§14. Smooth Numbers.

In preparation for an account of efficient differencing, we discuss the basic properties of smooth numbers. Let X be a large real number, and suppose that Y is a real number with $2 \le Y \le X$. We define the set of Y-smooth numbers not exceeding X by putting

$$\mathcal{A}(X,Y) = \{ n \le X : p \mid n \Rightarrow p \le Y \}.$$

We shall be interested in the situation in which $Y \approx X^\eta$, with η a very small positive number. In applications to factorisation algorithms, one is interested in the rather smoother situation in which $Y \approx \exp(c\sqrt{\log X \log\log X})$ for a positive c.

Put $$A(X,Y) = \operatorname{card}(\mathcal{A}(X,Y)).$$

The behaviour of $A(X,Y)$ in terms of X and Y is described by Dickman's function $\rho : \mathbb{R}_{\ge} \to \mathbb{R}_{\ge}$, defined for real numbers u by putting

$$\rho(u) = 0, \quad \text{for} \quad u \le 0,$$

$$\rho(u) = 1, \quad \text{for} \quad 0 < u \le 1,$$

and via the notation

$$u\rho'(u) = -\rho(u-1), \quad \text{for} \quad u > 1.$$

Implicit in this definition is the assertion that ρ is continuous for $u \neq 0$ and differentiable when $u \notin \{0,1\}$. For large values of u, one has $\rho(u) \approx u^{-u}$, and indeed $\rho(u) \le 1/\lfloor u \rfloor!$. Of importance to us is the observation that $\rho(u) > 0$ whenever $u > 0$.

Lemma 14.1. The function $\rho : \mathbb{R} \to \mathbb{R}$ is positive and strictly decreasing for $u \in [1,\infty)$.

Proof: When $u \ge 1$, one has

$$u\rho(u) = \int_{u-1}^{u} \rho(v)\,dv,$$

as we now confirm. Observe first that when $u = 1$, one has

$$\rho(1) = 1 = \int_0^1 \rho(v)\,dv.$$

On the other hand, when $u > 1$ one has

$$u\rho(u) = \int_0^u v\rho'(v) + \rho(v)\,dv$$

$$= \int_0^u \rho(v) - \rho(v-1)\,dv$$

$$= \int_{u-1}^{u} \rho(v)\,dv.$$

Suppose, by way of deriving a contradiction, that ρ is not positive on $[1,\infty)$. Then since $\rho(1) = 1$, it follows via continuity that there exists some $u_0 \in [1,\infty)$ with $\rho(u_0) = 0$, and we may suppose that u_0 is the least such value. But then

$$0 = u_0\rho(u_0) = \int_{u_0-1}^{u_0} \rho(v)\,dv > 0,$$

yielding a contradiction. Thus $\rho(u)$ is positive on $[1,\infty)$, and hence

$$\rho'(u) = -\frac{\rho(u-1)}{u} < 0 \quad \text{for } u > 1,$$

so that ρ is decreasing on $[1,\infty)$. //

Our interest in Dickman's function is connected with the asymptotic formula contained in the next lemma.

<u>Lemma 14.2.</u> There is a positive number B with the property that, whenever $u > 0$ and $X \geq 1$, one has

$$|A(X, X^{1/u}) - X\rho(u)| \leq B^u X (\log 2X)^{-1}.$$

Proof. We proceed by induction. First we observe that when $0 < u \le 1$, one has

$$|A(X, X^{1/u}) - X\rho(u)| = |\lfloor X \rfloor - X| < 1 \le X/(\log 2X).$$

Next, when $1 < u \le 2$, we see that $\rho'(u) = -\rho(u-1)/u$, whence

$$\rho(u) - \rho(1) = -\int_1^u \frac{\rho(v-1)}{v}\,dv = -\int_1^u \frac{dv}{v} = -\log u,$$

so that $\rho(u) = 1 - \log u$. On the other hand, one has

$$A(X, X^{1/u}) = \sum_{\substack{1 \le n \le X \\ p \mid n \Rightarrow p \le X^{1/u}}} 1 = \lfloor X \rfloor - \sum_{X^{\frac{1}{u}} < p \le X} \sum_{\substack{1 \le n \le X \\ p \mid n}} 1$$

$$= \lfloor X \rfloor - \sum_{X^{\frac{1}{u}} < p \le X} \left\lfloor \frac{X}{p} \right\rfloor$$

$$= X - X \sum_{X^{\frac{1}{u}} < p \le X} \frac{1}{p} + O\Big(\sum_{p \le X} 1 \Big).$$

Now recall from basic versions of the prime number theorem that

$$\sum_{p \le X} 1 \ll \frac{X}{\log X} \quad \text{and} \quad \sum_{p \le X} \frac{1}{p} = \log\log X + b + O(1/\log x),$$

for a suitable constant b (Mertens). Thus

$$A(X, X^{\frac{1}{u}}) = X - X \log\left(\frac{\log X}{\log X^{1/u}}\right) + O\left(\frac{X}{\log X}\right)$$

$$= X(1 - \log u) + O\left(\frac{X}{\log X}\right)$$

$$= X\rho(u) + O\left(\frac{X}{\log X}\right).$$

This confirms the conclusion of the lemma for $1 < u \le 2$. □

We now suppose that the conclusion of the lemma holds for $1 < u \le n$, for some integer $n \ge 2$, and seek to establish that it remains true for $n < u \le n+1$. The desired conclusion then follows by induction. We may therefore suppose that

$$|A(X, X^{1/u}) - X\rho(u)| \le B^u X (\log 2X)^{-1} \quad \text{for } 1 < u \le n.$$

Suppose that $n < u \le n+1$. We have

$$A(X, X^{1/u}) = \underset{\uparrow}{1} + \sum_{p \le X^{1/u}} |\{n \le X : \text{largest prime factor of } n \text{ is } p\}|.$$

for $n = 1$

$$= 1 + \sum_{p \le X^{1/u}} A(X/p, p),$$

so that

$$A(X, X^{1/n}) - A(X, X^{1/u}) = \sum_{X^{\frac{1}{u}} < p \le X^{\frac{1}{n}}} A(X/p, p).$$

(Buchstab's identity).

Notice that for the summands p occurring on the right hand side here,

$$n-1 < \frac{\log(X/p)}{\log p} = \frac{\log X}{\log p} - 1 \le u - 1 \le n,$$

so we may apply the inductive hypothesis to deduce that

$$\left| A(X, X^{1/n}) - A(X, X^{1/u}) - \sum_{X^{\frac{1}{u}} < p \le X^{\frac{1}{n}}} \frac{X}{p} \rho\left(\frac{\log(X/p)}{\log p}\right) \right| \le \sum_{X^{\frac{1}{u}} < p \le X^{\frac{1}{n}}} \frac{X/p}{\log(2X/p)} \cdot B^{\frac{\log(X/p)}{\log p}}.$$

Put

$$F(w) = \sum_{p \le w} \frac{1}{p},$$

so that $F(w) = \log\log w + b + r(w)$,

with $r(w) = O(1/\log w)$. Then by Riemann-Stieltjes integration, we obtain

$$\sum_{X^{\frac{1}{u}} < p \le X^{\frac{1}{n}}} \frac{1}{p} \rho\left(\frac{\log(X/p)}{\log p}\right) = \int_{X^{\frac{1}{u}}}^{X^{1/n}} \rho\left(\frac{\log X}{\log w} - 1\right) d F(w)$$

⑤

$$= \int_{X^{1/u}}^{X^{1/n}} \rho\left(\frac{\log X}{\log w} - 1\right) d(\log\log w)$$

$$+ \int_{X^{1/u}}^{X^{1/n}} \rho\left(\frac{\log X}{\log w} - 1\right) d\, r(w).$$

Put $t = \dfrac{\log X}{\log w}$, so that $d\log\log w = \dfrac{dw}{w\log w} = -\dfrac{dt}{t}$

$$\Downarrow$$

$$\log\log w = \log\log X - \log t.$$

Then

$$\int_{X^{1/u}}^{X^{1/n}} \rho\left(\frac{\log X}{\log w} - 1\right) d(\log\log w) = -\int_u^n \rho(t-1)\frac{dt}{t}.$$

Meanwhile, by integrating by parts, we find that

$$\int_{X^{1/u}}^{X^{1/n}} \rho\left(\frac{\log X}{\log w} - 1\right) dr(w) = \left[\rho\left(\frac{\log X}{\log w} - 1\right) r(w)\right]_{X^{1/u}}^{X^{1/n}}$$

$$- \int_{X^{1/u}}^{X^{1/n}} r(w)\, d\, \rho\left(\frac{\log x}{\log w} - 1\right)$$

$$\ll \frac{1}{\log X}\left(1 + \int_{X^{1/u}}^{X^{1/n}} \left| d\,\rho\left(\frac{\log X}{\log w} - 1\right)\right|\right)$$

$$\ll \frac{1}{\log X} \quad \text{(since } \rho \text{ is monotonic decreasing and bounded).}$$

Thus far we have shown that

$$\left| A(X, X^{1/n}) - A(X, X^{1/u}) + X\int_u^n \rho(t-1)\frac{dt}{t}\right| \ll \frac{X}{\log X} + X\sum_{X^{\frac{1}{u}} < p \le X^{\frac{1}{n}}} \frac{1/p}{\log(2X/p)}\, B^{\frac{\log(X/p)}{\log p}}.$$

The error term here is (with a uniformly bounded absolute constant)

at most

$$\tfrac{1}{4}B\left(\frac{X}{\log 2X} + \frac{X}{\log 2X}B^{u-1}\sum_{X^{\frac{1}{u}}<p\le X^{\frac{1}{n}}}\frac{1}{p}\right)$$

$$\le \tfrac{1}{4}B\left(\frac{X}{\log 2X}B^{u-1}\left(\log\left(\frac{\log X^{\frac{1}{n}}}{\log X^{1/u}}\right)+O\left(\frac{1}{\log 2X}\right)\right)\right.$$

$$\left. + X/\log 2X\right)$$

$$\le \tfrac{1}{4}B\left(1+B^{u-1}\log\left(\tfrac{u}{n}\right)\right)\frac{X}{\log 2X} + \frac{\frac{1}{4}BX}{\log 2X}.$$

Finally, by the inductive hypothesis, we have

$$|A(X,X^{1/n}) - X\rho(n)| \le B^n X(\log 2X)^{-1},$$

so that

$$\left|A(X,X^{1/u}) - X\left(\rho(n)+\int_u^n \rho(t-1)\frac{dt}{t}\right)\right| \le B^u X(\log 2X)^{-1}.$$

But $$\int_u^n \frac{\rho(t-1)}{t}\,dt = -\int_u^n \rho'(t)\,dt = \rho(u)-\rho(n),$$

so that

$$|A(X,X^{1/u}) - X\rho(u)| \le B^u X/(\log 2X),$$

confirming the inductive hypothesis for $n<u\le n+1$. //

In our subsequent applications, we shall use the set $\mathcal{A}(X,X^\eta)$, with η a sufficiently small positive number. We may henceforth assume that

$$|\mathcal{A}(X,X^\eta)| = c_\eta X + O(X/\log X),$$

with $c_\eta > 0$.

Suppose next that $n \in \mathcal{A}(X, X^\eta)$ and $n > Y$. Then it follows that there is a divisor m of n with

$$Y < m \leq YX^\eta.$$

To confirm this assertion, observe that each prime divisor of n is at most X^η. Then if m_0 is the largest divisor of n not exceeding Y, we have $Y < m_0 p \leq YX^\eta$ for any prime divisor p of n/m_0.

Our strategy is now to imitate the diminishing ranges argument in which one observes that if

$$x^k - y^k = h,$$

with $\frac{1}{2}X < x, y \leq 2X$ and $|h| < X^{k-1}$, then in fact $h = 0$ and $x = y$. To do this, we seek to arrive at a similar situation with

$$x^k - y^k = m^k h,$$

with $\frac{1}{2}X < x, y \leq 2X$, $|h| < X^{k-1}$ and $m^k > X$. It is tempting to suppose that this ensures that

$$x^k \equiv y^k \pmod{m^k} \quad \Rightarrow \quad x \equiv y \pmod{m^k},$$

whence $m^k \mid (x-y)$ and $m^k > |x-y| \Rightarrow x = y$.

This would follow when k is odd and m is a prime p with $(p-1, k) = 1$, for example, but not (quite) in general.

Our next step is to study this problem, and also to supply an auxiliary estimate.

§15. Congruences and divisibility :

In this section we shall be concerned with the solubility of the congruence

$$\Psi(z) \equiv h \pmod{m^k},$$

with $(\Psi'(z), m) = 1$, in which $\Psi \in \mathbb{Z}[z]$ is a polynomial of degree $d \geq 1$. Let $\mathcal{B}(h;m)$ denote the set of solutions of this congruence with $1 \leq z \leq m^k$ satisfying the associated coprimality condition.

Lemma 15.1. For each $\varepsilon > 0$, one has

$$\operatorname{card}(\mathcal{B}(h;m)) \ll m^{\varepsilon}.$$

Proof. Suppose that $m = \prod_{p^k \| m} p^{kl_p}$ is a prime factorisation of m into prime powers. Then it follows from the Chinese Remainder Theorem that

$$\operatorname{card}(\mathcal{B}(h;m)) = \prod_{p^k \| m} \operatorname{card}(\mathcal{B}(h; p^{kl_p})).$$

But $\mathcal{B}(h; p^{kl_p})$ is the set of solutions of the congruence

$$\Psi(z) \equiv h \pmod{p^{kl_p}},$$

with $(\Psi'(z), p) = 1$ and $1 \leq z \leq p^{kl_p}$. The number of solutions of this congruence modulo p is at most $\deg \Psi = d$, and each solution lifts uniquely to a corresponding solution modulo p^{kl_p}. Thus $\operatorname{card}(\mathcal{B}(h; p^{l_p})) \leq d$, whence

$$\operatorname{card}(\mathcal{B}(h;m)) \leq d^{\omega(m)} \leq d^{c \log m / \log\log m} \ll m^{\varepsilon}.$$

It may happen ~~that~~ given $n \in [X, X^2]$, we seek a divisor m of n which is coprime to a specified integer q. In this context, it is very awkward if all or much of n has all of its divisors dividing q, say $n \mid q^\infty$. Fortunately, the set of such integers is extremely sparse.

Lemma 15.2. Suppose that q is a natural number and X is a large real number. ~~Suppose also that for some fixed positive number C, one has $q \le X^C$~~. Then one has

$$\text{card}\{ n \le X : n \mid q^\infty \} \ll (qX)^\varepsilon.$$

Proof. One has, for each $\delta > 0$,

$$\sum_{\substack{n \le X \\ n \mid q^\infty}} 1 \le X^\delta \prod_{p \mid q} \left(1 + \frac{1}{p^\delta} + \frac{1}{p^{2\delta}} + \cdots\right)$$

$$= X^\delta \prod_{p \mid q} \left(1 - \frac{1}{p^\delta}\right)^{-1} \le X^\delta (1 - 2^{-\delta})^{-\omega(q)}$$

$$\le X^\delta e^{A\delta \log q / \log\log q}, \text{ for some fixed } A > 0 \text{ depending on } \delta.$$

Thus $\text{card}\{n \le X : n \mid q^\infty\} \ll X^\delta q^\varepsilon$. Since this holds for all $\delta > 0$, the conclusion of the lemma follows.

In accordance with the discussion in the preamble to this lemma, we write

$$x \; \mathcal{D}(X) \; y \qquad \text{(an extended divisor notation)}$$

to indicate that there is a divisor d of x with $d \le X$ such that $(x/d) \mid y^\infty$.

§16. The Fundamental Lemma.

We consider a fairly general situation. Let $\Psi(z; \underline{a})$ denote a polynomial with integer coefficients in the main variable z and auxiliary variables $\underline{a} = (a_1, \dots, a_t)$ of positive degree in terms of z. We then abbreviate

$$\frac{\partial}{\partial z}\Psi(z; \underline{a}) \quad \text{by} \quad \Psi'(z; \underline{a}).$$

Note: We assume that the integers c_i are bounded by some positive power of P and $1 \le z \le P$.

Our basic mean value is

$$S_s(P, Q, R) = S_s(P, Q, R; \Psi; \mathcal{U}),$$

the number of integral solutions of the equation

$$\Psi(z; \underline{\tilde{u}}) - \Psi(w; \underline{\tilde{v}}) = \sum_{i=1}^{s} (x_i^k - y_i^k), \qquad (16.1)$$

with

$$x_j, y_j \in \mathcal{A}(Q, R) \quad (1 \le j \le s), \qquad 1 \le z, w \le P,$$

$$\underline{\tilde{u}}, \underline{\tilde{v}} \in \mathcal{U},$$

where $\mathcal{U}$ is a subset of $([1, CP] \cap \mathbb{Z})^t$ for some fixed $C > 0$, $C = C(\Psi, k)$, and $\operatorname{card}(\mathcal{U}) = \mathcal{U}$, say.

We also have the auxiliary mean value

$$T_s(P, Q, R; M) = T_s(P, Q, R; M; \Psi; \mathcal{U})$$

which counts the number of integral solutions of the equation

$$\Psi(z; \underline{\tilde{u}}) - \Psi(w; \underline{\tilde{v}}) = m^k \sum_{i=1}^{s} (u_i^k - v_i^k), \qquad (16.2)$$

with

$$M < m \le MR, \qquad u_j, v_j \in \mathcal{A}(Q/M, R) \quad (1 \le j \le s),$$

$$1 \le z, w \le P, \qquad z \equiv w \pmod{m^k},$$

$$\underline{\tilde{u}} \in \mathcal{C}.$$

Finally, there is another (singular) mean value

$$N_s(P,Q,R) = N_s(P,Q,R;\Psi;\mathcal{U})$$

which counts the number of integral solutions of the equation (16.1) subject to

$$\Psi'(z;\underline{u}) = \Psi'(w;\underline{v}) = 0.$$

Theorem 16.1. (W' 1990) Suppose that $1 < M < Q \le P$. Then one has

$$S_s(P,Q,R) \ll_{\Psi} S_s(P,M,R) + N_s(P,Q,R) + P^{\varepsilon}QM\, S_{s-1}(P,Q,R) + P^{\varepsilon}|\mathcal{C}|(MR)^{2s-1}\, T_s(P,Q,R;M).$$

Proof. We classify the solutions of the equation (16.1) into four types, and examine each type in turn:

• Let $S^{(1)}$ denote the number of solutions of (16.1) counted by $S_s(P,Q,R)$ for which, for at least one index j, one has $\min\{x_j, y_j\} \le M$.

• Let $S^{(2)}$ denote the number of solutions of (16.1) counted by $S_s(P,Q,R)$ for which $\min\{x_j, y_j\} > M$ for every index j, and

$$\Psi'(z;\tilde{\underline{u}}) = 0 \quad \text{or} \quad \Psi'(w;\tilde{\underline{v}}) = 0.$$

• Let $S^{(3)}$ denote the number of solutions of (16.1) counted by $S_s(P,Q,R)$ for which $\min\{x_j, y_j\} > M$ for every index j, one has $\Psi'(z;\tilde{\underline{u}}) \neq 0$ and $\Psi'(w;\tilde{\underline{v}}) \neq 0$, and further, for at least one index j, one has

$$x_j\, \mathcal{D}(M)\, \Psi'(z;\tilde{\underline{u}}) \quad \text{or} \quad y_j\, \mathcal{D}(M)\, \Psi'(w;\tilde{\underline{v}}).$$

• Let $S^{(4)}$ denote the number of solutions of (16.1) counted by $S_s(P,Q,R)$ for which $\min\{x_j, y_j\} > M$ for every index j, one has $\Psi'(z;\tilde{\underline{u}}) \neq 0$ and $\Psi'(w;\tilde{\underline{v}}) \neq 0$, & one has neither $x_j\, \mathcal{D}(M)\, \Psi'(z;\tilde{\underline{u}})$ nor $y_j\, \mathcal{D}(M)\, \Psi'(w;\tilde{\underline{v}})$ for any index j.

Then

$$S_s(P,Q,R) \leq 4 \max\{S^{(1)}, S^{(2)}, S^{(3)}, S^{(4)}\}.$$

We now bound each $S^{(\ell)}$ $(\ell = 1,2,3,4)$ in turn:

(i) The treatment of $S^{(1)}$. Suppose first that $S^{(1)} \geq \max\{S^{(2)}, S^{(3)}, S^{(4)}\}$, so that $S_s(P,Q,R) \leq 4S^{(1)}$. We write

$$f(\alpha; X, R) = \sum_{x \in \mathcal{A}(X,R)} e(\alpha x^k)$$

and

$$F(\alpha; P[illegible]) = \sum_{\substack{1 \leq z \leq P \\ \tilde{u} \in \mathcal{C}}} e(\alpha \Psi(z; \tilde{u})).$$

Then, by orthogonality, one has

$$S^{(1)} \leq 2s \int_0^1 |F(\alpha; P[illegible])^2 f(\alpha; M, R) f(\alpha; Q, R)^{2s-1}| \, d\alpha.$$

By Hölder's inequality, therefore, we see that

$$\begin{aligned} S_s(P,Q,R) &\leq 8s \left(\int_0^1 |F(\alpha; P[illegible])^2 f(\alpha; M, R)^{2s}| \, d\alpha \right)^{\frac{1}{2s}} \\ &\quad \cdot \left(\int_0^1 |F(\alpha; P[illegible])^2 f(\alpha; Q, R)^{2s}| \, d\alpha \right)^{1-\frac{1}{2s}} \\ &= 8s \, S_s(P,M,R)^{\frac{1}{2s}} S_s(P,Q,R)^{1-\frac{1}{2s}}, \end{aligned}$$

whence

$$S_s(P,Q,R) \leq (8s)^{2s} S_s(P,M,R).$$

This confirms the conclusion of the theorem in the first case. □

(ii) The treatment of $S^{(2)}$. We suppose that $S^{(2)} \geq \max\{S^{(3)}, S^{(4)}, S^{(1)}\}$, so that $S_s(P,Q,R) \leq 4S^{(2)}$. We write

$$G(\alpha; P[illegible]) = \sum_{\substack{1 \leq z \leq P \\ \tilde{u} \in \mathcal{C} \\ \Psi'(z; \tilde{u}) = 0}} e(\alpha \Psi(z; \tilde{u})).$$

Then it follows from orthogonality that

$$S^{(2)} \le 2 \int_0^1 |F(\alpha; P) G(\alpha; P) f(\alpha; Q, R)^{2s}| \, d\alpha.$$

By Schwarz's inequality, therefore, one has

$$S_s(P,Q,R) \le 8 \Big(\int_0^1 |F(\alpha; P)^2 f(\alpha; Q, R)^{2s}| \, d\alpha \Big)^{\frac{1}{2}} \times \Big(\int_0^1 |G(\alpha; P)^2 f(\alpha; Q, R)^{2s}| \, d\alpha \Big)^{\frac{1}{2}}$$

$$= 8 S_s(P,Q,R)^{\frac{1}{2}} N_s(P,Q,R)^{\frac{1}{2}},$$

whence

$$S_s(P,Q,R) \le 64 N_s(P,Q,R).$$

This confirms the conclusion of the theorem in the second case. □

(iii) The treatment of $S^{(3)}$. We suppose that $S^{(3)} \ge \max\{S^{(4)}, S^{(1)}, S^{(2)}\}$, so that $S_s(P,Q,R) \le 4 S^{(3)}$. We must work harder in this situation. Consider a fixed value of z and $\underline{u}$ with $1 \le z \le P$ and $\tilde{\underline{u}} \in \mathcal{C}$ satisfying $\Psi'(z; \tilde{\underline{u}}) \ne 0$. Denote by $\mathcal{S}(z; \tilde{\underline{u}})$ the set of integers x with $1 \le x \le Q$ having the property that x has a divisor d with $1 \le d \le M$ such that x/d has all of its prime divisors amongst those of $\Psi'(z; \tilde{\underline{u}})$. We then write

$$H(\alpha; P, Q, R) = \sum_{\substack{1 \le z \le P \\ \tilde{\underline{u}} \in \mathcal{C} \\ \Psi'(z; \tilde{\underline{u}}) \ne 0}} \sum_{x \in \mathcal{S}(z; \tilde{\underline{u}})} e\big(\alpha(x^k + \Psi(z; \tilde{\underline{u}}))\big).$$

Then it follows via orthogonality that

$$S^{(3)} \le 2(\mathfrak{Q}) \int_0^1 |H(\alpha; P, Q, R) F(\alpha; P, R) f(\alpha; Q, R)^{2s-1}| \, d\alpha.$$

(z or w; x_j/y_j.)

Thus, an application of Schwarz's inequality shows that

$$S_s(P,Q,R) \le 8s\,(S^{(5)})^{\frac12}\Big(\int_0^1 |F(\alpha;P)^2 f(\alpha;Q,R)^{2s}|\,d\alpha\Big)^{\frac12},$$

where

$$S^{(5)} = \int_0^1 |H(\alpha;P,Q,R)^2 f(\alpha;Q,R)^{2s-2}|\,d\alpha.$$

Hence

$$S_s(P,Q,R) \le 8s\,(S_s(P,Q,R))^{\frac12}(S^{(5)})^{\frac12},$$

so that

$$S_s(P,Q,R) \le (8s)^2 S^{(5)}.$$

Here, the counting function $S^{(5)}$ counts the number of solutions of the equation

$$\Psi(z;\tilde{\underline{u}}) + x^k + x_1^k + \cdots + x_{s-1}^k = \Psi(w;\tilde{\underline{v}}) + y^k + y_1^k + \cdots + y_{s-1}^k,$$

with

$$x_j, y_j \in \mathcal{A}(Q,R) \quad (1\le j\le s), \qquad 1 \le z, w \le P,$$

$$\underline{u}, \underline{v} \in \mathcal{C}, \qquad \Psi'(z;\tilde{\underline{u}}) \neq 0 \text{ and } \Psi'(w;\tilde{\underline{v}}) \neq 0,$$

$$1 \le x, y \le Q, \qquad x \in \mathcal{S}(z;\tilde{\underline{u}}) \text{ and } y \in \mathcal{S}(w;\tilde{\underline{v}}).$$

We re-interpret $S^{(5)}$ as being bounded in the form

$$S^{(5)} \ll \sum_{r,r'\in\mathbb{N}} V(r,r'),$$

where $V(r,r')$ denotes the number of solutions of the equation

$$\Psi(z;\tilde{\underline{u}}) + (d\xi)^k + x_1^k + \cdots + x_{s-1}^k = \Psi(w;\tilde{\underline{v}}) + (e\eta)^k + y_1^k + \cdots + y_{s-1}^k,$$

with the variables $z, w, \tilde{\underline{u}}, \tilde{\underline{v}}, \underline{x}, \underline{y}$ as before, but now constrained by

$$1 \le d, e \le M, \qquad 1 \le \xi \le Q/d, \qquad 1 \le \eta \le Q/e,$$

$$r \mid \Psi'(z;\tilde{\underline{u}}), \qquad r' \mid \Psi'(w;\tilde{\underline{v}}),$$

$$(\xi \mid r^\infty), \qquad (\eta \mid (r')^\infty).$$

$$s_0(\xi) = r, \qquad s_0(\eta) = r'$$

[where $s_0(\xi) = \prod_{p\mid\xi} p$ = "squarefree kernel of ξ"].

Let

$$G_r(\alpha; P) = \sum_{\substack{1 \le z \le P \\ \tilde{\underline{u}} \in C \\ \Psi'(z;\tilde{\underline{u}}) \neq 0 \\ r \mid \Psi'(z;\tilde{\underline{u}})}} e(\alpha \Psi(z;\tilde{\underline{u}})).$$

Then, if we introduce the generating function

$$\zeta(\alpha) = \sum_{r \le Z} G_r(\alpha; P) \sum_{1 \le d \le M} \sum_{\substack{1 \le \xi \le Q/d \\ (\xi \mid r^\infty) \\ s_0(\xi) = r}} e(\alpha (d\xi)^k),$$

in which $Z = \sup_{\substack{1 \le z \le P \\ \tilde{\underline{u}} \in C}} |\Psi(z;\tilde{\underline{u}})|$, then we deduce that

$$S^{(5)} \le \int_0^1 |\zeta(\alpha)^2 f(\alpha; Q, R)^{2s-2}| \, d\alpha.$$

By Cauchy's inequality, we have

$$|\zeta(\alpha)|^2 \le \Big(\sum_{r \le Z} |G_r(\alpha; P)|^2 \Big) \Big(\sum_{r \le Z} \Big| \sum_{1 \le d \le M} \sum_{\substack{1 \le \xi \le Q/d \\ (\xi \mid r^\infty) \\ s_0(\xi) = r}} e(\alpha (d\xi)^k) \Big|^2 \Big).$$

By interchanging the order of summation here, the second expression on the right hand side here is equal to

$$\sum_{r \le Z} \Big| \sum_{\substack{1 \le \xi \le Q \\ (\xi \mid r^\infty) \\ s_0(\xi) = r}} \sum_{\substack{1 \le d \le M \\ d \le Q/\xi}} e(\alpha d^k \xi^k) \Big|^2.$$

Cauchy

$$\le \sum_{r \le Z} \Big(\sum_{\substack{1 \le \xi \le Q \\ (\xi \mid r^\infty)}} 1 \Big) \Big(\sum_{\substack{1 \le \xi \le Q \\ (\xi \mid r^\infty) \\ s_0(\xi) = r}} \Big| \sum_{\substack{1 \le d \le M \\ d \le Q/\xi}} e(\alpha d^k \xi^k) \Big|^2 \Big)$$

$$\ll \sum_{r \le Z} (rQ)^\varepsilon \sum_{\substack{1 \le \xi \le Q \\ (\xi \mid r^\infty), s_0(\xi) = r}} MQ/\xi,$$

where in the last step we applied Lemma 15.2 and trivial estimates.

Since $Z \ll_\Psi P^{\deg(\Psi)}$, it follows that this last expression is

$$\ll_\Psi P^\varepsilon MQ \sum_{1 \le \xi \le Q} \frac{1}{\xi} \ll_\Psi (PQ)^\varepsilon MQ.$$

Then we conclude that

$$|\mathcal{G}(\alpha)|^2 \ll_\Psi P^\varepsilon MQ \sum_{r \le Z} |G_r(\alpha; P, R)|^2.$$

Note here that we have essentially obtained a bound $P^\varepsilon MQ$ for $|f(\alpha; Q, R)|^2$, and this is a strong bound when M is much smaller than Q, as will be the case in our applications.

Thus far, we may suppose that

$$S_s(P, Q, R) \le (8s)^2 S^{(5)} \ll_\Psi P^\varepsilon MQ \int_0^1 \sum_{r \le Z} |G_r(\alpha; P)^2 f(\alpha; Q, R)| \, d\alpha. \qquad 25\text{-}2$$

The mean value here counts solutions of the equation

$$\Psi(z; \underline{u}) - \Psi(w; \underline{v}) = \sum_{i=1}^{s-1} (x_i^k - y_i^k),$$

with

$$x_j, y_j \in \mathcal{A}(Q, R) \quad (1 \le j \le s-1), \qquad 1 \le z, w \le P,$$

$$(\tilde{\underline{u}}, \tilde{\underline{v}}) \in \mathcal{C}^2, \qquad \Psi'(z; \tilde{\underline{u}}) \ne 0 \quad \text{and} \quad \Psi'(w; \tilde{\underline{v}}) \ne 0,$$

$$r \mid \Psi'(z; \tilde{\underline{u}}), \qquad r \mid \Psi'(w; \tilde{\underline{v}}).$$

Then for each solution counted by $S_{s-1}(P, Q, R)$, we should multiply by the number of common divisors r of $\Psi'(z; \tilde{\underline{u}})$ and $\Psi'(w; \tilde{\underline{v}})$ with $r \le Z$. The latter weight is bounded above by a divisor function no larger than $O_\Psi(P^\varepsilon)$, and hence

$$S_s(P,Q,R) \ll_\Psi P^{2\varepsilon} MQ\, S_{s-1}(P,Q,R).$$

This confirms the conclusion of the theorem in the third case. □

(iv) The treatment of $S^{(4)}$. We suppose that $S^{(4)} \geq \max\{S^{(1)}, S^{(2)}, S^{(3)}\}$, so that $S_s(P,Q,R) \leq 4S^{(4)}$. For a given solution of

$$\Psi(z;\underline{\tilde{u}}) - \Psi(w;\underline{\tilde{v}}) = \sum_{i=1}^{s}(x_i^k - y_i^k),$$

counted by $S^{(4)}$, we have

$$x_i, y_i \in \mathcal{A}(Q,R) \quad \text{and} \quad x_i > M, \quad y_i > M \quad (1 \leq i \leq s),$$

$$1 \leq z, w \leq P, \quad \underline{\tilde{u}}, \underline{\tilde{v}} \in \mathcal{C} \quad \text{and} \quad \Psi'(z;\underline{\tilde{u}}) \neq 0, \quad \Psi'(w;\underline{\tilde{v}}) \neq 0,$$

and neither $x_i \mathcal{D}(M) \Psi'(z;\underline{\tilde{u}})$ nor $y_i \mathcal{D}(M) \Psi'(w;\underline{\tilde{v}})$ for $1 \leq i \leq s$.

Consider a fixed index i with $1 \leq i \leq s$, and let m be the largest divisor of x_i with the property that $(m, \Psi(z;\underline{\tilde{u}})) = 1$. If one were to have $m \leq M$, then $x_i \mathcal{D}(M) \Psi'(z;\underline{\tilde{u}}))$, contradicting our assumptions concerning x_i and y_i. Thus $m > M$, and hence there is a divisor m_i of x_i (and, in fact, of m) with

$$M < m_i \leq MR \quad \text{and} \quad (m_i, \Psi(z;\underline{\tilde{u}})) = 1.$$

We may proceed similarly to show that there is a divisor m_i' of y_i with

$$M < m_i' \leq MR \quad \text{and} \quad (m_i', \Psi(w;\underline{\tilde{v}})) = 1. \quad \text{It follows that}$$

$S^{(4)} \leq S^{(6)}$, where $S^{(6)}$ denotes the number of solutions of

$$\Psi(z;\underline{\tilde{u}}) - \Psi(w;\underline{\tilde{v}}) = \sum_{i=1}^{s}\left((m_i u_i)^k - (m_i' v_i)^k\right),$$

with $z, w, \underline{\tilde{u}}, \underline{\tilde{v}}$ as above, and in addition

$u_i, v_i \in \mathcal{A}(Q/M, R)$, $M < m_i, m_i' \le MR$ $(1 \le i \le s)$,

$$(m_i, \Psi'(z;\underline{\tilde{u}})) = (m_i', \Psi'(w;\underline{\tilde{v}})) = 1.$$

Write $\tilde{m} = m_1 m_2 \cdots m_s$ and $\tilde{m}' = m_1' m_2' \cdots m_s'$, and for $\omega \in \mathbb{N}$, define

$$F^\dagger(\alpha;\omega) = \sum_{z,\underline{\tilde{u}}} e(\alpha \Psi(z;\underline{\tilde{u}})),$$

where the summation is over

$1 \le z \le P$, $\underline{\tilde{u}} \in \mathcal{C}$ subject to $(\Psi'(z;\underline{\tilde{u}}), \omega) = 1$.

Then we see by orthogonality that one has

$$S^{(6)} \le \sum_{\underline{m},\underline{m}'} \int_0^1 F^\dagger(\alpha;\tilde{m}) F^\dagger(-\alpha;\tilde{m}') \prod_{i=1}^{s} \left(f(m_i^k \alpha; Q/M, R) f(-m_i'^k \alpha; Q/M, R) \right) d\alpha,$$

where the summation is over m_i, m_i' satisfying

$$M < m_i, m_i' \le MR.$$

By Hölder's inequality, we see that

$$S^{(6)} \le \prod_{i=1}^{s} (I_i I_i')^{1/2s},$$

where

$$I_i = \sum_{\underline{m},\underline{m}'} \int_0^1 |F^\dagger(\underline{\alpha};\tilde{\underline{m}})^2 f(m_i^k \alpha; Q/M, R)^{2s}| \, d\alpha$$

and

$$I_i' = \sum_{\underline{m},\underline{m}'} \int_0^1 |F^\dagger(\underline{\alpha};\tilde{m}') f(m_i'^k \alpha; Q/M, R)^{2s}| \, d\alpha.$$

(Note that $I_i = I_i'$). By orthogonality, once again, we have

$$I_i' = I_i \le (MR)^{2s-1} S^{(7)},$$

where $S^{(7)}$ counts the number of solutions of the equation

$$\Psi(z;\underline{\tilde{u}}) - \Psi(w;\underline{\tilde{v}}) = m^k \sum_{i=1}^{s} (u_i^k - v_i^k),$$

with z, w, $\underline{\tilde{u}}$, $\underline{\tilde{v}}$ as above, and further with

$$M < m \le MR, \qquad (\Psi'(z;\underline{\tilde{u}}), m) = (\Psi'(z;\underline{\tilde{v}}), m) = 1,$$

$$u_i, v_i \in \mathcal{A}(Q/M, R) \qquad (1 \le i \le s).$$

Next, denote by $\mathcal{B}(h;m;\underline{\tilde{u}})$ the set of solutions of the congruence

$$\Psi(z;\underline{u}) \equiv h \pmod{m^k},$$

with $(\Psi'(z;\underline{\tilde{u}}), m) = 1$. Then Lemma 15.1 shows that

$$\operatorname{card}(\mathcal{B}(h;m;\underline{\tilde{u}})) \ll m^{\varepsilon}.$$

We now have

$$\Psi(z;\underline{\tilde{u}}) \equiv \Psi(w;\underline{\tilde{v}}) \pmod{m^k},$$

so we may classify solutions according to the common residue class, say h, modulo m^k. Write

$$g(\alpha;\ell;\underline{\tilde{u}};m) = \sum_{\substack{1 \le z \le P \\ z \equiv \ell \pmod{m^k}}} e(\alpha \Psi(z;\underline{\tilde{u}})).$$

Then we see that

$$S^{(7)} \ll \sum_{M < m \le MR} S^{(8)}(m),$$

where

$$S^{(8)}(m) = \int_0^1 G(\alpha;m) \, |f(m^k\alpha; Q/M, R)|^{28} \, d\alpha,$$

in which

$$G(\alpha;m) = \sum_{h=1}^{m^k} \Big| \sum_{\underline{\tilde{u}} \in \mathcal{C}} \sum_{\ell \in \mathcal{B}(h;m;\underline{\tilde{u}})} g(\alpha;\ell;\underline{\tilde{u}};m) \Big|^2.$$

By Cauchy's inequality, one has

$$|G(\alpha;m)| \le \sum_{h=1}^{m^k} \Big(\sum_{\tilde{u}\in\mathcal{C}} \sum_{l\in\mathcal{B}(h;m;\tilde{u})} 1 \Big) \Big(\sum_{\tilde{u}\in\mathcal{C}} \sum_{l\in\mathcal{B}(h;m;\tilde{u})} |g(\alpha;l;\tilde{u};m)|^2 \Big)$$

$$\ll |\mathcal{C}| m^{\varepsilon} \sum_{h=1}^{m^k} \sum_{\tilde{u}\in\mathcal{C}} \sum_{l\in\mathcal{B}(h;m;\tilde{u})} |g(\alpha;l;\tilde{u};m)|^2$$

$$\ll m^{\varepsilon} |\mathcal{C}| \sum_{\tilde{u}\in\mathcal{C}} \sum_{l=1}^{m^k} |g(\alpha;l;\tilde{u};m)|^2 .$$

On substituting this bound into the definition of $S^{(8)}(m)$, we see that

$$S^{(7)} \ll M^{\varepsilon}|\mathcal{C}| \sum_{M<m\le MR} \sum_{\tilde{u}\in\mathcal{C}} \sum_{l=1}^{m^k} \int_0^1 |g(\alpha;l;\tilde{u};m)|^2 |f(m^k\alpha;Q/M,R)|^{20} d\alpha .$$

By orthogonality, moreover, the expression on the right hand side here is at most $M^{\varepsilon}|\mathcal{C}|\, T_s(P,Q,R;M)$, since the sum over m counts solutions of the equation

$$\Psi(z;\underline{u}) - \Psi(w;\underline{u}) = m^k \sum_{i=1}^{s} (u_i^k - v_i^k),$$

with

$$M<m\le MR, \quad u_j, v_j \in \mathcal{A}(Q/M,R) \quad (1\le j\le s),$$

$$1\le z,w\le P, \quad z \equiv l \equiv w \pmod{m^k} \quad (\text{summed over } l)$$

and $\tilde{u}\in\mathcal{C}$. Hence we conclude that in this case we have

$$S_s(P,Q,R) \le 4S^{(4)} \ll S^{(6)} \ll \prod_{i=1}^{s} \big((MR)^{2s-1+\varepsilon} |\mathcal{C}|\, T_s(P,Q,R;M) \big)^{2/25}$$

$$\ll P^{\varepsilon}(MR)^{2s-1} |\mathcal{C}|\, T_s(P,Q,R;M). \quad \square //$$

We now simplify the bound given by Theorem 16.1 in circumstances wherein $N_s(P,Q,R)=0$.

Corollary 16.2. Suppose that $1<M<Q<P$ and $N_s(P,Q,R)=0$. Then one has

$$S_s(P,Q,R) \ll P^{\varepsilon}|\mathcal{C}|(MR)^{2s-1}T_s(P,Q,R;M).$$

Proof. We prove this statement by induction on s, using the bound

$$S_s(P,Q,R) \ll_{\Psi} S_s(P,M,R) + N_s(P,Q,R) + P^{\varepsilon}QMS_{s-1}(P,Q,R) + P^{\varepsilon}|\mathcal{C}|(MR)^{2s-1}T_s(P,Q,R;M)]$$

available from the Fundamental Lemma (Theorem 6.1).

Observe first that $N_s(P,Q,R)$ counts the solutions of

$$\Psi(z;\underline{\hat{u}}) - \Psi(w;\underline{\hat{v}}) = \sum_{i=1}^{s}(x_i^k - y_i^k),$$

with $x_i, y_i \in \mathcal{A}(Q,R)$, $\underline{\hat{u}}, \underline{\tilde{v}} \in \mathcal{C}$ and $1 \le z, w \le P$, satisfying $\Psi'(z;\underline{\tilde{u}}) = \Psi'(w;\underline{\tilde{v}}) = 0$. By considering solutions with $x_s = y_s$, we see that $N_s(P,Q,R) \ge QN_{s-1}(P,Q,R)$. Then our hypothesis that $N_s(P,Q,R)=0$ implies that $N_t(P,Q,R)=0$ for $1 \le t \le s$.

Next, observe that by considering solutions $z, w, \underline{\hat{u}}, \underline{\tilde{v}}, \underline{x}, \underline{y}$ counted by $S_s(P,M,R)$ with arbitrary choices of x_s and y_s, we have (by orthogonality and the triangle inequality) that

$$S_s(P,M,R) \le M^2 \int_0^1 |F(\alpha;P)^2 f(\alpha;M,R)^{2s-2}|\,d\alpha$$

$$\le QM\,S_{s-1}(P,M,R).$$

Thus, on considering the underlying Diophantine equation, we see that

$$S_s(P,M,R) \leq QM S_{s-1}(P,Q,R).$$

We now see that for $1 \leq t \leq s$, we have the relation

$$S_t(P,Q,R) \ll P^{\varepsilon} QM S_{t-1}(P,Q,R) + P^{\varepsilon} |\mathcal{C}| (MR)^{2t-1} T_t(P,Q,R;M).$$

We apply this relation inductively to show that for each t, one has

$$S_t(P,Q,R) \ll P^{\varepsilon} |\mathcal{C}| (MR)^{2t-1} T_t(P,Q,R;M).$$

First, when $t=1$, we observe that $S_0(P,Q,R)$ counts the solutions of the equation

$$\Psi(z;\underline{\tilde{u}}) = \Psi(w;\underline{\tilde{v}}),$$

with $\underline{\tilde{u}}, \underline{\tilde{v}} \in \mathcal{C}$ and $1 \leq z,w \leq P$. Thus, counting $\underline{\tilde{u}}, \underline{\tilde{v}} \in \mathcal{C}$ trivially, fixing w and then solving for z, we see that

$$S_0(P,Q,R) \ll \underset{w}{P} \cdot \underset{\underline{\tilde{u}},\underline{\tilde{v}}}{|\mathcal{C}|^2},$$

whence

$$P^{\varepsilon} QM S_0(P,Q,R) \ll P^{1+\varepsilon} QM |\mathcal{C}|^2.$$

Meanwhile, the quantity $T_1(P,Q,R;M)$ counts the solutions of

$$\Psi(z;\underline{\tilde{u}}) - \Psi(w;\underline{\tilde{v}}) = m^k(u^k - v^k),$$

with z,w, $\underline{\tilde{u}}, \underline{\tilde{v}}$ as before, $M < m \leq MR$ and $u,v \in \mathcal{A}(Q/M,R)$.

Counting solutions only with $u=v$, we obtain

$$T_1(P,Q,R;M) \gg \underset{u=v}{(Q/M)} \underset{m}{(MR)} \underset{z=w}{P} \underset{\underline{\tilde{u}}=\underline{\tilde{v}}}{|\mathcal{C}|},$$

whence

$$P^{\varepsilon} |\mathcal{C}| (MR) T_1(P,Q,R;M) \gg P^{1+\varepsilon} QMR^2 |\mathcal{C}|^2 \gg P^{\varepsilon} QM S_0(P,Q,R).$$

The inductive hypothesis therefore holds when $t=1$. Suppose then that the inductive hypothesis has been proved for $1 \le t < s$.

We then see that

$$S_s(P,Q,R) \ll P^{\varepsilon} QM\, S_{s-1}(P,Q,R) + P^{\varepsilon} |\mathcal{C}| (MR)^{2s-1} T_{s-1}(P,Q,R;M)$$

$$\ll P^{\varepsilon} QM \left(P^{\varepsilon} |\mathcal{C}| (MR)^{2s-3} T_{s-1}(P,Q,R;M) \right)$$

$$+ P^{\varepsilon} |\mathcal{C}| (MR)^{2s-1} T_s(P,Q,R;M)$$

$$\ll P^{\varepsilon} |\mathcal{C}| (MR)^{2s-1} \left(T_s(P,Q,R;M) + (Q/M)\, T_{s-1}(P,Q,R;M) \right).$$

But $T_s(P,Q,R;M)$ counts solutions of

$$\Psi(z;\underline{\tilde{u}}) - \Psi(w;\underline{\tilde{v}}) = m^k \sum_{i=1}^{s} (u_i^k - v_i^k),$$

with $1 \le z, w \le P$, $z \equiv w \pmod{m^k}$, $\underline{\tilde{u}}, \underline{\tilde{v}} \in \mathcal{C}$, $u_i, v_i \in \mathcal{A}(Q/M, R)$ and $M < m \le MR$. Considering only solutions with $u_s = v_s$, we see that

$$T_s(P,Q,R;M) \gg (Q/M) \cdot T_{s-1}(P,Q,R;M),$$

$u_s = v_s$ (provided that $R \ge P^{\eta_0}$, for some $\eta_0 > 0$).

and thus

$$S_s(P,Q,R) \ll P^{\varepsilon} |\mathcal{C}| (MR)^{2s-1} T_s(P,Q,R;M).$$

This establishes the inductive step, and thus the proof of the corollary is complete. //

§17. Efficient differencing. I.

We pause to extract the simplest consequences of our new bounds.

Define

$$f(\alpha; X, R) = \sum_{x \in \mathcal{A}(X,R)} e(\alpha x^k).$$

We consider the mean value

$$S_s(P,R) = \int_0^1 |f(\alpha; P, R)|^{2s} \, d\alpha.$$

Let λ_s be the least (positive) real number having the property that, given $\varepsilon > 0$, there exists a positive number $\eta = \eta(\varepsilon, s, k)$ having the property that, whenever $2 \le R \le P^\eta$, one has

$$S_s(P,R) \ll P^{\lambda_s + \varepsilon}.$$

One can interpret λ_s as

$$\lambda_s = \limsup_{\eta \to 0+} \limsup_{P \to \infty} \sup_{2 \le R \le P^\eta} \frac{\log S_s(P,R)}{\log P}.$$

Observe that $S_s(P,R)$ counts the solutions of the equation

$$z^k + \sum_{i=1}^{s-1} x_i^k = w^k + \sum_{i=1}^{s-1} y_i^k,$$

with $z, w, x_i, y_i \in \mathcal{A}(P,R)$. If we relax the conditions on z and w so that instead only $1 \le z, w \le P$, then we see that

$$S_s(P,R) \le S_{s-1}(P,P,R),$$

where $\mathcal{C}$ is trivial (say $\mathcal{C} = \{1\}$), one has $\Psi(z; \underline{\tilde{u}}) = z^k$, and we are assuming $s \geq 1$. Moreover, it is apparent from Hua's Lemma that

$$S_1(P,R) \leq P \quad \text{and} \quad S_2(P,R) \ll P^{2+\varepsilon},$$

so that $\lambda_1 = 1$ and $\lambda_2 = 2$ are admissible.

We now seek to apply Corollary 16.2 to bound $S_{s-1}(P,P,R)$, and hence also $S_s(P,R)$, when $s \geq 3$. We take $M = P^{1/k}$, and observe that

$$S_{s-1}(P,P,R) \ll P^{\varepsilon}(MR)^{2s-3} T_{s-1}(P,P,R;M),$$

where $T_{s-1}(P,P,R;M)$ counts the solutions of the equation

$$z^k - w^k = m^k \sum_{i=1}^{s-1} (u_i^k - v_i^k),$$

with $1 \leq z, w \leq P$, $z \equiv w \pmod{m^k}$, $M < m \leq MR$, and $u_i, v_i \in \mathcal{A}(P/M, R)$.

Observe that $m^k > M^k > P > |z-w|$. Then whenever $z \equiv w \pmod{m^k}$, we have $z = w$. But then we are left with the equation

$$\sum_{i=1}^{s-1} (u_i^k - v_i^k) = 0,$$

with $u_i, v_i \in \mathcal{A}(P/M, R)$. Hence

$$T_{s-1}(P,P,R;M) \ll \sum_{z=w}^{P} \sum_{m}^{MR} S_{s-1}(P/M, R),$$

whence

$$S_s(P,R) \ll P^{1+\varepsilon}(MR)^{2s-2} S_{s-1}(P/M, R)$$

Consequently, if $2 \le R \le P^{\eta}$ and η is a sufficiently small positive number, we see that

$$S_s(P,R) \ll P^{1+\varepsilon} (MR)^{2s-2} (P/M)^{\lambda_{s-1}+\varepsilon}$$

$$\ll P^{\lambda_s^* + 2\varepsilon},$$

where

$$\lambda_s^* = \lambda_{s-1}(1 - 1/k) + 1 + (2s-2)\cdot 1/k .$$

It follows that $\lambda_s \le \lambda_s^*$ is admissible.

This relation can be used to derive admissible exponents. We have

$$\lambda_2 = 2,$$

$$\lambda_3 \le 2(1-1/k) + 1 + 4\cdot\tfrac{1}{k} = 3 + 2/k$$

$$\vdots$$

$$\lambda_s \le 2s - k + (k-2)(1-1/k)^{s-2}.$$

Check: By induction —

$$\left(2s-2-k+(k-2)(1-1/k)^{s-3}\right)(1-1/k) + 1 + (2s-2)/k$$

$$= (2s-2) - (k-1) + 1 + (k-2)(1-1/k)^{s-2}. \quad \checkmark \quad \square$$

We have established the following:

Theorem 17.1 Suppose that $s \ge 2$ and that $\eta > 0$ is sufficiently small in terms of k, s and $\varepsilon > 0$. Then whenever $2 \le R \le P$, one has

$$\int_0^1 \Big| \sum_{x \in \mathcal{A}(P,R)} e(\alpha x^k) \Big|^{2s} d\alpha \ll P^{2s-k+(k-2)(1-1/k)^{s-2}+\varepsilon}.$$

Notice that

$$2s - k + (k-2)(1-1/k)^{s-2} \leq 2s - k + ke^{-s/k},$$

so that this exponent approaches the conjectural exponent $2s-k$ exponentially rapidly. In fact, this recovers the same strength as is available in diminishing ranges, but without losing density.

We can use these estimates as an alternative to the diminishing ranges treatment of $G(k)$. Consider representations of a large natural number n in the form

$$n = \sum_{i=1}^{t} x_i^k + \sum_{j=0}^{s-1} (y_j^k + z_j^k), \qquad (X := n^{1/k})$$

with $1 \leq x_i \leq X$ $(1 \leq i \leq t)$ and $y_j, z_j \in \mathcal{A}(X, X^\eta)$, with $\eta > 0$ sufficiently small. Then with $F(\alpha) = \sum_{1 \leq x \leq X} e(\alpha x^k)$ and $f(\alpha) = \sum_{x \in \mathcal{A}(X, X^\eta)} e(\alpha x^k)$,

$$\begin{aligned}\int_{\mathfrak{m}_\delta} F(\alpha)^t f(\alpha)^{2s} e(-n\alpha)\,d\alpha &\leq \Big(\sup_{\alpha \in \mathfrak{m}_\delta} |F(\alpha)|\Big)^t \int_0^1 |f(\alpha)|^{2s}\,d\alpha \\ &\ll \big(X^{1-\delta 2^{1-k}+\varepsilon}\big)^t X^{2s-k+(k-2)(1-1/k)^{s-2}+\varepsilon} \\ &\ll X^{2s+t-k-\tau},\end{aligned}$$

for a suitable $\tau > 0$, provided that

$$t\delta 2^{1-k} > (k-2)(1-1/k)^{s-2}.$$

Can take $t = 4k$ and $s = \lceil k^2 \log 2 \rceil$, just as in §13. Meanwhile

$$\int_{\mathfrak{m}_\delta} F(\alpha)^t f(\alpha)^{2s} e(-n\alpha)\,d\alpha = \sum_{\underline{y}, \underline{z}} \int_{\mathfrak{m}_\delta} F(\alpha)^t e\Big(-\Big(n - \sum_{j=0}^{s-1} (y_j^k + z_j^k)\Big)\Big)\,d\alpha$$

$$\gg \sum_{y,\underline{z}} \Big(n - \sum_{j=0}^{s-1} (y_j^k + z_j^k)\Big)^{\frac{t}{k}-1}$$

$$\gg n^{(2s+t)/k - 1}.$$

Hence the number of representations of n as the sum of $t+2s < (2\log 2)k^2 + 4k + 2$ k-th powers is $\gg n^{(t+2s)/k-1}$.

---

§18. Efficient differencing. II

We define a modified forward difference operator Δ_i^* by

$$\Delta_1^*(f(x); h; m) = m^{-k}(f(x+hm^k) - f(x)),$$

and then define Δ_j^* recursively by

$$\Delta_{j+1}^*(f(x); h_1, \dots, h_{j+1}; m_1, \dots, m_{j+1}) = \Delta_1^*(\Delta_j^*(f(x); h_1, \dots, h_j; m_1, \dots, m_j); h_{j+1}; m_{j+1}).$$

Also, we adopt the convention that

$$\Delta_0^*(f(x); h; m) = f(x).$$

For $0 \le j \le k$, put

$$\Psi_j = \Psi_j(z; h_1, \dots, h_j; m_1, \dots, m_j) = \Delta_j^*(z^k; h_1, \dots, h_j; m_1, \dots, m_j).$$

We will apply the Fundamental Lemma with $\Psi_j(z; \underline{h}; \underline{m})$ substituted for $\Psi(z; \underline{\alpha})$, with the additional parameters $\underline{\alpha}$ interpreted as $\underline{h}, \underline{m}$.

We need to specify a choice of parameters, so take $\varphi_i = \varphi_i(s,k)$ to be a real number with $0 < \varphi_i \le 1/k$ $(1 \le i \le k)$, and put

$$M_j = P^{\varphi_j}, \quad H_j = PM_j^{-k} \text{ and } Q_j = P(M_1 \dots M_j)^{-1} \quad (1 \le j \le k).$$

We then substitute the conditions

$M_i < m_i \le M_i R$ and $1 \le h_i \le H_i$ $(1 \le i \le j)$

for the previous conditions $\underline{\ell} \in \mathcal{L}$, and write

$$S_s(P, Q, R; \Psi_j) \text{ for } S_s(P, Q, R; \underline{\Psi}; \mathcal{L}),$$

and similarly for T_s and N_s.

We can now summarise Corollary 16.2 in this setting.

Lemma 18.1. Suppose that for some positive numbers η_0 and η_1, one has $P^{\eta_0} < R \le P^{\eta_1}$. Then for $0 \le j \le k-1$, one has

$$S_s(P, Q_j, R; \Psi_j) \ll P^{\varepsilon} \Big(\prod_{i=1}^{j} H_i M_i R \Big) (M_{j+1} R)^{2s-1} T_s(P, Q_j, R; \varphi_{j+1}; \Psi_j').$$

Proof. We have

$$\operatorname{card}(\mathcal{L}) \ll \prod_{i=1}^{j} (H_i M_i R),$$

so the conclusion follows on checking that $N_s(P, Q, R; \Psi_j) = 0$ for $0 \le j \le k-1$. But one checks by induction via the mean value theorem that

$$\Psi_j'(z; \underline{h}; \underline{m}) = m_j^{-k} \big(\Psi_{j-1}'(z + h_j m_j^k) - \Psi_{j-1}'(z) \big)$$
$$= m_j^{-k} \Psi_{j-1}''(z_j) \quad \text{for some } z_j \in (z, z + h_j m_j^k),$$

whence

$$\Psi_j'(z; \underline{h}; \underline{m}) = m_j^{-k} m_{j-1}^{-k} \Psi_{j-2}'''(z_{j-1}) \quad \text{for some } z_{j-1} \in (z_j, z_j + h_{j-1} m_{j-1}^k),$$

$$\vdots$$

so

$$\Psi_j'(z; \underline{h}; \underline{m}) = (m_j m_{j-1} \cdots m_1)^{-k} \Psi^{(j+1)}(z_1) \text{ for some } z_1 > 0.$$
$$= (m_j m_{j-1} \cdots m_1)^{-k} z_1^{k-j-1} \cdot \frac{k!}{(k-j-1)!} > 0. \quad (\text{since } j \le k-1).$$

Since we have $\Psi_j'(z; \underline{h}; \underline{m}) > 0$, we must have $N_s(P, Q, R; \Psi_j) = 0$.

Taking into account our notational conventions, the desired conclusion now follows from Corollary 16.2 of the Fundamental Lemma. //

Now we extract an efficient difference.

Lemma 18.2. Suppose that for some positive numbers η_0 and η_1, one has $P^{\eta_0} < R \le P^{\eta_1}$. Then for $0 \le j \le k-1$, we have

$$T_s(P, Q_j, R; \varphi_{j+1}; \Psi_j) \ll PM_{j+1}R\left(\prod_{i=1}^{j} H_i M_i R\right) S_s(Q_{j+1}, R) + \left(S_s(Q_{j+1}, R)\, S_s(P, Q_{j+1}, R; \Psi_{j+1})\right)^{\frac{1}{2}}.$$

Proof. Recall that $T_s(P, Q_j, R; \varphi_{j+1}; \Psi_j)$ counts the integral solutions of the equation

$$\Psi_j(z; \underline{h}; \underline{m}) - \Psi_j(w; \underline{h}; \underline{m}) = m^k \cdot \sum_{i=1}^{s} (u_i^k - v_i^k), \qquad (\dagger)$$

with $1 \le z, w \le P$, $1 \le h_i \le H_i$, $M_i < m_i \le M_i R$ $(1 \le i \le j)$, $z \equiv w \pmod{m^k}$, $M_{j+1} < m \le M_{j+1} R$, $u_i, v_i \in \mathcal{A}(Q_{j+1}, R)$. Thus $z = w + hm^k$, with $|h| \le PM_{j+1}^{-k} = H_{j+1}$.

Then on isolating the term with $h = 0$, we deduce that

$$T_s(P, Q_j, R; \varphi_{j+1}; \Psi_j) \le U_0 + 2U_1,$$

where U_0 denotes the number of solutions of $(\dagger)$ with $z = w$, and U_1 counts the solutions of the equation

$$\underbrace{m^{-k}\left(\Psi_j(w + hm^k; \underline{h}; \underline{m}) - \Psi_j(w; \underline{h}; \underline{m})\right)}_{\Delta_j^*(\Psi_j(w; \underline{h}; \underline{m}); h, m)} = \sum_{i=1}^{s} (u_i^k - v_i^k),$$

with $1 \le w \le P$, $1 \le h \le H_{j+1}$, $M_{j+1} < m \le M_{j+1} R$, $u_i, v_i \in \mathcal{A}(Q_{j+1}, R)$, $1 \le h_i \le H_i$, $M_i < m_i \le M_i R$.

We have

$$U_0 \ll \sum_{z=w}^{P} \cdot \sum_{m}^{M_{j+1}R} \left(\prod_{i=1}^{j} H_i M_i R \right) S_s(Q_{j+1}, R).$$

Moreover, we see that U_1 counts the solutions of the equation

$$\Psi_{j+1}(w; \underline{h}, h; \underline{m}, m) = \sum_{i=1}^{s} (u_i^k - v_i^k),$$

with the variables as before. Write

$$F_i(\alpha) = \sum_{\substack{m_1,\dots,m_i \\ M_l < m_l \le M_l R}} \sum_{\substack{h_1,\dots,h_i \\ 1 \le h_l \le H_l}} \sum_{1 \le z \le P} e(\alpha \Psi_j(z; \underline{h}; \underline{m})),$$

and

$$f_i(\alpha) = \sum_{x \in \mathcal{A}(Q_i, R)} e(\alpha x^k).$$

Then we see that

$$U_1 \le \int_0^1 F_{j+1}(-\alpha) |f_{j+1}(\alpha)|^{2s} d\alpha$$

$$\overset{\text{Cauchy-Schwarz}}{\le} \left(\int_0^1 |F_{j+1}(\alpha)^2 f_{j+1}(\alpha)^{2s}| d\alpha \right)^{\frac{1}{2}} \cdot \left(\int_0^1 |f_{j+1}(\alpha)|^{2s} | d\alpha \right)^{\frac{1}{2}}$$

$$\ll \left(S_s(P, Q_{j+1}, R; \Psi_{j+1}) \right)^{\frac{1}{2}} \left(S_s(Q_{j+1}, R) \right)^{\frac{1}{2}}.$$

Substituting these bounds for U_0 and U_1 into our earlier bound

$$T_s(P, Q_j, R; \varphi_{j+1}; \Psi_j) \le U_0 + 2U_1,$$

the conclusion of the lemma follows. //

In the last section, we showed that given an admissible exponent λ_s, one has an admissible exponent $\lambda_{s+1} \le \lambda_s(1 - 1/k) + 1 + 2s \cdot \frac{1}{k}$.

We now show that such remains true with

$$\lambda_{s+1} \leq \lambda_s (1-\theta) + 1 + 2s\theta,$$

where θ is significantly smaller than $1/k$.

Theorem 18.3. Suppose that t is a positive integer and μ is a positive real number with

$$2t - k < \mu \leq 2t,$$

and satisfying the property that, given $\varepsilon > 0$, there is a positive number $\eta_0 = \eta_0(k, \varepsilon)$ such that, whenever $0 < \eta < \eta_0$, then

$$S_t(P, P^\eta) \ll P^{\mu+\varepsilon} \qquad (\text{so } \lambda_t = \mu \text{ is admissible}).$$

Define the real numbers λ_s, θ_s, Δ_s $(s \geq t)$ successively by

$$\lambda_t = \mu, \quad \theta_t = 0, \quad \Delta_t = \mu - 2t + k,$$

and when $s > t$ by

$$\theta_s = \frac{1}{k + \Delta_{s-1}} + \left(\frac{1}{k} - \frac{1}{k+\Delta_{s-1}}\right)\left(\frac{k - \Delta_{s-1}}{2k}\right)^{k-1},$$

$$\Delta_s = \Delta_{s-1}(1-\theta_s) + k\theta_s - 1,$$

$$\lambda_s = 2s - k + \Delta_s.$$

Then given any positive number t' with $t' > t$ and $\varepsilon' > 0$, there exists $\eta_1 = \eta_1(k, \varepsilon', t')$ such that, whenever $0 < \eta < \eta_1$ and $t \leq s \leq t'$, one has

$$S_s(P, P^\eta) \ll P^{\lambda_s + \varepsilon'}.$$

Proof. We prove the results by induction, the case $s = t$ being assumed. Suppose then that the conclusion holds for all suffices not exceeding s, and seek to prove the conclusion for $s+1$. We consider

$$S_{s+1}(P, R^\eta) \ll S_s(P, P, R; \Psi_0) \quad \text{with} \quad R = P^\eta \text{ and } 0 \le \eta \le \eta_0/k.$$

For $1 \le j \le k$, define

$$\varphi_j = \frac{1}{k+\Delta_s} + \left(\frac{1}{k} - \frac{1}{k+\Delta_s}\right)\left(\frac{k-\Delta_s}{2k}\right)^{k-j}.$$

Also, write λ for λ_s. We prove inductively that for $0 \le j \le k-1$, one has

$$T_s(P, Q_j, R; \varphi_{j+1}; \Psi_j) \ll P^{1+(k-j)\varepsilon} M_{j+1} R^{2s(k-j)} \Big(\prod_{i=1}^{j} H_i M_i R\Big) Q_{j+1}^{\lambda+\varepsilon}. \qquad (*_1)$$

By making a trivial estimate, we observe first that

$$S_s(P, Q_k, R; \Psi_k) \ll \sum_{z,w} P^2 \Big(\prod_{i=1}^{k} H_i M_i R\Big)^2 S_s(Q_k, R).$$

Then Lemma 18.2 yields

$$T_s(P, Q_{k-1}, R; \varphi_k; \Psi_{k-1}) \ll T^{(1)} + T^{(2)},$$

where

$$T^{(1)} = P M_k R \Big(\prod_{i=1}^{k-1} H_i M_i R\Big) S_s(Q_k, R)$$

and

$$\begin{aligned} T^{(2)} &= \Big(S_s(Q_k, R) \cdot S_s(P, Q_k, R; \Psi_k)\Big)^{\frac{1}{2}} \\ &\ll \Big(S_s(Q_k, R) \cdot P^2 \Big(\prod_{i=1}^{k} H_i M_i R\Big)^2 S_s(Q_k, R)\Big)^{\frac{1}{2}} \\ &= P \Big(\prod_{i=1}^{k} H_i M_i R\Big) S_s(Q_k, R). \end{aligned}$$

But $\varphi_k = \frac{1}{k}$, so $H_k = 1$, and hence

$$T^{(2)} \ll P M_k R \Big(\prod_{i=1}^{k-1} H_i M_i R\Big) S_s(Q_k, R) = T^{(1)}.$$

We therefore conclude that

$$T_s(P, Q_{k-1}, R; \varphi_k; \Psi_{k-1}) \ll P^{1+\varepsilon} M_k R^{2s} \Big(\prod_{i=1}^{k-1} H_i M_i R\Big) Q_k^{\lambda+\varepsilon},$$

which establishes the desired conclusion when $j = k-1$.

Now suppose that the conclusion holds for $j \geq J$, where J is an integer with $1 \leq J \leq k-1$. In view of the above discussion, we may suppose that $J \leq k-1$, and hence

$$\varphi_1 + \cdots + \varphi_J < J/k \leq 1 - 1/k.$$

Then by Lemma 18.1 and (*),

$$S_s(P, Q_J, R; \Psi_J) \ll P^{\varepsilon} \Big(\prod_{i=1}^{J} H_i M_i R\Big) (M_{J+1} R)^{2s-1} T_s(P, Q_J, R; \varphi_{J+1}; \Psi_{J+1})$$
$$\ll P^{1+(k-J+1)\varepsilon} (M_{J+1} R)^{2s} \Big(\prod_{i=1}^{J} H_i M_i R\Big)^2 R^{2s(k-J+1)} Q_{J+1}^{\lambda+\varepsilon}.$$

Next we apply Lemma 18.2 to deduce that

$$T_s(P, Q_{J-1}, R; \varphi_J; \Psi_{J-1}) \ll T^{(3)} + T^{(4)},$$

where

$$T^{(3)} = P M_J R \Big(\prod_{i=1}^{J-1} H_i M_i R\Big) Q_J^{\lambda+\varepsilon}$$

and

$$T^{(4)} = \Big(Q_J^{\lambda+\varepsilon} \cdot P^{1+(k-J+1)\varepsilon} (M_{J+1} R)^{2s} \Big(\prod_{i=1}^{J} H_i M_i R\Big)^2 R^{2s(k-J+1)} Q_{J+1}^{\lambda+\varepsilon}\Big)^{\frac{1}{2}}$$
$$\ll P^{(k-J)\varepsilon} R^{s(k-J+1)} \Big(\prod_{i=1}^{J-1} H_i M_i R\Big) \cdot (T^{(5)})^{\frac{1}{2}},$$

in which

$$T^{(5)} = P M_{J+1}^{2s} (H_J M_J)^2 (Q_J Q_{J+1})^{\lambda+\varepsilon}.$$

We can write $T^{(5)} = P^{\textcircled{H}}$, where

$$\textcircled{H} = 1 + 2s\varphi_{J+1} + (\lambda+\varepsilon)(1 - \varphi_{J+1} - \varphi_J - \cdots - \varphi_1)$$
$$+ (\lambda+\varepsilon)(1 - \varphi_J - \cdots - \varphi_1) + 2(1 - (k-1)\varphi_J)$$

$$\leq 2(\lambda+\varepsilon)(1-\varphi_1-\cdots-\varphi_J) + 2 + 2\varphi_J$$
$$+ \Big(\underbrace{1 + (k-\Delta_s)\varphi_{J+1} - 2k\varphi_J}_{=0} \Big)$$

(using $\lambda = 2s-k+\Delta_s$)

$$\leq 2\Big(1 + \varphi_J + (\lambda+\varepsilon)(1-\varphi_1-\cdots-\varphi_J)\Big),$$

Thus

$$\big(T^{(5)}\big)^{\frac12} = P^{\frac12 (H)} \ll P M_J Q_J^{\lambda+\varepsilon}.$$

Notice how ~~that~~ we used the notation

$$(k-\Delta_s)\varphi_{J+1} = (k-\Delta_s)\left(\frac{1}{k+\Delta_s} + \left(\frac1k - \frac{1}{k+\Delta_s}\right)\left(\frac{k-\Delta_s}{2k}\right)^{k-J-1}\right)$$

$$= \frac{k-\Delta_s}{k+\Delta_s} + 2k\left(\frac1k - \frac{1}{k+\Delta_s}\right)\left(\frac{k-\Delta_s}{2k}\right)^{k-J}$$

$$= 2k\left(\frac{1}{k+\Delta_s} + \left(\frac1k - \frac{1}{k+\Delta_s}\right)\left(\frac{k-\Delta_s}{2k}\right)^{k-J}\right) - 1$$

$$= 2k\varphi_J - 1.$$

This justifies a step above.

Thus far, we have shown ~~that~~

$$T^{(4)} \ll P^{(k-J)\varepsilon} R^{2s(k-J+1)} \cdot P M_J Q_J^{\lambda+\varepsilon} \cdot \left(\prod_{i=1}^{J-1} H_i M_i R\right),$$

which majorises $T^{(3)}$. Thus

$$T_s(P, Q_{J-1}, R; \varphi_J; \Psi_{J-1}) \ll P^{1+(k-J+1)\varepsilon} M_J R^{2s(k-J+1)} \left(\prod_{i=1}^{J-1} H_i M_i R\right) Q_J^{\lambda+\varepsilon},$$

so that (*) is established when $j = J-1$. This completes the inner

inductive step.

We may now assume that (*) holds for $j=0$, and hence

$$T_s(P, Q_0, R; \varphi_1; \Psi_0) \ll P^{1+k\varepsilon} M_1 R^{2ks} Q_1^{\lambda+\varepsilon}.$$

Lemma 18.1 now shows that

$$S_s(P, P, R; \Psi_0) \ll P^{\varepsilon}(M_1 R)^{2s-1} \cdot P^{1+k\varepsilon} M_1 R^{2ks} Q_1^{\lambda+\varepsilon}$$

$$= P^{1+(k+1)\varepsilon} M_1^{2s} R^{2(k+1)s} Q_1^{\lambda+\varepsilon}.$$

But $\varphi_1 = \theta_{s+1}$, and so

$$\lambda_{s+1} = 2s+2-k+\Delta_{s+1}$$
$$= 2s+2-k+\Delta_s(1-\varphi_1)+k\varphi_1-1$$
$$= \lambda(1-\varphi_1)+1+2s\varphi_1.$$

Thus

$$S_{s+1}(P, R) \ll S_s(P, P, R; \Psi_0)$$
$$\ll P^{1+(k+1)\varepsilon+2s\varphi_1+(\lambda+\varepsilon)(1-\varphi_1)} R^{2(k+1)s}$$
$$\ll P^{(k+2)\varepsilon+\lambda_{s+1}} R^{2(k+1)s}.$$

Thus, provided that $R \leq P^{\eta}$ with η sufficiently small in terms of s, k and $\varepsilon' > 0$, on taking $\varepsilon < \varepsilon'/(2k+2)$, we obtain

$$S_{s+1}(P, R) \ll P^{\lambda_{s+1}+\varepsilon}.$$

This completes the inductive step in s, and completes the proof of the theorem. //

To gauge the strength of this conclusion, suppose that k is very large. Since Δ_{s-1} will be small for large s, we will have $\frac{k-\Delta_{s-1}}{2k} \leq \frac{1}{2}$ (in any case!), so

$$\theta_s = \frac{1}{k+\Delta_{s-1}} + O(2^{1-k}).$$

Since θ_s is very close to $1/(k+\Delta_{s-1})$, we see that

$$\Delta_s \lesssim \Delta_{s-1}\left(1 - \frac{1}{k+\Delta_{s-1}}\right) + k\left(\frac{1}{k+\Delta_{s-1}}\right) - 1$$

$$= \Delta_{s-1}\left(1 - \frac{1}{k+\Delta_{s-1}}\right) - \frac{\Delta_{s-1}}{k+\Delta_{s-1}}$$

$$= \Delta_{s-1}\left(1 - \frac{2}{k+\Delta_{s-1}}\right).$$

When Δ_{s-1} is small, therefore, we find that

$$\Delta_s \lesssim \Delta_{s-1}(1 - 2/k),$$

so Δ_s decays like $e^{-2s/k}$ (in place of $e^{-s/k}$ as in diminishing ranges and the result of the previous section).

We may therefore expect that $\lambda_s \sim 2s - k + ke^{A - 2s/k}$, for a suitable A.

Theorem 18.4. Let $k \geq 4$ and $t \in \mathbb{N}$. When $2 \leq s \leq t$, define the real numbers Δ_s to be the unique positive solution with $0 \leq \Delta_s \leq k$ of the equation

$$\Delta_s e^{\Delta_s/k} = e^{1 - 2s/k}.$$

Then given $\varepsilon > 0$, there is an $\eta_0 = \eta_0(k, \varepsilon, t) > 0$ such that, whenever $0 < \eta < \eta_0$ and $2 \leq s \leq t$, one has

$$S_s(P, P^\eta) \ll P^{\lambda_s + \varepsilon},$$

where $\lambda_s = 2s - k + \Delta_s$.

Proof. Put $\delta_s = \Delta_s/k$, where Δ_s is defined as in the statement. Then we have $0 \le \delta_s \le 1$. Note that when δ is positive, the function $\delta + \log\delta$ is an increasing function of δ. Then the equation

$$\delta_s + \log\delta_s = 1 - \frac{2s}{k} \qquad (*)$$

has a unique solution with $0 \le \delta_s \le 1$ for each $s \ge 2$.

We have that $\lambda_s = 2s - 2$ is admissible for $s \ge 2$ (by Hua's Lemma when $2s = 4$, and hence also when $s \ge 2$). Thus $\Delta_s = k-2$ is permissible. But

$$(1 - \tfrac{2}{k}) + \log(1 - \tfrac{2}{k}) < 1 - \tfrac{4}{k},$$

and thus the equation (*) has a solution with $\delta_2 \ge 1 - 2/k$. Then with Δ_2 a solution of $\Delta_2 e^{\Delta_2/k} = e^{1-4/k}$, we find that Δ_2 is permissible, and the desired conclusion follows when $s = 2$.

We now proceed inductively. Suppose that the conclusion of the lemma holds for s, when $s \le t$ with $t \ge 2$. Then we have

$$S_{t+1}(P, P^\eta) \ll P^{\lambda_{t+1}+\varepsilon},$$

with $\lambda_{t+1} = 2(t+1) - k + \Delta_{t+1}$, and $\Delta = \Delta_{t+1} = k\delta_t(1-\theta) + k\theta - 1$, in which

$$k\theta = \frac{1}{1+\delta_t} + \Big(1 - \frac{1}{1+\delta_t}\Big)\Big(\frac{1-\delta_t}{2}\Big)^{k-1}. \qquad \text{(Theorem 18.3)}$$

Write $\delta = \delta_t$. Then we have

$$k\theta \le \frac{1}{1+\delta}\,(1 + \delta\cdot 2^{1-k}),$$

and hence

$$\Delta \le k\delta\Big(1 - \frac{1+\delta 2^{1-k}}{k(1+\delta)}\Big) + \frac{1}{1+\delta} + \frac{\delta}{1+\delta}2^{1-k} - 1$$

$$= k\delta\Big(1 - \frac{2-\omega}{k(1+\delta)}\Big),$$

where we note $\omega = (1-\delta)2^{1-k}$.

Then we have

$$\frac{\Delta}{k} + \log\frac{\Delta}{k} = \delta\left(1 - \frac{2-\omega}{k(1+\delta)}\right) + \log\delta + \log\left(1 - \frac{2-\omega}{k(1+\delta)}\right)$$

$$\leq \delta + \log\delta - \frac{(2-\omega)\delta}{k(1+\delta)} - \frac{(2-\omega)}{k(1+\delta)} - \frac{(2-\omega)^2}{2k^2(1+\delta)^2}$$

$$= \delta + \log\delta - \frac{2}{k} + \frac{\omega}{k} - \frac{(2-\omega)^2}{2k^2(1+\delta)^2}.$$

But $(2-\omega) = 2 - (1-\delta)2^{1-k} \geq 2 - (1-\delta) = 1+\delta$, and hence

$$\frac{\omega}{k} - \frac{(2-\omega)^2}{2k^2(1+\delta)^2} \leq \frac{(1-\delta)2^{1-k}}{k} - \frac{(1+\delta)^2}{2k^2(1+\delta)^2}$$

$$= \frac{k2^{2-k}(1-\delta) - 1}{2k^2} \leq 0 \quad \text{when } k \geq 4.$$

Thus

$$\frac{\Delta}{k} + \log\frac{\Delta}{k} \leq \delta_t + \log\delta_t - \frac{2}{k}. = \left(1 - \frac{2t}{k}\right) - \frac{2}{k}$$

$$= \delta_{t+1} + \log\delta_{t+1}.$$

Hence, if

$$\frac{\Delta^*_{t+1}}{k} e^{\Delta^*_{t+1}/k} = e^{1 - 2(t+1)/k},$$

then we have that Δ^*_{t+1} is permissible, and

$$S_{t+1}(P, P^\eta) \ll P^{\lambda_{t+1}+\varepsilon}$$

with $\lambda_{t+1} = 2(t+1) - k + \Delta^*_{t+1}$. This confirms the inductive step, and the desired conclusion follows. //

§19. A cheap analogue of Weyl's inequality:

We now present a minor arc estimate derived via a method of Thanigasalam as modified by Vaughan.

Lemma 19.1. Let $\alpha \in \mathbb{R}$. Suppose that $a \in \mathbb{Z}$, $q \in \mathbb{N}$ satisfy $(a,q)=1$, $q \le 2(2X)^k$, $|\underbrace{\alpha - a/q}_{=:\beta}| \le \frac{1}{2} q^{-1} (2X)^{-k}$. Suppose further that whenever $q \le X$, one has $|\beta| > q^{-1} X^{1-k} Y^{-1}$. Then, whenever (b_y) is a sequence of complex numbers, one has

$$\sum_{X \le p \le 2X} \sum_{1 \le y \le Y} b_y e(\alpha p^k y) \ll X^{\varepsilon} (XY + X^k)^{\frac{1}{2}} \Big(\sum_{1 \le y \le Y} |b_y|^2 \Big)^{\frac{1}{2}}.$$

Proof. When $(b,q)=1$, the congruence $x^k \equiv b \pmod q$ has $O_\varepsilon(q^\varepsilon)$ solutions modulo q. Thus the primes p in $[X, 2X]$ can be divided into r classes $\mathcal{P}_1, \dots, \mathcal{P}_r$, with $r = O_\varepsilon(q^\varepsilon)$, with the property that whenever $p_1, p_2 \in \mathcal{P}_j$, then $p_1^k \equiv p_2^k \pmod q$ if and only if $p_1 \equiv p_2 \pmod q$. Then if we write

$$Q_0(\alpha) = \sum_{X \le p \le 2X} \sum_{1 \le y \le Y} b_y e(\alpha p^k y),$$

then we have

$$Q_0(\alpha) = \sum_{j=1}^{r} Q_j(\alpha),$$

where

$$Q_j(\alpha) = \sum_{1 \le y \le Y} b_y \sum_{p \in \mathcal{P}_j} e(\alpha p^k y).$$

By Cauchy's inequality, we have

$$|Q_j(\alpha)|^2 \le \Big(\sum_{1 \le y \le Y} |b_y|^2 \Big) \Big(\sum_{1 \le y \le Y} \Big| \sum_{p \in \mathcal{P}_j} e(\alpha p^k y) \Big|^2 \Big)$$

$$\ll \Big(\sum_{1\le y\le Y} |b_y|^2 \Big) \Big(XY + \sum_{\substack{p_1,p_2\in \mathcal{P}_j \\ p_1\neq p_2}} \Big| \sum_{1\le y\le Y} e(\alpha(p_1^k - p_2^k)y) \Big| \Big)$$

$$\ll \Big(\sum_{1\le y\le Y} |b_y|^2 \Big) \Big(XY + \sum_{\substack{p_1,p_2\in \mathcal{P}_j \\ p_1\neq p_2}} \min\{ Y, \|\alpha(p_1^k - p_2^k)\|^{-1} \} \Big).$$

Note that for $p_1, p_2 \in \mathcal{P}_j$ with $p_1 \neq p_2$, one has

$$|\beta|\,|p_1^k - p_2^k| \le \tfrac{1}{2} q^{-1} (2X)^{-k} \cdot (2X)^k = \tfrac{1}{2} q^{-1}. \quad \text{—— (*)}$$

If there are any terms in the above double sum with $p_1 \neq p_2$ and $p_1^k \equiv p_2^k \pmod q$, then we have $p_1 \equiv p_2 \pmod q$ and $q \le X$. Hence, in such circumstances,

$$\|\alpha(p_1^k - p_2^k)\| = |\beta(p_1^k - p_2^k)| \gg q^{-1} X^{1-k} Y^{-1} \cdot (|p_1 - p_2| X^{k-1}).$$

Thus,

$$\sum_{\substack{p_1,p_2\in \mathcal{P}_j \\ p_1\neq p_2 \\ p_1^k \equiv p_2^k \pmod q}} \min\{ Y, \|\alpha(p_1^k - p_2^k)\|^{-1} \} \ll \sum_{p\in\mathcal{P}_j} \sum_{h\le 2X/q} \frac{qY}{(qh)}$$

$$\ll XY \log(2X/q).$$

Meanwhile, when $p_1, p_2 \in \mathcal{P}_j$, $p_1 \neq p_2$ and $p_1 \not\equiv p_2 \pmod q$, we have

$$\|\alpha(p_1^k - p_2^k)\| \overset{(*)}{\ge} \tfrac{1}{2} \Big\| \frac{a}{q} (p_1^k - p_2^k) \Big\|.$$

But the number of solutions of $p_1^k - p_2^k = h$ is $\ll_\varepsilon X^\varepsilon$ via a divisor function estimate, for each fixed $h \neq 0$ with $|h| \ll X^k$. Thus

$$\sum_{\substack{p_1,p_2\in \mathcal{P}_j \\ p_1\not\equiv p_2 \pmod q}} \min\{ Y, \|\alpha(p_1^k - p_2^k)\|^{-1} \} \ll \sum_{\substack{|h|<(2X)^k \\ q\nmid h}} X^\varepsilon \Big\| \frac{ah}{q} \Big\|^{-1}$$

$$\ll \Big(\frac{X^k}{q} + 1 \Big) \sum_{\ell=1}^{q/2} \frac{q}{\ell}$$

$$\ll (X^k+q)(\log(2q)^2.$$

Collecting together these estimates, we see that

$$|Q_j(\alpha)|^2 \ll \Big(\sum_{1\le y\le Y} |b_y|^2\Big)\big(XY + XY\log(2X/q) + (X^k+q)\log(2q)\big),$$

whence

$$Q_0(\alpha) \ll X^{\varepsilon}(XY+X^k)^{\frac12}\Big(\sum_{1\le y\le Y}|b_y|^2\Big)^{\frac12}. \quad /$$

Lemma 19.2. Let $X = P^{\delta}$ with $0 < \delta \le k/(2k-1)$. Also, put $Z = PX^{-1}$, and define

$$\mathcal{C} = \{n\in\mathbb{N}: n = pz,\ \tfrac12 X < p \le X,\ p \text{ prime},\ \text{and } z\in\mathcal{A}(Z,Z^{\eta})\},$$

in which $\eta = \eta(\varepsilon) > 0$ is sufficiently small. Also, write

$$h(\alpha) = \sum_{x\in\mathcal{C}} e(\alpha x^k).$$

Next, let $r\in\mathbb{N}$ and put $Y = rZ^k$. Let $\mathfrak{m}$ denote the set of real numbers α such that, whenever $a\in\mathbb{Z}$ and $q\in\mathbb{N}$ satisfy $(a,q)=1$, and $|\alpha - a/q| \le q^{-1}X^{1-k}Y^{-1}$, one has $q > X$.

Then

$$h(\alpha) \ll_{\varepsilon} P^{1-\sigma(k)+\varepsilon},$$

where

$$\sigma(k) = \frac{\delta - (1-\delta)\Delta_{2r}}{4r}.$$

Proof. Observe that

$$|h(\alpha)|^{2r} = \Big|\sum_{\frac12 X<p\le X}\ \sum_{z\in\mathcal{A}(Z,Z^{\eta})} e(\alpha p^k z^k)\Big|^{2r}$$

$$\overset{\text{Hölder}}{\ll} X^{2r-1}\sum_{\frac12 X<p\le X}\Big|\sum_{z\in\mathcal{A}(Z,Z^{\eta})} e(\alpha p^k z^k)\Big|^{2r}$$

$$= X^{2r-1} \sum_{\frac{1}{2}X < p \le X} \sum_{|y| \le Y} c_y e(\alpha p^k y),$$

where c_y denotes the number of solutions of the equation

$$z_1^k - z_2^k + \cdots + z_{2r-1}^k - z_{2r}^k = y,$$

with $z_i \in \mathcal{A}(Z, Z^\eta)$, and $Y = r Z^k$. But $c_y = c_{-y}$, so by Lemma 19.1,

$$\sum_{\frac{1}{2}X < p \le X} \sum_{|y| \le Y} c_y e(\alpha p^k y) = \sum_{\frac{1}{2}X < p \le X} \Big(c_0 + 2\mathrm{Re}\Big(\sum_{1 \le y \le Y} c_y e(\alpha p^k y) \Big) \Big)$$

$$\ll X^\varepsilon (XY + X^k)^{\frac{1}{2}} \Big(\sum_{|y| \le Y} |c_y|^2 \Big)^{\frac{1}{2}}.$$

Thus, on considering the underlying Diophantine equations and applying orthogonality, we obtain

$$|h(\alpha)|^{4r} \ll X^{4r-2+\varepsilon} (XY + X^k) S_{2r}(Z, Z^\eta)$$

$$\ll X^{4r-2+\varepsilon} (XY + X^k) Z^{4r-k+\Delta_{2r}+\varepsilon}$$

$$= (ZX)^{4r} (XZ^k + X^k) Z^{-k+\Delta_{2r}+\varepsilon} \cdot X^{-2}.$$

Note that $X^k = P^{k\delta}$ and $XZ^k = P^k X^{1-k} = P^{k-(k-1)\delta}$, so that $X^k < XZ^k$ whenever $\delta \le k/(2k-1)$. Thus,

$$|h(\alpha)|^{4r} \ll P^{2\varepsilon} (P^{4r} X^{-1} Z^{\Delta_{2r}}) = P^{4r(1-\sigma)+2\varepsilon},$$

where

$$\sigma = \frac{\delta - (1-\delta)\Delta_{2r}}{4r}.$$

Thus,

$$|h(\alpha)| \ll P^{1-\sigma+\varepsilon},$$

and the proof of the lemma is complete. //

Let us now investigate a choice of parameters here. Recall that

$$\Delta_{2r} \leq k e^{1 - 4r/k}.$$

We take

$$r = \lceil \tfrac{k}{4}(\log k + 2\log\log k) \rceil. \quad \text{Then}$$

$$\Delta_{2r} \leq k e^{1 - \log k - 2\log\log k} = \frac{e}{(\log k)^2}.$$

In this way, we find that

$$\sigma(k) \geqslant \frac{\delta - (1-\delta) e / (\log k)^2}{k(\log k + 2\log\log k) + 4}.$$

So for a fixed value of δ, we see that

$$\sigma(k) \geqslant \frac{\delta + o(1)}{k \log k}, \quad \text{as } k \to \infty.$$

Corollary. As $k \to \infty$, one has

$$\sup_{\alpha \in \mathfrak{m}_\delta} |h(\alpha)| \ll P^{1 - \frac{\delta + o(1)}{k \log k} + \varepsilon}.$$

This should be compared with the output of Weyl's inequality, namely

$$\sup_{\alpha \in \mathfrak{m}_\delta} \Big| \sum_{1 \leq x \leq P} e(\alpha x^k) \Big| \ll P^{1 - \delta 2^{1-k} + \varepsilon}.$$

---

§20. A new upper bound for $G(k)$.

Consider the number $R(n)$ of representations of a large natural number n in the form

$$n = \sum_{i=1}^{t} x_i^k + \sum_{j=1}^{u} y_j^k + \sum_{l=1}^{25} z_l^k,$$

with $1 \le x_i \le X$ $(1 \le i \le t)$, $y_j \in \mathcal{C}$ $(1 \le j \le u)$, $z_l \in \mathcal{A}(X, X^\eta)$,

where $X = n^{1/k}$ and

$$\mathcal{C} = \{m \in \mathbb{N} \cap [1, X] : \quad m = pw, \ \tfrac{1}{2}X^\delta < p \le X^\delta \text{ and } p \text{ prime}, \ w \in \mathcal{A}(X^{1-\delta}, X^\eta)\}$$

Here, we take $\delta = 1/10$, say. We take $t = 4k$ and u and s large enough so that the minor arcs are small enough — we optimise u and s shortly. Thus, writing

$$F(\alpha) = \sum_{1 \le x \le X} e(\alpha x^k), \quad g(\alpha) = \sum_{y \in \mathcal{C}} e(\alpha y^k), \quad h(\alpha) = \sum_{z \in \mathcal{A}(X, X^\eta)} e(\alpha z^k),$$

we see that

$$R(n) = \int_0^1 F(\alpha)^t g(\alpha)^u h(\alpha)^{2s} e(-n\alpha)\, d\alpha.$$

Moreover, since $t \ge 4k$, we see that

$$\int_{\mathfrak{m}_\delta} F(\alpha)^t g(\alpha)^u h(\alpha)^{2s} e(-n\alpha)\, d\alpha = \sum_{\mathbf{y}, \mathbf{z}} \int_{\mathfrak{m}_\delta} F(\alpha)^t e\Big(-\Big(n - \sum_{j=1}^u y_j^k - \sum_{l=1}^{2s} z_l^k\Big)\alpha\Big)\, d\alpha$$

$$\gg \sum_{\mathbf{y}, \mathbf{z}} \Big(n - \sum_{j=1}^u y_j^k - \sum_{l=1}^{2s} z_l^k\Big)^{\frac{t}{k} - 1}$$

$$\gg n^{(2s+u+t)/k - 1} (\log n)^{-u},$$

using our standard major arc machinery.

Meanwhile, we have

$$\Big| \int_{\mathfrak{m}_\delta} F(\alpha)^t g(\alpha)^u h(\alpha)^{2s} e(-n\alpha)\, d\alpha \Big| \le X^t \Big(\sup_{\alpha \in \mathfrak{m}_\delta} |g(\alpha)|\Big)^u \int_0^1 |h(\alpha)|^{2s}\, d\alpha$$

$$\ll X^t \cdot \big(X^{1 - \sigma(k) + \varepsilon}\big)^u \, X^{\lambda_s + \varepsilon},$$

where $\sigma(k) \ge \dfrac{\delta + o(1)}{k \log k}$ and $\lambda_s = 2s - k + \Delta_s$ with $\Delta_s \le k e^{1 - 2s/k}$.

We therefore obtain

$$\left| \int_{\mathfrak{m}_s} F(\alpha)^t g(\alpha)^u h(\alpha)^{2s} e(-n\alpha)\, d\alpha \right| \ll X^{t+u+2s-k-\tau},$$

for a positive number τ, provided that

$$u\sigma(k) > \Delta_s,$$

and since $X = n^{1/k}$, this shows that

$$R(n) \gg n^{(2s+u+t)/k - 1} (\log n)^{-u} \to \infty \quad \text{as } n \to \infty,$$

whence $G(k) \le 2s + u + t$.

The condition $u\,\sigma(k) > \Delta_s$ is satisfied provided that

$$u > \frac{\Delta_s}{(\delta + o(1))/(k \log k)} = (10 + o(1))\, k e^{1 - 2s/k} \cdot k \log k$$

$$= (10e + o(1))\, k^2 \log k\, e^{-2s/k}.$$

Take $u = \lceil 30 k^2 \log k \cdot e^{-2s/k} \rceil$ and k large. Then we have

$$G(k) \le 2s + u + t = 2s + \lceil 30 k^2 \log k \cdot e^{-2s/k} \rceil + 4k.$$

The smallest value obtained here occurs with

$$s \le \tfrac{1}{2} k(\log k + \log\log k + C),$$

for some positive number C. With such a value of s, one has

$$30 k^2 \log k \cdot e^{-2s/k} \le 30 k e^{1-C},$$

whence

$$G(k) \le k(\log k + \log\log k + C) + 30 k e^{1-C} + 4k$$

$$= k(\log k + \log\log k + O(1)), \quad \text{as } k \to \infty.$$

<u>Theorem 20.1</u> (W., 1992) When k is large, one has $G(k) \le k(\log k + \log\log k + O(1))$.

§21. Fractional parts of polynomials.

We consider a class of problems concerning equidistribution modulo 1. Let $x_1, x_2, \dots$ be a sequence of real numbers in $[0,1)$, and suppose that

$$Z(N,\alpha) = \operatorname{card}\{1 \le j \le N : x_j \in [0,\alpha)\}.$$

We say that (x_n) is <u>equidistributed</u> or <u>uniformly distributed</u> if

$$\lim_{N\to\infty} N^{-1} Z(N,\alpha) = \alpha \qquad \text{for all } \alpha \in [0,1).$$

Notice that

$$\frac{1}{N}\operatorname{card}\{1 \le j \le N : x_j \in [\alpha,\beta)\} = \frac{1}{N}\big(Z(N,\beta) - Z(N,\alpha)\big),$$

$$= \beta - \alpha \qquad \text{if} \qquad 0 < \alpha < \beta < 1,$$

and (x_j) is equidistributed.

We focus here on the situation for small values of α, and illustrate ideas by considering sequences of the shape $(\alpha n^k \bmod 1)_{n=1}^{\infty}$, with $\alpha \in \mathbb{R}$. Here we have:

Dirichlet's Theorem: $\min_{1\le n\le N} \|n\theta\| \le N^{-1}$.

More generally (Vinogradov, 1927; Heilbronn, 1948, ...): $\min_{1\le n\le N} \|n^k\theta\| \ll N^{-\tau}$,

for suitable $\tau = \tau(k) > 0$.

Lemma 21.1 Let $0 < \Delta \le \frac{1}{4}$ and $r \in \mathbb{N}$. There is a periodic function $\psi : \mathbb{R} \to \mathbb{R}$ having period 1 such that:

$$\psi(x) \ge 0, \qquad \text{for all } x \in \mathbb{R},$$

$$\psi(x) = 0, \qquad \text{when } \|x\| \ge 2\Delta,$$

$$\psi(x) = 2\Delta + \sum_{m\in\mathbb{Z}\setminus\{0\}} a_m e(mx), \qquad \text{for all } x \in \mathbb{R},$$

in which a_m are real coefficients with $|a_m| \ll_r |m|^{-r-1}\Delta^{-r}$ $(m \ne 0)$.

Proof: Let $\psi_0 : \mathbb{R} \to \mathbb{R}$ be periodic with period 1, defined by

$$\psi_0(x) = \begin{cases} 1, & \text{when } -\Delta \le x < \Delta, \\ 0, & \text{whence } \Delta \le x < 1-\Delta. \end{cases}$$

Then the Fourier coefficients of ψ_0 are

$$\hat{\psi}_0(m) = \int_{-\frac{1}{2}}^{\frac{1}{2}} \psi_0(x)\, e(-mx)\, dx = \frac{\sin(2\pi m\Delta)}{\pi m} \qquad (m \neq 0).$$

Moreover, one has $\hat{\psi}_0(0) = 2\Delta$.

Now let $\gamma = \Delta/r$, and define the functions $\psi_1, \dots, \psi_r$, each periodic with period 1, by the recurrence formula

$$\psi_\ell(x) = \frac{1}{2\gamma} \int_{-\gamma}^{\gamma} \psi_{\ell-1}(x+z)\, dz \qquad (1 \le \ell \le r).$$

We prove by induction that:

(i) $\psi_\ell(x) = 0$ for $\Delta + \ell\gamma < x < 1 - \Delta - \ell\gamma$,

(ii) $\psi_\ell(x) \ge 0$ for all $x \in \mathbb{R}$,

(iii) $$\psi_\ell(x) = \sum_{m \in \mathbb{Z}} \hat{\psi}_\ell(m)\, e(mx), \qquad \text{for all } x \in \mathbb{R},$$

with $\hat{\psi}_\ell(0) = 2\Delta$, and

$$|\hat{\psi}_\ell(m)| \ll_{\ell, r} |m|^{-\ell-1} \Delta^{-\ell} \qquad (m \neq 0).$$

Observe first that (i) and (ii) both hold when $\ell = 0$, by virtue of our discussion concerning $\psi_0(x)$. If these properties hold also for $\ell = L-1$, when $L \ge 1$, then since $\psi_L(x)$ is the average of $\psi_{L-1}(x)$ on the interval $(x-\gamma, x+\gamma)$, we find that (i) and (ii) holds also for $\ell = L$. For the property (iii), observe that

$$\hat{\psi}_L(m) = \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{1}{2\gamma} \int_{-\gamma}^{\gamma} \psi_{L-1}(x+z)\, e(-mx)\, dz\, dx$$

$$= \frac{1}{2\gamma} \int_{-\gamma}^{\gamma} \int_{-\frac{1}{2}}^{\frac{1}{2}} \psi_{L-1}(x+z)\, e(-mx)\, dx\, dz$$

$$= \hat{\psi}_{L-1}(m) \cdot \frac{1}{2\gamma} \int_{-\gamma}^{\gamma} e(mz)\, dz .$$

Thus, we have $\hat{\psi}_L(0) = 2\Delta$ and

$$|\hat{\psi}_L(m)| = |\hat{\psi}_{L-1}(m)| \cdot \left| \frac{\sin(2\pi m\gamma)}{2\pi m\gamma} \right| \le \frac{r}{2\pi|m|\Delta} |\hat{\psi}_{L-1}(m)|,$$

whence $|\hat{\psi}_L(m)| \le \left| \left(\frac{r}{2\pi m\Delta}\right)^L \cdot \frac{1}{\pi m} \right| \ll_{L,r} |m|^{-L-1} \Delta^{-L}$. (since $\gamma = \Delta/r$).

Then $\sum_{m \in \mathbb{Z}} |\hat{\psi}_\ell(m)| < \infty$ for $\ell \ge 1$. Since $\psi_1, \psi_2, \dots$, are continuous, it follows that $\psi_\ell(x)$ is the sum of its Fourier series for $\ell \ge 1$ (Zygmund). Then (iii) follows by this inductive argument.

The proof is completed by choosing $\psi = \psi_r$. //

We now have a means of detecting small values (mod 1) of a given sequence.

Lemma 21.2. (Vinogradov). Let (b_n) be a sequence of non-negative real numbers (weights). Further, let (x_n) be a sequence of real numbers. Let $M > C(\varepsilon)$, and suppose that $\|x_n\| \ge M^{-1}$ for $1 \le n \le N$. Then one has

$$\sum_{1 \le m \le M^{1+\varepsilon}} \left| \sum_{n=1}^{N} b_n\, e(m x_n) \right| > \frac{1}{4} \sum_{n=1}^{N} |b_n| .$$

[Note: The ε here can be removed with extra effort.]

Proof. Let $\Delta = \frac{1}{2M}$ and put $r = \left[\frac{2}{\varepsilon}\right] + 1$. Then there exists a non-negative function $\psi : \mathbb{R} \to \mathbb{R}$, periodic with period 1,

such that

$$\psi(x) = 0, \quad \text{when } \|x\| \geq 2\Delta,$$

$$\psi(x) = \sum_{m \in \mathbb{Z}} a_m e(mx), \quad \text{for all } x \in \mathbb{R},$$

where a_m is a suitable real number satisfying

$$a_0 = 2\Delta \quad \text{and} \quad |a_m| \ll_\varepsilon |m|^{-r-1}\Delta^{-r}. \qquad (m \in \mathbb{Z}).$$

Thus, we have

$$\sum_{m > M^{1+\varepsilon}} |a_m| \ll_\varepsilon \sum_{m > M^{1+\varepsilon}} |m|^{-r-1}\Delta^{-r}$$

$$\ll_\varepsilon (M^{1+\varepsilon})^{-r}\Delta^{-r} \ll M^{-r\varepsilon} \ll M^{-2} < a_0/2.$$

Now observe that $\psi(x_n) = 0$ for $1 \leq n \leq N$, since $\|x_n\| \geq M^{-1}$. Then if we sum over n, with weights b_n, we see that

$$\sum_{m \in \mathbb{Z}} a_m \sum_{n=1}^{N} b_n e(mx_n) = \sum_{n=1}^{N} b_n \psi(x_n) = 0.$$

Hence,

$$\sum_{m \in \mathbb{Z}\setminus\{0\}} |a_m| \left| \sum_{n=1}^{N} b_n e(mx_n) \right| \geq a_0 \sum_{n=1}^{N} |b_n|,$$

and also

$$\sum_{|m| > M^{1+\varepsilon}} |a_m| \left| \sum_{n=1}^{N} b_n e(mx_n) \right| \leq \sum_{n=1}^{N} |b_n| \cdot \sum_{|m| > M^{1+\varepsilon}} |a_m|$$

$$< \frac{a_0}{2} \sum_{n=1}^{N} |b_n|.$$

Consequently,

$$\sum_{1 \leq |m| \leq M^{1+\varepsilon}} |a_m| \left| \sum_{n=1}^{N} b_n e(mx_n) \right| > \tfrac{1}{2} a_0 \sum_{n=1}^{N} |b_n|$$

But we also have

$$|a_m| = \left| \int_{-\frac{1}{2}}^{\frac{1}{2}} \psi(x)\, e(mx)\, dx \right| \leq \int_{-\frac{1}{2}}^{\frac{1}{2}} |\psi(x)|\, dx = a_0,$$

and thus

$$\sum_{\ell \in |m| \leq M^{1+\varepsilon}} \left| \sum_{n=1}^{N} b_n\, e(m x_n) \right| > \tfrac{1}{2} \sum_{n=1}^{N} b_n .$$

Since $\left| \sum_{n=1}^{N} b_n\, e(m x_n) \right| = \left| \sum_{n=1}^{N} b_n\, e(-m x_n) \right|$, this delivers the conclusion of the lemma. //

Let us first consider a simple estimate obtained via Weyl differencing. Here we write

$$f(\alpha) = \sum_{1 \leq x \leq P} e(\alpha x^k).$$

<u>Lemma 21.3.</u> Suppose that $L \leq P$, and

$$\sum_{m=1}^{L} |f(m\alpha)|^{2^{k-1}} \gg A,$$

where $A \gg L P^{2^{k-1} - 1 + \varepsilon}$, for some $\varepsilon > 0$. Then there exist integers r and s with $(r,s) = 1$, $r \leq L P^{2^{k-1} + \varepsilon} A^{-1}$ and

$$|\alpha r - s| \leq A^{-1} P^{2^{k-1} - k + \varepsilon}.$$

<u>Proof.</u> We apply the Weyl-differencing lemma to deduce that

$$|f(m\alpha)|^{2^{k-1}} \ll P^{2^{k-1} - 1} + P^{2^{k-1} - k} \sum_{1 \leq y_1 \leq P} \cdots \sum_{1 \leq y_{k-1} \leq P} \left| \sum_{x \in I(y)} e(k! m y_1 \cdots y_{k-1} \alpha x + \beta) \right|$$

where $I(y)$ is an interval of integers contained in $[1, P]$, and $\beta = \beta(y)$. Thus

$$\sum_{m=1}^{L} |f(m\alpha)|^{2^{k-1}} \ll P^{2^{k-1}-1} L + P^{2^{k-1}-k} \sum_{1 \le y_1, \dots, y_{k-1} \le P} \sum_{m=1}^{L} \min\{P, \|k! m y_1 \cdots y_{k-1} \alpha\|^{-1}\}$$

$$\ll_\varepsilon P^{2^{k-1}-1} L + P^{2^{k-1}-k+\varepsilon} \sum_{1 \le z \le k! P^{k-1} L} \min\{P, \|z\alpha\|^{-1}\}.$$

(using a divisor function estimate).

By the hypothesis of the Lemma, therefore, we have

$$A \ll \sum_{m=1}^{L} |f(m\alpha)|^{2^{k-1}} \ll_\varepsilon P^{2^{k-1}-1} L + P^{2^{k-1}-k+\varepsilon/2} \sum_{1 \le z \le k! P^{k-1} L} \min\{P, \|z\alpha\|^{-1}\},$$

$\vee$

$L P^{2^{k-1}-1+\varepsilon}$

(This is smaller than LHS)

Whence

$$\sum_{1 \le z \le k! P^{k-1} L} \min\{P, \|z\alpha\|^{-1}\} \gg A P^{k-2^{k-1}-\varepsilon/2}.$$

By Dirichlet's approximation theorem, we may choose $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $(a,q) = 1$, $q \le A P^{k-2^{k-1}-\varepsilon}$, and $|\alpha - a/q| \le \frac{1}{q} A^{-1} P^{2^{k-1}-k+\varepsilon}$. Then

$$A P^{k-2^{k-1}-\varepsilon/2} \ll k! P^k L \left(q^{-1} + P^{-1} + q P^{-k} L^{-1}\right) \log(2Pq),$$

whence

$$q^{-1} + P^{-1} + q P^{-k} L^{-1} \gg A L^{-1} P^{-2^{k-1}-3\varepsilon/4}.$$

But $A \geqslant LP^{2^{k-1}-1+\varepsilon}$, and hence

$$AL^{-1}P^{-2^{k-1}-3\varepsilon/4} \gg P^{\varepsilon/4-1}.$$

Then we deduce that since $qP^{-k}L^{-1} \leqslant AP^{-2^{k-1}-\varepsilon}L^{-1}$, one must have $q^{-1} \gg AL^{-1}P^{-2^{k-1}-3\varepsilon/4}$, whence

$$q \ll A^{-1}LP^{2^{k-1}+3\varepsilon/4}.$$

Provided that q is large enough, therefore, we have $q \leqslant LP^{2^{k-1}+\varepsilon}A^{-1}$, and then $|q\alpha - a| \leqslant A^{-1}P^{2^{k-1}-k+\varepsilon}$.

This completes the proof of the lemma. //

Notice that this lemma shows that when $|f(m\alpha)|$ is large (on average), then there is a good rational approximation to α.

<u>Theorem 21.4.</u> Suppose that $\alpha \in \mathbb{R}$. Then one has

$$\min_{1\leqslant n\leqslant N} \|\alpha n^k\| \ll_\varepsilon N^{\varepsilon - 2^{1-k}}.$$

<u>Proof.</u> Suppose that there exists no integer n with $1 \leqslant n \leqslant N$ for which $\|\alpha n^k\| \leqslant N^{\varepsilon-2^{1-k}}$. Then, if we put $M = \lceil N^{2^{1-k}-\varepsilon}\rceil$, we find from Lemma 21.2 that

$$\sum_{1\leqslant m\leqslant M^{1+\varepsilon^2}} |f(m\alpha)| > \frac{N}{4}$$

(note – we have put $b_n = 1$ for $n \in \mathbb{N}$), where $f(\alpha) = \sum_{1\leqslant n\leqslant N} e(\alpha n^k)$.

By Hölder's inequality, we infer that

$$\frac{N}{4} < \left(M^{1+\varepsilon^2}\right)^{1-2^{1-k}} \left(\sum_{1 \le m \le M^{1+\varepsilon^2}} |f(m\alpha)|^{2^{k-1}} \right)^{2^{1-k}},$$

whence

$$\sum_{1 \le m \le M^{1+\varepsilon^2}} |f(m\alpha)|^{2^{k-1}} \gg N^{2^{k-1}} M^{1-2^{k-1}-\varepsilon}.$$

We may now apply Lemma 21.3 with $A = N^{2^{k-1}} M^{1-2^{k-1}-\varepsilon}$ and $L = M^{1+\varepsilon^2}$, $P = N$, since

$$A = \left(N^{2^{k-1}-1+\varepsilon}\right) M^{1+\varepsilon^2} \cdot N^{1-\varepsilon} M^{-2^{k-1}-\varepsilon-\varepsilon^2}$$
$$\geqslant L P^{2^{k-1}-1+\varepsilon}.$$

Thus, there exist integers r and s with $(r,s)=1$,

$$r \le L P^{2^{k-1}+\varepsilon} A^{-1} \ll M^{2^{k-1}+\varepsilon} N^{\varepsilon}$$

and

$$|\alpha r - s| \le A^{-1} P^{2^{k-1}-k+\varepsilon} \ll M^{2^{k-1}-1+\varepsilon} N^{-k+\varepsilon}.$$

In particular, we have $r \le N$ and

$$\|\alpha r^k\| \le r^{k-1} \|\alpha r\| \le N^{k-1} \cdot M^{2^{k-1}-1+\varepsilon} N^{-k+\varepsilon} < M^{-1}.$$

We therefore conclude that

$$\min_{1 \le r \le N} \|\alpha r^k\| < N^{\varepsilon - 2^{1-k}}.$$

The latter conclusion therefore holds in all circumstances. //

We can extract a cheap refinement (for large values of k) by applying our work from §19 on smooth Weyl sums.

Suppose that there exists no integer n with $1 \le n \le N$ for which $\|\alpha n^k\| \le N^{\varepsilon - \nu(k)}$, where $\nu(k)$ is an exponent to be chosen later. We put $M = \lceil N^{\nu(k)-\varepsilon} \rceil$, and find from Lemma 21.2 that

$$\sum_{1 \le m \le M^{1+\varepsilon^2}} |h(m\alpha)| > \tfrac{1}{4} \sum_{x \in \mathcal{L}} 1 \gg \frac{N}{\log N}$$

where

$$h(\alpha) = \sum_{x \in \mathcal{L}(N)} e(\alpha x^k) = \sum_{\frac{1}{2}X < q \le X} \sum_{z \in \mathcal{A}(z, z^\eta)} e(\alpha (qz)^k)$$

$$Z = NX^{-1}, \quad X = N^\delta \text{ with } 0 < \delta \le k/(2k-1).$$

Thus, for some integer m with $1 \le m \le M^{1+\varepsilon^2}$, one has

$$|h(m\alpha)| \gg N^{1-\varepsilon} M^{-1}.$$

But we have shown in the corollary to Lemma 19.2 that whenever $\beta \in \mathfrak{m}_\delta$, we have

$$|h(\beta)| \ll N^{1 - \frac{\delta + o(1)}{k \log k} + \varepsilon}.$$

Here, $\mathfrak{m}_\delta$ is the complement $[0,1) \setminus \mathfrak{M}_\delta$, of the set

$$\mathfrak{M}_\delta = \bigcup_{\substack{0 \le a \le q \le N^\delta \\ (a,q)=1}} \{\alpha \in [0,1) : |\alpha - a/q| \le q^{-1} N^{\delta - k}\}.$$

$$= \mathfrak{M}(N^\delta), \text{ say.}$$

Thus, we have $m\alpha \in \mathfrak{m}_\delta$ when we take $\begin{cases} \nu(k) = \frac{\delta + o(1)}{k \log k}. \\ M = N^{\varepsilon + \frac{\delta + o(1)}{k \log k} - \varepsilon} \end{cases}$

But then $\alpha \in \mathfrak{M}(N^\delta M)$, so there exist $a \in \mathbb{Z}$, $q \in \mathbb{N}$ with $0 \le a \le q \le MN^\delta$, $(a,q) = 1$ and $|\alpha - a/q| \le MN^{\delta - k}$.

We therefore find that

$$\|\alpha q^k\| = |\alpha q^k - a q^{k-1}| \leq (MN^\delta)^k \cdot MN^{\delta-k}$$

$$\leq N^{\frac{(k+1)(\delta+o(1))}{k\log k} + k\delta - k}.$$

Take $\delta = 1/10$, say, and then we find that

$$\|\alpha q^k\| \ll N^{-\frac{4}{5}k}.$$

This gives a contradiction. Thus there exists an integer n with $1 \leq n \leq N$ such that $\|\alpha n^k\| \leq N^{\varepsilon - \frac{\delta+o(1)}{k\log k}}$.

We can do better, and this is the subject of the next section.

§22. Unlocalised results on $\|\alpha n^k\|$.

We apply an idea of Karatsuba also used by Heath-Brown.

Theorem 22.1. Define

$$\tau(k) = \max_{s \geq 1} \frac{k - 2\Delta_s}{4s^2}. \qquad \text{(where } \Delta_s \text{ is a permissible exponent)}$$

Let $\alpha \in \mathbb{R}$ and $\varepsilon > 0$ be given. Then for each $k \geq 2$, there are infinitely many integers $n \in \mathbb{N}$ with

$$\|\alpha n^k\| \leq n^{\varepsilon - \tau(k)}.$$

Proof. The result is plain if $\alpha \in \mathbb{Q}$, so we may suppose that α is irrational. There are consequently infinitely many pairs $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $|\alpha - a/q| \leq 1/q^2$, as a consequence of Dirichlet's approximation theorem. We put

$N = \lfloor q^{2/k} \rfloor$, and then put

$$a_n = \#\{ n = xy : x, y \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta}) \}.$$

Suppose, if possible, that there are no solutions of the inequality

$$\| \alpha n^k \| \leq M^{-1}$$

for $1 \leq n \leq N$. Then from Lemma 21.2 we have

$$\sum_{1 \leq m \leq M^{1+\varepsilon^2}} \Big| \sum_{x,y \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta})} e(m\alpha(xy)^k) \Big| > \tfrac{1}{4} \sum_{n=1}^{N} a_n$$

$$\gg (N^{\frac{1}{2}})^2 \gg N^{1+\eta}.$$

We aim to choose M in such a manner that this leads to a contradiction.

Observe first that, writing

$$T(\alpha) = \sum_{x \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta})} \sum_{y \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta})} e(\alpha(xy)^k),$$

we have

$$|T(\alpha)|^s \leq (N^{\frac{1}{2}})^{s-1} \sum_{x \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta})} \Big| \sum_{y \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta})} e(\alpha(xy)^k) \Big|^s$$

$$= (N^{\frac{1}{2}})^{s-1} \sum_{x \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta})} \omega_x \Big(\sum_{y \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta})} e(\alpha(xy)^k) \Big)^s,$$

where ω_x is a unimodular complex number. Hence

$$|T(\alpha)|^s = (N^{\frac{1}{2}})^{s-1} \sum_{1 \leq u \leq sN^{\frac{1}{2}k}} r_u \sum_{x \in \mathcal{A}(N^{\frac{1}{2}}, N^{\eta})} \omega_x e(\alpha u x^k),$$

where

$$r_u = \#\{ u = y_1^4 + \cdots + y_s^4 : y_i \in \mathcal{A}(N^{\frac{1}{2}}, N^\eta)\}.$$

Now apply Hölder's inequality again. We find that

$$|T(\alpha)|^{2s^2} \le (N^{\frac{1}{2}})^{2s(s-1)} \Big(\sum_{1 \le u \le sN^{\frac{1}{2}k}} r_u \Big)^{2s-2} \Big(\sum_{1 \le u \le sN^{\frac{1}{2}k}} r_u^2 \Big) \times \sum_{1 \le u \le sN^{\frac{1}{2}k}} \Big| \sum_{x \in \mathcal{A}(N^{\frac{1}{2}}, N^\eta)} \omega_x e(\alpha u x^k) \Big|^{2s}.$$

But

$$\sum_u r_u \le N^{\frac{1}{2}s}, \qquad \sum_u r_u^2 \le S_s(N^{\frac{1}{2}}, N^\eta) \ll (N^{\frac{1}{2}})^{2s-k+\Delta_s+\varepsilon},$$

and

$$\Big| \sum_{x \in \mathcal{A}(N^{\frac{1}{2}}, N^\eta)} \omega_x e(\alpha u x^k) \Big|^{2s} = \sum_{|v| \le sN^{\frac{1}{2}k}} \tilde{r}_v e(\alpha u v),$$

where $\tilde{r}_v$ counts solutions of the equation $\sum_{i=1}^{s} (x_i^k - y_i^k) = v$, with $x_i, y_i \in \mathcal{A}(N^{\frac{1}{2}}, N^\eta)$ $(1 \le i \le s)$, with each solution being counted with weight

$$\prod_{i=1}^{s} (\omega_{x_i} \overline{\omega}_{y_i}).$$ (which is unimodular).

Thus

$$|\tilde{r}_v| \le \Big| \int_0^1 \Big| \sum_{x \in \mathcal{A}(N^{\frac{1}{2}}, N^\eta)} \omega_x e(\theta x^k) \Big|^{2s} e(-\theta v)\, d\theta$$

$$\le \int_0^1 \Big| \sum_{x \in \mathcal{A}(N^{\frac{1}{2}}, N^\eta)} \omega_x e(\theta x^k) \Big|^{2s} d\theta \le S_s(N^{\frac{1}{2}}, N^\eta)$$

$$\ll (N^{\frac{1}{2}})^{2s-k+\Delta_s+\varepsilon}.$$

We ~~therefore~~ conclude ~~that~~

$$|T(\alpha)|^{2s^2} \ll (N^{\frac{1}{2}})^{2s(s-1)+(2s-2)s+2s-k+\Delta_s+\varepsilon} \cdot \sum_{1\le u\le sN^{\frac{1}{2}k}} \sum_{|v|\le sN^{\frac{1}{2}k}} \tilde{r}_v e(\alpha uv)$$

$$\ll (N^{\frac{1}{2}})^{4s^2-2s-k+\Delta_s+\varepsilon} \sum_{|v|\le sN^{\frac{1}{2}k}} |\tilde{r}_v| \Big| \sum_{1\le u\le sN^{\frac{1}{2}k}} e(\alpha uv)\Big|$$

$$\ll (N^{\frac{1}{2}})^{4s^2-2s-k+\Delta_s+\varepsilon} \cdot N^{2s-k+\Delta_s+\varepsilon} \sum_{|v|\le sN^{\frac{1}{2}k}} \min\{N^{\frac{1}{2}k}, \|\alpha v\|^{-1}\}.$$

But ~~then~~, by Hölder's inequality, one has

$$\Big(\sum_{1\le m\le M^{1+\varepsilon^2}} |T(\alpha m)|\Big)^{2s^2} \ll (M^{1+\varepsilon^2})^{2s^2-1} \sum_{1\le m\le M^{1+\varepsilon^2}} |T(\alpha m)|^{2s^2}$$

$$\ll (M^{1+\varepsilon^2})^{2s^2-1} (N^{\frac{1}{2}})^{4s^2-2k+2\Delta_s+2\varepsilon} \times \sum_{1\le m\le M^{1+\varepsilon^2}} \sum_{|v|\le sN^{\frac{1}{2}k}} \min\{N^{\frac{1}{2}k}, \|\alpha mv\|^{-1}\}$$

$$\ll (M^{1+\varepsilon^2})^{2s^2-1} (N^{\frac{1}{2}})^{4s^2-2k+2\Delta_s+2\varepsilon} \times M^{1+\varepsilon^2} N^{k+\varepsilon} \big(q^{-1} + N^{-\frac{1}{2}k} + qN^{-k}M^{-1-\varepsilon^2}\big)$$

Moreover, we choose N in such a way ~~that~~ $N^{\frac{k}{2}} \le q \le (N+1)^{\frac{k}{2}}$, whence

$$\Big(\sum_{1\le m\le M^{1+\varepsilon^2}} |T(\alpha m)|\Big)^{2s^2} \ll (M^{1+\varepsilon^2})^{2s^2} (N^{\frac{1}{2}})^{4s^2+2\Delta_s+4\varepsilon} N^{-\frac{1}{2}k},$$

so that

$$\sum_{1 \le m \le M^{1+\varepsilon^2}} |T(\alpha m)| \ll M^{1+\varepsilon^2} N^{1+2\varepsilon-\tau},$$

where

$$\tau = \frac{k - 2\Delta_s}{4s^2}.$$

This is smaller than $N^{1-2\varepsilon}$ whenever

$$M^{1+\varepsilon^2} N^{3\varepsilon-\tau} \le 1,$$

which is to say that $M \le N^{\frac{\tau-3\varepsilon}{1+\varepsilon^2}}$. Since $\varepsilon > 0$ is arbitrary, we obtain a contradiction whenever $M \le N^{\tau-4\varepsilon}$.

Thus, there exists $n \in \mathbb{N}$ with

$$\|\alpha n^k\| \le n^{\varepsilon - \tau(k)},$$

with $n \le N = \lfloor q^{2/k} \rfloor$, for each convergent a/q to the contained fraction of α. //

Corollary. For each $k \ge 4$, there are infinitely many integers $n \in \mathbb{N}$ with

$$\|\alpha n^k\| \le n^{-\frac{1}{9.028k}}.$$

Proof. We can assume that Δ_s is permissible, with

$$\Delta_s e^{\Delta_s/k} = k e^{1-2s/k}.$$

Put $s = k$ and take ξ to be the positive real solution of the equation $\frac{1}{3} e^{\frac{1}{3}} = e^{-1}$. Then we see that $\Delta_s = \frac{1}{3}k$

is permissible, and there are infinitely many solutions $n \in \mathbb{N}$ to the inequality

$$\|\alpha n^4\| \leq n^{-\tau},$$

where

$$\tau = \frac{k-2\Delta_5}{4k^2} = \frac{k-2\frac{1}{3}k}{4k^2} = \frac{1-2\frac{1}{3}}{4} \cdot \frac{1}{k}.$$

A modicum of computation shows that

$$\tfrac{1}{3} = 0.278464543\ldots$$

and

$$\frac{4}{1-2\frac{1}{3}} = 9.027900\ldots.$$

[One can apply a Newton iteration formula $\xi_{n+1} = -\frac{\xi_n \log \xi_n}{\xi_n + 1}$.].

The conclusion follows. //

Corollary. Suppose that α is algebraic and $k \geq 4$. Then one has

$$\min_{1 \leq n \leq N} \|\alpha n^4\| \ll N^{\varepsilon - \frac{1}{9.028k}}.$$

Proof. By Dirichlet's approximation theorem, there exist $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $|\alpha - a/q| \leq q^{-1} N^{-k/2}$ and $1 \leq q \leq N^{k/2}$. By a theorem of Roth (1955), given any algebraic number α, and $\varepsilon > 0$, there exists a positive number $C(\alpha, \varepsilon)$ with the property that

$$|\alpha - \frac{a}{q}| > \frac{C(\alpha,\varepsilon)}{q^{2+\varepsilon}}.$$

Thus, we may assume that

$$\frac{C(\alpha,\varepsilon)}{q^{2+\varepsilon}} < \frac{N^{-k/2}}{q},$$

Whence $q > (a(\varepsilon) N^{k/2})^{\frac{1}{1+\varepsilon}} > c' N^{\frac{k}{2} - \varepsilon}$, say. Thus, we may replace the inequality $N^{k/2} \le q \le (N+1)^{k/2}$ from the proof of Theorem 22.1 by the analogue $c' N^{k/2 - \varepsilon} \le q \le N^{k/2}$. This alteration generates at worst an additional factor of N^{ε} in the ensuing argument. Thus

$$\sum_{1 \le m \le M^{1+\varepsilon^2}} |T(\alpha m)| \ll M^{1+\varepsilon^2} N^{1+3\varepsilon-\tau},$$

where

$$\tau = \frac{k - 2\Delta_s}{4s^2},$$

and hence

$$\min_{1 \le n \le N} \|\alpha n^k\| \le N^{2\varepsilon - \tau(k)}.$$

The desired conclusion therefore follows as in the argument of the first corollary. //

---

§23. Sketch of an improvement to $G(k)$.

The sharpest bound currently available on $G(k)$ is:

Theorem 23.1 (Brüdern & W., 2022) For all $k \in \mathbb{N}$, one has

$$G(k) \le \lceil k(\log k + 4.20032) \rceil.$$

We now seek to outline a treatment that gives the bound

$$G(k) \le k \log k + O(k).$$

This improves on our earlier bound $G(k) \le k(\log k + \log\log k + O(1))$.

The set-up: Consider a large natural number n, put $P = n^{1/k}$, and consider representations of n in the shape

$$n = x_1^k + \dots + x_{4k}^k + y_1^k + \dots + y_{2s+t}^k ,$$

where s and t are positive numbers to be chosen in due course, and

$$1 \le x_i \le P \quad (1 \le i \le 4k), \qquad y_i \in \mathcal{A}(P, P^\eta),$$

with η sufficiently small in terms of k (and $\varepsilon > 0$).

Write

$$F(\alpha) = \sum_{1 \le x \le P} e(\alpha x^k) \quad \text{and} \quad f(\alpha) = \sum_{y \in \mathcal{A}(P, P^\eta)} e(\alpha y^k).$$

Then the number of representations of n in the above form is given by

$$r(n) = \int_0^1 F(\alpha)^{4k} f(\alpha)^{2s+t} e(-n\alpha)\, d\alpha .$$

We require a Hardy-Littlewood dissection, and here we proceed in some generality. When $1 \le Q \le P^{k/2}$, $q \in \mathbb{N}$ satisfies $1 \le q \le Q$, we define

$$\mathfrak{M}_q(Q, P) \text{ to be the union of the sets}$$

$$\mathfrak{M}_{q,a}(Q, P) = \{ \alpha \in [0,1) : |q\alpha - a| \le Q P^{-k} \},$$

with $0 \le a \le q$ and $(a, q) = 1$. We then put

$$\mathfrak{M}(Q, P) = \bigcup_{1 \le q \le Q} \mathfrak{M}_q(Q, P).$$

Then put

$$\mathfrak{N}(Q, P) = \mathfrak{M}(Q, P) \setminus \mathfrak{M}(Q/2, P).$$

One then has, by Dirichlet's approximation theorem, that for each $\alpha \in [0,1)$, there exist $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ with

$$0 \le a \le q \le P^{k/2}, \quad (a, q) = 1 \quad \text{and} \quad |q\alpha - a| \le P^{-k/2}.$$

Thus $\alpha \in \mathfrak{M}(P^{k/2}, P)$. In particular,

$$[0,1) = \bigcup_{j=0}^{L} \mathfrak{N}(2^{-j} P^{k/2}, P), \quad \text{where } L = \left\lfloor \frac{k \log P}{2 \log 2} \right\rfloor .$$

Thus

$$\int_0^1 |f(\alpha)|^{2s} d\alpha = \sum_{j=0}^{L} \int_{\mathfrak{N}(2^{-j}P^{k/2},P)} |f(\alpha)|^{2s} d\alpha$$

$$\ll (\log P) \max_{1 \le Q \le P^{k/2}} \int_{\mathfrak{N}(Q,P)} |f(\alpha)|^{2s} d\alpha .$$

Observation: Our sharpest minor arc estimate hitherto takes the shape

$$\sup_{\alpha \in \mathfrak{m}_\delta} \Big| \sum_{x \in \mathcal{C}(P)} e(\alpha x^k) \Big| \ll P^{1 - \frac{\delta + o(1)}{k \log k}} \qquad (0 < \delta < \tfrac{1}{2})$$

Here, one can identify $\mathfrak{m}_\delta$ as being contained in

$$\bigcup_{Q \ge P^\delta} \mathfrak{N}(Q,P).$$

But the argument of the proof of Theorem 22.1 shows that

$$f(\alpha) \ll P^{1+\varepsilon} \left(q^{-1} + P^{-\frac{1}{2}k} + qP^{-k} \right)^{\frac{1}{2u^2}},$$

when $\alpha \in \mathfrak{N}_q(Q,P)$, where $\tau = \dfrac{k - 2\Delta_u}{4u^2}$ with $u \asymp k$.

The point here is that when $q \approx P^{\frac{1}{2}k}$, this estimate is as strong as

$$f(\alpha) \ll P^{1 - \frac{1}{9.028k} + \varepsilon}$$

But this estimate, which saves a $\log k$ in the exponent, is only available when we are in this "extreme" region of the minor arcs.

The key observation:

Lemma 23.1. Let $F : \mathbb{R} \to \mathbb{C}$ be a 1 periodic integrable function. Suppose that $W \in \mathbb{N}$ satisfies the property that $1 \le Q \le \frac{1}{2}(P/W)^{k/2}$. Then whenever $(q, W) = 1$, one has

$$\int_{\mathfrak{M}_q(Q,P)} F(\alpha W^k)\, d\alpha = W^{-k} \int_{\mathfrak{M}_q(Q,P/W)} F(\beta)\, d\beta.$$

Proof. Let

$$I = [-q^{-1}QP^{-k}, q^{-1}QP^{-k}] \quad \text{and} \quad J = [-q^{-1}QW^kP^{-k}, q^{-1}QW^kP^{-k}].$$

The hypothesis $Q \le \frac{1}{2}(P/W)^{k/2}$ ensures that the arcs comprising $\mathfrak{M}_q(Q, P/W)$ are disjoint. Then (using periodicity), one sees that

$$\int_{\mathfrak{M}_q(Q,P/W)} F(\beta)\, d\beta = \sum_{\substack{b=1 \\ (b,q)=1}}^{q} \int_J F\left(\frac{b}{q} + \gamma\right) d\gamma$$

and

$$\int_{\mathfrak{M}_q(Q,P)} F(\alpha W^k)\, d\alpha = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_I F\left(\left(\frac{a}{q} + \beta\right) W^k\right) d\beta$$

$$= W^{-k} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_J F\left(\frac{aW^k}{q} + \gamma\right) d\gamma.$$

But since $(q, W) = 1$, the mapping $a \mapsto aW^k$ gives a bijection of reduced residues mod q to the same. Thus

$$\int_{\mathfrak{M}_q(Q,P)} F(\alpha W^k)\, d\alpha = W^{-k} \sum_{\substack{b=1 \\ (b,q)=1}}^{q} \int_J F\left(\frac{b}{q} + \gamma\right) d\gamma = \int_{\mathfrak{M}_q(Q,P/W)} F(\beta)\, d\beta.$$

Now define $\mathcal{C}_q(P,R) = \{n \in \mathcal{A}(P,R) : n \mid q^\infty\}$

$\mathcal{B}(M,\pi,R) = \{v \in \mathcal{A}(M\pi,R) : v > M,\ \pi \mid v \ \&\ \pi' \mid v \Rightarrow \pi' \ge \pi\}$.

We claim:

$$f(\alpha;P,R) = \underbrace{\sum_{\substack{v\in\mathcal{A}(P,R)\\ v>M\\ (v,q)=1}} \sum_{u\in\mathcal{C}_q(P/v,R)} e(\alpha(uv)^4)}_{f_q^*} + \underbrace{\sum_{\substack{v\in\mathcal{A}(M,R)\\ (v,q)=1}} \sum_{u\in\mathcal{C}_q(P/v,R)} e(\alpha(uv)^4)}_{f_q^\dagger}$$

and $$\int_{\mathfrak{M}_q(Q,P)} |f_q^\dagger(\alpha)|^{2s}\,d\alpha \ll \underbrace{QP^{-4}}_{\text{meas}(\mathfrak{M})}\cdot P^{\varepsilon}M^{2s}. \qquad (\text{small}).$$

So

$$\int_{\mathfrak{M}_q(Q,P)} |f(\alpha;P,R)|^{2s}\,d\alpha \ll \int_{\mathfrak{M}_q(Q,P)} |f^*(\alpha)|^{2s}\,d\alpha + O(QM^{2s}P^{\varepsilon-4})$$

"error".

$$\int_{\mathfrak{M}_q(Q,P)} |f^*(\alpha)|^{2s}\,d\alpha = \sum_{\pi\le R}\sum_{\substack{m\in\mathcal{B}(M,\pi,R)\\ (m,q)=1}} \cdot \underbrace{\sum_{\substack{w\in\mathcal{A}(P/m,\pi)\\ (w,q)=1}} \sum_{u\in\mathcal{C}_q(P/mw),R)} e(\alpha m^k(wu)^4)}_{g^*_{q,\pi}(\alpha m^4;P,m,R)}$$

Can focus on

$$M^{2s}\int_{\mathfrak{N}_q(Q,P)} |g^*_{q,\pi}(\alpha m^k;P,m,R)|^{2s}\,d\alpha = M^{2s}m^{-k}\int_{\mathfrak{N}_q(Q,P/m)} |g^*_{q,\pi}(\alpha;P,m,R)|^{2s}\,d\alpha.$$

Hölder.

Can think of this as essentially

$$T_q := m^{-k}\int_{\mathfrak{N}_q(Q,P/m)} |f(\alpha;P/m,R)|^{2s}\,d\alpha.$$

Choose $m \approx PQ^{-2/k}$, so that $P/m \approx Q^{2/k}$. Then

$$T_q = m^{-k}\int_{\mathfrak{N}_q(Q,Q^{2/k})} |f(\alpha;Q^{2/k},R)|^{2s}\,d\alpha.$$

$$\sum_q T_q \ll^{2s-k} \cdot \int_0^1 |f(\alpha; Q^{2/k}, R)|^{2s} d\alpha$$

$$\ll (PQ^{-2/k})^{2s-k} \cdot (Q^{2/k})^{2s-k+\Delta_{sk}+\varepsilon}$$

$$\ll P^{2s-k+\varepsilon} Q^{\frac{2\Delta_{sk}}{k}}.$$

Then

$$\int_{\mathfrak{N}(Q,P)} |f(\alpha; P, R)|^{2s} d\alpha \ll P^{2s-k+\varepsilon} Q^{\frac{2}{k}\Delta_s},$$

which provides non-trivial major arc estimates (and matches our previous bounds when $Q = P^{k/2}$).

Notice though that

$$\int_{\mathfrak{N}_q(Q, Q^{2/k})} |f(\alpha; Q^{2/k}, R)|^{2s} d\alpha$$

is an estimate over "extreme" minor arcs — we have

$$\alpha \in \mathfrak{N}_q(Q, Q^{2/k}) \Rightarrow \text{whenever } a \in \mathbb{Z} \text{ and } q \in \mathbb{N} \text{ satisfy}$$
$$|q\alpha - a| \le (Q^{2/k})^{-\frac{k}{2}}, \text{ then } q > Q = (Q^{2/k})^{\frac{k}{2}}.$$

Thus $$\sup_{\alpha \in \mathfrak{N}_q(Q, Q^{2/k})} |f(\alpha; Q^{2/k}, R)| \ll (Q^{2/k})^{1 - \frac{1}{9.1k}}.$$

So we can apply this estimate more or less as a substitute for Weyl's inequality, yielding

$$\int_{\mathfrak{N}(Q,P)} |f(\alpha; P, R)|^{2s+t} d\alpha \ll P^{2s-k+\varepsilon} \cdot P^t \cdot Q^{\frac{2}{k}\Delta_s - \frac{t}{9.1k}}.$$

Using $\Delta_s \le ke^{1-2s/k}$, we find that by taking $s = \frac{1}{2}k(\log k + 1)$, we have $\Delta_s \le k/e$, and putting $t = 20k$ shows that

$$\int_{\mathfrak{n}(Q,P)} |f(\alpha;P,R)|^{2s+t}\,d\alpha \ll P^{2s+t-k+\varepsilon}Q^{-1}.$$

This is enough to obtain a minor arc bound smaller than the anticipated major arc bound. But

$$\int_{\mathfrak{M}} F(\alpha)^{4k} f(\alpha)^{2s+t} e(-n\alpha)\,d\alpha \gg n^{\frac{2s+t}{k}+3},$$

using the $4k$ complete Weyl sums. Thus

$$r(n) \gg n^{\frac{2s+t}{k}+3} \to \infty \quad \text{as } n \to \infty,$$

whence

$$G(k) \le 2s+t+4k = k(\log k + O(1)).$$