the singular terms

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\bar{S}_{a,q}\right)^s e(-Na/q) \; ; \; \bar{S}_{a,q} = \frac{1}{q} \sum_{r=1}^{q} e\left(\frac{r^k a}{q}\right) \tag{7.1}$$

Note $\mathfrak{S}(N)$ will be closely related to

$$r_q(N) = \left\{(x_1, \dots, x_s) \in (\mathbb{Z}/q\mathbb{Z})^s \; ; \; x_1^k + \dots + x_s^k \equiv N \pmod q\right\}$$

for all $q \in \mathbb{N}$.

Write $\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q)$; $A(q) = \sum_{(a,q)=1} \left(q^{-1} S_{a,q}\right)^s e\left(-\frac{aN}{q}\right)$

Lemm 7.1. If $(q_1, q_2) = 1$, then $A(q_1 q_2) = A(q_1) A(q_2)$.

Pf Let $f(a,q) = \left(S_{a,q}\right)^s e(-aN/q)$. First we prove that if

$$\frac{a}{q} \equiv \frac{a_1}{q_1} + \frac{a_2}{q_2} \pmod 1 \quad \text{with } (a_1, q_1) = (a_2, q_2) = 1$$

$$\Leftrightarrow \; a \equiv a_1 q_2 + a_2 q_1 \pmod{q_1 q_2}$$

$$\Leftrightarrow \; a \equiv a_1 q_2 \; (q_1) \;\&\; a \equiv a_2 q_1 \; (q_2).$$

and $q = q_1 q_2$

then $f(a,q) = f(a_1, q_1) f(a_2, q_2)$. (7.2)

Using the Chinese Rem. Thm $\frac{a}{q}$ is in 1-1 correspondence with pairs $\left(\frac{a_1}{q_1}, \frac{a_2}{q_2}\right)$

(why?)

$q \equiv a_1 q_2 + a_2 q_1 \quad (q_1, q_2)$

$a \equiv$

Again $\forall\, x \pmod q \quad \exists!\ x_1 \pmod{q_1},\ x_2 \pmod{q_2}$

$\forall\, 1 \le x \le q \quad \exists!\ 1 \le x_1 \le q_1,\ 1 \le x_2 \le q_2$ s.t.

$$\frac{x}{q} \equiv \frac{x_1}{q_1} + \frac{x_2}{q_2} \pmod 1 \iff x \equiv q_2 x_1 + q_1 x_2 \pmod{q_1 q_2}$$

Then $$S_{a,q} = \sum_{x=1}^{q} e\left(\frac{a}{q} x^k\right) = \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e\left(\frac{a}{q}(q_2 x_1 + q_1 x_2)^k\right)$$

$$= \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e\left(\frac{a}{q}\left(q_2^k x_1^k + q_1^k x_2^k\right)\right) =$$

$$= \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e\left(\frac{a_1}{q_1}\underbrace{(q_2 x_1)^k}_{y_1}\right) e\left(\frac{a_2}{q_2}\underbrace{(q_1 x_2)^k}_{y_2}\right) = S_{a_1,q_1} \cdot S_{a_2,q_2}$$

$$\Rightarrow f(a,q) = f(a_1,q_1)\cdot f(a_2,q_2) \quad \text{as} \quad e\left(-\frac{a}{q}N\right) = e\left(-\frac{q_1}{q_1}N\right) e\left(-\frac{a_2}{q_2}N\right)$$

Then $$A(q) = \sum_{(a,q)=1} f(a,q) = \sum_{(a_1,q_1)=1} \sum_{(a_2,q_2)=1} f(a_1,q_1)\, f(a_2,q_2) \Rightarrow$$

$$A(q) = A(q_1)\, A(q_2)$$

Let $S \ge 2^k + 1$. □

Lemma 7.2. For p prime, Let $\chi(p) := 1 + \sum_{r=1}^{\infty} A(p^r)$.

Then

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

ii) $\sigma(N) = \prod_p \chi(p)$

Pf We had that $\frac{1}{q}|S(a,q)| \ll q^{-\frac{s}{2^{k-1}}} \leq q^{-2-\delta}$

thus $\chi(p)-1 \ll \sum_{r=1}^{\infty} p^{-(2-\delta)r} \ll p^{-2-\delta}$

$\Rightarrow \prod_{p \in \mathbb{P}} \chi(p)$ converges absolutely.

Since for $n = p_1^{r_1} \cdots p_m^{r_m}$, we have that $A(n) = A(p_1^{r_1}) \cdots A(p_m^{r_m})$,

it follows $\prod_{p} \left(1 + \sum_{r=1}^{\infty} A(p^r)\right) = \sum_{q=1}^{\infty} A(q)$ □

Lemma 7.3. Let $M(q) = \#\{(x_1, \dots, x_s) \in (\mathbb{Z}/q\mathbb{Z})^s : x_1^k + \cdots + x_s^k \equiv N \pmod q\}$

We have $1 + \sum_{r=1}^{n} A(p^r) = M(p^n)/p^{n(s-1)}$

thus $\chi(p) = \lim_{n\to\infty} M(p^n)/p^{n(s-1)}$

Pf We prove, more generally, that

$$q^{-(s-1)} M(q) = \sum_{q_1 \mid q} A(q_1)$$

$$M(q) = \frac{1}{q} \sum_{x_1, \dots, x_s \in \mathbb{Z}/q\mathbb{Z}} \sum_{b \in \mathbb{Z}/q\mathbb{Z}} e\left(\frac{x_1^k + \cdots + x_s^k - N}{q} b\right)$$

To any $1 \leq b \leq q$ $\exists!$ $q_1 \mid q$ and $1 \leq a_1 \leq q_1$, $(a_1, q_1) = 1$

such that $\frac{b}{q} = \frac{a_1}{q_1}$ (i.e. $\frac{a_1}{q_1}$ is the reduced form of th fraction $\frac{b}{q}$).

Thus

$$M(q) = \frac{1}{q} \sum_{q_1 | q} \sum_{(a_1,q_1)=1} \sum_{\substack{x_1,\dots x_s \\ (\mathrm{mod}\, q)}} e\left(\frac{a_1}{q_1}(x_1^k + \dots + x_s^k)\right) e\left(-\frac{a_1}{q_1} N\right)$$

$$= \frac{1}{q} \sum_{q_1 | q} \sum_{(a_1,q_1)=1} \left(\sum_{x \,(\mathrm{mod}\, q)} e\left(\frac{a_1}{q_1} x^k\right)^s e\left(-\frac{a_1}{q_1} N\right)\right.$$

Note, that

$$\sum_{x \,(\mathrm{mod}\, q)} e\left(\frac{a_1}{q_1} x^k\right) = \frac{q}{q_1} \sum_{x \,(\mathrm{mod}\, q_1)} e\left(\frac{a_1}{q_1} x^k\right) = \frac{q}{q_1} S(a_1, q_1)$$

$$M(q) = q^{s-1} \sum_{q_1 | q} \sum_{(a_1,q_1)=1} \left(\frac{1}{q_1} S(a_1, q_1)\right)^s e\left(-\frac{a_1}{q_1} N\right)$$

$$= q^{s-1} \sum_{q_1 | q} A(q_1)$$

□

Note • We expect that $\#\{(x_1,\dots x_s) \in (\mathbb{Z}/q\mathbb{Z})^s ;\ x_1^k + \dots + x_s^k \equiv N \ (q)\}$

$\approx q^{s-1}$ ($x_1^k + \dots + x_s^k$ can take q possibly different values)

thus $q^{-(s-1)} M(q)$ is the density of solutions $(\mathrm{mod}\, q)$.

and $\chi(p)$ is the limit of density of solutions $(\mathrm{mod}\, p^n)$ as $n \longrightarrow \infty$.

- Since $\sum_p |\chi(p)-1| < \infty$, it follows that

$$G(N) = \prod_p \chi(p) \neq 0 \iff \forall p \ \chi(p) \neq 0.$$

- We will show if we have a solution to

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma}$$

s.t. $x_i \not\equiv 0 \pmod p$ for some $1 \le i \le s$, then $\chi(p) > 0$.

- We need to carefully consider the quantity

$$\gamma = \begin{cases} \tau+1, & p^\tau \| k, \text{ for } p>2 \\ \tau+2; & 2^\tau \| k \text{ for } p=2 \end{cases}$$

$\phi(21) = \phi(5^2) = 5(5-1)$

$g^2 \equiv 1 \ (5) \quad (5-1)$

(25)

$\log g$

Lemma (Lifting) Given $m \not\equiv 0 \pmod p$.

If $\exists y : y^k \equiv m \pmod{p^\gamma}$ then $\forall \nu > \gamma \ \exists x : x^k \equiv m \ (p^\nu)$

Pf Let $\nu > \gamma$.

$\phi : \mathbb{Z}_{p^\nu}^* \to \mathbb{Z}_{p^\gamma}^*$ onto

$g \longrightarrow \phi(g)$

- $p>2$. Let $\mathbb{Z}_{p^\nu}^* :=$ reduced residue classes $\pmod{p^\nu}$ with "$\cdot$" (multiplication)

We use the fact that $\mathbb{Z}_{p^\nu}^*$ is cyclic, i.e. $\exists g$ s.t. $\mathbb{Z}_{p^\nu}^* = \{ g^a ; \ 1 \le a \le \phi(p^\nu) = p^{\nu-1}(p-1) \}$

i.e. g is a primitive root $\pmod{p^\nu}$

Then g is also a primitive root $\pmod{p^\gamma}$ (why?)

$\phi : \mathbb{Z}_{p^\nu}^* \to \mathbb{Z}_{p^\gamma}^*$, $x \mapsto x \pmod{p^\gamma}$

$1, g, g^2, \ldots, g^{p^{\gamma-1}(p-1)}$ all distinct $\pmod{p^\nu} \Rightarrow 1, g, g^2, \ldots, g^{p^{\gamma-1}(p-1)}$ must be distinct $\pmod{p^\gamma}$

write $y \equiv g^a \pmod{p^\nu}$, $m \equiv g^b \pmod{p^\nu} \Rightarrow g^{ak} \equiv g^b \pmod{p^\nu}$

$\Leftrightarrow ak \equiv b \pmod{p^{\nu-1}(p-1)}$

$\Leftrightarrow p^{\nu-1} ak_0 \equiv b \pmod{p^{\nu-1}(p-1)}$ as $k = p^{\nu-1}k_0$

$\Rightarrow p^{\nu-1} \mid b$ and $(k_0, p-1) \mid b \Rightarrow (k, p^{\nu-1}(p-1)) \mid b$

(as $ak_0 \equiv b \pmod{p-1}$) $\quad = p^{\nu-1}(k_0, p-1) = d$

$ak \equiv b \pmod{p^{\nu-1}(p-1)} \Rightarrow \exists\, c$ s.t. $ck \equiv b \pmod{p^{\nu-1}(p-1)}$

$ck \equiv b \pmod{p^{\nu-1}(p-1)}$ $\quad b/c$ $\quad c\frac{k}{d} \equiv \frac{b}{d} \pmod{\frac{q}{d}}$, $q = p^{\nu-1}(p-1)$

$(= ck \equiv ak \pmod{p^{\nu-1}(p-1)})$

$ck_0 \equiv ak_0 \pmod{p-1}$

$ck' \equiv b' \pmod{q'}$

can be always solved as $(k', q') = 1$.

So $c \equiv (k')^{-1} b' \pmod{q'}$

but $ck \equiv b \pmod{p^{\nu-1}(p-1)} \Rightarrow g^{ck} \equiv g^b \equiv m \pmod{p^\nu}$.

- $p = 2$. If k is odd then $x^k \equiv m \pmod{2^\nu}$ can always be solved for $m \not\equiv 0 \pmod 2$ (i.e. m odd)

$g^{ak} \equiv g^b \pmod{2^\nu}$ (why?)

$\Leftrightarrow ak \equiv b \pmod{2^{\nu-1}}$ solvable as $(k, 2) = 1$.

Let $k = 2^\tau k_0$ $(\tau \geq 1)$. Then $x^k \equiv 1 \pmod 4$ for x odd.

Let $G_{2^\nu} = \{x \pmod{2^\nu},\ x \equiv 1 \pmod 4\}$, $|G_{2^\nu}| = 2^{\nu-2}$

We use the fact that $G_{2^\nu} = \{5^a \pmod{2^\nu};\ a \in \mathbb{N}\}$

Let $y \equiv 5^a \pmod{2^\nu}$, $m \equiv 5^b \pmod{2^\nu} \Rightarrow ak \equiv b \pmod{2^{\nu-2}}$

Since $k = 2^\tau k_0 = 2^{\gamma-2} k_0 \Rightarrow 2^{\gamma-2} \mid b = a_1 k_0$

$\Rightarrow \exists c$ s.t. $kc \equiv b \pmod{2^{\gamma-2}}$

as $(k, 2^{\gamma-2}) = 2^{\gamma-2}$

□

Lemma 7.5. Let γ be as before. If

$$X_1^k + \cdots + X_s^k \equiv N \pmod{p^\gamma}$$

has a solution $x_1, \ldots, x_s$ s.t. $p \nmid x_i$ for some i, then $\chi(p) > 0$.

Pf Suppose $a_1^k + \cdots + a_s^k \equiv N \pmod{p^\gamma}$ with $a_1 \not\equiv 0 \pmod{p}$

Construct solutions to $X_1^k + \cdots + X_s^k \equiv N \pmod{p^\nu}$ $(\nu > k)$

as follows.

Choose $X_2, \ldots, X_s \pmod{p^\nu}$ arbitrarily, subject to $X_j \equiv a_j \pmod{p^\gamma}$

Then for $m := N - X_2^k + \cdots + X_s^k$ we have

that $a_1^k \equiv m \pmod{p^\gamma}$, thus by Lemma 7.4.

$\exists X_1 \; ; \; X_1^k \equiv m \pmod{p^\nu} \Rightarrow X_1^k + \cdots + X_s^k \equiv N \pmod{p^\nu}$

This way we construct at least $p^{(\nu-\gamma)(s-1)}$ solutions

thus $p^{-\nu(s-1)} M(p^\nu) \geq p^{-\nu(s-1)} p^{(\nu-\gamma)(s-1)} = p^{-\gamma(s-1)}$ $\forall \nu$

$\Rightarrow \chi(p) \geq p^{-\gamma(s-1)} > 0$

■