# Telhcirid's theorem on arithmetic progressions

Yuta Suzuki (Rikkyo University)
joint work with Gautami Bhowmik (University of Lille)

October 17th, 2024

RIMS Workshop 2024
Analytic Number Theory and Related Topics

Dirichlet (1805–1859)

Telhcirid (5081–9581)

# 1. Digital properties of prime numbers

Take

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

as the base of the radix representation of integers.

## Base-$g$ representation

Every $n \in \mathbb{N}$ is uniquely represented as

$$n = \sum_{0 \leq i < N} n_i g^i =: (n_{N-1} \cdots n_0)_{(g)}$$

with

$$n_0, \ldots, n_{N-1} \in \{0, \ldots, g-1\} \quad \text{and} \quad n_{N-1} \neq 0.$$

For the above base-$g$ representation of $n$,

- The numbers $n_0, \ldots, n_{N-1}$ are called the *digits* of $n$.
- The number $N$ is called the *length* of $n$.

Notation: In this talk, the letter $p$ always denotes a prime.

## Theorem 1 (Mauduit–Rivat (2010))

For any base $g \in \mathbb{Z}_{\geq 2}$ and $a, q \in \mathbb{N}$ satisfying

$$(a, q, g-1) = 1,$$

we have

$$\#\{p \mid (\text{sum of digits of } p) \equiv a \pmod{q}\} = \infty.$$

Note: (sum of digits of $p$) $\equiv p \pmod{g-1}$.

## Theorem 2 (Maynard (2022))

For any base $g \geq 10$ and $a_0 \in \{0, \ldots, g-1\}$, we have

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

(An asymptotic formula is also obtained if $g \geq 12$.)

Asymptotic formulas are also obtained for both of the above results.

## Definition 1 (Digital reverse)

For $n \in \mathbb{N}$ with the base-$g$ representation

$$n = (n_{N-1} \cdots n_0)_{(g)} = \sum_{0 \le i < N} n_i g^i \quad \text{with} \quad \begin{cases} n_0, \ldots, n_{N-1} \in \{0, \ldots, g-1\}, \\ n_{N-1} \neq 0, \end{cases}$$

we define its **digital reverse** $\overleftarrow{n}$ by

$$\overleftarrow{n} := (n_0 \cdots n_{N-1})_{(g)} = \sum_{0 \le i < N} n_{N-i-1} g^i = \sum_{0 \le i < N} n_i g^{N-i-1},$$

i.e. $\overleftarrow{n}$ is the integer obtained by reading $n$ "backwards".

## Definition 2 (Palindromic number (回文数))

$$n \text{ is } \textbf{palindromic} \overset{\text{def}}{\iff} n = \overleftarrow{n}.$$

## Conjecture 1

There are infinitely many palindromic primes, i.e.

$$\#\{p \mid p = \overleftarrow{p}\} = \infty.$$

(A **palindromic prime** is a prime which is palindromic.)

## Conjecture 2

There are infinitely many primes whose digital reverse is also prime, i.e.

$$\#\{p \mid \overleftarrow{p} : \text{prime}\} = \infty.$$

(A **reversible prime** is a prime whose digital reverse is also a prime.)

## Theorem 3 (Tuxanidy–Panario (2023))

For any $g \geq 2$, there are infinitely many palindromic 6-almost primes, i.e.

$$\#\{n \mid n = \overleftarrow{n} \text{ and } \Omega(n) \leq 6\} = \infty,$$

where $\Omega(n)$ is the number of prime factors of $n$ counted with multiplicity.

# 2. Main Results

## Theorem 4 (Dirichlet's theorem on A.P. (1837))

For any $a, q \in \mathbb{N}$ satisfying

$$(a, q) = 1,$$

we have

$$\#\{p \mid p \equiv a \pmod{q}\} = \infty.$$

## Theorem 4 (Dirichlet's theorem on A.P. (1837))

For any $a, q \in \mathbb{N}$ satisfying

$$(a, q) = 1,$$

we have

$$\#\{p \mid p \equiv a \pmod{q}\} = \infty.$$

## Main Theorem 1 (Telhcirid's theorem on A.P. by Bhowmik–S. (2024+))

For any base $g \geq 31699$ and $a, q \in \mathbb{N}$ satisfying

$$(*) \qquad (a, q, g^2 - 1) = 1 \quad \text{and} \quad g \nmid (a, q),$$

we have

$$\#\{p \mid \overleftarrow{p} \equiv a \pmod{q}\} = \infty.$$

## Theorem 4 (Dirichlet's theorem on A.P. (1837))

For any $a, q \in \mathbb{N}$ satisfying

$$(a, q) = 1,$$

we have

$$\#\{p \mid p \equiv a \pmod{q}\} = \infty.$$

## Main Theorem 1 (Telhcirid's theorem on A.P. by Bhowmik–S. (2024+))

For any base $g \geq 31699$ and $a, q \in \mathbb{N}$ satisfying

$$(*) \qquad (a, q, g^2 - 1) = 1 \quad \text{and} \quad g \nmid (a, q),$$

we have

$$\#\{p \mid \overleftarrow{p} \equiv a \pmod{q}\} = \infty.$$

We use decimal (base-10) representation in everyday life because we have 10 fingers in our hands.

## Theorem 4 (Dirichlet's theorem on A.P. (1837))

For any $a, q \in \mathbb{N}$ satisfying

$$(a, q) = 1,$$

we have

$$\#\{p \mid p \equiv a \pmod{q}\} = \infty.$$

## Main Theorem 1 (Telhcirid's theorem on A.P. by Bhowmik–S. (2024+))

For any base $g \geq 31699$ and $a, q \in \mathbb{N}$ satisfying

$$(*) \qquad (a, q, g^2 - 1) = 1 \quad \text{and} \quad g \nmid (a, q),$$

we have

$$\#\{p \mid \overleftarrow{p} \equiv a \pmod{q}\} = \infty.$$

We use decimal (base-10) representation in everyday life because we have 10 fingers in our hands. If we had $\geq 31699$ fingers in our hands...

## Theorem 4 (Dirichlet's theorem on A.P. (1837))

For any $a, q \in \mathbb{N}$ satisfying

$$(a, q) = 1,$$

we have

$$\#\{p \mid p \equiv a \pmod{q}\} = \infty.$$

## Main Theorem 1 (Telhcirid's theorem on A.P. by Bhowmik–S. (2024+))

For any base $g \geq 31699$ and $a, q \in \mathbb{N}$ satisfying

$$(*) \qquad (a, q, g^2 - 1) = 1 \quad \text{and} \quad g \nmid (a, q),$$

we have

$$\#\{p \mid \overleftarrow{p} \equiv a \pmod{q}\} = \infty.$$

We use decimal (base-10) representation in everyday life because we have 10 fingers in our hands. If we had $\geq 31699$ fingers in our hands...

$\rightsquigarrow$ Senju-Kannon (千手観音): A goddess of mercy in Bhuddhism having 1000 hands!

# Oh... is it a scam?

But the statue of Senju-Kannon in Sanjusangendo (in Kyoto) has only 42 hands so

$$42 \times 5 = 210$$

fingers...

# Ah! That's enough!

Still, there are 1001 Senju-Kannon statues in Sanjusangendo so

$$42 \times 5 \times 1001 = 210210 > 31699$$

fingers! So let's use base-210210 representation with the aid of Senju-KannonS.

## Main Theorem 1 (Telhcirid's theorem on A.P. by Bhowmik–S. (2024+))

For any base $g \geq 31699$ and $a, q \in \mathbb{N}$ satisfying

$$(*) \qquad (a, q, g^2 - 1) = 1 \quad \text{and} \quad g \nmid (a, q),$$

we have

$$\#\{p \mid \overleftarrow{p} \equiv a \pmod{q}\} = \infty.$$

## Why do we need the conditions $(*)$?

- By definition, $\overleftarrow{p}$'s lowest digit is $\neq 0$. Thus,

$$\overleftarrow{p} \not\equiv 0 \pmod{g} \text{ and } \overleftarrow{p} \equiv a \pmod{q} \quad \rightsquigarrow \quad g \nmid (a, q).$$

- By using $g^{-1} \equiv g \pmod{g^2 - 1}$, we get

$$p = \sum_{0 \leq i < N} n_i g^i \equiv g^{-(N-1)} \sum_{0 \leq i < N} n_i g^{N-i-1} = g^{-(N-1)} \overleftarrow{p} \pmod{g^2 - 1}$$

and so

$$\overleftarrow{p} \equiv a \pmod{q} \quad \rightsquigarrow \quad p \equiv g^{-(N-1)} a \pmod{(q, g^2 - 1)} \quad \rightsquigarrow \quad (a, q, g^2 - 1) = 1.$$

Let

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

Also, let $\varphi$ be the Euler totient function.

## Theorem 5 (Siegel–Walfisz theorem (1936))

For any $a, q \in \mathbb{N}$ with $(a, q) = 1$ and $x, A \geq 1$, we have

$$\pi(x; a, q) = \frac{1}{\varphi(q)}\pi(x) + O_A(\pi(x)(\log x)^{-A}).$$

Note that this result is meaningful only for $q \leq (\log x)^A$ (roughly).

Let

$$\mathscr{G}_N := \{n \in [g^{N-1}, g^N) \mid n \not\equiv 0 \pmod{g}\},$$
$$\overleftarrow{\pi}_N(a,q) := \#\{p \in \mathscr{G}_N \mid \overleftarrow{p} \equiv a \pmod{q}\}.$$

We then have the following quantitative result:

## Main Theorem 2 (Zsiflaw–Legeis theorem by Bhowmik–S. (2024+))

For any base $g \geq 31699$ and $a, q \in \mathbb{N}$ satisfying

$$(*) \qquad (a, q, g^2 - 1) = 1 \quad \text{and} \quad g \nmid (a, q),$$

we have

$$\overleftarrow{\pi}_N(a,q) = \frac{\rho_g(a,q)}{q} \frac{g^N}{\log(g^N)} \left(1 + O\left(\frac{1}{N}\right)\right) + O_g(g^N \exp(-c\sqrt{N})),$$

where $c = c(g) > 0$ is some constant and

$$\rho_g(a,q) := \left(1 - \mathbb{1}_{(q,g)|a} \frac{(q,g)}{g}\right) \frac{(q, g^2-1)}{\varphi((q, g^2-1))}.$$

Note that this result is meaningful only for $q \leq \exp(c\sqrt{N})$ (roughly).

# Comparison: Siegel–Walfisz vs. Zsiflaw–Legeis

| | Siegel–Walfisz | | Zsiflaw–Legeis |
|---|---|---|---|
| Length $L$ of the range | $x$ | $\leftrightsquigarrow$ | $g^N$ |
| $\log L$ | $\log x$ | $\leftrightsquigarrow$ | $N$ |
| Admissible level of S–W | $(\log x)^A$ | $\leftrightsquigarrow$ | $N^A$ |
| Admissible level of Z–L | $\exp(c\sqrt{\log x})$ | $\leftrightsquigarrow$ | $\exp(c\sqrt{N})$ |

- Zsiflaw–Legeis has a wider range of modulus than Siegel–Walfisz!
- The implication is (probably)

  "*primality and digital property are rather uncorrelated*" ...?

## 3. Proof of theorem: Setting up discrete circle method

# Expansion by the additive characters (mod $q$)

Write $e(x) := \exp(2\pi i x)$. By the orthogonality of additive characters (mod $q$), i.e.

$$\mathbb{1}_{n\equiv a \pmod q} = \frac{1}{q}\sum_{k \pmod q} e\left(\frac{k}{q}(n-a)\right),$$

we get

$$\overleftarrow{\pi}_N(a,q) := \sum_{\substack{p\in\mathscr{G}_N \\ \overleftarrow{p}\equiv a \pmod q}} 1 = \frac{1}{q}\sum_{k \pmod q} e\left(-\frac{k}{q}a\right)\sum_{p\in\mathscr{G}_N} e\left(\frac{k}{q}\overleftarrow{p}\right).$$

By rewriting the fractions $\frac{k}{q}$ to the reduced fractions

$$\frac{k}{q} \rightsquigarrow \frac{c}{s} \quad \text{with} \quad (c,s)=1,$$

we get

$$\overleftarrow{\pi}_N(a,q) = \frac{1}{q}\sum_{s|q}\sideset{}{^*}\sum_{c \pmod s} e\left(-\frac{c}{s}a\right)\sum_{p\in\mathscr{G}_N} e\left(\frac{c}{s}\overleftarrow{p}\right),$$

where

$$\sideset{}{^*}\sum_{c \pmod s} := \sum_{\substack{c \pmod q \\ (c,q)=1}}.$$

# Extract the main term

We make two observations:

- As we saw in the necessary conditions $(*)$ of Telhcirid's theorem, we know

$$\overleftarrow{p} \equiv a \pmod{g^2-1} \iff p \equiv g^{-(N-1)}a \pmod{g^2-1}.$$

  so the $\pmod{g^2-1}$ condition on $\overleftarrow{p}$ is reduced to the $\pmod{g^2-1}$ condition on $p$.
- Take the least $M$ with $(q, g^N) \mid g^M$. Since

$$n = (n_{N-1}\cdots n_0)_{(g)} \implies \overleftarrow{n} = (n_0\cdots n_{N-1})_{(g)} \equiv (n_{N-M}\cdots n_{N-1})_{(g)} \pmod{g^M},$$

  we have

$$\begin{aligned}&\overleftarrow{n} \equiv (a_{M-1}\cdots a_0)_{(g)} \pmod{g^M}\\ \iff\ & n \in (a_0\cdots a_{M-1})_{(g)}g^{N-M} + [0, g^{N-M-1})\end{aligned}$$

  so the $\pmod{g^M}$ condition on $\overleftarrow{p}$ is reduced to the "short interval" condition on $p$.

Expecting the other conditions behave randomly, we decompose the sum as

$$\begin{aligned}\overleftarrow{\pi}_N(a,q) &= \frac{1}{q}\sum_{s\mid q}\ \sideset{}{^*}\sum_{c \pmod s} e\left(-\frac{c}{s}a\right)\sum_{p\in\mathscr{G}_N} e\left(\frac{c}{s}\overleftarrow{p}\right)\\ &= \frac{1}{q}\sum_{s\mid (q,(g^2-1)g^N)} + \frac{1}{q}\sum_{\substack{s\mid q\\ s\nmid (g^2-1)g^N}} =: M+E, \quad \text{say.}\end{aligned}$$

# Calculation of the main term

The main term can be calculated backwards as

$$\begin{aligned} M &= \frac{1}{q} \sum_{s \mid (q,(g^2-1)g^N)} \sideset{}{^*}\sum_{c \pmod s} e\left(-\frac{c}{s}a\right) \sum_{p \in \mathscr{G}_N} e\left(\frac{c}{s}\overleftarrow{p}\right) \\ &= \frac{1}{q} \sum_{k \pmod{(q,(g^2-1)g^N)}} e\left(-\frac{k}{(q,(g^2-1)g^N)}a\right) \sum_{p \in \mathscr{G}_N} e\left(\frac{k}{(q,(g^2-1)g^N)}\overleftarrow{p}\right) \\ &= \frac{(q,(g^2-1)g^N)}{q} \sum_{\substack{p \in \mathscr{G}_N \\ \overleftarrow{p} \equiv a \pmod{(q,(g^2-1)g^N)}}} 1. \end{aligned}$$

The last sum can be calculated by using

$$\text{Prime number theorem in A.P. of } (\mathrm{mod}\ g^2-1).$$

In order to deal with the $(\mathrm{mod}\ (q, g^N))$ condition, PNT in A.P. over short intervals

$$x + [0, g^{N-M}) \quad \text{with some } x \in [0, g^N) \qquad ((a, g^N) \mid g^M)$$

seems neccessary. However, $(q, g^N)$ is now small enough to use just

$$\pi(x; a, q) = \frac{1}{\varphi(q)}\pi(x) + O_q(x \exp(-c_q\sqrt{\log x})) \quad \text{with} \quad q = g^2 - 1 \ll_g 1.$$

# Circle method for the remainder term

We just bound the remainder term pointwise as

$$E = \frac{1}{q} \sum_{\substack{s \mid q \\ s \nmid (g^2-1)g^N}} \sideset{}{^*}\sum_{c \pmod s} e\left(-\frac{c}{s}a\right) \sum_{p \in \mathscr{G}_N} e\left(\frac{c}{s}\overleftarrow{p}\right)$$

$$\ll \max_{\substack{s \mid q \\ s \nmid (g^2-1)g^N \\ (c,s)=1}} \left| \sum_{p \in \mathscr{G}_N} e\left(\frac{c}{s}\overleftarrow{p}\right) \right|.$$

Thus, our task is to bound the sum

$$R \coloneqq \sum_{p \in \mathscr{G}_N} e\left(\frac{c}{s}\overleftarrow{p}\right).$$

By the orthogonality on $\mathbb{T}$, we have

$$R = \int_0^1 \left( \sum_{p \in \mathscr{G}_N} e(-\alpha p) \right) \left( \sum_{n \in \mathscr{G}_N} e\left(\alpha n + \frac{c}{s}\overleftarrow{n}\right) \right) d\alpha = \int_0^1 S_{\mathrm{P}}(-\alpha) F(\alpha, \tfrac{c}{s}) d\alpha$$

with the exponential sums

$$S_{\mathrm{P}}(\alpha) \coloneqq \sum_{p \in \mathscr{G}_N} e(\alpha p) \quad \text{and} \quad F(\alpha, \beta) \coloneqq \sum_{n \in \mathscr{G}_N} e(\alpha n + \beta \overleftarrow{n}).$$

We employ the diophantine approximation

$$\alpha = \frac{b}{r} + \eta \quad \text{with} \quad (b, r) = 1 \text{ and } |\eta| \leq r^{-2}$$

and define the major and minor arcs

$$\mathfrak{M} := \{\alpha \in [0, 1) \mid r, |\eta| : \text{small}\} \quad \text{and} \quad \mathfrak{m} := [0, 1) \setminus \mathfrak{M}.$$

We then decompose the integral as

$$R = \int_0^1 S_{\mathrm{P}}(-\alpha) F(\alpha, \tfrac{c}{s}) d\alpha = \int_{\mathfrak{M}} + \int_{\mathfrak{m}} =: R_{\mathfrak{M}} + R_{\mathfrak{m}}.$$

We bound $R_{\mathfrak{M}}$, $R_{\mathfrak{m}}$ in two different manners.

# 4. Treatment of the major arc

On the major arc, we estimate the exponential sum over primes trivially

$$S_{\mathrm{P}}(\alpha) = \sum_{p \in \mathscr{G}_N} e(\alpha p) \ll g^N$$

while we use the fact that the major arc is very small

$$\mu(\mathfrak{M}) \ll g^{-N} \exp(c\sqrt{N}) \qquad (\mu : \text{Lebesgue measure}).$$

This gives

$$\begin{aligned} R_{\mathfrak{M}} = \int_{\mathfrak{M}} S_{\mathrm{P}}(-\alpha) F(\alpha, \tfrac{c}{s}) d\alpha &\ll \mu(\mathfrak{M}) g^N \max_{\alpha \in [0,1)} |F(\alpha, \tfrac{c}{s})| \\ &\ll \exp(c\sqrt{N}) \max_{\alpha \in [0,1)} |F(\alpha, \tfrac{c}{s})|. \end{aligned}$$

We then prepare the non-trivial $L^\infty$-bound (pointwise bound) of

$$F(\alpha, \tfrac{c}{s}) = \sum_{n \in \mathscr{G}_N} e(\alpha n + \tfrac{c}{s} \overleftarrow{n}) = \sum_{n \in \mathscr{G}_N} e(\alpha \overleftarrow{n} + \tfrac{c}{s} n)$$

by using the cancellation caused by the $\frac{c}{s}$ side.

# Product formula

Consider "the exponential sum over digits", i.e.

$$\phi(\alpha) := \sum_{0 \le n < g} e(\alpha n).$$

For $n$ represented as

$$n = \sum_{0 \le i < N} n_i g^i \quad \rightsquigarrow \quad \overleftarrow{n} = \sum_{0 \le i < N} n_i g^{N-i-1},$$

we have

$$\alpha \overleftarrow{n} + \beta n = \sum_{0 \le i < N} (\alpha g^{N-i-1} + \beta g^i) n_i.$$

Accordingly, we (essentially) have a factorization

$$F(\alpha, \beta) \approx \sum_{0 \le n_0, \dots, n_{N-1} < g} e\left( \sum_{0 \le i < N} (\alpha g^{N-i-1} + \beta g^i) n_i \right) = \prod_{i=0}^{N-1} \phi(\alpha g^{N-i-1} + \beta g^i).$$

This "product formula" is the key of the estimate for both of $R_{\mathfrak{M}}$ and $R_{\mathfrak{m}}$.

# Using the product formula to the $L^\infty$-bound of $F(\alpha,\beta)$

Note that the consecutive argument of the product formula satisfies

$$\beta g^i(g^2-1) = (-1)\cdot(\alpha g^{N-i-1}+\beta g^i) + g\cdot(\alpha g^{N-(i+1)-1}+\beta g^{i+1})$$

and so the triangle inequality of $\|\alpha\| := \min_{n\in\mathbb{Z}}|\alpha-n|$ implies

$$\|\beta g^i(g^2-1)\| \le 1\cdot\|\alpha g^{N-i-1}+\beta g^i\| + g\cdot\|\alpha g^{N-(i+1)-1}+\beta g^{i+1}\|$$
$$\rightsquigarrow \max(\|\alpha g^{N-i-1}+\beta g^i\|, \|\alpha g^{N-(i+1)-1}+\beta g^{i+1}\|) \ge \frac{1}{g+1}\|\beta g^i(g^2-1)\|.$$

For small $|\alpha|$, we have approximations (the values of $c_g$ may change)

$$|\phi(\alpha)| = \left|\frac{\sin\pi g\|\alpha\|}{\sin\pi\|\alpha\|}\right| = \left|\frac{\pi g\|\alpha\| - \frac{1}{6}(\pi g\|\alpha\|)^3+\cdots}{\pi\|\alpha\| - \frac{1}{6}(\pi\|\alpha\|)^3+\cdots}\right| \approx g(1-c_g\|\alpha\|^2) \approx g\exp\bigl(-c_g\|\alpha\|^2\bigr)$$

and so, by pairing the consecutive indices, the product formula essentially gives

$$F(\alpha,\tfrac{c}{s}) = \prod_{i=0}^{N-1}\phi(\alpha g^{N-i-1}+\tfrac{c}{s}g^i) \ll g^N\exp\biggl(-c_g\sum_{0\le i<N}\biggl\|\frac{(g^2-1)g^i c}{s}\biggr\|^2\biggr).$$

We thus need some observation on $\frac{(g^2-1)g^i c}{s} \pmod 1$.

# A bit about the distribution of $\frac{(g^2-1)g^i c}{s} \pmod 1$

Suppose that we have a sad news at the $i_0$-th step: "$\|\frac{(g^2-1)g^{i_0} c}{s}\|$ is small" as

$$\left\| \frac{(g^2-1)g^{i_0} c}{s} \right\| \leq \frac{1}{2g}$$

It is also a good news: "we can controll the next value" as

$$g \cdot \left\| \frac{(g^2-1)g^{i_0} c}{s} \right\| \leq \frac{1}{2} \quad \rightsquigarrow \quad \left\| \frac{(g^2-1)g^{i_0+1} c}{s} \right\| = g \cdot \left\| \frac{(g^2-1)g^{i_0} c}{s} \right\|.$$

How long can this continues? Assume that this process continues $L$ times so that

$$\left\| \frac{(g^2-1)g^{i_0+L} c}{s} \right\| = g^L \cdot \left\| \frac{(g^2-1)g^{i_0} c}{s} \right\|$$

and recall that $s \nmid (g^2-1)g^N$ and $(c,s)=1$. We then have

$$\frac{g^L}{s} \leq g^L \cdot \left\| \frac{(g^2-1)g^{i_0} c}{s} \right\| = \left\| \frac{(g^2-1)g^{i_0+L} c}{s} \right\| \leq \frac{1}{2} \quad \rightsquigarrow \quad L \ll \log s.$$

Thus, once per $\log s$ steps of $i$, we have $\|\frac{(g^2-1)g^i c}{s}\| \geq \frac{1}{2g}$.

By combining the estimate given by the product formula

$$F(\alpha, \tfrac{c}{s}) \ll g^N \exp\left(-c_g \sum_{0 \le i < N} \left\| \frac{(g^2-1)g^i c}{s} \right\|^2\right)$$

and our small knowledge on the distribution of $\frac{(g^2-1)g^i c}{s} \pmod 1$:

$$\text{once per } \log s \text{ steps of } i, \text{ we have } \left\| \frac{(g^2-1)g^i c}{s} \right\| \ge \frac{1}{2g},$$

we get the bound

$$F(\alpha, \tfrac{c}{s}) \ll g^N \exp\left(-c_g \frac{N}{\log s}\right) \ll g^N \exp\left(-c_g \frac{N}{\log q}\right).$$

This gives a non-trivial $L^\infty$-bound of $F(\alpha, \beta)$.

# 5. Treatment of the minor arc

# Circle method for binary additive problem?

A general expectation on the size of exponential sum is the "square-root" cancellation

$$|(\text{exponential sum})| \asymp (\text{trivial bound})^{\frac{1}{2}}$$

which follows by some probabilistic argument with Parseval's formula.

By recalling the measure of $\mathfrak{M}$ is very small, we should have

$$\int_{\mathfrak{m}} |S_{\mathrm{P}}(-\alpha)||F(\alpha, \tfrac{c}{s})|d\alpha \gg \mu(\mathfrak{m}) \cdot g^{\frac{N}{2}} \cdot g^{\frac{N}{2}} \gg g^N \gg (\text{main term}).$$

This implies our circle method seems fail...?

We can indeed use the product formula (shown in the next slide)

$$F(\alpha, \beta) = \prod_{i=0}^{N-1} \phi(\alpha g^{N-i-1} + \beta g^i)$$

for overcoming this difficulty. We shall show the $L^1$-bound

$$\int_0^1 |F(\alpha, \beta)|d\alpha \ll (A_g \log g)^N \qquad (A_g > 0 : \text{constant}),$$

which shows a bound stronger than the square-root cancellation on average over $\alpha$.

# The $L^1$-bound of $F(\alpha, \beta)$

Recall a bound based on the summation formula for geometric series

$$|\phi(\alpha)| = \left| \sum_{0 \le n < g} e(\alpha n) \right| \le \min\left(g, \frac{1}{\|\alpha\|}\right) \quad \text{where} \quad \|\alpha\| = \min_{n \in \mathbb{Z}} |\alpha|.$$

By using this bound in the product formula, we get

$$|F(\alpha, \beta)| = \prod_{i=0}^{N-1} |\phi(\alpha g^{N-i-1} + \beta g^i)| \le \prod_{i=0}^{N-1} \min\left(g, \frac{1}{\|\alpha g^{N-i-1} + \beta g^i\|}\right).$$

By approximating the integral by the Riemann sum with mesh of width $g^{-N}$, we get

$$\int_0^1 |F(\alpha, \beta)| d\alpha \ll \frac{1}{g^N} \sum_{0 \le h < g^N} |F(hg^{-N}, \beta)|.$$

By using the above bound based on the product formula, we get

$$\int_0^1 |F(\alpha, \beta)| d\alpha \ll \frac{1}{g^N} \sum_{0 \le h < g^N} \prod_{i=0}^{N-1} \min\left(g, \frac{1}{\|hg^{-(i+1)} + \beta g^i\|}\right).$$

What we obtained so far:

$$\int_0^1 |F(\alpha,\beta)|d\alpha \ll \frac{1}{g^N} \sum_{0\le h<g^N} \prod_{i=0}^{N-1} \min\left(g, \frac{1}{\|hg^{-(i+1)} + \beta g^i\|}\right).$$

We now express $h$ by the base-$g$ representation as

$$h = \sum_{0\le j<N} h_j g^j \quad \text{with} \quad h_0, \dots, h_{N-1} \in \{0, \dots, g-1\},$$

where $h_{N-1}$ is now not necessarily non-zero. We then have

$$hg^{-(i+1)} = \sum_{0\le j<N} h_j g^{j-(i+1)} \equiv h_i g^{-1} + \underbrace{\delta(h_0, \dots, h_{i-1})}_{\text{lower order terms}} \pmod 1.$$

Thus, essentially (ignoring $\beta g^i$ and $\delta(h_0, \dots, h_{i-1})$), we have

$$\begin{aligned}\int_0^1 |F(\alpha,\beta)|d\alpha &\ll \frac{1}{g^N} \sum_{0\le h_0,\dots,h_{N-1}<g} \prod_{i=0}^{N-1} \min\left(g, \frac{1}{\|h_i g^{-1}\|}\right) \\ &= \left(\frac{1}{g} \sum_{0\le n<g} \min\left(g, \frac{1}{\|hg^{-1}\|}\right)\right)^N \ll (A_g \log g)^N.\end{aligned}$$

Note: We may ignore $\beta g^i$ and $\delta(h_0, \dots, h_{i-1})$ (to some extent) by

- Taking the summation in the order $\sum_{h_0} \cdots \sum_{h_{N-1}}$.
- Remove the effect of $\beta g^i$ and $\delta(h_0, \dots, h_{i-1})$ by shifting the summation variable.