Almost primes with square digital reverses

Yuta Suzuki (Rikkyo University)

March 8th, 2026
DARF2026 @ University of Tsukuba

Congratulations for retirement,
Prof. Shigeki Akiyama and Prof. Hiroshi Mikawa!

1. Approximations of Landau’s problem with almost primes

Landau's problems

Landau's problems (1912)

1. Are there infinitely many primes of the form $n^2 + 1$?
2. Can every even number > 2 be written as a sum of two primes?
3. Are there infinitely many pair of primes with difference 2?
4. Does there exist a prime between two consecutive positive squares?

Almost prime

Definition 1 (Number of prime factors counted with multiplicity)

$$\Omega(n) := \sum_{p^{\nu} | n} 1 = (\text{number of prime factors of } n \text{ counted with multiplicity}).$$

Definition 2 (Almost prime)

Let $r \in \mathbb{N}$. For $n \in \mathbb{N}$, we say

$$n : r\text{-}\textbf{almost prime} \text{ (or } P_r) \overset{\text{def}}{\iff} \Omega(n) \leq r.$$

Let $\mathscr{P}_r$ be the set of all r-almost primes.

Pairs of almost primes

Theorem 1

We have

$$\#\{n \in \mathbb{N} \mid n \text{ is } P_r \text{ and } n+2 \text{ is } P_s\} = \infty$$

with (the following list is not comprehensive)

$(r, s) = (9, 9)$	by Brun	(1920),
$(r, s) = (7, 7)$	by Rademacher	(1924),
$(r, s) = (6, 6)$	by Estermann	(1936),
$(r, s) = (5, 5)$	by Buchstab	(1938),
$(r, s) = (4, 4)$	by Tartakowski	(1939),
$(r, s) = (1, K)$	by Rényi	(1947),
$(r, s) = (1, 4)$	by Pan Cheng Dong	(1962),
$(r, s) = (1, 3)$	by Buchstab	(1965),
$(r, s) = (1, 2)$	by Chen	(1973).

Almost primes of the form $n^2 + 1$

Theorem 2

We have

$$\#\{n \in \mathbb{N} \mid n^2 + 1 \text{ is } P_r\} = \infty$$

with (the following list might be not comprehensive)

$r = 7$	by Rademacher	(1924),
$r = 5$	by Ricci	(1936),
$r = 3$	by Kuhn	(1953),
$r = 2$	by Iwaniec	(1978).

Local distribution of sequences

Those approximations to Landau's problem were obtained via sieve methods.

The basic settings are: Take sequences

$$\begin{aligned}\mathscr{A} &:= \{n(n+2) \mid n \leq x\},\\ \mathscr{A} &:= \{p+2 \mid p \leq x\},\\ \mathscr{A} &:= \{n^2+1 \mid n \leq x\}\end{aligned}$$

and consider its local distribution

$$\mathscr{A}_d := \{a \in \mathscr{A} \mid a \equiv 0 \pmod{d}\}$$

with expecting the approximation

$$\#\mathscr{A}_d = \rho(d)X + R(d) = (\text{local density}) \cdot X + (\text{remainder})$$

and the error term estimate

$$\sum_{d \leq D} |R(d)| \ll X(\log X)^{-A}.$$

The resulting value of r is affected by the possible size of D. ("level of distribution")

(Note: For some of the preceding result, we need to modify the above setting.)

2. Digital number theory

Digital representation of integers

Take

$$b \in \mathbb{Z}_{\geq 2}$$

as the base of the digital representation of integers.

Base-b representation

Every $n \in \mathbb{Z}_{\geq 0}$ is uniquely represented as

$$n = \sum_{i \geq 0} \varepsilon_i(n) b^i \quad \text{with} \quad \varepsilon_i(n) \in \{0, \ldots, b-1\}.$$

For the above base-b representation of n,

- The number $\varepsilon_i(n)$ is called the i-th **digit** of n.
- We define the **length** $\operatorname{len}(n)$ of n by

$$\operatorname{len}(n) \coloneqq \min\{\ell \in \mathbb{Z}_{\geq 0} \mid \varepsilon_i(n) = 0 \text{ for all } i \geq \ell\}.$$

- In real life, we usually write

$$(\varepsilon_{\operatorname{len}(n)-1}(n) \cdots \varepsilon_0(n))_{(b)} \coloneqq \sum_{0 \leq i < \operatorname{len}(n)} \varepsilon_i(n) b^i.$$

Sum-of-digits function

Definition 3 (Sum-of-digits function)

$$s(n) = s_b(n) := \sum_{i \geq 0} \varepsilon_i(n) = (\text{sum of the digits of } n).$$

Theorem 3 (Gelfond (1968))

For $a, q \in \mathbb{N}$ with $(q, b-1) = 1$, we have

$$\#\{n \leq x \mid s(n) \equiv a \pmod{q}\} = \frac{x}{q} + O(x^{\theta(q)})$$

where

$$\theta(q) := \frac{1}{2 \log b} \log\left(\frac{b \sin \frac{\pi}{2q}}{\sin \frac{\pi}{2qb}}\right) \in (0, 1).$$

Gelfond's problems

Gelfond's problems (1968)

1. Joint distribution of $s(n)$ for different basis: Prove

$$\#\{n \leq x \mid s_{b_i}(n) \equiv a_i \pmod{q_i} \text{ for } i = 1, 2\} = \frac{x}{q_1 q_2} + O(x^{\theta})$$

with $\theta \in (0,1)$ provided $(b_1, b_2) = (q_1, b_1 - 1) = (q_2, b_2 - 1) = 1$.
$\rightsquigarrow$ Proved by Bésineau (1972) and D. H. Kim (1999).

2. Distribution of $s(n)$ over primes: Get an asymptotic formula for

$$\#\{p \leq x \mid s(p) \equiv a \pmod{q}\}.$$

$\rightsquigarrow$ Solved by Mauduit–Rivat (2010).

3. Distribution of $s(n)$ over polynomial: Get an asymptotic formula for

$$\#\{n \leq x \mid s(f(n)) \equiv a \pmod{q}\}$$

with a given polynomial $f(X) \in \mathbb{Z}[X]$.
$\rightsquigarrow$ General case is unsolved.

Gelfond's third problem

Get an asymptotic formula for

$$\#\{n \leq x \mid s(f(n)) \equiv a \pmod{q}\}$$

with a given polynomial $f(X) \in \mathbb{Z}[X]$.

Theorem 4 (Mauduit–Rivat (2009))

For $b \geq 2$, $f(X) \in \mathbb{Z}[X]$ with $\deg f = 2$, we have

$$\#\{n \leq x \mid s(f(n)) \equiv a \pmod{q}\} = \frac{\rho(q)}{q} x + O(x^{1-\sigma_b(q)})$$

with some $\sigma_b(q) > 0$ provided the leading coefficient of f is coprime to q, where

$$\rho(q) := \#\{u \pmod{q} \mid f(u) \equiv a \pmod{(q, b-1)}\}.$$

Theorem 5 (Drmota–Mauduit–Rivat (2011))

The above result holds for any $f(X) \in \mathbb{Z}[X]$ with $\deg f \geq 1$ provided $b \geq b_0(\deg f)$.

Digital reverse of integers

Definition 4 (Digital reverse)

For $n \in \mathbb{Z}_{\geq 0}$ with the base-b representation

$$n = (\varepsilon_{\mathrm{len}(n)-1}(n) \cdots \varepsilon_0(n))_{(b)} = \sum_{0 \leq i < \mathrm{len}(n)} \varepsilon_i(n) b^i,$$

we define its **digital reverse** $\mathrm{rev}(n)$ by

$$\mathrm{rev}(n) \coloneqq (\varepsilon_0(n) \cdots \varepsilon_{\mathrm{len}(n)-1}(n))_{(b)}$$

i.e. $\mathrm{rev}(n)$ is the integer obtained by reading n "backwards". We may also write

$$\mathrm{rev}(n) = \sum_{0 \leq i < \mathrm{len}(n)} \varepsilon_{\mathrm{len}(n)-i-1}(n) b^i = \sum_{0 \leq i < \mathrm{len}(n)} \varepsilon_i(n) b^{\mathrm{len}(n)-i-1}.$$

Digital reverse analogues?

For twin prime problem

$$\#\{p \leq x \mid p+2 : \text{prime}\} \overset{?}{=} \infty,$$

by replacing "$\bullet + 2$" by "rev($\bullet$)", we get the following conjecture

Conjecture 1 (Reversible prime conjecture)

$$\#\{p \mid \mathrm{rev}(p) : \text{prime}\} \overset{?}{=} \infty.$$

For Landau's first problem

$$\#\{n \leq x \mid n^2+1 : \text{prime}\} \overset{?}{=} \infty,$$

by replacing "$\bullet + 1$" by "rev($\bullet$)", we get the following conjecture

Conjecture 2

$$\#\{n \in \mathbb{N} \mid \mathrm{rev}(n^2) : \text{prime}\} \overset{?}{=} \infty.$$

A small pitfall!

Let $b = 10$. Note that

$$\mathrm{rev}((40\cdots0)^2) = \mathrm{rev}(160\cdots0) = 61 \leftarrow \text{prime!}$$

so the last conjecture is trivial for $b = 10$.
(It seems not clear if we can get the same phenomenon for general b.)

We thus modify the conjecture as

Conjecture 2

$$\#\{p \mid \mathrm{rev}(p) : \text{square}\} \overset{?}{=} \infty.$$

Local distribution of reversed primes

Let us call the integers of the form $\mathrm{rev}(p)$ the “reversed primes”.

To apply the sieve methods to get approximations of the reversed prime conjecture with almost primes, we need to study the local distribution of reversed primes.

An analogue of the Siegel–Walfisz theorem is given by

Theorem 6 (Dartyge–Rivat–Swaenepoel (2025), Bhowmik–S. (2025))

For any base $b \geq 2$ and $a, q \in \mathbb{N}$ satisfying $(q, b(b^2 - 1)) = 1$, we have

$$\overleftarrow{\pi}(x, a, q) = \frac{1}{q}\pi(x) + O_b(x \exp(-c\sqrt{\log x})),$$

where

$$\overleftarrow{\pi}(x, a, q) := \#\{p \leq x \mid \mathrm{rev}(p) \equiv a \pmod{q}\} \quad \text{and} \quad \pi(x) := \#\{p \leq x\}$$

and $c = c_b > 0$ is some constant.

Local distribution of reversed primes on average

An analog of the Bombieri–Vinogradov theorem has been already obtained!

Theorem 7 (Dartyge–Rivat–Swaenepoel (2025))

For any base $b \geq 2$, there is $\theta_{\mathrm{DRS}} = \theta_{\mathrm{DRS},b} > 0$ such that

$$\sum_{\substack{q \leq Q \\ (q, b(b^2-1))=1}} \max_{a \pmod{q}} \left| \overleftarrow{\pi}(x, a, q) - \frac{1}{q}\pi(x) \right| \ll x \exp(-c\sqrt{\log x})$$

for $Q \leq x^{\theta_{\mathrm{DRS},b} - \varepsilon}$, where the implicit constant and $c > 0$ depend on b and $\varepsilon > 0$.

As for the level of distribution, for example, DRS obtained $\theta_{\mathrm{DRS},10} = 0.00072623\ldots$

As a corollary (via a linear weighted sieve), we have

Theorem 8 (Dartyge–Rivat–Swaenepoel (2025))

For any base $b \geq 2$, there is $r_b \in \mathbb{N}$ such that

$$\#\{p \mid \mathrm{rev}(p) : r_b\text{-almost prime}\} = \infty.$$

As for the value of r_b, for example, DRS obtained $r_{10} = 1378$.

Related problem: Palindromic prime problem

Definition 5 (Palindromic number)

$$n \text{ is } \textbf{palindromic} \overset{\text{def}}{\iff} n = \mathrm{rev}(n).$$

Conjecture 3 (Palindromic prime conjecture)

$$\#\{p \mid \mathrm{rev}(p) = p\} \overset{?}{=} \infty.$$

Theorem 9 (Tuxanidy–Panario (2024))

For any base $b \geq 2$, we have

$$\#\{n \mid n : 6\text{-almost prime and } \mathrm{rev}(n) = n\} = \infty.$$

This is also obtained via the sieve method with the Bombieri–Vinogradov type result.

3. Almost primes with square digital reverse

Local distribution of $\mathrm{rev}(n^2)$ on average

Let

$$\overleftarrow{Q}_0(x, a, q) := \#\{n \le x \mid \mathrm{rev}(n^2) \equiv a \pmod{q} \text{ and } (n, b(b^2-1)) = 1\}.$$

Main Theorem 1 (S. (2026+))

For $b \ge 700$, there is $\theta_b > 0$ such that

$$\sum_{\substack{q \le Q \\ (q, b(b^2-1))=1}} \max_{1 \le a \le q} \left| \overleftarrow{Q}_0(x, a, q) - \frac{\phi(b(b^2-1))}{b(b^2-1)} \frac{x}{q} \right| \ll x \exp(-c\sqrt{\log x})$$

for $Q \le x^{\theta_b - \varepsilon}$, where the implicit constant and $c > 0$ depend only on b and $\varepsilon > 0$.

The value of θ_b is effectively computable.

Almost primes with square digital reverses

By combining the previous equidistribution result with a linear sieve, we get:

Main Theorem 2 (S. (2026+))

For $b \geq 700$, we have

$$\#\{n \in \mathbb{N} \mid n : \ r_b\text{-almost prime and } \mathrm{rev}(n) \text{ is square}\} = \infty$$

with

$$r_b := \left[\frac{4}{\theta_b}\right].$$

Note: The above "4" is just (sieving limit of linear sieve) × (the exponent of n^2).

The value of θ_b

We can calculate the value of θ_b using the results of Dartyge–Rivat–Swaenepoel.

Write $e(x) := \exp(2\pi i x)$. Let

$$\phi(x) = \phi_b(x) := \frac{1}{b} \sum_{0 \le n < b} e(\alpha n),$$

$$\psi_b(x) := \sum_{0 \le h < b} \left| \phi_b\left(\frac{h}{b} + x \right) \right| \quad \text{and} \quad T_{b,\kappa}(\alpha) := \frac{1}{b} \sum_{0 \le h < b} \left| \phi_b\left(\frac{1}{b+1} \left\| \frac{h+x}{b} \right\| \right) \right|^{\kappa}.$$

For $\kappa > 0$, we then let

$$\max_{x \in \mathbb{R}} |\psi_b(x)| = b^{\eta_b} \quad \text{and} \quad \max_{x \in \mathbb{R}} |T_{b,\kappa}(x)| = b^{-\zeta_{b,\kappa}}.$$

We further let

$$\kappa_b := \min\{\kappa \in \mathbb{Z}_{\ge 0} \mid 1 - \zeta_{b,1} - \zeta_{b,\kappa} < 0\}$$

which exists since $\zeta_{b,\kappa} \to 1$ as $\kappa \to \infty$.

The value of θ_b in the main theorems is then effectively computable as

$$\theta_b = \frac{1 - 4\eta_b}{2 + (1 - 2\eta_b)(\kappa_b + 1)}.$$

Numerical values (calculated just two hours ago)

According to some numerical calculation (without error estimate):

$$\begin{aligned}
\theta_{700} &\geq 5.683232019873788^{-11} \qquad \text{and} \quad r_{700} \leq 70382486338, \\
\theta_{800} &\geq 3.8913576117383143^{-10} \quad \text{and} \quad r_{800} \leq 10279188908, \\
\theta_{900} &\geq 5.390281537700084^{-10} \qquad \text{and} \quad r_{900} \leq 7420762667, \\
\theta_{1000} &\geq 5.987019309772515^{-10} \qquad \text{and} \quad r_{1000} \leq 6681120926.
\end{aligned}$$

4. Sketch of the proof

The method

The method is a combination of

- Maynard's argument with the discrete circle method used for the result below,
- The tools of Dartyge–Rivat–Swaenepoel to take the average over moduli.

Theorem 10 (Maynard (2015))

For $b \geq 2000000$ and $a_0 \in \{0, \dots, b-1\}$, we have

$$\#\{p \mid a_0 \notin \{\text{digits of } p\}\} = \infty$$

with a certain asymptotic formula for the counting function of the left-hand side.

Maynard (2016) obtained the above infinitude for $b \geq 10$ by a different argument.

Preparation

For simplicity, we ignore the condition $(n, b(b^2-1)) = 1$ in

$$\overleftarrow{Q}_0(x,a,q) \coloneqq \#\{n \le x \mid \operatorname{rev}(n^2) \equiv a \pmod{q} \text{ and } (n, b(b^2-1)) = 1\}$$

so we consider instead

$$\overleftarrow{Q}(x,a,q) \coloneqq \#\{n \le x \mid \operatorname{rev}(n^2) \equiv a \pmod{q}\}.$$

Also, instead of rev, we use the function

$$f_\lambda(n) \coloneqq \sum_{0 \le i < \lambda} \varepsilon_i(n) b^{\lambda-i-1} \quad \text{with} \quad \lambda \in \{2\xi-1, 2\xi\}.$$

Note that rev and f_λ are essentially the same since

$$n \in [b^{\lambda-1}, b^\lambda), \text{ i.e. } \operatorname{len}(n) = \lambda \implies f_\lambda(n) = \operatorname{rev}(n).$$

Orthogonality

Write $e(x) \coloneqq \exp(2\pi i x)$. Assume $b^{\xi-1} \le x < b^{\xi}$. Let

$$S(\alpha) \coloneqq \sum_{n<x} e(\alpha f_\lambda(n^2)).$$

By the orthogonality, we get

$$\overleftarrow{Q}(x,a,q) - \frac{x}{q} = \frac{1}{q} \sum_{1\le h<q} S\left(\frac{h}{q}\right) e\left(-\frac{ha}{q}\right) + O\left(\frac{1}{q}\right).$$

Thus, by reducing the fraction as $h/q \rightsquigarrow k/d$ with $(k,d)=1$, we essentially have

$$\begin{aligned}\sum_{\substack{q\le Q\\(q,b(b^2-1))=1}} \max_{1\le a\le q}\left|\overleftarrow{Q}(x,a,q) - \frac{x}{q}\right| &\ll (\log x) \sum_{\substack{d\le Q\\(d,b(b^2-1))=1}} \frac{1}{d} \sideset{}{^*}\sum_{k \pmod d}\left|S\left(\frac{k}{d}\right)\right|\\ &\ll (\log x)^2 \max_{1\le D\le Q} D^{-1} \sum_{\substack{D\le d<2D\\(d,b(b^2-1))=1}} \sideset{}{^*}\sum_{k \pmod d}\left|S\left(\frac{k}{d}\right)\right|.\end{aligned}$$

Discrete circle method: Farey dissection

Recall

$$S(\alpha) \coloneqq \sum_{n<x} e(\alpha f_\lambda(n^2)).$$

We then introduce the exponential sums

$$W(\alpha) \coloneqq \sum_{n\leq x} e(\alpha n^2) \quad \text{and} \quad F_\lambda(\alpha,\beta) \coloneqq \frac{1}{b^\lambda} \sum_{0\leq n<b^\lambda} e(\alpha f_\lambda(n) - \beta n).$$

By the orthogonality again, we get

$$S\left(\frac{k}{d}\right) = \sum_{0\leq h<b^\lambda} W\left(\frac{h}{b^\lambda}\right) F_\lambda\left(\frac{k}{d}, \frac{h}{b^\lambda}\right).$$

By using Dirichlet's approximation theorem, we write

$$\frac{h}{b^\lambda} = \frac{a}{q} + \gamma \quad \text{with} \quad a, q \in \mathbb{Z},\ (a,q)=1,\ q\geq 1,\ |\gamma| \leq \frac{1}{qQ}.$$

This gives

$$\left|S\left(\frac{k}{d}\right)\right| \ll \sum_{q\leq Q} \sideset{}{^*}\sum_{a \pmod q} \sum_{\substack{|\gamma|<\frac{1}{qQ} \\ b^\lambda(\frac{a}{q}+\gamma)\in\mathbb{Z}}} \left| W\left(\frac{a}{q}+\gamma\right) F_\lambda\left(\frac{k}{d}, \frac{a}{q}+\gamma\right)\right|.$$

Product formula

The usual square-root cancellation may imply that the above circle method fails.

However, the key for the digital problem is that the exponential sum $F(\alpha, \beta)$ has a very nice structure so that we can expect bounds better than the square-root cancellation.

Lemma 1 (Product formula)

$$F_\lambda(\alpha, \beta) = \prod_{0 \le i < \lambda} \phi(\alpha b^{\lambda-i-1} - \beta b^i) \quad \text{with} \quad \phi(\alpha) := \frac{1}{b} \sum_{0 \le n < b} e(\alpha n).$$

Lemma 2 (Split formula)

$$F_\lambda(\alpha, \beta) = F_\kappa(\alpha b^{\lambda-\kappa}, \beta) F_{\lambda-\kappa}(\alpha, \beta b^\kappa) \quad \text{for} \quad 0 \le \kappa \le \lambda.$$

A uniform bound and L^∞-bound for $F_\lambda(\alpha, \beta)$

Definition 6

For $\lambda \in \mathbb{Z}_{\geq 0}$ and $\alpha \in \mathbb{R}$, let

$$G_\lambda(\alpha) := \left(\prod_{0 \leq i < \lambda} \left| \phi\left(\frac{\|\alpha b^i\|}{b+1} \right) \right| \right)^{\frac{1}{2}} > 0.$$

By using basic properties of $\phi(\alpha)$ and the identity

$$b(\alpha b^{\lambda-i-1} - \beta b^i) - \alpha b^{\lambda-(i+1)-1} - \beta b^{i+1} = \alpha(b^2-1)b^{\lambda-(i+1)-1},$$

we can remove the effect of β to get

Lemma 3

$$F_\lambda(\alpha, \beta) \ll G_\lambda(\alpha(b^2-1))$$

By considering the distribution of αb^i (mod 1), we further get

Lemma 4 (L^∞-bound)

$$F_\lambda\left(\frac{k}{d}, \beta\right) \ll x^{-\frac{\Upsilon_b}{\log d}} \quad \text{with some} \quad \Upsilon_b > 0 \quad \text{provided} \quad (d, b(b^2-1)) = 1.$$

L^1-bound for $F_\lambda(\alpha,\beta)$

Recall

$$\max_{x\in\mathbb{R}} \sum_{0\le h<b} \left|\phi_b\left(\frac{h}{b}+x\right)\right| = b^{\eta_b} \quad \text{and} \quad F_\lambda(\alpha,\beta) = \prod_{0\le i<\lambda} \phi(\alpha b^{\lambda-i-1} - \beta b^i).$$

We then have

$$\begin{aligned}\int_0^1 |F_\lambda(\alpha,\beta)| d\beta &= \int_0^1 |\phi(\alpha b^{\lambda-1} - \beta)||F_{\lambda-1}(\alpha,\beta b)| d\beta \\ &= \sum_{0\le h<b} \int_0^{\frac{1}{b}} \left|\phi\left(\alpha b^{\lambda-1} - \left(\frac{h}{b}+\beta\right)\right)\right| |F_{\lambda-1}(\alpha,\beta b)| d\beta \\ &= \int_0^1 \left(\sum_{0\le h<b} \left|\phi\left(\alpha b^{\lambda-1} - \left(\frac{h+\beta}{b}\right)\right)\right|\right) |F_{\lambda-1}(\alpha,\beta)| d\beta.\end{aligned}$$

By iterating this estimate, we get

Lemma 5 (L^1-bound)

$$\int_0^1 |F_\lambda(\alpha,\beta)| d\beta \ll x^{\eta_b}.$$

Gallagher–Sobolev + Bernstein–Zygmund

Lemma 6 (Gallagher–Sobolev + Bernstein–Zygmund)

Consider a Fourier polynomial with complex coefficients

$$f(\alpha) = \sum_{|n|\leq N} a(n)e(\alpha n).$$

Let $\delta > 0$ and $(\alpha_i)_{i=1}^R$ be a sequence of real numbers which is δ-spaced (mod 1), i.e.

$$\|\alpha_i - \alpha_j\| \geq \delta \quad \text{for any} \quad i, j \in \{1, \ldots, R\} \text{ with } i \neq j.$$

We then have

$$\sum_{i=1}^{R} |f(\alpha_i)| \leq \left(\frac{1}{\delta} + \pi N\right) \int_0^1 |f(\alpha)| d\alpha.$$

Note: To get better effect, it is better to adjust the length N as $N \asymp \frac{1}{\delta}$.

Moment of $G_\lambda(\alpha)$

Lemma 7 (Dartyge–Rivat–Swaenepoel (2025))

Let $\theta, \Delta, \kappa \in \mathbb{Z}_{\geq 0}$ and $(\alpha_i)_{i=1}^N$ be a sequence of real numbers such that

1. For $0 \leq \ell \leq \kappa$, the sequence $(\alpha_i b^{\ell\theta})_{i=1}^N$ is $b^{-\theta}$-well spaced (mod 1), i.e.
$$\|(\alpha_i - \alpha_j) b^{\ell\theta}\| \geq b^{-\theta} \quad \text{for all } i, j \in \{1, \ldots, N\} \text{ with } i \neq j.$$
2. We have $(\kappa + 1)\theta \leq \Delta$.

We then have
$$\sum_{i=1}^N G_\Delta(\alpha_i) \ll (\kappa+2)^{\frac{1}{2}} b^{\frac{1}{2}(2-\zeta_{b,1}-\zeta_{b,\kappa})\theta}$$

Our choice of $(\alpha_i)_{i=1}^N$ will be

$$k/d \quad \text{with} \quad k, d \in \mathbb{Z},\ 1 \leq k \leq d,\ D \leq d < 2D,\ (k,d) = 1,\ (d, b(b^2-1)) = 1.$$

By writing $D = b^\delta$, this gives $\theta = 2\delta$ and so

$$\sum_{D \leq d < 2D} \sideset{}{^*}\sum_{k \pmod d} G_\Delta\left(\frac{k}{d}\right) \ll_\kappa b^{(2-\zeta_{b,1}-\zeta_{b,\kappa})\delta} = D^{2-\zeta_{b,1}-\zeta_{b,\kappa}}.$$

Estimate for the quadratic Weyl sum

For the quadratic Weyl sum, we use the standard bound

Theorem 11 (Weyl bound)

For a, q, γ with

$$a, q \in \mathbb{Z},\ \gamma \in \mathbb{R},\ q \geq 1,\ (a, q) = 1,\ |\gamma| \leq \frac{1}{q^2},$$

we have

$$W\left(\frac{a}{q} + \gamma\right) \ll \left(q^{-\frac{1}{2}} \min(x, |\gamma|^{-\frac{1}{2}}) + q^{\frac{1}{2}} x \min(x, |\gamma|^{-\frac{1}{2}})^{-1}\right)(\log 2x)^{\frac{1}{2}},$$

where the implicit constant is absolute.

Note: We need to take care of the decay caused by γ.

Estimate for small modulus: Major arc part

The bound for small modulus follows essentially from Mauduit–Rivat (2009).

Let $D_0 := \exp(c_0\sqrt{\log x})$ and we treat those d with $d \le D_0$ as "small".
In this case, we estimate the sum over k/d trivially.

For the "major arc" part

$$\max(q, b^\lambda|\gamma|) \le P := \exp(c_1\sqrt{\log x}),$$

we use L^∞-bound of $F_\lambda(\alpha,\beta)$ and the trivial bound of $W(\alpha)$ to get

$$D^{-1}\sum_{D\le d<2D}\ \sideset{}{^*}\sum_{k \pmod d}\ \sum_{q\le P}\ \sideset{}{^*}\sum_{a \pmod q}\ \sum_{\substack{b^\lambda|\gamma|<P\\ |\gamma|<\frac{1}{qQ}\\ b^\lambda(\frac{a}{q}+\gamma)\in\mathbb{Z}}} \left|W\left(\frac{a}{q}+\gamma\right)F_\lambda\left(\frac{k}{d},\frac{a}{q}+\gamma\right)\right|$$

$$\ll D_0P^3x^{1-\frac{\Upsilon_b}{\log D_0}} \ll x\exp(-c_2\sqrt{\log x}).$$

Estimate for small modulus: Minor arc part

For a part of minor arc part

$$q \asymp R, \quad b^{\lambda}|\gamma| \asymp H, \quad \max(R, H) > P,$$

we decompose $F_{\lambda}(\alpha, \beta)$ by using the split formula as

$$F_{\lambda}(\alpha, \beta) = F_{\rho} F_{\ell} F_{\lambda-(\rho+\ell)} \quad \text{with} \quad b^{\rho} \asymp R^2 \quad \text{and} \quad b^{\ell} \asymp H$$

and use

- The L^1-bound for F_{ρ} with the sequence a/q.
- The L^1-bound for F_{ℓ} with the sequence γ.
- The trivial bound for $F_{\lambda-(\rho+\ell)}$.
- The Weyl bound for $W(\alpha)$.

After some calculations, this gives

$$D^{-1} \sum_{D \le d < 2D} \sideset{}{^*}\sum_{k \pmod{d}} \sum_{q \le P} \sideset{}{^*}\sum_{a \pmod{q}} \sum_{\substack{b^{\lambda}|\gamma| < P \\ |\gamma| < \frac{1}{qQ} \\ b^{\lambda}(\frac{a}{q}+\gamma) \in \mathbb{Z}}} \left| W\left(\frac{a}{q} + \gamma\right) F_{\lambda}\left(\frac{k}{d}, \frac{a}{q} + \gamma\right) \right|$$

$$\ll D_0 x R^{-(\frac{1}{2} - 2\eta_b)} (\log x)^{\frac{1}{2}} \ll D_0 x P^{-(\frac{1}{2} - 2\eta_b)} (\log x)^{\frac{1}{2}} \ll x \exp(-c_2 \sqrt{\log x})$$

provided c_0 is sufficiently small compared to c_1.

Estimate for large modulus: Major arc part

For large $D \geq D_0$, we work similarly to the minor arc estimate for small d.

For a part of minor arc part

$$q \asymp R, \quad b^{\lambda}|\gamma| \asymp H, \quad \max(R, H) > P,$$

we decompose $F_\lambda(\alpha, \beta)$ by using the split formula as

$$F_\lambda(\alpha, \beta) = F_\rho F_\ell F_{\lambda-(\rho+\ell)} \quad \text{with} \quad b^\rho \asymp R^2 \quad \text{and} \quad b^\ell \asymp H$$

and use

- The L^1-bound for F_ρ with the sequence a/q.
- The L^1-bound for F_ℓ with the sequence γ.
- The uniform bound $F_{\lambda-(\rho+\ell)} \leq G_{\lambda-(\rho+\ell)}$ and the moment bound of $G_{\lambda-(\rho+\ell)}$ if possible, i.e. $\lambda - (\rho + \ell) \geq \Delta := 2(\kappa_b + 1)\delta$.
- The Weyl bound for $W(\alpha)$.

If the condition $\lambda - (\rho + \ell) \geq \Delta$ does not hold, we have large R and H so the average over a/q and γ produce enough cancellation.