数理解析研究所講究録
294巻 1977年 145-180

On the Weber theorem and some consequent problems

東京水産大　竜沢周雄

§1. Introduction

有理数体 $\mathbb{Q}$ 上に n 次の代数体 F があってその判別式を d とする。$F^{(l)}$ $(1 \leqq l \leqq r_1)$ は r_1 ケの実共役，$F^{(m)}$，$F^{(m+r_2)}$ $(r_1+1 \leqq m \leqq r_1+r_2)$ は r_2 対の複素共役，したがって $n = r_1 + 2r_2$ とする。F の整イデアル $\mathfrak{m}$，$F^{(i)}$ に対応する無限素点 $\mathfrak{p}_\infty^{(i)}$ との形式的積であるイデアルモドル $\tilde{\mathfrak{m}} = \mathfrak{m}\mathfrak{p}_\infty^{(1)} \cdots \mathfrak{p}_\infty^{(q)}$ $(q=0 \text{ or } 1 \leqq q \leqq r_1)$ を作る。$\mathfrak{m}$ と素な F のイデアルの作る乗法群を $A(\tilde{\mathfrak{m}})$，

$$\alpha \equiv 1 \mod \tilde{\mathfrak{m}}, \quad (\alpha, \mathfrak{m}) = \mathfrak{o}$$

なる α から単項イデアル (α) を作り，その全体のなす $A(\tilde{\mathfrak{m}})$ の部分群を $S(\tilde{\mathfrak{m}})$ と書く。$A(\tilde{\mathfrak{m}})/S(\tilde{\mathfrak{m}})$ の coset C を mod $\tilde{\mathfrak{m}}$ の residue class とよぶことにしすべての類の個数を $h(\tilde{\mathfrak{m}})$ で表わす。そのとき次の定理が成立つ。

Theorem 1. We denote by $T(x, C)$ the number of integral ideals $\mathfrak{a}$, prime to $\mathfrak{m}$, satisfying

$$N\mathfrak{a} \leqq x, \quad \mathfrak{a} \in C.$$

Let R be the regulator of F, h_0 be the absolute class number of F and w be the number of roots of unity in F. If we set

$$\lambda = \frac{2^{r_1}(2\pi)^{r_2}|R|h_0}{\sqrt{|d|}\ w},$$

then

$$T(x, C) = \frac{1}{h(\tilde{\mathfrak{m}})} \prod_{\mathfrak{p}|\mathfrak{m}} \left(1 - \frac{1}{N\mathfrak{p}}\right) \lambda x +$$

$$O\left\{\frac{1}{h(\tilde{\mathfrak{m}})} \prod_{\mathfrak{p}|\mathfrak{m}} \left(1 - \frac{1}{N\mathfrak{p}}\right) N\mathfrak{m}^{\frac{1}{n}} x^{1-\frac{1}{n}}\right\} + O\left\{\frac{N(\mathfrak{m})}{h(\tilde{\mathfrak{m}})}\right\}.$$

このことについて以前［6］に発表した筆者の論文には間違いがありMarburg大学のHinz氏より注意をいただいたので，最近同じ雑誌で訂正をした。これがWeberの定理で高木類体論の礎石となったものである。

これに関連して次のような問題も生じよう。

(i) $T(x; q, l)$ の評価：それは

$$N\mathfrak{a} \leqq x, \quad N\mathfrak{a} \equiv l \mod q$$

をみたす正整数 q と素な整イデアルの個数。

(ii) $\Pi(x; q, l)$ の評価：それは

$$N\mathfrak{p} \leq x, \quad N\mathfrak{p} \equiv l \mod q$$

をみたす正整数qと素な素イデヤルの個数

それらの計算ができたら，その種々なる応用を考えることである。筆者の頭にうかんだのは，十分大きな正整数Nを与えて，Fの素イデヤル$\mathfrak{p}_i$によるDiophantine equation

$$N\mathfrak{p}_1^{k} + N\mathfrak{p}_2^{k} + \cdots\cdots + N\mathfrak{p}_s^{k} = N \qquad (1)$$

の解の個数を考えることである。勿論k, sは与えられた自然数である。この問題は$k=1$, $\mathfrak{p}$は単項なる素イデヤルとして始めて三井君[4],[5]によって考案された問題である。

こゝでnorm residueということについて説明しておく。$(q, l)=1$としqと素な整イデヤル$\mathfrak{a}$を適当にとって

$$N\mathfrak{a} \equiv l \mod q$$

となることがあればlを$\mod q$のnorm residueとよぶことにする。$\mod q$に関するnorm residueの全体Nは既約類全体のつくる群の部分群となるので，Nをnorm residue class group $\mod q$とよぶことにする。類体論の推進定理を使うならば

<u>Theorem 2.</u> Let ζ be a primitive q th root of unity. Then

$$\text{the order of } N = [Q(\zeta) : Q(\zeta) \cap F]$$

Minkowski の定理によれば

<u>Theorem 3.</u> If $(q, |d|) = 1$, then N is equal to the whole reduced residue class group mod q.

講演当時筆者は(1)の問題が解決できると思っていたのであるが，それは次の事が成立つと思っていたからである。

<u>Hopeless Conjecture</u>: Let N_1, N_2 and N be norm residue class groups mod q_1, q_2 an q respectively. If $q = q_1 q_2$ and $(q_1, q_2) = 1$, then

(the order of N_1) × (the order of N_2) = (the order of N)

この問題は多分代数的整数論の問題として先人がさんざん苦杯を飲まされたところだと思う。これを避ければやはり三井君の線にまで問題を下げねばならず，あらためて同君に敬意を表せざるをえない。また非常に興味深い問題なので将来は同君と共著の形でまとめたいと思っている。以下の論説でも重要なところは同君の蕩着想を拝借したところが多い。

§2 On $A_S(N, q)$

A を q と素な F の ideal 全体の作る乗法群, $S=\{(\alpha);\ \alpha\equiv 1 \bmod \tilde{q}\}$, たゞし $\tilde{q}=q\,\mathfrak{p}_\infty^{(1)}\cdots\mathfrak{p}_\infty^{(r_1)}$。したがって $\alpha\equiv 1 \bmod \tilde{q}$ は乗法合同で $\alpha\equiv 1 \bmod q$ そして α が總正という意味になる。$\bmod \tilde{q}$ の完全剰余代表系を $\alpha_1,\cdots,\alpha_l$, それから單項イデヤル (α_j) を作ると例えば u 個ずつ等しいものができ, イデヤルとして異るものは $(\alpha_1),\cdots,(\alpha_m)$ であったとする。F の絶対イデヤル類から q と素な代表系をとって $\mathfrak{a}_1,\cdots,\mathfrak{a}_{h_0}$ とすれば A/S の完全代表系は

$$\mathfrak{a}_i(\alpha_j),\quad i=1,\cdots,h_0;\ j=1,\cdots,m$$

となる。Hasse 流に指数関係を示すと

$$(A:S)=(\mathfrak{a}:(\alpha))((\alpha):(\nu))=(\mathfrak{a}:(\alpha))\frac{(\alpha:\nu)}{(\varepsilon:\eta)}$$
$$=h\frac{l}{u}=hm。$$

こゝで ε は單数群, η は總正な單数群, ν は $\nu\equiv 1 \bmod \tilde{q}$ なる ν のつくる群。

(α_j) $(1\leqq j\leqq m)$ から $N((\alpha_j))$ (略して $N(\alpha_j)$ とかく) を作ると m/r 個ずつ $\bmod q$ で合同となり異なるものが丁度 r 個できたとする。In what follows, we shall denote by N the residue class group mod q

formed by norms of principal ideals in F, and by $r=r(q)$ the number of N.

<u>Theorem 4.</u> If $q=q_1q_2$ and $(q_1,q_2)=1$, then

$$r(q)=r(q_1)r(q_2)。$$

Proof。 mod q_1, mod q_2 の単項イデヤルの norm による residue class group を

$$N_1=\{b_1,\cdots,b_{r_1} \bmod q_1\},\quad N_2=\{c_1,\cdots,c_{r_2} \bmod q_2\}$$

とする。 $N(\alpha)\equiv l \bmod q$ となったとすれば

$$l\equiv b_i \bmod q_1,\quad l\equiv c_j \bmod q_2$$

となる b_i, c_j がある。 そこで

$$q_1x_1\equiv 1 \bmod q_2,\quad q_2x_2\equiv 1 \bmod q_1$$

となる x_1, x_2 を定めると

$$l\equiv b_i(q_2x_2)^n+c_j(q_1x_1)^n \bmod q.$$

となる。

逆に $N(\beta)\equiv b_i \bmod q_1$, $N(\gamma)\equiv c_j \bmod q_2$ であるとき, $\beta\equiv\tilde{\beta} \bmod q_1$, $\gamma\equiv\tilde{\gamma} \bmod q_2$ そして $\tilde{\beta}$, $\tilde{\gamma}$ は總正である $\tilde{\beta}$, $\tilde{\gamma}$ を作って

$$\alpha=\tilde{\beta}q_2x_2+\tilde{\gamma}q_1x_1$$

とおけば

$$N(\alpha)=N(\tilde{\beta}q_2x_2+\tilde{\gamma}q_1x_1)$$

$$\equiv N(\tilde{\beta})(q_2x_2)^n+N(\tilde{\gamma})(q_1x_1)^n\equiv b_i(q_2x_2)^n+c_j(q_1x_1)^n \bmod q$$

また mod q で $r_1 r_2$ ケの数

$$b_i (q_2 x_2)^n + c_j (q_1 x_1)^n$$

は互に不合同であるから

$$r(q) = r(q_1)\, r(q_2) \qquad \text{q.e.d.}$$

こゝで

$$A_s(N, q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e^{-2\pi i \frac{a}{q} N} \frac{1}{r^s} B\left(\frac{a}{q}\right)^s$$

と定義する。たゞし，$b_1, \cdots, b_r$ を単項イデヤルの norm による mod q の residue class 全体として

$$B\left(\frac{a}{q}\right) = \sum_{j=1}^{r} e^{2\pi i \frac{a}{q} b_j^k} \qquad (2)$$

とおく。

Theorem 5。 If $q = q_1 q_2$ and $(q_1, q_2) = 1$, then

$$A_s(N, q) = A_s(N, q_1)\, A_s(N, q_2)$$

Proof。 始めに (2) より

$$B\left(\frac{a}{q}\right) = B\left(\frac{a q_2^{nk-1}}{q_1}\right) B\left(\frac{a q_1^{nk-1}}{q_2}\right), \quad B\left(\frac{a_1}{q_1}\right) B\left(\frac{a_2}{q_2}\right) = B\left(\frac{a_1}{q_1} + \frac{a_2}{q_2}\right)$$

を導けば，自然と

$$A_s(N, q_1)\, A_s(N, q_2) = A_s(N, q_1 q_2)$$

が証明される。

後の計算に必要になつてくるから $A_s(N, q)$ の大きさ

について概略の評価をしておこう。準備として χ を mod q の character とし

$$\tau(\chi)=\sum_{m=1}^{q}\chi(m)e^{2\pi i\frac{a}{q}m}$$

とおく。

<u>Theorem 6.</u> $|\tau(\chi)|\leqq\sqrt{q}$

Proof. (Karacuba [2])

$$|\tau(\chi)|^2=\frac{1}{\varphi(q)}\sum_{\substack{l=1\\(l,q)=1}}^{q}\Big|\sum_{m=1}^{q}\chi(lm)e^{2\pi i\frac{a}{q}lm}\Big|^2$$

$$=\frac{1}{\varphi(q)}\sum_{\substack{l=1\\(l,q)=1}}^{q}\Big|\sum_{m=1}^{q}\chi(m)e^{2\pi i\frac{a}{q}lm}\Big|^2$$

$$\leqq\frac{1}{\varphi(q)}\sum_{\substack{m=1\\(m,q)=1,}}^{q}\sum_{\substack{m_1=1\\(m_1,q)=1}}^{q}\sum_{l=1}^{q}\chi(m)\overline{\chi}(m_1)e^{2\pi i\frac{a}{q}l(m-m_1)}$$

$$=\frac{1}{\varphi(q)}\sum_{\substack{m=1\\m\equiv m_1 \bmod q}}^{q}\sum_{m_1=1}^{q}\chi(m)\overline{\chi}(m_1)q=q \qquad \text{q.e.d.}$$

mod q の既約類群を G, 単項イデヤルの norm による mod q の residue class group を N とすれば

$$q=p^l,\ p=\text{odd prime},\ (p,|d|)=1$$

という特別の場合について

$$(G:N)=\frac{\varphi(q)}{r},\quad \text{the order of } N^k=\frac{r}{(r,k)}$$

したがって $(G:N^k)=\varphi(q)\frac{(r,k)}{r}$ それを便宜上 s とおく。N^k の元を 1 とする G の character は s 個ある

からそれらを

$$\chi_1, \cdots\cdots, \chi_s$$

とする。そのとき

$$\tau(\chi_1)+\cdots+\tau(\chi_s)=\frac{s}{(r,k)}\sum_{j=1}^{r}e^{2\pi i\frac{a}{q}b_j^k}$$

定理6により

$$|B(\tfrac{a}{q})|=|\sum_{j=1}^{r}e^{2\pi i\frac{a}{q}b_j^k}|\leqq(r,k)\sqrt{q}\leqq kp^{\frac{l}{2}}$$

したがって

$$|A_s(N,p^l)|\leqq\frac{\varphi(q)}{r^s}(kp^{\frac{l}{2}})^s$$

しかるに $N\supseteqq\{a^n \bmod q,\ (a,q)=1\}$ であるから

$$r=\#N\geqq\frac{\varphi(q)}{(\varphi(q),n)}\geqq\frac{\varphi(q)}{n}$$

よって、 $$|A_s(N,p^l)|\leqq n^s\frac{(kp^{\frac{l}{2}})^s}{\varphi(p^l)^{s-1}}$$

これより

<u>Theorem 7.</u> If q has odd prime factors, the number of which being t, and $(q,|d|)=1$, then

$$|A_s(N,q)|\leqq(nk)^{ts}\frac{q^{\frac{s}{2}}}{\varphi(q)^{s-1}}$$

したがって、$s>4$ ならば

$$\sum_{q=1}^{\infty}A_s(N,q)$$

が絶対収束することがわかり，それを $\mathfrak{S}(N)$ とおき

$$\chi_p(N) = \sum_{l=1}^{\infty} A_s(N, p^l) \tag{3}$$

と定義すれば定理5より

$$\mathfrak{S}(N) = \prod_p \chi_p(N)$$

が証明される。後に (3) は有限項できれ，s が適当に大きくなってくれば $\chi_p(N)$ も $\mathfrak{S}(N)$ も 0 とならないことが証明される。勿論細かな条件も必要になってくるが，こゝでは

$$s \geqq 12, \quad p \geqq (2nk)^6, \quad p \nmid |d|$$

ならば

$$|\chi(p)| \geqq 1 - \frac{1}{p^2} \tag{4}$$

となることを注意しておこう。定理7により

$$\sum_{l=1}^{\infty} |A_s(N, p^l)| \leqq (nk)^s \sum_{l=1}^{\infty} \frac{p^{\frac{ls}{2}}}{(p^{l-1}(p-1))^{s-1}}$$

$$\leqq (2nk)^s \sum_{l=1}^{\infty} \frac{1}{p^{l(\frac{s}{2}-1)}} \leqq \left(\frac{2nk}{p^{\frac{1}{6}}}\right)^s \frac{1}{p^{\frac{s}{6}}}。$$

なお前述の N について

$$N^k \geqq \{a^{nk} \bmod q, \ (a, q) = 1\}$$

から

$$\text{The order of } N^k = \# N^k \geqq \frac{\varphi(q)}{(\varphi(q), nk)} \tag{5}$$

を注意しておく。p が奇素数で $q = p^l$ ならば $\bmod q$ の既約類群は巡回群となるからである。

§3. Local theory。

Fの整数環を$\mathfrak{o}$とし

$$\mathfrak{d}^{-1} = \{\alpha' ;\ \mathrm{Trace}(\alpha\alpha') = \text{有理整数},\ \text{for all } \alpha \in \mathfrak{o}\}$$

によってFの different $\mathfrak{d}$ を定義する。

<u>Theorem 8</u>。 Let $\mathfrak{a}$ be an integral ideal in F, $s = N\mathfrak{a}$ and $\alpha_1, \cdots, \alpha_s$ be a set of complete residue class representatives mod $\mathfrak{a}$. If we take a number ρ in F satisfying $\rho = (\mathfrak{a}\mathfrak{d})^{-1}\mathfrak{b}$, $(\mathfrak{b}, \mathfrak{a}) = \mathfrak{o}$, then

$$\sum_{j=1}^{s} e^{2\pi i\, \mathrm{trace}(\rho\alpha_j\alpha)} = \begin{cases} N\mathfrak{a} & \alpha \in \mathfrak{o} \\ 0 & \alpha \notin \mathfrak{o} \end{cases}$$

<u>Theorem 9</u>. Assume that $p^{\theta} \parallel k$, $p^{d_p} \parallel \mathfrak{d}$ (which means, for example, $p^{\theta} \mid k$, $p^{\theta+1} \nmid k$)。 If $t_1, \cdots, t_r$ are the residue classes mod q formed by norms of principal ideals of F and $q = p^m$,

$$m \geqq 2d_p + 2\theta + 2,$$

then

$$\sum_{j=1}^{r} e^{2\pi i \frac{a}{p^m} t_j^{k}} = 0 \qquad (a, p) = 1.$$

それが証明されれば (3) において

$$\chi_p(N) = \sum_{l=1}^{2d_p+2\theta+1} A_s(N, p^l). \tag{6}$$

となる。また定理9を証明するには mod $\tilde{q}$ の完全剰余系を $\alpha_1, \cdots, \alpha_l$ とし

$$\sum_{j=1}^{l} e^{2\pi i \frac{a}{p^m} N(\alpha_j)} = 0 \qquad (a, p)=1.$$

を証明すればよい。それについては三井[4]によるすぐれた研究がある。

素イデヤルに関するSiegel-Walfiszの定理は三井[4]によつて得られている。それより次の定理も容易にえられる。

<u>Theorem 10.</u> Let $x \geqq e^{q^{\varepsilon}}$ (ε is an arbitrary positive number). We denote by $\pi(x; q, l)$ the number of prime ideals in F satisfying

$\mathfrak{p}=(\alpha)$ principal ideal, $N\mathfrak{p} \leqq x$, $N\mathfrak{p} \equiv l \bmod q$,

l belonging to the residue class formed by norms of principal ideals in F with respect mod q. Then

$$\pi(x; q, l) = \frac{1}{h_0 r} \int_2^x \frac{du}{\log u} + O\left(\frac{1}{h_0 r} x e^{-c\sqrt{\log x}}\right).$$

The result is also true when we restrict $\mathfrak{p}$ is of degree one, namely $N\mathfrak{p} = p$ (prime).

なぜなら $N\mathfrak{p} = p^f \leqq x$ $(f>1)$ となる$\mathfrak{p}$の個数は

$$O(n\sqrt{x}) + O(n\sqrt[3]{x}) + \cdots\cdots = O(n\sqrt{x}\log x)$$

に過ぎないから。

さて $\mathfrak{p}_i$ $(i=1, \cdots, s)$ を一次のそして單項なる

素イデアルとし, $N\mathfrak{p}_i^k \leqq x$ を動くものとする。そのとき

$$N\mathfrak{p}_1^k + \cdots\cdots + N\mathfrak{p}_s^k \equiv N \mod q$$

の解の個数を $M(q, s, z, N)$ で表わせば

$$qM(q, s, z, N) = \sum_{\mathfrak{p}_1}\cdots\cdots\sum_{\mathfrak{p}_s}\sum_{a=1}^{q} e^{2\pi i \frac{a}{q}(N\mathfrak{p}_1^k+\cdots+N\mathfrak{p}_s^k - N)}$$

$$= \sum_{a=1}^{q} e^{-2\pi i\frac{a}{q}N}\Big(\sum_{N\mathfrak{p}^k\leqq x} e^{2\pi i \frac{a}{q}N\mathfrak{p}^k}\Big)^s$$

$$= \sum_{q_1|q}\ \sum_{\substack{(a,q)=q_1\\ 1\leqq a\leqq q}} e^{-2\pi i\frac{a}{q}N}\Big(\sum_{N\mathfrak{p}^k\leqq x} e^{2\pi i \frac{a}{q}N\mathfrak{p}^k}\Big)^s$$

$$= \sum_{q_1|q}\ \sum_{\substack{a_1=1\\ (a_1,q_1)=1}}^{q_1} e^{-2\pi i \frac{a_1}{q_1}N}\Big(\sum_{N\mathfrak{p}^k\leqq x} e^{2\pi i\frac{a_1}{q_1}N\mathfrak{p}^k}\Big)^s$$

定理10を使って $x \geqq e^{q^{\varepsilon}}$ ならば

$$qM(q, s, z, N) = \sum_{q_1|q}\ \sum_{\substack{a_1=1\\ (a_1,q_1)=1}}^{q_1} e^{-2\pi i \frac{a_1}{q_1}N}\Big\{\frac{1}{h_0 r}\int_2^{x^{\frac{1}{k}}}\frac{du}{\log u}\times$$

$$\Big(e^{2\pi i\frac{a_1}{q_1}\epsilon_1^k}+\cdots+e^{2\pi i \frac{a_1}{q_1}\epsilon_r^k}\Big) + O\Big(\frac{1}{h_0}x^{\frac{1}{k}}e^{-c\sqrt{\log z}}\Big)\Big\}^s$$

$$=\Big(\sum_{q_1|q}A(q_1,N)\Big)\frac{1}{h_0^s}\Big(\int_2^{x^{\frac{1}{k}}}\frac{du}{\log u}\Big)^s + O\Big(x^{\frac{s}{k}}e^{-c_1\sqrt{\log z}}\Big) \qquad (7)$$

特に

$$s \equiv N \mod q \qquad (8)$$

なる関係がある場合は $N\mathfrak{p}_i \equiv 1 \mod q$ なる $\mathfrak{p}_i$ のみとって解がえられるから

$$M(q, s, z, N) \geqq \left(\frac{c}{h_0 r} \int_z^{z^{\frac{1}{k}}} \frac{du}{\log u} \right)^s \qquad 0<c<1$$

(7) より

$$\sum_{q_1|q} A(q_1, N) \geqq \frac{c^s}{r^s} q$$

$c \to 1$ とできるから

$$\sum_{q_1|q} A(q_1, N) \geqq \frac{q}{r^s} \geqq \frac{q}{\varphi(q)^s} \qquad (8).$$

(6) により

$$\lambda_p(N) \geqq \frac{p^l}{\varphi(p^l)^s} \quad \text{ただし } l = 2d_p + 2\theta + 1 \quad (9)$$

Theorem 11. (Chowla-Davenport) Assume that $x_1, \cdots, x_m$ and $y_1, \cdots, y_n$ belong respectively to m and to n distinct residue classes mod p^l, and that $y_i \not\equiv y_j$ mod p for $i \neq j$; then the number of distinct residue classes mod p^l represented by $x_u + y_v$ $(1 \leqq u \leqq m,\ 1 \leqq v \leqq n)$ is

$$\geqq \min(m+n-1, p^l)$$

Proof. Hua [1].

さて奇素数 p について

$$p \nmid |d|, \quad k = p^\theta k_0 \quad (k_0, p)=1, \qquad m = 2\theta + 1$$

と仮定する。 N を F の単項なる一次の素イデヤルの norm によって与えられる mod p^m の residue class

全体の作る群とする。§2に示したように

$$r = \# N \geqq \frac{\varphi(p^m)}{(\varphi(p^m),\ n)} \geqq \frac{\varphi(p^m)}{n}$$

かゝる norm residue が mod p では t ケの class を与めるとすれば

$$t \geqq \frac{p-1}{n}$$

また

$$N_{\mathfrak{f}}^{k} \equiv N_{\mathfrak{f}}^{k_0} \mod p$$

となるから，mod p で N^k と N^{k_0} とは同じで

$$d = \frac{t}{(t,\ k_0)}$$

だけの residue class を与めることになる。したがって定理11の結果は

$$\geqq \min\left(d + (d-1)(s-1),\ p^m\right) \qquad (10)$$

ということになる

(i) $t \nmid k_0$, $k_0 \mid t$ の場合

$d = \dfrac{t}{k_0} > 1$ となるから $t \geqq 2k_0$。よって

$$s \geqq 4n k^2 + 1$$

となれば

$$(d-1)(s-1) \geqq \left(\frac{t}{k_0} - 1\right) 4n k^2 \geqq \frac{t}{2k_0} 4n k_0^2 p^{2\theta}$$

$$\geqq \frac{p-1}{2n k_0} 4n k_0^2 p^{2\theta} \geqq 2k_0 (p-1) p^{2\theta} \geqq p^{1+2\theta}$$

で (10) は

$$\geqq p^m$$

となる

(ii) $t \nmid k_0$, $k_0 \nmid t$ の場合

$\dfrac{k_0 t}{(t,\ k_0)} \geqq 2t$ となるから $s \geqq 2nk^2+1$ となれば

$$(d-1)(s-1) \geqq \left(\frac{t}{(t,\ k_0)} - 1\right) 2nk_0^2 p^{2\theta} \geqq \frac{t}{2(t,\ k_0)} 2nk_0^2 p^{2\theta}$$

$$\geqq 2ntk_0 p^{2\theta} \geqq 2(p-1)k_0 p^{2\theta} \geqq p^{1+2\theta} = p^m$$

で (10) は $\geqq p^m$ となる

(iii) $t \mid k_0$ の場合

このときは n のある約数 n_1 によって $n_1 t = p-1$ とできる. したがって

$$p-1 = n_1 t \mid n_1 k_0 \mid n k_0 \mid nk$$

よって

$$K = \prod_{p-1 \mid nk} p^{1+2\theta}$$

とおき

$$s \equiv N \mod K$$

の場合には $q = p^m$ として (8) が成立ち (9) がえられる.

上記 (i) (ii) の場合には無条件で (9) が成立つのであり結局次の定理がえられる。

Theorem 12. Define

$$K = \prod_{\substack{p-1 \mid nk \\ p \nmid |d|}} p^{2\theta+1} \prod_{p \mid |d|} p^{2d_p+2\theta+1}$$

If $s \geq 4nk^2+1$, ~~then~~ there exist a constant c such that

$$\mathfrak{S}(N) \geq c > 0,$$

provided that $s \equiv N \bmod K$.

§4 Major arcs.

$N = P^k$ とする。h は後にきめる十分大きい正数で

$$\sigma = (\log P)^{2h}, \qquad \tau = \frac{N}{(\log P)^h}$$

とおく。$0 < a \leq q \leq \sigma$, $(a, q) = 1$ なる正整数 a, q に対し区間 $\left[\frac{1}{\tau}, 1+\frac{1}{\tau}\right]$ の部分小区間

$$\left[\frac{a}{q} - \frac{1}{\tau}, \frac{a}{q} + \frac{1}{\tau}\right]$$

を一つの major arc とよび，$\mathfrak{M}\left(\frac{a}{q}\right)$ で表わす。また

$$\mathfrak{m} = \left[\frac{1}{\tau}, 1+\frac{1}{\tau}\right] - \sum \mathfrak{M}\left(\frac{a}{q}\right)$$

を minor arc とよぶ。N が十分大ならば major arc はすべて overlap しない。Dirichlet の抽出法を使って

$\alpha \in \mathfrak{m}$ のとき

$$\alpha = \frac{a}{q} + \frac{\theta}{q\tau}, \quad |\theta| \leqq 1, \quad \sigma < q \leqq \tau, \quad (a, q) = 1$$

となる a, q が定まることが分る。

ここでは一つの major arc $\mathfrak{M}\left(\frac{a}{q}\right)$ に属する α に対して

$$S(\alpha) = \sum_{N\mathfrak{p} \leqq P} e^{2\pi i \alpha (N\mathfrak{p})^k}$$

の評価をする。単項イデアルのノルムによって作られる residue class group mod q を

$$\{b_1, \cdots, b_r \mod q\}.$$

とする。$m \leqq N = P^k$ とし

$$S_m = \sum_{(N\mathfrak{p})^k \leqq m} e^{2\pi i \frac{a}{q} (N\mathfrak{p})^k}$$

とおけば $q \leqq \sigma = (\log P)^{2h}$ より $P \geqq e^{\frac{1}{q^{2h}}}$ したがって定理 10 が使えて

$$S_m = \sum_{j=1}^{r} e^{2\pi i \frac{a}{q} b_j^k} \pi(m^{\frac{1}{k}}; q, b_j) + O(q)$$

$$= \frac{1}{h_0 r} B\left(\frac{a}{q}\right) \int_2^{m^{\frac{1}{k}}} \frac{du}{\log u} + O\left(\frac{1}{h_0} P e^{-c\sqrt{\log P}}\right);$$

ただし h_0 は F の絶対イデアル類の類数である。

$\alpha = \frac{a}{q} + \beta$ とすれば

$$S(\alpha) = \sum_{m=2}^{N} (S_m - S_{m-1}) e^{2\pi i \beta m}$$

$$= \sum_{m=2}^{N} S_m(e^{2\pi i\beta m} - e^{2\pi i\beta(m+1)}) + S_N e^{2\pi i\beta(N+1)}$$

$$= \sum_{m=2}^{N} \left\{ \frac{1}{h_0 r} B\left(\frac{a}{q}\right) \int_2^{m^{\frac{1}{k}}} \frac{du}{\log u} + O\left(\frac{1}{h_0} P e^{-c\sqrt{\log P}}\right) \right\} \times$$
$$(e^{2\pi i\beta m} - e^{2\pi i\beta(m+1)})$$

$$+ \left\{ \frac{1}{h_0 r} B\left(\frac{a}{q}\right) \int_2^{P} \frac{du}{\log u} + O\left(\frac{1}{h_0} P e^{-c\sqrt{\log P}}\right) \right\} e^{2\pi i\beta(N+1)}$$

$$= \frac{1}{h_0 r} B\left(\frac{a}{q}\right) \sum_{m=2}^{N} \left(\int_{(m-1)^{\frac{1}{k}}}^{m^{\frac{1}{k}}} \frac{du}{\log u} \right) e^{2\pi i\beta m} + O\left(\frac{1}{h_0} P e^{-c\sqrt{\log P}} \frac{N}{\tau}\right)$$

こゝで $|1-e^{2\pi i\beta}| \ll |\beta| \leq \frac{1}{\tau}$ に注意すれば

$$S(\alpha) = \frac{1}{h_0 r} B\left(\frac{a}{q}\right) J(\beta) + O(P e^{-c_1\sqrt{\log P}})$$

がえられる。こゝに

$$J(\beta) = \int_2^P \frac{e^{2\pi i\beta u^k}}{\log u} du.$$

<u>Theorem 13.</u> If $\alpha = \frac{a}{q} + \beta \in \mathfrak{M}\left(\frac{a}{q}\right)$, then

$$S(\alpha) = \frac{1}{h_0 r} B\left(\frac{a}{q}\right) J(\beta) + O(P e^{-c_1\sqrt{\log P}})$$

$J(\beta)$ については第2平均値定理を使って

<u>Theorem 14</u>

$$J(\beta) \ll \frac{1}{|\beta|^{\frac{1}{k}}}$$

がえられる。

上記の結果より

$$\int_{\mathfrak{M}\left(\frac{a}{q}\right)} e^{-2\pi i \alpha N} S(\alpha)^s \, d\alpha = \frac{1}{h_0^s r^s} B\left(\frac{a}{q}\right)^s e^{-2\pi i \frac{a}{q} N} \times$$

$$\int_{-\frac{1}{\tau}}^{\frac{1}{\tau}} e^{-2\pi i \beta P^k} \left\{ \int_2^P \frac{e^{2\pi i \beta z^k}}{\log z} dz \right\}^s d\beta$$

$$+ O\left(P^{s-k} e^{-c_2\sqrt{\log P}}\right).$$

さて

$$\int_{\frac{1}{\tau}}^{\infty} e^{-2\pi i \beta P^k} \left\{ \int_2^P \frac{e^{2\pi i \beta z^k}}{\log z} dz \right\}^s d\beta \ll \int_{\frac{1}{\tau}}^{\infty} \frac{d\beta}{\beta^{\frac{s}{k}}} \ll \frac{P^{s-k}}{(\log P)^{h\left(\frac{s}{k}-1\right)}}$$

また

$$\int_{-\infty}^{\infty} e^{-2\pi i \beta P^k} \left\{ \int_2^{\sqrt{P}} \frac{e^{2\pi i \beta z^k}}{\log z} dz \right\}^s d\beta \ll P^{\frac{s}{2}} \int_0^{P^{-\frac{k}{2}}} d\beta + \int_{P^{-\frac{k}{2}}}^{\infty} \frac{d\beta}{\beta^{\frac{1}{k}}}$$

$$\ll P^{\frac{s-k}{2}}$$

よって

$$\int_{-\frac{1}{\tau}}^{\frac{1}{\tau}} e^{-2\pi i \beta P^k} \left\{ \int_2^P \frac{e^{2\pi i \beta z^k}}{\log z} dz \right\}^s d\beta$$

$$= \int_{-\infty}^{\infty} e^{-2\pi i \beta P^k} \left\{ \int_{\sqrt{P}}^P \frac{e^{2\pi i \beta z^k}}{\log z} dz \right\}^s d\beta + O\left(\frac{P^{s-k}}{(\log P)^{h\left(\frac{s}{k}-1\right)}}\right)$$

$\beta P^k = v,\ z = P w$ と変換して

$$= P^{s-k} \int_{-\infty}^{\infty} e^{-2\pi i v} \left\{ \int_{\frac{1}{\sqrt{P}}}^{1} \frac{e^{2\pi i v w^k}}{\log P w} dw \right\}^s dv + O\left(\frac{P^{s-k}}{(\log P)^{h\left(\frac{s}{k}-1\right)}}\right).$$

$\frac{1}{\sqrt{P}} \leqq w \leqq 1$ ならば $\frac{1}{\log Pw} - \frac{1}{\log P} \ll \frac{1}{\log^2 P}$ 。第2平均値の定理を使って、

$$\int_{\frac{1}{\sqrt{P}}}^{1} \frac{e^{2\pi i v w^k}}{\log Pw} dw,\quad \frac{1}{\log P}\int_{\frac{1}{\sqrt{P}}}^{1} e^{2\pi i v w^k} dw \ll \frac{1}{\log P}\frac{1}{v^{\frac{1}{k}}}$$

よって

$$\left(\int_{\frac{1}{\sqrt{P}}}^{1} \frac{e^{2\pi i v w^k}}{\log Pw} dw\right)^s = \left(\frac{1}{\log P}\int_{\frac{1}{\sqrt{P}}}^{1} e^{2\pi i v w^k} dw\right)^s$$

$$+ O\left(\frac{1}{\log^2 P}\left(\frac{1}{\log P}\frac{1}{v^{\frac{1}{k}}}\right)^{s-1}\right) \ll \cancel{\frac{1}{(\log P)^{s+1}}\frac{1}{v^{\frac{s-1}{k}}}}$$

それより

$$\int_{-\infty}^{\infty} e^{-2\pi i v}\left\{\int_{\frac{1}{\sqrt{P}}}^{1} \frac{e^{2\pi i v w^k}}{\log Pw} dw\right\}^s dv$$

$$= \int_{-\infty}^{\infty} e^{-2\pi i v}\left\{\frac{1}{\log P}\int_{\frac{1}{\sqrt{P}}}^{1} e^{2\pi i v w^k} dw\right\}^s dv + O\left(\frac{1}{(\log P)^{s+1}}\right).$$

故に

$$\int_{-\frac{1}{\tau}}^{\frac{1}{\tau}} e^{-2\pi i \beta P^k}\left\{\int_{2}^{P} \frac{e^{2\pi i \beta z^k}}{\log z} dz\right\}^s d\beta$$

$$= P^{s-k}\int_{-\infty}^{\infty} e^{-2\pi i v}\left\{\frac{1}{\log P}\int_{\frac{1}{\sqrt{P}}}^{1} e^{2\pi i v w^k} dw\right\}^s dv + O\left(\frac{P^{s-k}}{(\log P)^{s+1}}\right)$$

$$= \frac{P^{s-k}}{(\log P)^s}\int_{-\infty}^{\infty} e^{-2\pi i v}\left\{\int_{0}^{1} e^{2\pi i v w^k} dw\right\}^s dv + O\left(\frac{P^{s-k}}{(\log P)^{s+1}}\right).$$

なぜならば

$$\int_{-\infty}^{\infty} e^{-2\pi i v} \left\{ \int_0^{\frac{1}{\sqrt{P}}} e^{2\pi i v w^k} dw \right\}^s dv$$

$$\ll P^{-\frac{s}{2}} \int_0^{P^{-\frac{k}{2}}} dv + \int_{P^{-\frac{k}{2}}}^{\infty} \frac{dv}{v^{\frac{s}{k}}} \ll \frac{1}{P^{\frac{s-k}{2}}}$$

であるから。Landau [3] の計算を使えば

$$\int_{-\frac{1}{\tau}}^{\frac{1}{\tau}} e^{-2\pi i \beta P^k} \left\{ \int_2^P \frac{e^{2\pi i \beta z^k}}{\log z} dz \right\}^s d\beta$$

$$= \frac{\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})} \frac{P^{s-k}}{(\log P)^s} + O\left(\frac{P^{s-k}}{(\log P)^{s+1}}\right).$$

したがって,

$$\int_{\mathfrak{M}(\frac{a}{q})} e^{-2\pi i \alpha N} S(\alpha)^s d\alpha = \frac{1}{h_0^s} \frac{1}{r^s} B\left(\frac{a}{q}\right)^s e^{-2\pi i \frac{a}{q} N} \times$$

$$\frac{\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})} \frac{P^{s-k}}{(\log P)^s} + O\left(\frac{P^{s-k}}{(\log P)^{s+1}}\right).$$

かくて

<u>Theorem 15</u> Assume that

$$s \geqq 4nk^2 + 1 \quad \text{and} \quad s \equiv N \mod K.$$

Then

$$\int_{\mathfrak{M}} e^{-2\pi i \alpha N} S(\alpha)^s d\alpha = \frac{\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k}) h_0^s} \mathfrak{S}(N) \frac{P^{s-k}}{(\log P)^s} + O\left(\frac{P^{s-k}}{(\log P)^{s+1}}\right),$$

where $\mathfrak{M} = \sum \mathfrak{M}\left(\frac{a}{q}\right)$. $(0 < a \leqq q \leqq \sigma,\ (a, q) = 1)$.

§5 Minor arc

$\tau(d)$ を約数関数とすれば

Theorem 16 Vinogradov [7], Hua [1]

$$\sum_{d\leqq N}\tau(d)^{l}\ll N(\log N)^{2^{l}-1}$$

こゝで

$$S=\sum_{M<x\leqq M'}{}' e^{2\pi i\alpha(x^{l}+\alpha_1 x^{l-1}+\cdots+\alpha_l)} \quad (M'\leqq 2M)$$

のような Weyl の和の評価を問題とする。簡便のため

$$\sum_{x}^{M},\quad \sum_{x}^{M}{}'$$

のような記号を使うが，それは x が大きさにおいても個数についても $O(M)$ の範囲にあることを示し，前者の場合は x がその範囲内の連続整数を動くことを示し後者の場合はその範囲内の整数をとびとびに動く意味となる。通常の Weyl の和の取扱いで

Theorem 17

(i) $$|S|^{2^{l-1}}\ll M^{2^{l-1}-l}\sum_{x_1}^{M}\cdots\sum_{x_{l-1}}^{M}\Bigl|\sum_{x}^{M}{}' e^{2\pi i\alpha l!\,x_1\cdots x_{l-1}x}\Bigr|$$

(ii) $$|S|^{2^{l}}\ll M^{2^{l}-l}\sum_{x_1}^{M}\cdots\sum_{x_{l-1}}^{M}\sum_{x_l}^{M}{}' e^{2\pi i\alpha l!\,x_1\cdots x_l}.$$

後に必要になる計算を準備しておく

$S=\sum_{x}^{P}{}' e^{2\pi i\alpha(x^{l}+\alpha_1 x^{l-1}+\cdots+\alpha_l)}$ とおく．

<u>Theorem 18</u> Let $(a, q)=1$ and $\left|\alpha-\frac{a}{q}\right| \leqq \frac{1}{q^2}$.

Then

$$S \ll P(\log P)^{2^l-4}\left(\frac{1}{q}+\frac{1}{P}+\frac{q}{P^l}\right)^{\frac{1}{2^l}} \qquad (q \leqq P^l)$$

Proof. 定理 17 (i) より

$$|S|^{2^l} \ll P^{2^l-2}+P^{2^l-2l}\sum_{m}^{l!P^{l-1}} \tau(m)^{2l-4}\sum_{m}^{l!P^{l-1}}\left|\sum_{x}^{P}{}' e^{2\pi i \alpha m x}\right|^2$$

しかるに

$$\sum_{m}^{l!P^{l-1}}\left|\sum_{x}^{P}{}' e^{2\pi i \alpha m x}\right|^2 = \sum_{x_1}^{P}{}' \sum_{x_2}^{P}{}' \sum_{m}^{l!P^{l-1}} e^{2\pi i \alpha m (x_1-x_2)}$$

$$\ll \sum_{x_1}^{P}\sum_{x_2}^{P}\left|\sum_{m}^{l!P^{l-1}} e^{2\pi i \alpha m (x_1-x_2)}\right|$$

$$\ll \sum_{x_1}^{P}\sum_{x_2}^{P} \mathrm{Min}\left(P^{l-1}, \frac{1}{2\{\alpha(x_1-x_2)\}}\right).$$

$$\ll P\left(\frac{P}{q}+1\right)\left(P^{l-1}+q\log q\right).$$

定理 16 を使って

$$|S|^{2^l} \ll P^{2^l-2}+P^{2^l-2l}P^{l-1}(\log P)^{2^{2l-4}-1}P^{l+1}\left(\frac{1}{q}+\frac{1}{P}\right)\left(1+\frac{q\log q}{P^{l-1}}\right).$$

これより上述の結果をうる. q.e.d.

次に $(a, q)=1$

$$S=\sum_{x_1}^{M}\cdots\sum_{x_l}^{M}\left|\sum_{y}^{P}{}' e^{2\pi i \frac{a}{q} l!\, x_1\cdots x_l (y^l+\alpha_1 y^{l-1}+\cdots+\alpha_l)}\right|$$

とおく。

<u>Theorem 19</u>

$$S \ll M^l P(\log MP)^{2^{2l-4}}\left(\frac{1}{q}+\frac{1}{P}+\frac{1}{M^2}+\frac{1}{M^lP^{l-1}}+\frac{q}{M^lP^l}\right)^{\frac{1}{2^l}}$$

$$(q \leqq M^l P^l)$$

Proof. 定理 17 (i) により

$$S^{2^{l-1}} \ll M^{l(2^{l-1}-1)} P^{2^{l-1}-l} M^{l-1} P^{l-1} (P+M)$$
$$+ M^{l(2^{l-1}-1)} P^{2^{l-1}-l} \sum_{z}^{M^{l}P^{l-1}} \tau(z)^{2l-2} \left| \sum_{y}^{P}{}' e^{2\pi i \frac{a}{q} zy} \right|$$

と変形するが細部の計算は省略する.

α が minor arc $\mathfrak{m}$ に属していれば

$$\alpha = \frac{a}{q} + \frac{\theta}{q\tau}, \quad (a, q)=1, \quad |\theta| \leqq 1$$

とするとき $\sigma < q \leqq \tau$ となるのであった。こゝで

$\sum_{N\mathfrak{p} \leqq P} e^{2\pi i \alpha N\mathfrak{p}^{k}}$ を評価するのに

$$S(\alpha) = \sum_{N\mathfrak{p} \leqq P} e^{2\pi i \frac{a}{q} N\mathfrak{p}^{k}}$$

を考えても大差はない。なぜなら

$$\sum_{N\mathfrak{p} \leqq P} e^{2\pi i \frac{a}{q} N\mathfrak{p}^{k}} (e^{2\pi i \beta N\mathfrak{p}^{k}} - 1) \ll \frac{P}{\log P} \frac{P^{k}}{q\tau} \ll \frac{P}{(\log P)^{h+1}}$$

$\mathfrak{P} = \prod_{N\mathfrak{p} \leqq \sqrt{P}} \mathfrak{p}$ とおいて $\sum_{\substack{N\mathfrak{a} \leqq P \\ (\mathfrak{a}, \mathfrak{P}) = \mathfrak{o}}} e^{2\pi i \frac{a}{q} N\mathfrak{a}^{k}}$ を考える.

それは一方では

$$e^{2\pi i \frac{a}{q}} + \sum_{\sqrt{P} < N\mathfrak{p} \leqq P} e^{2\pi i \frac{a}{q} N\mathfrak{p}^{k}}$$

他方では

$$\sum_{N\mathfrak{a} \leqq P} e^{2\pi i \frac{a}{q} N\mathfrak{a}^{k}} \sum_{\mathfrak{d} | (\mathfrak{a}, \mathfrak{P})} \mu(\mathfrak{d})$$

$$= \sum_{\substack{\mathfrak{d} \mid \mathfrak{k} \\ N\mathfrak{d} \leqq P}} \mu(\mathfrak{d}) \sum_{N\mathfrak{m} \leqq \frac{P}{N\mathfrak{d}}} e^{2\pi i \frac{a}{q} N\mathfrak{d}^k N\mathfrak{m}^k}$$

したがって

$$S(\mathfrak{d}) = \sum_{N\mathfrak{m} \leqq \frac{P}{N\mathfrak{d}}} e^{2\pi i \frac{a}{q} N\mathfrak{d}^k N\mathfrak{m}^k}$$

とおいて

$$S(\alpha) = \sum_{\substack{\mathfrak{d} \mid \mathfrak{k} \\ N\mathfrak{d} \leqq P}} \mu(\mathfrak{d}) S(\mathfrak{d}) + O(\sqrt{P}).$$

以下 Vinogradoff 独特の細かい計算で $S(\alpha)$ の評価を行うのであるが [7],

$$\Sigma_1 = \sum_{N\mathfrak{d} \leqq (\log P)^{\bar{h}}} |S(\mathfrak{d})| , \qquad \Sigma_2 = \sum_{(\log P)^{\bar{h}} < N\mathfrak{d} \leqq \frac{P}{(\log P)^{\bar{h}}}} |S(\mathfrak{d})|$$

$$\Sigma_3 = \sum_{\substack{\frac{P}{(\log P)^{\bar{h}}} < N\mathfrak{d} \leqq P \\ \mu(\mathfrak{d}) = +1}} S(\mathfrak{d}) , \qquad \Sigma_4 = \sum_{\substack{\frac{P}{(\log P)^{\bar{h}}} < N\mathfrak{d} \leqq P \\ \mu(\mathfrak{d}) = -1}} S(\mathfrak{d})$$

と分ける。$\bar{h}$ の大きさについては後に考えることゝするが今まででてきた $\mathfrak{f}$, $\mathfrak{a}$ などはすべて単項イデヤルである。こゝで

$$\tilde{\mathfrak{f}} = \mathfrak{f}_\infty^{(1)} \cdots \mathfrak{f}_\infty^{(r_1)}$$

とし F の数を mod $\tilde{\mathfrak{f}}$ で類別しさらにいくつかずつ

類をまとめ mod $\tilde{\mathfrak{f}}$ による F の単項イデアルの類別をする。すなわち (α) と (β) とが同じ類に属するのは α と $\beta\varepsilon$ とが r_1 個のすべての実共役で同符号となるような F の単数 ε が存在するときと考える。上述の $S(\vartheta)$ でたとえば $\mathfrak{m}$ がこの意味における一つの類 C だけに属するものだけを動かす場合には $S(\vartheta, C)$ などとかく。

<u>Σ_1 の評価</u>

$$\Sigma_1 = \sum_{N\vartheta \leqq (\log P)^{\frac{1}{k}}} |S(\vartheta)| , \quad S(\vartheta) = \sum_{N\mathfrak{m} \leqq \frac{P}{N\vartheta}} e^{2\pi i \frac{a}{q} N\vartheta^k N\mathfrak{m}^k}$$

このとき、$q_1 = \dfrac{q}{(q, N\vartheta^k)}$ とおけば

$$S(\vartheta) = \sum_{N\mathfrak{m} \leqq \frac{P}{N\vartheta}} e^{2\pi i \frac{b}{q_1} N\mathfrak{m}^k} , \qquad (b, q_1) = 1$$

となる b が存在し

$$q_1 N\vartheta^k \geqq q \quad より \quad \frac{1}{q_1} \leqq \frac{N\vartheta^k}{q}$$

となる。$S(\vartheta, C)$ の評価がえられれば それを各類の個数だけ集めて $S(\vartheta)$ の評価ができる。$\mathfrak{b}$ を C^{-1} に属して q_1 と素な整イデアルとすれば

$$S(\vartheta, C)\, w = \sum_{N\gamma \leqq t N\mathfrak{b}} e^{2\pi i \frac{b}{q_1} (N\mathfrak{b}^{-1})^k N(\gamma)^k}$$

こゝで $t = \dfrac{P}{N\vartheta}$ である。γ は総正で

$$\log \frac{\gamma^{(j)}}{N(\gamma)^{\frac{1}{n}}} = v_1 \log |\varepsilon_1^{(j)}| + \cdots + v_r \log |\varepsilon_r^{(j)}|$$

$$0 \leqq v_s < 1$$

なる条件をみたすものを動く[6]。$(\gamma) = mb \leqq b$ で

$[\mu_1, \cdots, \mu_n]$ を

$$|\mu_i^{(j)}| \leqq c\, Nb^{\frac{1}{n}}$$

なる条件をみたす b の一組の底とすれば

$$\gamma = \mu_1 x_1 + \cdots + \mu_n x_n$$

と書くことができる。この際 μ_1 は q_1 と素であると考えてよい。

連立方程式

$$\mu_1^{(j)} x_1 + \cdots + \mu_n^{(j)} x_n = \gamma^{(j)} \qquad 1 \leqq j \leqq n$$

より

$$x_i \ll \frac{t^{\frac{1}{n}}\, Nb^{\frac{1}{n}}\, (Nb)^{\frac{1}{n}(n-1)}}{\sqrt{|d|}\; Nb} \ll t^{\frac{1}{n}}$$

そこで

$$N(\gamma)^{k} = \left\{ \prod_{j=1}^{n} (\mu_1^{(j)} x_1 + \cdots + \mu_n^{(j)} x_n) \right\}^{k}$$

より

$$(Nb^{-1})^{k} (N(\gamma))^{k} = N\left(\frac{\mu_1}{b}\right)^{k} x_1^{nk} + \cdots\cdots$$

故に

$$S(\vartheta, C)\, w = \sum_{x_1}{}' \cdots \sum_{x_n}^{\left(\frac{P}{N\vartheta}\right)^{\frac{1}{n}}}{}' e^{2\pi i \frac{c}{q_1} (x_1^{nk} + \cdots\cdots)}$$

こゝに $(c, q_1) = 1$, $x_1^{nk} + \cdots\cdots$ は $x_1, \cdots, x_n$ に関する nk 次の同次整式である。こゝで定理 18 を使えば

$$S(\vartheta, C) \ll \left(\frac{P}{N\vartheta}\right)^{\frac{n-1}{n}} \left(\frac{P}{N\vartheta}\right) (\log P)^{2^{nk}-4} \left(\frac{1}{q_1} + \frac{N\vartheta}{P} + \frac{N\vartheta^{nk} q}{P^{nk}}\right)^{\frac{1}{2^{nk}}}$$

$\frac{1}{q_1} \ll \frac{(N\vartheta)^k}{q}$, $q \leqq \frac{P^k}{(\log P)^h}$ に注意して

$$\ll \frac{P}{N\vartheta} (\log P)^{2^{nk}-4} \left\{ \frac{(N\vartheta)^k}{q} + \frac{N\vartheta}{P} + \frac{(N\vartheta)^{nk}}{P^{nk}} \frac{P^k}{(\log P)^h} \right\}^{\frac{1}{2^{nk}}}$$

また $(\log P)^h \leqq q$, $N\vartheta \leqq (\log P)^{\bar{h}}$ に注意し, $\bar{h}$ を任意にとるとき それに対し h を十分大きくすれば

$$\Sigma_1 \ll \frac{P}{(\log P)^{h_1}}$$

とでき、この h_1 はいかほどでも大きくすることができることに気がつく。

Σ_2 の評価

$$\Sigma_2 = \sum_{(\log P)^{\bar{h}} < N\vartheta \leqq \frac{P}{(\log P)^h}} \left| \sum_{Nm \leqq \frac{P}{N\vartheta}} e^{2\pi i \frac{a}{q} N\vartheta^k Nm^k} \right|$$

は

$$S(M) = \sum_{M < N\vartheta \leqq M'} \left| \sum_{Nm \leqq \frac{P}{N\vartheta}} e^{2\pi i \frac{a}{q} N\vartheta^k Nm^k} \right|$$

型の $O(\log P)$ 個の和となる。しかるに

$$|S(M)|^2 \leqq M \sum_{M < N\vartheta \leqq M'} \left| \sum_{Nm \leqq \frac{P}{N\vartheta}} e^{2\pi i \frac{a}{q} N\vartheta^k Nm^k} \right|$$

$$\leqq M \sum_{\vartheta} \sum_{m} \sum_{m_1} e^{2\pi i \frac{a}{q} N\vartheta^k (Nm^k - Nm_1^k)}$$

こゝに

$$N\mathfrak{m},\ N\mathfrak{m}_1 \leqq \frac{P}{N\vartheta} \leqq \frac{P}{M},\qquad M < N\vartheta \leqq \mathrm{Min}\left(\frac{P}{N\mathfrak{m}}, \frac{P}{N\mathfrak{m}_1}, M'\right)$$

よって

$$\leqq M\frac{P}{M}\,\mathrm{Max}_{\mathfrak{m}_1}\sum_{\mathfrak{m}}|S_{\mathfrak{m}}|$$

$$\leqq P\ \mathrm{Max}_{\mathfrak{m}_1}\left(\frac{P}{M}\right)^{1-\frac{1}{2^{nk}}}\left(\sum_{\mathfrak{m}}|S_{\mathfrak{m}}|^{2^{nk}}\right)^{\frac{1}{2^{nk}}}$$

たゞし,

$$S_{\mathfrak{m}} = \sum_{\vartheta} e^{2\pi i\frac{a}{q}N\vartheta^k(N\mathfrak{m}^k - N\mathfrak{m}_1^k)}$$

こゝで前述のような計算をしていけば

$$|S_{\mathfrak{m}}|^{2^{nk}} \ll M^{2^{nk}(1-\frac{1}{n})}\, M^{\frac{1}{n}(2^{nk}-nk)} \sum_{\xi_1}^{M^{\frac{1}{n}}}\cdots\sum_{\xi_{nk-1}}^{M^{\frac{1}{n}}}\sum_{\xi_{nk}}^{M^{\frac{1}{n}}}{}' e^{2\pi i\frac{b}{q}(N\mathfrak{m}^k - N\mathfrak{m}_1^k)(nk)!\,\xi_1\cdots\xi_{nk}}$$

それよりまた

$$\sum_{\mathfrak{m}}|S_{\mathfrak{m}}|^{2^{nk}} \ll M^{2^{nk}-k}\left(\frac{P}{M}\right)^{1-\frac{1}{n}} S$$

$$S = \sum_{\xi_1}^{M^{\frac{1}{n}}}\cdots\sum_{\xi_{nk}}^{M^{\frac{1}{n}}}\left|\sum_{y_1}^{(\frac{P}{M})^{\frac{1}{n}}}{}' e^{2\pi i\frac{c}{q}(y_1^{nk}+\cdots)(nk)!\,\xi_1\cdots\xi_{nk}}\right|$$

こゝで $y_2\cdots y_n$ は fix, $(c, q)=1$ である。こゝで定理19を使うことによって

$$S(M) \ll P(\log P)^{2^{nk-5}}\left(\frac{1}{q}+\frac{M^{\frac{1}{n}}}{P^{\frac{1}{n}}}+\frac{1}{M^{\frac{2}{n}}}+\frac{1}{MP^{k-\frac{1}{n}}}+\frac{q}{P^k}\right)^{\frac{1}{2\cdot 4^{nk}}}$$

そして Σ_2 についても Σ_1 同様 $\Sigma_2 \ll \frac{P}{(\log P)^{h_1}}$ とできる。

Σ_3, Σ_4 の評価

$M' \leqq 2M$, $M \leqq (\log P)^h$ とし

$$S_0(M) = \sum_{M < N\mathfrak{m} \leqq M'} \sum_{\substack{\frac{P}{(\log P)^h} < N\vartheta_0 \leqq \frac{P}{N\mathfrak{m}} \\ \mu(\vartheta_0) = +1}} e^{2\pi i \frac{a}{q} N(\vartheta_0)^k N\mathfrak{m}^k}$$

$$S_1(M) = \sum_{M < N\mathfrak{m} \leqq M'} \sum_{\substack{\frac{P}{(\log P)^h} < N\vartheta_1 \leqq \frac{P}{N\mathfrak{m}} \\ \mu(\vartheta_1) = -1}} e^{2\pi i \frac{a}{q} N(\vartheta_1)^k N\mathfrak{m}^k}$$

とおけば

$$\Sigma_3 = \sum_{M}^{\log\log P} S_0(M), \qquad \Sigma_4 = \sum_{M}^{\log\log P} S_1(M)$$

となる。また

$$S_0(M) = A_0(M) + A_1(M) + \cdots + A_r(M) + \cdots\cdots$$

$$S_1(M) = B_0(M) + B_1(M) + \cdots\cdots + B_r(M) + \cdots\cdots$$

$$H = (\log P)^h$$

とおき, $A_r(M)$ は $S_0(M)$ の中で ϑ_0 の素イデヤル因子のうちノルムが H をこえるものが丁度 r 個あるものについての和, $B_r(M)$ についても同じように考えるとする。

$A_0(M)$ について ϑ_0 が $\varkappa$ 個の素イデヤル因子をもつとする。すなわち

$$\vartheta_0 = \mathfrak{p}_1^{l_1} \cdots\cdots \mathfrak{p}_s^{l_s}, \qquad \varkappa = l_1 + \cdots\cdots + l_s$$

それらの norm はすべて H 以下だから

$$H^{x} \geqq N\vartheta_0 > \frac{P}{(\log P)^{h}} \quad より \quad x+1 > \frac{\log P}{\log H}$$

そして

$$\tau(\vartheta_0) = 2^{x} > 2^{\frac{\log P}{\log H}-1}$$

$$A_0(M) \leqq \sum_{M < N\mathfrak{m} \leqq M'} \sum_{\frac{P}{(\log P)^h} < N\vartheta_0 \leqq \frac{P}{N\mathfrak{m}}} 1 \ll M \sum_{N\vartheta_0 \leqq \frac{P}{M}} \frac{2\tau(\vartheta_0)}{2^{\frac{\log P}{\log H}}}$$

$$\ll \frac{P}{(\log P)^{h_1}}$$

$A_r(M)$ について。

$$A_r(M) = \sum_{M < N\mathfrak{m} \leqq M'} \sum_{\frac{P}{(\log P)^h} < N\vartheta_r \leqq \frac{P}{N\mathfrak{m}}} e^{2\pi i \frac{a}{q} N\vartheta_r^{k} N\mathfrak{m}^{k}}$$

この ϑ_r には norm が H より大きい素イデアル因子が r 個あって $\mu(\vartheta_r) = +1$. そこで

$$T_r(M) = \sum_{M < N\mathfrak{m} \leqq M'} \sum_{\frac{P}{(\log P)^h} < N\mathfrak{p} \cdot N\mathfrak{q} \leqq \frac{P}{N\mathfrak{m}}} e^{2\pi i \frac{a}{q} N\mathfrak{p}^{k} N\mathfrak{q}^{k} N\mathfrak{m}^{k}}$$

とし, $\mathfrak{p}$ は $\sqrt{P} \geqq N\mathfrak{p} \geqq H$, $\mathfrak{q}$ には norm が H より大きい素イデアル因子が r−1 個入っていて $\mu(\mathfrak{q}) = -1$. それより

$$A_r(M) - \frac{1}{r} T_r(M) \ll \frac{P \log\log P}{(\log P)^{h}}$$

を導き, $T_r(M)$ を評価するために さらに

$$T_r'(M)=\sum_{M<N\mathfrak{m}\leqq M'}\ \sum_{Q<N\mathfrak{q}\leqq Q'}\ \sum_{N\vartheta_{r-1}N\mathfrak{q}N\mathfrak{m}\leqq P} e^{2\pi i\frac{a}{q}N\mathfrak{q}^k N\vartheta_{r-1}^k N\mathfrak{m}^k}$$

を作る。こゝに $Q'\leqq 2Q$ で このような和 $O(\log P)$ ケで

$T_r(M)$ができると考える。そこで

$$\mathfrak{m}\mathfrak{q}=\mathfrak{b}\qquad \vartheta_{r-1}=\mathfrak{d}$$

として

$$T_r'(M)=\sum_{MQ<N\mathfrak{b}\leqq M'Q'}{}'\ \sum_{N\mathfrak{b}\mathfrak{d}\leqq P}{}' e^{2\pi i\frac{a}{q}(N\mathfrak{b})^k(N\mathfrak{d})^k}$$

と書ける。さて

$$|T_r'(M)|^2\ll MQ\sum_{MQ<N\mathfrak{b}\leqq M'Q'}\Big|\sum_{N\mathfrak{b}\mathfrak{d}\leqq P} e^{2\pi i\frac{a}{q}(N\mathfrak{b})^k(N\mathfrak{d})^k}\Big|^2$$

$$\ll MQ\sum\sum_{N\mathfrak{d},\,N\mathfrak{d}_1\leqq\frac{P}{MQ}}\Big|\sum_{MQ<N\mathfrak{b}\leqq M'Q'} e^{2\pi i\frac{a}{q}(N\mathfrak{b})^k(N\mathfrak{d}^k-N\mathfrak{d}_1^k)}\Big|$$

常に使う不等式

$$a_1+\cdots+a_r\leqq r^{1-\frac{1}{m}}(a_1^m+\cdots+a_r^m)^{\frac{1}{m}}$$

によって

$$\ll P\left(\frac{P}{MQ}\right)^{1-\frac{1}{2^{nk}}}\Big(\sum_{\mathfrak{d}}\Big|\sum_{\mathfrak{b}} e^{2\pi i\frac{a}{q}N\mathfrak{b}^k(N\mathfrak{d}^k-N\mathfrak{d}_1^k)}\Big|^{2^{nk}}\Big)^{\frac{1}{2^{nk}}}$$

この右辺は前に計算したことがあり結局

$$\ll P^2(\log P)^{2^{nk}-4}\left(\frac{1}{q}+\frac{(MQ)^{\frac{1}{n}}}{P^{\frac{1}{n}}}+\frac{1}{(MQ)^{\frac{2}{n}}}+\frac{1}{MQ\cdot P^{k-\frac{1}{n}}}+\frac{q}{P^k}\right)^{\frac{1}{4^{nk}}}$$

よって $A_r(M)\ll\frac{P}{(\log P)^{h_1+1}}$, $S_0(M)\ll\frac{P}{(\log P)^{h_1}}$

Theorem 20

$$\alpha \in \mathfrak{m} \implies \sum_{N\mathfrak{g} \leqq P} e^{2\pi i \alpha N\mathfrak{g}^k} \ll \frac{P}{(\log P)^{h_1}}$$

We can make h_1 sufficiently large by making h appropriately large.

§7 Final result

始めに

$$T(\alpha) = \sum_{x=1}^{P} e^{2\pi i \alpha x^k}$$

とおく。Vinogradoff, Hua などによる mean value theorem を使えば

$$t \geqq k^2(2\log k + \log\log k + 3)$$

ならば

$$\int_0^1 |T(\alpha)|^{2t} d\alpha \ll P^{2t-k}$$

となることが知られている [1]。

よって $s = 2t+1$ ならば定理20により

$$\left| \int_{\mathfrak{m}} e^{-2\pi i \alpha N} S(\alpha)^s d\alpha \right|$$

$$\leqq \operatorname*{Max}_{\alpha \in \mathfrak{m}} |S(\alpha)| \int_0^1 |S(\alpha)|^{2t} d\alpha \leqq \frac{P}{(\log P)^{h_1}} \int_0^1 |T(\alpha)|^{2t} d\alpha$$

$$\leqq \frac{P^{s-k}}{(\log P)^{h_1}}$$

よって以前の結果とあわせて

<u>Main theorem</u> Assuming that

$$s \geqq 4nk^2+1, \quad 2k^2(2\log k + \log\log k + 3) + 1$$

$$s \equiv N \mod K,$$

we have

$$\int_0^1 e^{-2\pi i \alpha N} \Big\{ \sum_{N\mathfrak{p} \leqq P} e^{2\pi i \alpha N\mathfrak{p}^k} \Big\}^s d\alpha$$

$$= \frac{\Gamma\left(1+\frac{1}{k}\right)^s}{\Gamma\left(\frac{s}{k}\right) h_0^s} \mathfrak{S}(N) \frac{P^{s-k}}{(\log P)^s} + O\left(\frac{P^{s-k}}{(\log P)^{s+1}} \right)$$

今回の seminar に出席して下さった E. Bombieri 氏によれば，Karacuba の方法を改良して mean value theorem に関して氏は次のような結果をえられた．この論文は目下のところ未発表であるが優れたものとおもう．

<u>Bombieri's result for the mean value theorem</u>

If $b \geqq kl + k$, then

$$\int_0^1 \cdots \int_0^1 \Big| \sum_{x=1}^{P} e^{2\pi i(\alpha_1 x + \cdots + \alpha_k x^k)} \Big|^{2b} d\alpha_1 \cdots d\alpha_k$$

$$\leqq c(b,k,l) P^{2b - \frac{1}{2}k(k+1) + \frac{1}{2}k(k+1)\left(1-\frac{1}{k}\right)^l}$$

References

[1] L.K. Hua ; Additive theory of prime numbers, American Math. Soc. 1965

[2] A. A. Karacuba ; ОСНОВЫ АНАЛИТИЧЕСКОЙ ТЕОРИИ ЧИСЕЛ, Moscow 1975.

[3] E. Landau ; Über die neue Winogradoffsche Behandlung des Waringschen Problems, Math. Zeitschr. 31, 1930.

[4] T. Mitsui ; 加法的素数論におけるある問題について — Goldbach の問題のある拡張 — 第3回代数学シンポジウム, Nagoya 1962.

[5] T. Mitsui ; On a problem in the additive prime number theory, Seminar on modern methods in number theory, Tokyo 1971.

[6] T. Tatuzawa ; On the number of integral ideals in algebraic number fields, whose norms not exceeding x, Sci. Paper of Tokyo Univ. 23, 1973

[7] I. M. Vinogradoff ; Некоторые общие теоремы, относящиеся к теории простых чисел, Труды Тбилисского матем института, 3, 1937.