QUADRATIC CONGRUENCES and WEYL SUMS

Hieu T. Ngo
Hanoi University of Science and Technology

PanAsian Number Theory 2021
Research Institute for Mathematical Sciences, Kyoto University

1. Equidistribution
2. Roots
3. Kloostermania
4. Roots

1. UNIFORM DISTRIBUTION MODULO ONE

We say a sequence of real numbers $(\gamma_n)_{n \in \mathbb{N}}$ is uniformly distributed modulo one if for $0 \leqslant a < b \leqslant 1$,

$$\lim_{N \to \infty} \frac{\#\{n \leqslant N : \gamma_n \in [a, b) + \mathbb{Z}\}}{N} = b - a$$

Weyl criterion :

$(\gamma_n)_{n \in \mathbb{N}}$ is uniformly distributed modulo one (UD mod 1)

$$\Leftrightarrow \forall h \in \mathbb{Z} \setminus \{0\}, \sum_{n < x} e(h\gamma_n) = o(x) \quad \text{as } x \longrightarrow \infty$$

$\Leftrightarrow$ $\forall$ continuous 1-periodic function f,

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} f(\gamma_n) = \int_0^1 f(t)\, dt$$

- $e(z) = e^{2\pi i z}$, $\quad f(x) = o(x)$ means $\frac{f(x)}{x} \longrightarrow 0$

We write $W\left((\gamma_n)\,;\,x\right) = \sum_{n<x} e\left(h\gamma_n\right)$ $\left(h \in \mathbb{Z}\setminus\{0\} \text{ fixed}\right)$

and call it the Weyl sum associated to the sequence $(\gamma_n)_{n\in\mathbb{N}}$.

A sequence $(\gamma_p)_{p\in\mathbb{P}}$ indexed by primes is uniformly distributed modulo one

$$\Longleftrightarrow \quad W\left((\gamma_p)\,;\,x\right) = \sum_{p<x} e\left(h\gamma_p\right) = o\left(\frac{x}{\log x}\right)$$

$$W\left((\gamma_n)\,;\,x\right) = \sum_{n<x} e\left(h\gamma_n\right)$$

$$W\left((\gamma_p)\,;\,x\right) = \sum_{p<x} e\left(h\gamma_p\right)$$

We seek not only nontrivial cancellation,

but also STRONG quantitative estimates

for the Weyl sums!

SEQUENCES :

- Let α be a real irrational number.

Weyl : $(n\alpha)_{n\in\mathbb{N}}$ is UD mod 1

Vinogradov : $(p\alpha)_{p\in\mathbb{P}}$ is UD mod 1

$$\sum_{n<x} e(n\alpha)\,\Lambda(n)$$

sums over primes : use combinatorial identities

- $P(x) = \alpha_k x^k + \dots + \alpha_1 x + \alpha_0 \in \mathbb{R}[x]$

$k \geqslant 1, \quad \alpha_k \notin \mathbb{Q}, \quad K = 2^{k-1}.$

If α_k has rational approximation $\left|\alpha_k - \frac{a}{q}\right| \leqslant \frac{1}{q^2}$, then

$$\sum_{n<N} e(P(n)) \ll_\varepsilon N^{1+\varepsilon} \underbrace{\left(N + q + \frac{N^k}{q}\right)^{-\frac{1}{2^{k-1}}}}_{\text{power - saving factor}}$$

Hardy - Littlewood 1920 (Waring's problem)

- $(\log n)_{n \in \mathbb{N}}$ is NOT UD mod 1

  $(\log p)_{p \in \mathbb{P}}$ is NOT UD mod 1

The above sequences concern function values.

How about roots ?

2. POLYNOMIAL CONGRUENCES

Let $P(x) \in \mathbb{Z}[x]$.

Consider $P(x) \equiv 0 \pmod{n}$.

How are the fractions $\frac{\nu}{n}$,

where $P(\nu) \equiv 0 \pmod{n}$, distributed ?

Define $\rho(n) = \rho_{P,h}(n) = \sum_{\substack{0 \leq \nu < n \\ P(\nu) \equiv 0 \pmod{n}}} e\left(h \cdot \frac{\nu}{n}\right)$.

The goal is to study congruence Weyl sums

$\sum_{n<x} \rho(n)$ polynomial congruences modulo integers

$\sum_{p<x} \rho(p)$ polynomial congruences modulo primes

Christopher Hooley 1964

Let $P(x)$ be primitive, irreducible of degree $n \geqslant 2$.

Let $\delta_n = \dfrac{n - \sqrt{n}}{n!}$ and $h \in \mathbb{Z} \setminus \{0\}$.

Then $$\sum_{n < x} \sum_{\substack{0 \leqslant \nu < n \\ P(\nu) \equiv 0 \ (\mathrm{mod}\ n)}} e\left(h \cdot \frac{\nu}{n}\right) \ll_{\varepsilon} \frac{x}{(\log x)^{\delta_n - \varepsilon}}$$

Roots of nonlinear polynomial congruences are equidistributed!

QUADRATIC CONGRUENCES MODULO INTEGERS

Let d be a squarefree integer.

Consider $X^2 \equiv d \pmod{n}$; let $h \in \mathbb{Z} \setminus \{0\}$.

Root harmonic $\rho(n) = \rho_{d,h}(n) = \sum_{\substack{0 \leq \nu < n \\ \nu^2 \equiv d \pmod{n}}} e\left(h \cdot \frac{\nu}{n}\right)$

Weyl sum $W_{\mathbb{N}}(x) = W_{d,h}(x) = \sum_{n < x} \rho(n)$

Christopher Hooley 1963 $\quad W_{\mathbb{N}}(x) \ll_{\varepsilon} x^{\frac{3}{4}+\varepsilon}$

for both $d > 0$ and $d < 0$

Hejhal 1986 $\quad W_{\mathbb{N}}(x) \ll_{\varepsilon} x^{\frac{2}{3}+\varepsilon}$

for $d > 0$

Bykovskii 1987 $\quad W_{\mathbb{N}}(x) \ll_{\varepsilon} x^{\frac{2}{3}+\varepsilon}$

for $d < 0$

QUADRATIC CONGRUENCES MODULO PRIMES

Let d be a squarefree integer.

Consider $X^2 \equiv d \pmod{p}$; let $h \in \mathbb{Z} \setminus \{0\}$.

Root harmonic $\rho(n) = \rho_{d,h}(n) = \sum_{\substack{0 \leq \nu < n \\ \nu^2 \equiv d \ (\mathrm{mod}\ n)}} e\left(h \cdot \frac{\nu}{n}\right)$

Weyl sum $W_{\mathbb{P}}(x) = W_{\mathbb{P},d,h}(x) = \sum_{p < x} \rho(p)$

Roots of quadratic congruences modulo primes are equidistributed!

$$W_{\mathbb{P}}(x) = o\left(\frac{x}{\log x}\right)$$

Duke - Friedlander - Iwaniec 1995 for $d < 0$

Toth 2000 for $d > 0$

Consider quadratic congruences with moduli in arithmetic progressions.

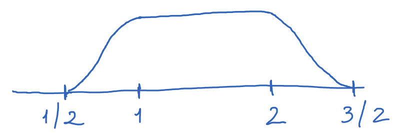
Weyl sums in arithmetic progressions :

$$W(x;N) = \sum_{\substack{x < n < 2x \\ n \equiv 0 \,(\mathrm{mod}\, N)}} \; \sum_{\substack{0 \leqslant \nu < n \\ \nu^2 \equiv d \,(\mathrm{mod}\, n)}} e\left(h \cdot \frac{\nu}{n}\right)$$

$$W_\varphi(x;N) = \sum_{\substack{x < n < 2x \\ n \equiv 0 \,(\mathrm{mod}\, N)}} \varphi\left(\frac{n}{x}\right) \sum_{\substack{0 \leqslant \nu < n \\ \nu^2 \equiv d \,(\mathrm{mod}\, n)}} e\left(h \cdot \frac{\nu}{n}\right)$$

φ is a dyadic bump function

$\varphi^{(j)} \ll 1$



Trivial bound : $W_\varphi(x;N)$ and $W(x;N)$ are $O\left(\frac{x}{N}\right)$

Duke - Friedlander - Iwaniec $(d<0)$:

$$W_\varphi(x;N) \ll \left(\frac{x}{N}\right)^{\frac{3}{4}+\varepsilon} \cdot N^{\frac{1}{4}} + x^{\frac{1}{2}+\varepsilon}$$

$$W(x;N) \ll \left(\frac{x}{N}\right)^{1+\varepsilon} \cdot \left(\frac{N^2}{x}\right)^{\frac{1}{20}}$$

Toth $(d>0)$:

$$W(x;N) \ll \left(\frac{x}{N}\right)^{1+\frac{1}{L^2}} \cdot \left(\frac{N^2}{x}\right)^{\frac{1}{4L}} \qquad (L \text{ large})$$

Effective range : $N = O\left(x^{\frac{1}{2}-\delta}\right)$

Duke - Friedlander - Iwaniec $(d<0)$:

$$W_\varphi(x;N) \ll \left(\frac{x}{N}\right)^{\frac{3}{4}+\varepsilon} \cdot N^{\frac{1}{4}} + x^{\frac{1}{2}+\varepsilon}$$

$$W(x;N) \ll \left(\frac{x}{N}\right)^{1+\varepsilon} \cdot \left(\frac{N^2}{x}\right)^{\frac{1}{20}}$$

H.N. 2021 $(d>0)$:

$$W_\varphi(x;N) \ll \left(\frac{x}{N}\right)^{\frac{3}{4}+\varepsilon} \cdot N^{\frac{1}{4}} + x^{\frac{1}{2}+\varepsilon}$$

$$W(x;N) \ll \left(\frac{x}{N}\right)^{1+\varepsilon} \cdot \left(\frac{N^2}{x}\right)^{\frac{1}{13}}$$

3. KLOOSTERMAN SUMS

Let $h, k, q \in \mathbb{Z}$ with $q \geqslant 1$.

Kloosterman sum $S(h,k;q) = \sum_{\substack{x,y \bmod q \\ xy \equiv 1 \pmod q}} e\left(\frac{hx+ky}{q}\right)$

Weil 's bound : $\left| S(h,k;q) \right| \leqslant \sqrt{q} \cdot \tau(q) \sqrt{\gcd(h,k,q)}$

Linnik conjecture (ICM 1962)

For $\varepsilon > 0$ and $x \geqslant \sqrt{|k|}$, $\sum_{q \leqslant x} \frac{S(1,k;q)}{q} \ll_{\varepsilon} x^{\varepsilon}$.

Sarnak - Selberg conjecture

For $\varepsilon > 0$ and $x \geqslant \gcd(h,k)^{\frac{1}{2}}$, $\sum_{q \leqslant x} \frac{S(h,k;q)}{q} \ll_{\varepsilon} \left(|hk| x\right)^{\varepsilon}$.

Kuznetsov 1980 : $\sum_{q \leqslant x} \frac{S(h,k;q)}{q} \ll_{h,k} x^{\frac{1}{6}} (\log x)^{\frac{1}{3}}$

Averaging versions of the Linnik - Sarnak - Selberg conjecture hold true : Iwaniec , Deshouillers - Iwaniec , ...

Iwaniec 1982 :

Let φ be a C^2 function, compactly supported on $(0,1)$

Suppose $\int t \left|\varphi''(t)\right| dt \leqslant 1$. Then

$$\sum_{\substack{H<h<2H \\ K<k<2K}}\sum \xi_h \lambda_k \sum_q \frac{S(h, \pm k ; q)}{q} \varphi\left(\frac{4\pi\sqrt{hk}}{q}\right)$$

$$\ll_\varepsilon (HK)^{\frac{1}{2}+\varepsilon}\left(\sum |\xi_h|^2\right)^{\frac{1}{2}}\left(\sum |\lambda_k|^2\right)^{\frac{1}{2}}$$

Deshouillers - Iwaniec 1982 :

$$\sum_{\substack{H<h<2H \\ K<k<2K}}\sum \gamma_h \lambda_k \sum_{q \leqslant x \cdot \sqrt{\frac{hk}{HK}}} \frac{S(h, \pm k ; q)}{q}$$

$$\ll_\varepsilon \left((HK)^{\frac{1}{2}+\varepsilon} + (x\, HK)^{\frac{1}{6}+\varepsilon}\right)\left(\sum |\gamma_h|^2\right)^{\frac{1}{2}}\left(\sum |\lambda_k|^2\right)^{\frac{1}{2}}$$

If $HK \geqslant x^{\frac{1}{2}}$, then $(HK)^{\frac{1}{2}} + (x\,HK)^{\frac{1}{6}} \asymp (HK)^{\frac{1}{2}}$.

KLOOSTERMAN SUMS FOR HECKE CONGRUENCE SUBGROUPS

$\Gamma = \Gamma_0(N)$ acts on the Poincaré upper half-plane.

Cusps are points $\mathfrak{U}$ in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$
with parabolic stabilizers $\Gamma_{\mathfrak{U}}$ in Γ.

For each cusp $\mathfrak{U}$, choose a scaling matrix $\sigma_{\mathfrak{U}}$
satisfying $\sigma_{\mathfrak{U}} \infty = \mathfrak{U}$, $\sigma_{\mathfrak{U}}^{-1} \Gamma_{\mathfrak{U}} \sigma_{\mathfrak{U}} = \Gamma_\infty = \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}$

$$S_{\sigma_{\mathfrak{U}} \sigma_{\mathfrak{V}}}(h, k; q) = \sum_{\begin{pmatrix} a & b \\ q & d \end{pmatrix} \in \Gamma_\infty \backslash \sigma_{\mathfrak{U}}^{-1} \Gamma \sigma_{\mathfrak{V}} / \Gamma_\infty} e\left(\frac{ha + kd}{q}\right) \qquad (h, k \in \mathbb{Z})$$

Many useful computations concerning Kloosterman sums for $\Gamma_0(N)$
were carried out by Professor Motohashi
concerning spectral analysis of the Riemann zeta function.

A cusp $\mathfrak{U}$ is <u>bounded</u> if $\mathfrak{U} = \frac{r}{s}$ with $r, s = O(1)$.

For a bounded cusp $\mathfrak{U}$, Kloosterman moduli for $S_{\sigma_\infty \sigma_{\mathfrak{U}}}$ are roughly

$$\left\{ q\sqrt{N} : \gcd(q, N) = 1 \right\}$$

Pitt 2012

If U is a bounded cusp, then

$$\sum_k \sum_q \frac{S_{\sigma_\infty \sigma_U}(h, k; q\sqrt{N})}{q} \varphi\left(\frac{q}{Q}, \frac{k}{K}\right) \lesssim\ll K^{\frac{3}{4}} Q^{\frac{1}{2}} N^{-\frac{1}{4}} + \dots$$

Applicable range: $K \approx Q \approx N \Rightarrow$ RHS is $\approx K$

this is Linnik - Sarnak - Selberg on average!

4. ROOTS OF QUADRATIC CONGRUENCES

Roots and Forms :

Write $\alpha X^2 + 2\beta XY + \gamma Y^2 = (\alpha, \beta, \gamma)$

$$F_d = \{ (\alpha, \beta, \gamma) \ : \ \beta^2 - \alpha\gamma = d \}$$

A root $r^2 \equiv d \pmod n$ gives $f_{d,r} = \left(\frac{r^2 - d}{n}, r, n \right)$

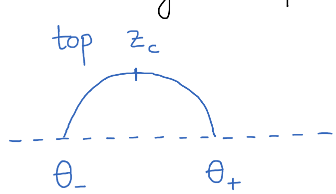
$$f_{d,r+kn}(X, Y) = f_{d,r}(X, Y + kX)$$

$$\{ r^2 \equiv d \pmod n \} \xrightarrow{\sim} \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix} \backslash F_d$$

$$r \longmapsto f_{d,r}$$

Forms and Geodesics $(d > 0)$

Solutions of an indefinite quadratic define endpoints of a geodesic c.



The form $f_{d,r}(X,Y) = \ell X^2 + 2rXY + nY^2$

give solutions $\theta_\pm = \dfrac{-r \pm \sqrt{d}}{n}$, so $\mathrm{Re}(z_c) = \dfrac{-r}{n}$.

This geodesic projects to a closed geodesic on the modular surface.

The stabilizer of this geodesic is the group of automorphs of the form.

Geometry and Symmetry of Roots ($d > 0$)

Let h be the narrow class number of $\mathbb{Q}(\sqrt{d})$, $\Gamma = SL_2(\mathbb{Z})$.

There are closed geodesics $c_1, \ldots, c_h$ of $\Gamma \backslash \mathbb{H}$ such that

$$\left\{ r^2 \equiv d \pmod{n} \right\} \xleftrightarrow{\sim} \bigcup_{1 \leq i \leq h} \Gamma_\infty \backslash \Gamma / \Gamma_{c_i}$$

cf. Marklof - Welsh 2021

Roots and Large Sieve :

Large sieve inequality for well-spaced points :

Let $\alpha_1, \alpha_2, \ldots, \alpha_R$ be reals which are distinct mod 1.
Let $\delta > 0$ be such that $\|\alpha_r - \alpha_s\| \geqslant \delta$ for $r \neq s$. Then

$$\sum_{r=1}^{R} \left| \sum_{h=1}^{H} \lambda_h \cdot e(h\alpha_r) \right|^2 \leqslant \left(\frac{1}{\delta} + H \right) \sum_{h=1}^{H} |\lambda_h|^2$$

Large sieve inequality for modular square roots :

Let d be a non-square integer. Then

$$\sum_{N < n < 2N} \sum_{\substack{0 \leq \nu < n \\ \nu^2 \equiv d \pmod{n}}} \left| \sum_{h < H} \lambda_h \, e\left(\frac{h\nu}{n}\right) \right|^2 \ll (N + H) \sum_{h < H} |\lambda_h|^2$$

Fouvry - Iwaniec 1997

Balog - Blomer - Dartyge - Tenenbaum 2012

Variations on a theme :

Let d be a squarefree integer.

Consider $X^2 \equiv d \pmod{n}$ with $n \equiv 0 \pmod{N}$.

How is the sequence of modular square root fractions

$$\frac{\nu}{n}, \quad \nu^2 \equiv d \pmod{n}$$

distributed ?

Parameters : residue / discriminant d, progression N, modulus n.

Different ranges of uniformity in the parameters.

Duke - Friedlander - Iwaniec 2012 : $(d > 0)$

The root fractions

$$\left\{ \frac{\nu}{n} : \nu^2 \equiv d \pmod{n}, \; n \equiv 0 \pmod{N}, \; n \leqslant x \right\}$$

are uniformly distributed mod 1 when $x > d^{\frac{1}{2} - \delta}$, $\delta > 0$.

Dunn - Kerr - Shparlinski - Zaharescu 2020

The root fractions

$$\left\{ \frac{\nu}{n} : \nu^2 \equiv \ell \pmod{n} \text{ for some prime } \ell \leqslant L \right\}$$

are uniformly distributed mod 1 when $L > n^{\frac{13}{20} + \varepsilon}$ (n fixed).

H.N. 2021

The root fractions

$$\left\{ \frac{\nu}{n} : \nu^2 \equiv d \ (\text{mod } n), \ n \equiv 0 \ (\text{mod } N), \ n \leqslant x \right\}$$

are uniformly distributed mod 1 in subintervals I of $[0,1]$ of possibly shrinking length $|I| \gg_\varepsilon \left(\frac{N^2}{x}\right)^{\frac{1}{14}} x^\varepsilon$.

Effective range: $N = O\left(x^{\frac{1}{2}-\delta}\right)$, $\delta > 0$.

$$\frac{\#\text{ root fractions in } I}{\#\text{ root fractions}} \sim |I|$$

THANK YOU !