$$

其中 y_4, y_5, y_6 的值是任意的。此外

$$\frac{\partial C}{\partial y_1}(py_1, \dots, py_6, x_7, \dots, x_n) \equiv p^2Q_1 \not\equiv 0 \pmod{p^3}.$$

对 $i = 1, \dots, 6$ 取 $x_i = py_i$, 并注意到 $\partial/\partial x_1 = p^{-1}\partial/\partial y_1$, 我们便有使 $C \equiv 0 \pmod{p^3}$ 且 $\partial C/\partial x_1 \not\equiv 0 \pmod{p^2}$ 的 $x_1, \dots, x_n$ 之值。这与" C 不具有性质 $\mathcal{A}(p)$ 或 $\mathcal{A}(p^2)$ 中的任何一个"这一假设矛盾。

于是 Q_1, Q_2, Q_3 都恒 $\equiv 0 \pmod{p}$, 而 (18.8) 变为

$$C(py_1, \dots, py_6, x_7, \dots, x_n) \equiv p^2C^{(3)}(0, \dots, 0, x_7, \dots, x_n) \pmod{p^3}.$$

最后，我们对型 $C^{(3)}(0, \dots, 0, x_7, \dots, x_n)$ （如已指出，它不具有性质 $\mathcal{A}(p)$ ）应用引理 18.3。我们得到

$$C^{(3)}(0, \dots, 0, x_7, \dots, x_n) \equiv C^{(4)}(x_7, x_8, x_9) \pmod{p}.$$

对 $i = 1, \dots, 9$ 令 $x_i = py_i$ ，我们得到

$$C(py_1, \dots, py_9, x_{10}, \dots, x_n) \equiv 0 \pmod{p^3},$$

并且这关于 $y_1, \dots, y_9, x_{10}, \dots, x_n$ 恒等地成立。把左端的型记为

$$p^3 C^*(y_1, \dots, y_9, x_{10}, \dots, x_n),$$

我们便有恒等式

$$C(x_1, \dots, x_n) = C^*(x_1, \dots, x_9, px_{10}, \dots, px_n).$$

引理 18.6. 设 $n \geq 10$ 。若在引理 18.5 的结果中，型 $C^*(x_1, \dots, x_n)$ 具有性质 $\mathcal{A}(p^\lambda)$ ，则型 $C(x_1, \dots, x_n)$ 对某个 $\ell \leq \lambda + 3$ 具有性质 $\mathcal{A}(p^\ell)$ 。

证。正如我们在引理 18.4 的证明开头所指出的，" C^* 具有性质 $\mathcal{A}(p^\lambda)$ "这一假设蕴含着存在值 $y_1, \dots, y_n$ ，使得

$$C^*(y_1, \dots, y_n) \equiv 0 \pmod{p^{2\lambda+2}}, \quad p^{\lambda-1} \parallel \left(\frac{\partial C^*}{\partial y_1}, \dots, \frac{\partial C^*}{\partial y_n} \right).$$

由于

$$C(py_1, \dots, py_9, y_{10}, \dots, y_n) = p^3 C^*(y_1, \dots, y_9, y_{10}, \dots, y_n)$$

恒等地成立，我们有

$$C(py_1, \dots, py_9, y_{10}, \dots, y_n) \equiv 0 \pmod{p^{2\lambda+5}},$$

并且 $\partial C / \partial y_1, \dots, \partial C / \partial y_9, \partial C / \partial y_{10}, \dots, \partial C / \partial y_n$ 中至少有一个不能被 $p^{\lambda+3}$ 整除。对 $i = 1, \dots, 9$ 令 $x_i = py_i$ ，对 $i \geq 10$ 令 $x_i = y_i$ ，我们便得到 $\partial C / \partial x_1, \dots, \partial C / \partial x_n$ 中至少有一个不能被 $p^{\lambda+3}$ 整除，由此即得结论。 ■

引理 18.7. 任何变量个数至少为 10 的、具有整系数的非退化三次型，对每个素数 p 和某个依赖于 p 的适当的 ℓ ，都具有性质 $\mathcal{A}(p^\ell)$ 。 ℓ 有一个仅依赖于该三次型的上界。

证。设 $C(\mathbf{x})$ 是一个具有整系数的三次型，它不具有性质 $\mathcal{A}(p), \mathcal{A}(p^2), \dots, \mathcal{A}(p^{3m})$ 中的任何一个，其中 m 是一个正整数。由引理 18.5，这个型等价于一个类型 (18.5) 的型。这意味着

存在一个线性变换

$$x'_i = \sum_{r=1}^n q_{ir} x_r, \quad (1 \leq i \leq n),$$

具有整系数和行列式 p^{n-9} , 它把 $C(x_1, \dots, x_n)$ 变换为另一个具有整系数的型 $C^{(1)}(x'_1, \dots, x'_n)$ 。由引理 18.6, 型 $C^{(1)}$ 不具有性质 $\mathcal{A}(p), \mathcal{A}(p^2), \dots, \mathcal{A}(p^{3m-3})$ 中的任何一个。如此重复下去, 可知存在一个具有整系数和行列式 $p^{(n-9)m}$ 的线性变换, 它把 $C(\mathbf{x})$ 变换为一个具有整系数的型 $C^{(m)}(\mathbf{y})$ 。

由引理 18.1 可知, $h(C)$ 能被 $p^{(n-9)m}$ 整除。又由引理 18.2, $h(C)$ 是一个正整数。于是

$$(n-9)m \leq \log h(C) / \log p \leq \log h(C) / \log 2,$$

这就给出 m 的一个上界, 它与 p 无关。这就完成了引理 18.7 的证明。 ■

鉴于定理 17.1 以及第 17 章随后的注记, 我们看到引理 18.7 完成了下述结果的证明。

定理 18.1. 若 $C(x_1, \dots, x_n)$ 是任意具有整系数的三次型, 且 $n \geq 17$, 则方程

$$C(x_1, \dots, x_n) = 0$$

有不全为零的整数解 $x_1, \dots, x_n$ 。

1. 参见文献 [23], 例如。 ⇐