7

The equation $c_1x_1^k + \cdots + c_sx_s^k = N$

We next consider the problem of representing a large positive integer N in the form $c_1x_1^k + \cdots + c_sx_s^k$, where $c_1, \ldots, c_s$ are given positive integers and $x_1, \ldots, x_s$ are arbitrary positive integers. It is not true, without some further supposition, that every large N is representable if $s \geq s_0(k)$ for some $s_0(k)$. For suppose that $c_1, \ldots, c_{s-1}$ are all divisible by some prime p and that c_s is not. Then an integer N, not divisible by p, can certainly not be representable if it does not have the same kth power character as c_s to the modulus p.

We can obviously suppose, in treating the equation in the title, that $c_1, \ldots, c_s$ do not all have a common factor. We shall find it necessary to postulate, in order to ensure solubility, that the congruence

$$c_1x_1^k + \cdots + c_sx_s^k \equiv N \pmod{p^\nu}$$

is soluble for each prime p and all sufficiently large ν, with not all the terms $c_1x_1^k, \cdots, c_sx_s^k$ divisible by p (or to make some other supposition from which this can be deduced).

Only slight changes are needed in the preceding work to adapt it to this more general equation. We define $P_j = [(N/c_j)^{1/k}]$ to be the integer part of $(N/c_j)^{1/k}$, and we define

$$T_j(\alpha) = \sum_{x=1}^{P_j} e(\alpha c_j x^k). \tag{7.1}$$

Weyl's inequality (Lemma 3.1) applies to the sum $T_j(\alpha)$; if $\alpha = a/q + \beta$ and $|\beta| < q^{-2}$ then $c_j\alpha = c_ja/q + c_j\beta$, and $|c_j\beta| \ll q^{-2}$. This is sufficient for the proof of Lemma 3.1, since all we used about β was that $|\beta| \ll q^{-2}$.

Hua's inequality (Lemma 3.2) remains valid for any one sum, since

$$\begin{aligned}\int_0^1 |T_j(\alpha)|^{2^k}\ d\alpha &= \int_0^1 \left|\sum_{x=1}^{P_j} e(\alpha c_j x^k)\right|^{2^k} d\alpha \\ &= \frac{1}{c_j}\int_0^{c_j} \left|\sum_{x=1}^{P_j} e(\alpha x^k)\right|^{2^k} d\alpha \\ &= \int_0^1 \left|\sum_{x=1}^{P_j} e(\alpha x^k)\right|^{2^k} d\alpha \quad \text{(by periodicity)} \\ &\ll P_j^{2^k-k+\varepsilon}.\end{aligned}$$

This inequality also extends to any product of 2^k sums, by Hölder's inequality; we obtain

$$\int_0^1 |T_1(\alpha)\cdots T_{2^k}(\alpha)|\ d\alpha \ll (P_1\cdots P_{2^k})^{1-k/2^k+\varepsilon}. \tag{7.2}$$

We define major and minor arcs as before. Lemma 4.1 now states that if $s \geq 2^k+1$, then

$$\int_{\mathfrak{m}} |T_1(\alpha)\cdots T_s(\alpha)|\ d\alpha \ll P^{s-k-\delta'},$$

the proof being as before, using (7.2). Lemma 4.2 is unchanged, except that $I(\beta)$ is replaced by

$$I_j(\beta) = \int_0^{P_j} e(\beta c_j \xi^k)\ d\xi.$$

It simplifies the later calculations slightly, however, if the upper limit is replaced by $Pc_j^{-1/k}$, where $P = N^{1/k}$; the difference is negligible.

The proofs of Lemma 4.3 and Theorem 4.1 apply to the present problem with only slight changes. One difference is that the change of variable which is made in $I_j(\beta)$ in order to express it in terms of $\int_0^1 e(\gamma\xi^k)\ d\xi$ produces a factor $|c_j|^{-1/k}$. Another difference is that the singular series is of a slightly more general form; it is now given by

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-s} S_{c_1 a,q}\cdots S_{c_s a,q} e(-Na/q). \tag{7.3}$$

To establish the absolute convergence of this series for $s \geq 2^k + 1$ using the Corollary to Lemma 3.1, or for $s \geq 2k + 1$ using Lemma 6.4, we need to extend an estimate for $S_{a,q}$ when $(a, q) = 1$ so that it applies to $S_{ca,q}$, where c is any fixed positive integer. This is an easy matter, for if $ca/q = a'/q'$ then

$$S_{ca,q} = \frac{q}{q'} S_{a',q'},$$

and q/q', being a divisor of c, is bounded.

In this way we can prove the following more general form of Theorem 4.1:

Theorem 7.1. *Let $c_1, \ldots, c_s$ be fixed positive integers. Then if $s \geq 2^k + 1$, the number $r(N)$ of representations of N as*

$$N = c_1x_1^k + \cdots + c_sx_s^k, \quad (x_1, \ldots, x_s > 0),$$

satisfies

$$r(N) = \frac{C_{k,s}}{(c_1c_2 \cdots c_s)^{1/k}} N^{s/k-1}\mathfrak{S}(N) + O(N^{s/k-1-\delta}) \tag{7.4}$$

for some fixed $\delta > 0$, where $C_{k,s}$ is as in Theorem 4.1, and $\mathfrak{S}(N)$ is defined by (7.3). The series (7.3) is absolutely convergent for $s \geq 2k+1$.

Lemmas 5.1, 5.2, 5.3 on the factorization of the singular series and on the relation between the singular series and $M(p^\nu)$, still apply. Thus in order that $\mathfrak{S}(N)$ may have a positive lower bound independent of N, it suffices if, for each p, the number $M(p^\nu)$ of solutions of

$$c_1x_1^k + \cdots + c_sx_s^k \equiv N \pmod{p^\nu}$$

satisfies

$$M(p^\nu) \geq C_p p^{\nu(s-1)}$$

for all sufficiently large ν.

Defining γ as before, and using Lemma 5.4, we find, as in Lemma 5.5, that a sufficient condition for this is that the congruence

$$c_1x_1^k + \cdots + c_sx_s^k \equiv N \pmod{p^\nu} \tag{7.5}$$

shall have a solution with not all of $c_1x_1^k, \ldots, c_sx_s^k$ divisible by p. Hence:

Theorem 7.2. *Let γ be defined by (5.11). Suppose that $s \geq 2k + 1$,*

and suppose that for each[1] *prime p the congruence (7.5) has a solution in which not all of $c_1x_1^k, \ldots, c_sx_s^k$ are divisible by p. Then for all N satisfying this hypothesis, we have*

$$\mathfrak{S}(N) \geq C(k,s) > 0.$$

By Theorems 7.1 and 7.2, if $s \geq 2^k + 1$ then $r(N) \to \infty$ as $N \to \infty$, provided N is restricted to numbers which satisfy the congruence condition of Theorem 7.2. Since the congruence condition is needed only for $p \leq p_0$, and since γ is independent of N, the numbers N which satisfy the congruence condition will certainly include all numbers in some arithmetic progression.

If we make the hypothesis that the coefficients $c_1, \ldots, c_s$ are relatively prime in pairs, we can show that the congruence condition is satisfied for all N provided s exceeds some specific function of k. We prove:

Theorem 7.3. *Suppose that $(c_i, c_j) = 1$ for $1 \leq i < j \leq s$, and suppose that $s \geq k(2k-1)+2$ (k odd) or $s \geq 2k(4k-1)+2$ (k even). Then*

$$\mathfrak{S}(N) \geq C(k,s) > 0.$$

Proof. We have to prove that, under the conditions stated, the congruence (7.5) has a solution with not all of $c_1x_1^k, \ldots, c_sx_s^k$ divisible by p. Since at most one of $c_1, \ldots, c_s$ can be divisible by p, it will be enough to solve

$$c_1x_1^k + \cdots + c_sx_s^k \equiv N \pmod{p^\gamma} \tag{7.6}$$

with not all of $x_1, \ldots, x_{s-1}$ divisible by p, on the supposition that none of $c_1, \ldots, c_{s-1}$ is divisible by p.

Suppose $p > 2$. We saw in the proof of Lemma 5.6 that the number of distinct values assumed by z^k to the modulus p^γ, when $z \not\equiv 0 \pmod{p}$, is $(p-1)/\delta$, where $\delta = (k_0, p-1)$. Hence the number of different classes of kth power residues and non-residues (mod p^γ) is

$$\frac{\phi(p^\gamma)}{(p-1)/\delta} = \frac{p^{\gamma-1}(p-1)\delta}{p-1} = p^{\gamma-1}\delta.$$

(These classes are the cosets of the subgroup of kth powers in the whole group of the relatively prime residue classes.)

[1] It suffices, of course, to suppose this for $p \leq p_0(k,s)$; see the Corollary to Lemma 5.2.

If we divide the coefficients $c_1, \ldots, c_{s-1}$ into sets according to the class of kth power residues or non-residues to which a coefficient belongs, there will be one class containing at least $(s-1)/p^{\gamma-1}\delta$ coefficients. Let t be the least integer $\geq (s-1)/p^{\gamma-1}\delta$. We can take the coefficients in question to be the first t coefficients, and then $c_2 \equiv d_2^k c_1, \ldots, c_t \equiv d_t^k c_1 \pmod{p^\gamma}$, where the d_i are not divisible by p. Putting the variables $x_{t+1}, \ldots$ in (7.6) equal to 0, and cancelling c_1, we see that it suffices to solve

$$x_1^k + (d_2x_2)^k + \cdots + (d_tx_t)^k \equiv N' \pmod{p^\gamma}$$

with not all the variables divisible by p. This is in effect the same as the congruence considered in Lemma 5.6 in connection with Waring's problem. We proved there that the result holds provided $t \geq 2k$. Hence it suffices if

$$\frac{s-1}{p^{\gamma-1}\delta} > 2k - 1.$$

Since $\gamma - 1 = \tau$ and $p^\tau\delta \leq p^\tau k_0 = k$, it suffices if $s - 1 > k(2k-1)$.

Suppose $p = 2$. First, if $\tau = 0$ (so that k is odd), the congruence (7.6) is soluble even if it has only one term provided N is odd, since x^k assumes all values (mod p^γ). Hence it is soluble with two terms whether N is odd or even, so it suffices if $s - 1 \geq 2$. Thus the conclusion of the theorem holds if k is odd.

Now suppose $\tau \geq 1$, so that k is even. Since each coefficient c_i is odd (for $i \leq s-1$), it can assume $2^{\gamma-1}$ possible values to the modulus 2^γ. Hence there is some set of t mutually congruent coefficients, where $t \geq (s-1)/2^{\gamma-1}$. Putting the variables corresponding to the other coefficients equal to 0, we see that it suffices to solve

$$x_1^k + \cdots + x_t^k \equiv N' \pmod{2^\gamma}$$

with not all the variables even. As in the proof of Lemma 5.6, it suffices if $t \geq 4k$. Hence it suffices if

$$\frac{s-1}{2^{\gamma-1}} > 4k - 1.$$

Since $k \geq 2^\tau$ and $\gamma = \tau + 2$, we have $2^{\gamma-1} \leq 2k$. Hence it suffices if $s - 1 > 2k(4k-1)$. This proves Theorem 7.3 in the case when k is even. □

It follows from Theorems 7.1 and 7.3 that we can name a number $s_1(k)$ such that if $s \geq s_1(k)$ then $r(N) \to \infty$ as $N \to \infty$; always on the assumption that the coefficients c_j are relatively prime in pairs. The numbers given in Theorem 7.3 are by no means best possible; we

have merely given those which turn up naturally from the simple line of argument used in the proof. In principle, one can relax the condition that the coefficients are relatively prime in pairs; what is essential for the truth of the result just stated is that, for any prime p, a certain number of the coefficients are not divisible by p.