18

Cubic forms: the p-adic problem

The assertion that for any p there exists some ℓ such that $C(\mathbf{x})$ has the property $\mathcal{A}\left(p^{\ell}\right)$ is equivalent to the assertion that the equation $C(\mathbf{x}) = 0$ has a non-singular solution in the p-adic number field. We shall prove that this is true for $n \geq 10$. Several mathematicians have proved independently that the equation $C(\mathbf{x}) = 0$ always has a non-trivial p-adic solution provided $n \geq 10$, and any one of their proofs would serve our purpose, because (as Professor Lewis pointed out to me) it is possible to deduce a non-singular solution from any non-trivial solution. However, I prefer to follow my own proof, as this was designed to lead directly to the property $\mathcal{A}\left(p^{\ell}\right)$.

Let $N = \frac{1}{2}n\,(n+1)$. Let $\mathcal{C}$ denote the matrix of n rows and N columns whose general element is c_{ijk}, where i indicates the row and the pair j, k (with $j \leq k$) indicates the column, on the understanding that these pairs are arranged in some fixed order. Let Δ denote a typical determinant of order n formed from any n columns of $\mathcal{C}$, the number of possible determinants being $\binom{N}{n}$. We can assume (multiplying $C(\mathbf{x})$ by a factor of 6 if necessary) that the c_{ijk} are integral, hence that the various Δ are integral.

Definition. Let $h(C)$ denote the highest common factor of all the determinants Δ, if they are not all 0, and in the latter case let $h(C) = 0$.

Lemma 18.1. *Let*

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

be a linear transformation with integral coefficients q_{ir} of determinant

$q \neq 0$, and let

$$C\left(x_1, \ldots, x_n\right) = C'\left(x_1', \ldots, x_n'\right)$$

identically. Then $h(C)$ is divisible by $qh(C')$.

Proof. The coefficients in the two forms C and C' are related by

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

In defining the matrix $\mathcal{C}$ above, we chose a one-to-one correspondence between pairs j, k with $1 \leq j \leq k \leq n$ and integers $1 \leq \mu \leq N$. Thus the general element of $\mathcal{C}'$ is $c_{ijk}' = c_{i\mu}'$, say, where $i = 1, 2, \ldots, n$ and $\mu = 1, 2, \ldots, N$. Similarly, representing the pair s, t with $s \leq t$ by ν, the general element of $\mathcal{C}$ is $c_{rst} = c_{r\nu}$. Put

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

where μ denotes the pair j, k and ν the pair s, t. Then the relation between the two sets of coefficients can be written

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

where $r = 1, 2, \ldots, n$ and $\nu = 1, 2, \ldots, N$. In matrix notation this is

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

where $\mathcal{Q} = (q_{ir})$ is an $n \times n$ matrix and $\mathcal{U} = (u_{\mu\nu})$ is an $N \times N$ matrix, and T denotes the transpose.

Let Δ be the determinant formed from the columns $\nu_1, \ldots, \nu_n$ of $\mathcal{C}$, or symbolically:

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

Since the matrix $\mathcal{Q}$ has determinant q, it follows that

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

By a well known result we have

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

where the summation is over all $\binom{N}{n}$ selections of $\rho_1, \ldots, \rho_n$ from $1, \ldots, N$ without regard to order.

In each term of the sum, the first factor is one of the determinants Δ' of order n that can be formed from $\mathcal{C}'$, and the second factor is an integer. Hence the sum is divisible by $h(C')$ and it follows that Δ is divisible by $qh(C')$. This proves the result. □

Corollary. *$h(C)$ is an arithmetic invariant of C. That is, it has the same value for any two equivalent forms.*

Proof. If C and C' are equivalent forms the lemma applies with $q = 1$, and shows that $h(C)$ is divisible by $h(C')$. Similarly $h(C')$ is divisible by $h(C)$, whence the result. □

Lemma 18.2. *If $C(\mathbf{x})$ is non-degenerate then $h(C) \neq 0$.*

Proof. If $h(C) = 0$ then all the determinants of order n formed from $\mathcal{C}$ vanish, that is the n rows of $\mathcal{C}$ are linearly dependent. Thus there exist $p_1, \ldots, p_n$, not all 0, such that

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

for all j, k; and we can take $p_1, \ldots, p_n$ to be integers with highest common factor 1. Since

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

we have

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

identically in $x_1, \ldots, x_n$. It is well known that there exists an $n \times n$ matrix of integers p_{ir}, of determinant ± 1, such that $p_{in} = p_i$ for $i = 1, 2, \ldots, n$. Putting

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

we have

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

identically, and consequently $C(\mathbf{x})$ is equivalent to a form in $y_1, \ldots, y_{n-1}$ and is degenerate. □

The converse of this last lemma is also true, for the above argument is reversible, but it will not be needed.

Lemma 18.3. *If $n \geq 4$ and $C(\mathbf{x})$ does not have the property $\mathcal{A}(p)$, then $C(\mathbf{x})$ is equivalent to a form of the type*

$$C'(x_1, x_2, x_3) + pC''(x_1, \ldots, x_n). \tag{18.1}$$

Proof. By a theorem of Chevalley[1] there is a solution of $C(\mathbf{x}) \equiv 0 \pmod{p}$ other than $\mathbf{x} = \mathbf{0}$, since the number of variables exceeds the degree of the congruence. As $C(\mathbf{x})$ does not have the property $\mathcal{A}(p)$, we must have

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

for all i. After a suitable integral unimodular transformation, we can take the solution in question to be

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

Then $C(\mathbf{x})$ has the form

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

where B and C_{n-1} are quadratic and cubic forms respectively. Indeed the coefficients of $x_1^2x_j$ are all divisible by p because they are the values of

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

at the solution.

If some of the coefficients of B are not divisible by p, we can choose $x_2, \ldots, x_n$ so that

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

by taking values of the type $1, 0, \ldots, 0$ or of the type $1, 1, 0, \ldots, 0$. We can then choose x_1 so that

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

and this gives a solution of $C(\mathbf{x}) \equiv 0 \pmod{p}$ with $\partial C/\partial x_1 \not\equiv 0 \pmod{p}$, contrary to the hypothesis.

[1] See [23], for example.

We can therefore assume that all the coefficients of B are divisible by p. Thus $C(\mathbf{x})$ is equivalent to

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

where Q_n is a quadratic form.

If $n \geq 5$, we can put $x_1 = 0$ and apply the argument to $C_{n-1}(x_2, \ldots, x_n)$ since this form also cannot have the property $\mathcal{A}(p)$. Thus C_{n-1} is equivalent to

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

This process continues until we reach $C_3(x_{n-2}, x_{n-1}, x_n)$, to which Chevalley's theorem does not apply. Hence $C(\mathbf{x})$ is equivalent to a form of the type

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

Reversing the order of writing the variables, we obtain a form of the type (18.1). $\square$

Lemma 18.4. *If, in the result of Lemma 18.3, the form*

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

in $x_4, \ldots, x_n$ has the property $\mathcal{A}(p^\lambda)$, then $C(\mathbf{x})$ has the property $\mathcal{A}(p^\ell)$ for some $\ell \leq \lambda + 1$.

Proof. In the proof of Lemma 17.1 we saw that if a form C^* had property $\mathcal{A}(p^\lambda)$ then for every $\nu \geq 0$ the congruences

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

$$\frac{\partial C^*}{\partial x_i} \equiv 0 \pmod{p^{\lambda-1}}, \tag{18.3}$$

were soluble for all i, and in addition, for some j,

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

For brevity, we express (18.3) and (18.4) by

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

The hypothesis that $C''(0, 0, 0, x_4, \ldots, x_n)$ has property $\mathcal{A}(p^\lambda)$ implies (taking $\nu = 1$) the existence of integers $x_4, \ldots, x_n$ such that

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

Hence

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

If, for these values of $x_1, x_2, \ldots, x_n$, we define ℓ by

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

then $\ell \leq \lambda + 1$ and $C(\mathbf{x})$ has property $\mathcal{A}(p^\ell)$. □

Lemma 18.5. *If $n \geq 10$ and $C(\mathbf{x})$ does not have any of the properties $\mathcal{A}(p)$, $\mathcal{A}(p^2)$, $\mathcal{A}(p^3)$, then it is equivalent to a form of the type*

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

Proof. In the expression (18.1) for a form equivalent to C, which we denote again by C, we put $x_i = py_i$ for $i = 1, 2, 3$. This gives

$$\begin{aligned} &C(py_1, py_2, py_3, x_4, \ldots, x_n) \\ &\quad \equiv p^3 C'(y_1, y_2, y_3) + pC''(py_1, py_2, py_3, x_4, \ldots, x_n). \end{aligned}$$

Ignoring multiples of p^3, we have

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

where $C_{1,2}$ denotes a form which is of first degree in y_1, y_2, y_3 and of second degree in $x_4, \ldots, x_n$.

By Lemma 18.4, the form $C''(0,0,0,x_4,\ldots,x_n)$ does not have either property $\mathcal{A}(p)$ or $\mathcal{A}(p^2)$. We apply Lemma 18.3 to this form and put $x_i = py_i$ for $i = 4, 5, 6$ in the result. Neglecting multiples of p^2, we obtain

$$\begin{aligned} &C''(0,0,0,py_4,py_5,py_6,x_7,\ldots,x_n) \\ &\quad \equiv pC^{(3)}(0,\ldots,0,x_7,\ldots,x_n) \pmod{p^2}. \end{aligned} \tag{18.7}$$

Further, by Lemma 18.4, the form $C^{(3)}(0,\ldots,0,x_7,\ldots,x_n)$ in $x_7, \ldots, x_n$ does not have the property $\mathcal{A}(p)$.

Putting $x_i = py_i$ for $i = 4, 5, 6$ in (18.6), and using (18.7), we obtain a result which can be written

$$C(py_1, \ldots, py_6, x_7, \ldots, x_n) \\ \equiv p^2(y_1Q_1 + y_2Q_2 + y_3Q_3) + p^2C^{(3)}(0, \ldots, 0, x_7, \ldots, x_n) \pmod{p^3}, \tag{18.8}$$

where Q_1, Q_2, Q_3 are quadratic forms in $x_7, \ldots, x_n$. It should be noted that y_4, y_5, y_6 do not appear on the right of (18.8).

Suppose one of the quadratic forms, say Q_1, is not identically $\equiv 0 \pmod{p}$. Then there exists $x_7, \ldots, x_n$ for which $Q_1 \not\equiv 0 \pmod{p}$, and we can choose y_1, y_2, y_3 so that

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

This gives

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

the values of y_4, y_5, y_6 being arbitrary. Also

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

Taking $x_i = py_i$ for $i = 1, \ldots, 6$ and noting that $\partial/\partial x_1 = p^{-1}\partial/\partial y_1$,we have values of $x_1, \ldots, x_n$ for which $C \equiv 0 \pmod{p^3}$ and $\partial C/\partial x_1 \not\equiv 0 \pmod{p^2}$. This contradicts the hypothesis that C does not have either of the properties $\mathcal{A}(p)$ or $\mathcal{A}(p^2)$.

Thus Q_1, Q_2, Q_3 are all identically $\equiv 0 \pmod{p}$ and (18.8) becomes

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

Finally, we apply Lemma 18.3 to the form $C^{(3)}(0, \ldots, 0, x_7, \ldots, x_n)$ which (as already noted) does not have the property $\mathcal{A}(p)$. We obtain

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

Putting $x_i = py_i$ for $i = 1, \ldots, 9$ we get

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

and this holds identically in $y_1, \ldots, y_9, x_{10}, \ldots, x_n$. Denoting the form on the left by

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

we have the identity

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

$\square$

Lemma 18.6. *Suppose $n \geq 10$. If in the result of Lemma 18.5 the form $C^*(x_1, \ldots, x_n)$ has the property $\mathcal{A}(p^\lambda)$ then the form $C(x_1, \ldots, x_n)$ has the property $\mathcal{A}(p^\ell)$ for some $\ell \leq \lambda + 3$.*

Proof. As we observed at the start of the proof of Lemma 18.4, the hypothesis that C^* has the property $\mathcal{A}(p^\lambda)$ implies the existence of values $y_1, \ldots, y_n$ such that

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

Since

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

identically, we have

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

and one, at least, of $\partial C/\partial y_1, \ldots, \partial C/\partial y_9, \partial C/\partial y_{10}, \ldots, \partial C/\partial y_n$ is not divisible by $p^{\lambda+3}$. Putting $x_i = py_i$ for $i = 1, \ldots, 9$ and $x_i = y_i$ for $i \geq 10$, we have one at least of $\partial C/\partial x_1, \ldots, \partial C/\partial x_n$ not divisible by $p^{\lambda+3}$, whence the result. □

Lemma 18.7. *Any non-degenerate cubic form with integral coefficients in at least 10 variables has the property $\mathcal{A}(p^\ell)$ for every prime p and a suitable ℓ depending on p. There is an upper bound for ℓ depending only on the cubic form.*

Proof. Suppose $C(\mathbf{x})$ is a cubic form with integer coefficients which does not have any of the properties $\mathcal{A}(p), \mathcal{A}(p^2), \ldots, \mathcal{A}(p^{3m})$, where m is a positive integer. By Lemma 18.5, this form is equivalent to a form of type (18.5). This implies that there is a linear transformation

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

with integral coefficients and determinant p^{n-9}, which transforms $C(x_1, \ldots, x_n)$ into another form $C^{(1)}(x_1', \ldots, x_n')$ with integral coefficients. By Lemma 18.6, the form $C^{(1)}$ does not have any of the properties $\mathcal{A}(p)$, $\mathcal{A}(p^2), \ldots, \mathcal{A}(p^{3m-3})$. By repetition, it follows that there is a linear transformation with integral coefficients and determinant $p^{(n-9)m}$ which transforms $C(\mathbf{x})$ into a form $C^{(m)}(\mathbf{y})$ with integral coefficients.

It follows from Lemma 18.1 that $h(C)$ is divisible by $p^{(n-9)m}$. Further $h(C)$ is a positive integer by Lemma 18.2. Thus

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

and this gives an upper bound for m, independent of p. This completes the proof of Lemma 18.7. $\square$

In view of Theorem 17.1 and the subsequent remarks of Chapter 17, we see that Lemma 18.7 completes the proof of the following result.

Theorem 18.1. *If $C(x_1, \ldots, x_n)$ is any cubic form with integral coefficients, and $n \geq 17$, the equation*

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

has a solution in integers $x_1, \ldots, x_n$, not all 0.