17

Cubic forms: the singular series

Putting together the results of Lemmas 15.1, 15.4 and 16.1, we have now proved that if $n \geq 17$, and if alternative A of Lemma 13.4 is excluded, and if the box $\mathfrak{B}$ is suitably chosen, then the number $\mathcal{N}(P)$ of integer points with $C(\mathbf{x}) = 0$ in the box $P\mathfrak{B}$ satisfies

$$\mathcal{N}(P) = P^{n-3}\mathfrak{S}(P^{\Delta})\left\{J_0 + o(1)\right\} + O(P^{n-3-\delta}),$$

where $\delta > 0$. The series for $\mathfrak{S}(P^{\Delta})$ in Lemma 15.4 converges absolutely if continued to infinity, provided $n \geq 17$ and alternative A is excluded, since then

$$q^{-n}\left|S_{a,q}\right| \ll q^{-\frac{1}{8}n+\varepsilon-2-\delta}$$

by Lemma 15.3. By the work of Chapter 14, the alternative A implies that $C(\mathbf{x}) = 0$ has a non-trivial integral solution. Thus we have proved:

Theorem 17.1. *If $n \geq 17$ and $\mathfrak{S} > 0$, then the equation $C(\mathbf{x}) = 0$ has a non-trivial integral solution.*

For if there is no non-trivial solution we get

$$\mathcal{N}(P) \sim P^{n-3}\mathfrak{S}J_0 \quad \text{as } P \to \infty,$$

whence $\mathcal{N}(P) \to \infty$, giving a contradiction.

Here, of course, $\mathfrak{S}$ denotes the singular series continued to infinity, i.e.

$$\mathfrak{S} = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} q^{-n}S_{a,q}.$$

It remains to prove that $\mathfrak{S} > 0$ for every cubic form in 17 or more variables. The proof of Lemma 5.1 applies to exponential sums in general (as remarked at the time), and shows that if

$$A(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} q^{-n} S_{a,q}$$

then $A(q)$ is a multiplicative function of q (for relatively prime values of q). Provided $n \geq 17$ and $C(\mathbf{x})$ does not represent zero, we have

$$|A(q)| \ll q^{1-\frac{1}{8}n+\varepsilon} \ll q^{-1-\delta}$$

by Lemma 15.3. Hence $\mathfrak{S} = \sum_q A(q)$ is absolutely convergent, and it follows that

$$\mathfrak{S} = \prod_p \chi(p),$$

where

$$\chi(p) = 1 + \sum_{\nu=1}^{\infty} A(p^\nu).$$

We also have (under the above conditions)

$$|\chi(p) - 1| \ll p^{-1-\delta},$$

so there exists p_0 such that

$$\prod_{p>p_0} \chi(p) \geq \frac{1}{2},$$

as in the Corollary to Lemma 5.2. The argument of Lemma 5.3 shows that

$$\chi(p) = \lim_{\nu\to\infty} \frac{M(p^\nu)}{p^{\nu(n-1)}},$$

where $M(p^\nu)$ denotes the number of solutions of

$$C(x_1, \ldots, x_n) \equiv 0 \pmod{p^\nu}, \quad 0 \leq x_j < p^\nu.$$

Hence, in order to prove that $\mathfrak{S} > 0$ (under the present conditions) it will suffice to prove that, for each prime p, we have

$$M(p^\nu) \geq C_p p^{\nu(n-1)}, \quad C_p > 0, \tag{17.1}$$

for all sufficiently large ν.

When we were dealing with forms of additive type, we found that the existence of just one solution of the congruence

$$a_1 x_1^k + \cdots + a_n x_n^k \equiv 0 \pmod{p^{\gamma_1}},$$

with not all of $x_1, \ldots, x_n$ divisible by p, implied the truth of (17.1) for all sufficiently large ν, provided γ_1 was a suitable exponent depending on p and k and on the powers of p dividing the various coefficients a_j. For a general form, the position is not quite so simple. It appears that one needs more than just a solution (mod p^{γ_1}); one needs a solution for which the partial derivatives $\partial C/\partial x_1, \ldots, \partial C/\partial x_n$ are not all divisible by too high a power of p. For an additive form, there is an obvious limit to the power of p, since the derivative with respect to x_j is $a_j k x_j^{k-1}$, and there is some j for which x_j is not divisible by p.

Definition. Let p be a prime and ℓ a positive integer. We say $C(\mathbf{x})$ has the property $\mathcal{A}(p^\ell)$ if there is a solution of

$$C(x_1, \ldots, x_n) \equiv 0 \pmod{p^{2\ell-1}} \tag{17.2}$$

with

$$\partial C/\partial x_i \equiv 0 \pmod{p^{\ell-1}} \quad \text{for all } i \tag{17.3}$$

and

$$\partial C/\partial x_i \not\equiv 0 \pmod{p^{\ell}} \quad \text{for some } i. \tag{17.4}$$

Lemma 17.1. *Suppose $C(\mathbf{x})$ has the property $\mathcal{A}(p^\ell)$. Then*

$$M\left(p^{2\ell-1+\nu}\right) \geq p^{(n-1)\nu},$$

and consequently $\chi(p) > 0$.

Proof. We prove by induction on ν that the congruence

$$C(x_1, \ldots, x_n) \equiv 0 \pmod{p^{2\ell-1+\nu}} \tag{17.5}$$

has at least $p^{(n-1)\nu}$ solutions satisfying (17.3) and (17.4), these solutions being mutually incongruent to the modulus $p^{\ell+\nu}$ (and therefore *a fortiori* to the modulus $p^{2\ell-1+\nu}$). This will imply the result. When $\nu = 0$ the assertion is simply that of the hypothesis.

For any integers $x_1, \ldots, x_n$, $u_1, \ldots, u_n$ we have

$$C(\mathbf{x} + p^{\ell+\nu}\mathbf{u}) \equiv C(\mathbf{x}) + p^{\ell+\nu}(u_1 \partial C/\partial x_1 + \cdots) \pmod{p^{2\ell+2\nu}}.$$

We assume that the result just stated holds for a particular ν, and we take $x_1, \ldots, x_n$ to be any one of the $p^{(n-1)\nu}$ solutions of (17.5) which satisfy (17.3) and (17.4), these solutions being mutually incongruent to the modulus $p^{\ell+\nu}$. We can put

$$C(\mathbf{x}) = ap^{2\ell-1+\nu}, \quad \partial C/\partial x_i = D_i p^{\ell-1},$$

where $a, D_1, \dots, D_n$ are integers and $D_i \not\equiv 0 \pmod{p}$ for some i. The congruence

$$C(\mathbf{x} + p^{\ell+\nu}\mathbf{u}) \equiv 0 \pmod{p^{2\ell+\nu}}$$

holds if

$$a + D_1 u_1 + \cdots + D_n u_n \equiv 0 \pmod{p}.$$

This has p^{n-1} solutions in $\mathbf{u}$, mutually incongruent (mod p).

Thus corresponding to each $\mathbf{x}$ we get p^{n-1} values of $\mathbf{y} = \mathbf{x} + p^{\ell+\nu}\mathbf{u}$. These satisfy

$$C(\mathbf{y}) \equiv 0 \pmod{p^{2\ell+\nu}}, \quad \mathbf{y} \equiv \mathbf{x} \pmod{p^{\ell+\nu}}.$$

From the latter it follows that each $\mathbf{y}$ satisfies (17.3) and (17.4). We obtain altogether $p^{(n-1)(\nu+1)}$ values for $\mathbf{y}$ and they are mutually incongruent to the modulus $p^{\ell+\nu+1}$. Hence the assertion holds for $\nu+1$ in place of ν, and this proves the result. $\square$

The proof that for each p there is some ℓ such that $C(\mathbf{x})$ has the property $\mathcal{A}(p^\ell)$ forms the subject of the next chapter.