Exponential and Character Sums

Katalin Gyarmati

katalin.gyarmati@ttk.elte.hu

András Sárközy

andras.sarkozy@ttk.elte.hu

Eötvös Loránd University

Lecture Notes

ELTE TTK, Institute of Mathematics

2024

Contents

Introduction

This course is taught at Eötvös Loránd University to MSc and PhD mathematics students who would like to study the basics of deeper number theory.

We wish the readers a pleasant time!

Books on which the material is based:

References

[1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics 74, Springer New York, 2013, Originally published by Markham Publishing Co., 1967, chapters 2, 5, 23 and 27.

[2] S. W. Graham, G. Kolesnik, *Van der Corput's Method of Exponential Sums*, Cambridge University Press, 1991.

[3] A. Ivič, *The Riemann Zeta-Function: Theory and Applications*, Dover Publications, 2003, 55-83.

[4] H. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227, Springer Berlin, Heidelberg 2006, 1-49.

[5] R. C. Vaughan, *The Hardy-Littlewood Method*, Cambridge University Press, 1997.

[6] I. M. Vinogradov, *Elements of Number Theory*, Dover Publications, Reprint edition 2016.

[7] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, Dover Publications, Revised edition 2004.

The basic concepts were discussed mainly using [6] and [7]. The description of the large sieve is based on the books [1], [4]. In addition to the above, the lecture note is based on a few papers, these references are given at the end of each chapter.

For further studies, we suggest [2] for Weyl sums, the van-der Corput method, and exponent pairs. Those who are interested in the continuation might also study the books [3] and [5].

1 Notations

What exactly is an exponential sum?

Trigonometric form of complex numbers:

$$z = r(\cos\alpha + i\sin\alpha) = re^{i\alpha}.$$

Exponential sum: is a sum that contains complex numbers in exponential form.

$$e^{i(\alpha_1+\alpha_2)} = e^{i\alpha_1}e^{i\alpha_2}$$
$$\left(e^{i\alpha}\right)^n = e^{in\alpha}.$$

Complex Analysis theory::

$$f(x) = e^x : \mathbb{R} \to \mathbb{R}$$

can be uniquely extended

$$f(z) = e^z : \mathbb{C} \to \mathbb{C}.$$

Here, by writing $i\alpha$ instead of z, we get $e^{i\alpha}$ defined above.

$$\overline{e^{i\alpha}} = e^{i(-\alpha)}.$$

Real analysis:

$$f : \mathbb{R} \to \mathbb{R}.$$

Complex analysis:

$$f : \mathbb{C} \to \mathbb{C}.$$

Analytic number theory: complex variable functions.

Here:

$$f : \mathbb{R} \to \mathbb{C},$$

i.e., complex functions with real variables.

It is almost the same as real analysis

$$f(t) = g(t) + ih(t),$$

where g, h are real functions, i.e., the study of f can be reduced to g and h.

The definition of continuity, differentiability, integrability can be reduced to the real case.

$$f'(t) = g'(t) + ih'(t)$$
$$\int_a^b f(t)dt = \int_a^b g(t)dt + i\int_a^b h(t)dt$$

Differentiability and integrability rules are the same.

E.g., for $f(t) = e^{it}$

$$\begin{aligned} f'(t) &= (\cos t + i \sin t)' \\ &= (\cos t)' + i(\sin t)' \\ &= -\sin t + i \cos t \\ &= i(\cos t + i \sin t) \\ &= ie^{it}. \end{aligned}$$

Similarly,

$$\int_a^b e^{it}dt = \left[\frac{e^{it}}{i}\right]_a^b$$

$$= \frac{1}{i}\left(e^{ib} - e^{ia}\right).$$

Why is this function $f(t) = e^{it}$ so important in number theory?

Since

$$f(t) = e^{it} = \cos t + i \sin t$$

is periodic with period length 2π.

$\Rightarrow$

Here $g(t) = e^{2\pi i t}$ is periodic with period 1.

The value of $g(t)$ depends only on the fractional part of t.

We use this function so often that we introduce a new notation:

Definition 1.1 *Let* $e(\alpha) \stackrel{\text{def}}{=} e^{2\pi i\alpha}$. *Then the value of* $e(\alpha)$ *depends only on the fractional part of* α. *In addition, we also use the notation* $e_m(\alpha)$, *where* $e_m(\alpha) \stackrel{\text{def}}{=} e^{2\pi i\frac{\alpha}{m}} = e\left(\frac{\alpha}{m}\right)$.

The following play a particularly important role:

$$\begin{aligned} f(t) &= \sum_{n=0}^{N} a_n e(nt) \\ &= \sum_{n=0}^{N} a_n \left(e(t)\right)^n \end{aligned}$$

is an exponential (trigonometric) polynomial and

$$F(t) = \sum_{n=0}^{\infty} a_n e(nt)$$

is a power series; here we assume that it is absolutely convergent:

$$\sum_{n=0}^{\infty} |a_n| < \infty.$$

As in real analysis, here as well, every piecewise continuous function $F(t)$ can be expressed as a power series, so-called Fourier series.

Let

$$f(t)= \sum_{n=0}^{N} a_n e(nt).$$

Then what is $f'(t)$ and $\int_a^b f(t)dt$ equal to?

Clearly

$$f'(t) = \sum_{n=0}^{N} 2\pi i n a_n e(nt).$$

Next, instead of computing $\int_0^1 f(t)dt$, we study more generally, namely for integers $0 \leq k \leq N$ we have

$$\begin{aligned}
\int_0^1 f(t)e(-kt)dt &= \sum_{n=0}^{N} a_n \int_0^1 e((n-k)t)dt \\
&= a_k \int_0^1 e(0)dt + \sum_{\substack{n=0,\\ n\neq k}}^{N} a_n \int_0^1 e((n-k)t)dt \\
&= a_k + \sum_{\substack{n=0,\\ n\neq k}}^{N} a_n \left[\frac{e((n-k)t)}{2\pi i(n-k)}\right]_0^1 \\
&= a_k.
\end{aligned}$$

Similarly,

$$\int_0^1 f(t)e(-kt)dt = 0 \text{ if } k < 0 \text{ or } k > N.$$

2 Parseval formula and Ramanujan sums

The following theorem is one of the most fundamental techniques for estimating exponential sums.

Theorem 2.1 (Parseval formula)

a) *If* $f(t) = \sum_{n=0}^{N} a_n e(nt)$ *then*

$$\int_0^1 |f(t)|^2 \, dt = \sum_{n=0}^{N} |a_n|^2.$$

b) *If* $f(t) = \sum_{n=0}^{\infty} a_n e(nt)$ *and* $\sum_{n=0}^{\infty} |a_n|^2$ *is absolute convergent, then*

$$\int_0^1 |f(t)|^2 \, dt = \sum_{n=0}^{\infty} |a_n|^2.$$

The proof of Theorem 2.1.

a)

$$\begin{aligned}
\int_0^1 |f(t)|^2 \, dt &= \int_0^1 f(t)\overline{f(t)}dt \\
&= \int_0^1 \sum_{n=0}^{N} a_n e(nt) \sum_{m=0}^{N} \overline{a_m} e(-mt)dt \\
&= \int_0^1 \sum_{n=0}^{N} \sum_{m=0}^{N} a_n \overline{a_m} e((n-m)t)dt \\
&= \sum_{n=0}^{N} \sum_{m=0}^{N} a_n \overline{a_m} \int_0^1 e((n-m)t)dt.
\end{aligned}$$

Here, the last integral is 0 if $n \neq m$ and 1 if $n = m$, i.e.,

$$\int_0^1 |f(t)|^2 \, dt = \sum_{n=0}^{N} a_n \overline{a_n}$$

$$= \sum_{n=0}^{N} |a_n|^2 .$$

b) similarly.

Lemma 2.1 a) *For $\alpha \in \mathbb{R}$ we have*

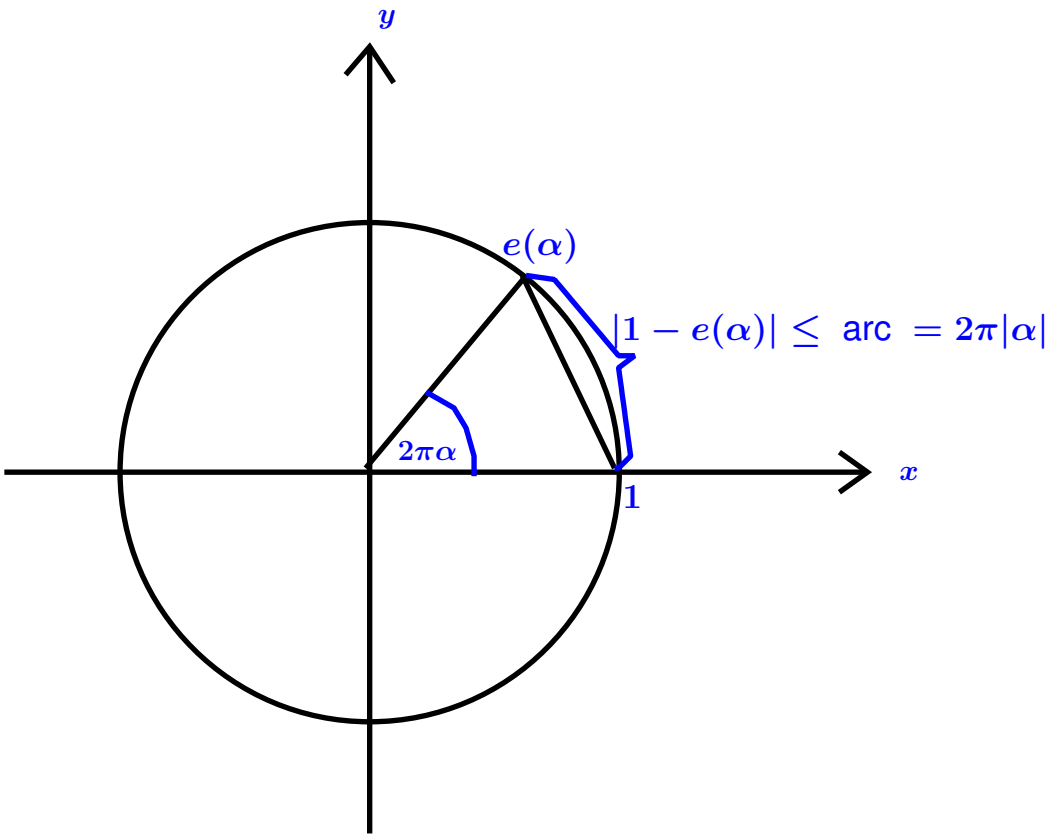
$$|1 - e(\alpha)| \leq 2\pi\,|\alpha| .$$

b) *For $|\alpha| \leq \frac{1}{2}$ we have*

$$|1 - e(\alpha)| \geq 4\,|\alpha| .$$

The proof of Lemma 2.1.

a)



b)

$$\begin{aligned}|1-e(\alpha)|^2 &= (1-e(\alpha))\,\overline{(1-e(\alpha))}\\ &= (1-e(\alpha))\,(1-e(-\alpha))\\ &= 1-e(\alpha)-e(-\alpha)+1\\ &= 2-2\mathrm{Re}\,e(\alpha)\\ &= 2(1-\cos 2\pi\alpha)\\ &= 2\cdot 2\sin^2\pi\alpha.\end{aligned}$$

Taking the square root:

$$|1-e(\alpha)| = 2|\sin\pi\alpha| = 2\sin\pi|\alpha|.$$

Since $\frac{\sin x}{x}$ is monotonically decreasing in $[0,\pi/2]$:

$$\frac{\sin x}{x} \geq \frac{\sin \pi/2}{\pi/2} = \frac{2}{\pi},$$

thus

$$\sin x \geq \frac{2}{\pi}x.$$

That is

$$|1-e(\alpha)| = 2\sin|\pi\alpha| \geq 2\cdot\frac{2}{\pi}\pi|\alpha| = 4\,|\alpha|\,.$$

Example. $p\in\mathbb{Z}$, $q\in\mathbb{N}$

$$\begin{aligned}\sum_{n=0}^{q-1} e\left(n\frac{p}{q}\right) &= \sum_{n=0}^{q-1} e\left(\frac{p}{q}\right)^n\\ &= \begin{cases} q & \text{if } q\mid p,\\ \frac{1-e\left(q\frac{p}{q}\right)}{1-e\left(\frac{p}{q}\right)} = \frac{1-1}{1-e\left(\frac{p}{q}\right)} = 0 & \text{if } q\nmid p.\end{cases}\end{aligned}$$

Theorem 2.2 (Jensen-Ramanujan formula) *If $q \in \mathbb{N}$ then*

$$S = \sum_{\substack{0 \le p < q \\ (p,q)=1}} e\left(\frac{p}{q}\right) = \mu(q).$$

That is, the sum of the primitive qth roots of unity is $\mu(q)$.

The proof of Theorem 2.2. Let μ denote the Möbius function. We use the following:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

Then:

$$\begin{aligned} S &= \sum_{p=0}^{q-1} \left(\sum_{d|(p,q)} \mu(d) \right) e\left(\frac{p}{q}\right) \\ &= \sum_{d|q} \mu(d) \sum_{\substack{0 \le p \le q-1 \\ d|p}} e\left(\frac{p}{q}\right). \end{aligned}$$

In the last sum, write $p = kd$. Then $kd \le q - 1$, so $k \le \frac{q}{d} - 1$. Thus:

$$S = \sum_{d|q} \mu(d) \sum_{k=0}^{\frac{q}{d}-1} e\left(k\frac{d}{q}\right).$$

In the first sum, we distuingish the cases $d = q$ and $d < q$. Then

$$\begin{aligned} S &= \mu(q) + \sum_{\substack{d|q \\ d<q}} \mu(d) \sum_{k=0}^{\frac{q}{d}-1} e\left(k\frac{d}{q}\right) \\ &= \mu(q) + \sum_{\substack{d|q \\ d<q}} \mu(d) \frac{1 - e\left(\frac{q}{d} \cdot \frac{d}{q}\right)}{1 - e\left(\frac{d}{q}\right)} \qquad = \mu(q) + \sum_{\substack{d|q \\ d<q}} \mu(d) 0 \\ &= \mu(q). \end{aligned}$$

3 Group characters

In number theory, characters usually mean multiplicative characters, possibly additive characters, these will be discussed later.

First, let's define the so-called group characters, using minimal group theory (so it looks better, more modern).

First, let's see what we mean by the group character in algebra. We now only look at the case of finite Abel groups (much simpler and enough for us).

Definition 3.1 *Let $\mathcal{G}$ be a finite Abelian group,*

$$\chi : \mathcal{G} \to \mathbb{C}$$

with the following properties

1. $\chi(g) \not\equiv 0$ in $\mathcal{G}$
2. $\chi(g)$ *multiplicative in* $\mathcal{G}$*:*

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2) \quad \forall g_1, g_2 \in \mathcal{G}.$$

Then χ is called a group character (defined on $\mathcal{G}$).

Corollary 3.1

1. *If e is the identity element of $\mathcal{G}$, then $\chi(e) = 1$.*
2. *$\forall\, g \in \mathcal{G}$ we have $(\chi(g))^{|\mathcal{G}|} = 1$.*
3. *Define $\chi_0 : \mathcal{G} \to \mathbb{C}$ by*

$$\chi_0(g) \equiv 1 \quad \forall\, g \in \mathcal{G},$$

then χ_0 is a character in $\mathcal{G}$, this is the so-called main character, trivial character or principal character.

4. *If χ is a character on $\mathcal{G}$, then we define*

$$\overline{\chi} : \mathcal{G} \to \mathbb{C} \text{ by}$$
$$\overline{\chi}(g) \stackrel{\text{def}}{=} \overline{\chi(g)} \quad \forall g \in \mathcal{G},$$

Then $\overline{\chi}$ is also a character on $\mathcal{G}$, this is the so-called conjugate character.

5. *If $\chi_1,\ \chi_2$ are characters on $\mathcal{G}$, then define χ by*

$$\chi(g) \stackrel{\text{def}}{=} \chi_1(g)\chi_2(g) \quad \forall\, g \in \mathcal{G},$$

then χ is also a character on $\mathcal{G}$. (So the product of two characters is also a character, in fact, the characters form a group.)

6. *If $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$, then $\chi : \mathcal{G} \to \mathbb{C}$ is a character in $\mathcal{G}$ if and only if $\exists$ character χ_1 in $\mathcal{G}_1$ and character χ_2 in $\mathcal{G}_2$ such that $\forall\, g = g_1 g_2 \in \mathcal{G}$ we have*

$$\chi(g) = \chi(g_1 g_2) = \chi_1(g_1)\chi_2(g_2).$$

7. *If $\mathcal{G} = C_n = \{g\}_n$ is the cyclic group of order n, then χ is a character on $\mathcal{G}$ if and only if $\exists\ a \in \{0, 1, 2, \ldots, n-1\}$ such that*

$$\chi(g^k) = e\left(k\frac{a}{n}\right) \quad \forall\, k \in \mathbb{Z}.$$

8. *The explicit form of characters defined in $\mathcal{G} = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ is*

$$\chi(g_1^{k_1} \cdots g_r^{k_r}) = e\left(k_1\frac{a_1}{n_1} + \cdots + k_r\frac{a_r}{n_r}\right),$$

where $a_i \in \{0, 1, 2, \ldots, n_i - 1\} \quad \forall\ 1 \le i \le r$. Note that if $\chi = \chi_0 \ \Leftrightarrow\ a_i = 0 \quad \forall i$.

(9) *The number of (different) characters defined on $\mathcal{G}$ is $|\mathcal{G}|$.*

Proof of Corollary 3.1.

(1) $\exists\, g:\ \chi(g) \neq 0$, thus

$$\chi(e)\chi(g) = \chi(eg) = \chi(g) \qquad / : \chi(g)(\neq 0)$$
$$\chi(e) = 1.$$

(2)

$$(\chi(g))^{|\mathcal{G}|} = \chi\left(g^{|\mathcal{G}|}\right) \quad = \chi(e) = 1$$
$$\uparrow \qquad\qquad \uparrow$$
property 2. Lagrange t.

(3) Trivial.

(4) Trivial. Remark:

$$1 = \chi(e) = \chi(gg^{-1}) = \chi(g)\chi(g^{-1}) \quad / \cdot \overline{\chi}(g)$$
$$\overline{\chi}(g) = \left(\chi(g)\overline{\chi(g)}\right)\chi(g^{-1})$$

By (2) we have $\chi(g)\overline{\chi(g)} = |\chi(g)|^2 = 1$. Thus

$$\overline{\chi}(g) = \chi(g^{-1}).$$

(5), (6) Trivial, HW.

(7) Follows from (2) and $\chi(g^k) = \chi(g)^k$.

(8) This is a corollary of (7).

(9) This is a corollary of (8).

Corollary 3.2

(10) *If χ is a group character defined on $\mathcal{G}$, then*

$$\sum_{g\in\mathcal{G}}\chi(g)=\begin{cases}|\mathcal{G}| & \text{if } \chi=\chi_0\\ 0 & \text{if } \chi\neq\chi_0.\end{cases}$$

(11) *$\forall\, g\in\mathcal{G}$ we have*

$$\sum_{\chi}\chi(g)=\begin{cases}|\mathcal{G}| & \text{if } g=e\\ 0 & \text{if } g\neq e.\end{cases}$$

Proof of Corollary 3.2. (10): Let $\mathcal{G}=C_{n_1}\times C_{n_2}\times\cdots\times C_{n_r}=\{g_1\}_{n_1}\times\{g_2\}_{n_2}\times\cdots\times\{g_r\}_{n_r}$. Then $\forall g\in\mathcal{G}$ can be uniquely written in the form $g_1^{k_1}\cdots g_r^{k_r}$, where $0\le k_i<n_i$. Since, according to (8) the explicit form of $\forall\,\chi$ is

$$\chi(g_1^{k_1}\cdots g_r^{k_r})=e\left(k_1\frac{a_1}{n_1}+\cdots+k_r\frac{a_r}{n_r}\right),$$

where $a_i\in\{0,1,\ldots,n_i-1\}$, thus

$$\sum_{g\in\mathcal{G}}\chi(g)=\sum_{k_1=0}^{n_1-1}\cdots\sum_{k_r=0}^{n_r}e\left(k_1\frac{a_1}{n_1}+\cdots+k_r\frac{a_r}{n_r}\right).$$

So:

$$\begin{aligned}\sum_{g\in\mathcal{G}}\chi(g)&=\left(\sum_{k_1=0}^{n_1-1}e\left(k_1\frac{a_1}{n_1}\right)\right)\cdots\left(\sum_{k_r=0}^{n_r-1}e\left(k_r\frac{a_r}{n_r}\right)\right)\\&=\begin{cases}n_1 & \text{if } a_1=0\\ 0 & \text{if } a_1\neq 0\end{cases}\cdots\begin{cases}n_r & \text{if } a_r=0\\ 0 & \text{if } a_r\neq 0.\end{cases}\end{aligned}$$

That is

$$\sum_{g\in\mathcal{G}}\chi(g)=\begin{cases} n_1\cdots n_r=|C_1|\cdots|C_r|=|\mathcal{G}|\,, & \text{if } a_1=\cdots=a_r=0,\\ & \Leftrightarrow\ \chi=\chi_0,\\ 0, \quad \text{if } \exists\, a_i\neq 0 \Leftrightarrow\ \chi\neq\chi_0. \end{cases}$$

Proof of (11):

Let $\mathcal{G}=C_{n_1}\times\cdots\times C_{n_r}=\{g_1\}_{n_1}\times\cdots\times\{g_r\}_{n_r}$. Furthermore, we write the fixed element $g\in\mathcal{G}$ in the form $g=g_1^{k_1}\cdots g_r^{k_r}$, where $0\le k_i<n_i$.

Again by (8) we get:

$$\sum_{g\in\mathcal{G}}\chi(g)=\sum_{a_1=0}^{n_1-1}\cdots\sum_{a_r=0}^{n_r}e\left(k_1\frac{a_1}{n_1}+\cdots+k_r\frac{a_r}{n_r}\right).$$

Thus:

$$\begin{aligned}\sum_{\chi}\chi(g)&=\left(\sum_{a_1=0}^{n_1-1}e\left(a_1\frac{k_1}{n_1}\right)\right)\cdots\left(\sum_{a_r=0}^{n_r-1}e\left(a_r\frac{k_r}{n_r}\right)\right)\\ &=\begin{cases} n_1 & \text{if } k_1=0\\ 0 & \text{if } k_1\neq 0\end{cases}\cdots\begin{cases} n_r & \text{if } k_r=0\\ 0 & \text{if } k_r\neq 0.\end{cases}\end{aligned}$$

That is

$$\sum_{\chi}\chi(g)=\begin{cases} n_1\cdots n_r=|\mathcal{G}|\,, & \text{if } k_1=\cdots=k_r=0,\ \Leftrightarrow\ g=e,\\ 0, & \text{if } \exists\, k_i\neq 0\ \Leftrightarrow\ g\neq e.\end{cases}$$

Theorem 3.1 *Let $\mathcal{G}$ be an arbitrary finite Abelian group, $g\in\mathcal{G}$ and $g_1,g_2,\ldots,g_t\in\mathcal{G}$ elements (where $g_i=g_j$ is allowed). Then*

$$|\{i:\ 1\le i\le t,\ g_i=g\}|=\frac{1}{|\mathcal{G}|}\sum_{\chi}\overline{\chi}(g)\sum_{i=1}^{t}\chi(g_i).$$

Proof of Theorem 3.1.

$$\begin{aligned}
\sum_{\chi}\overline{\chi}(g)\sum_{i=1}^{t}\chi(g_i) &= \sum_{i=1}^{t}\left(\sum_{\chi}\overline{\chi}(g)\chi(g_i)\right)\\
&= \sum_{i=1}^{t}\left(\sum_{\chi}\chi(g^{-1})\chi(g_i)\right)\\
&= \sum_{i=1}^{t}\left(\sum_{\chi}\chi(g^{-1}g_i)\right)\\
&= \sum_{i=1}^{t}\begin{cases} |\mathcal{G}| & \text{if } g^{-1}g = e \;\Leftrightarrow\; g_i = g\\ 0 & \text{if } g^{-1}g \neq e \;\Leftrightarrow\; g_i \neq g\end{cases}\\
&= \sum_{\substack{1\leq i\leq t\\ g_i=g}}|\mathcal{G}|\\
&= |\mathcal{G}|\cdot|\{i:\ 1\leq i\leq t,\ g_i = g\}|\,,
\end{aligned}$$

from which, dividing by $|\mathcal{G}|$, we get the statement of the theorem.

In number theory, there are two important special cases:

1. $\mathcal{G} =< \mathbb{Z}_m, + >$, the additive group of residue classes $\mathbf{mod}\ m \Rightarrow$ additive characters.

2. $\mathcal{G} =< Z_m^*, \times >$, where the group of reduced residue classes of $\mathbb{Z}_m$ is Z_m^*, the operation is multiplication $\Rightarrow$ multiplicative characters.

4 Additive characters

In the case of fixed $m, k \in \mathbb{Z}$, we denote the residue class modulo m represented by k by $\overline{k}$:

$$\overline{k} = \{x : \ x \in \mathbb{Z}, \ x \equiv k \pmod{m}\}.$$

Then, according to (7) of Corollary 3.1, the characters defined on $\mathbb{Z}_m$ are:

$$\Psi(\overline{k}) = e\left(k\frac{a}{m}\right),$$

where $a \in \{0, 1, \ldots, m-1\}$. From now on, for the sake of simplicity, we omit the overline from k, so

$$\Psi(k) = e\left(k\frac{a}{m}\right),$$

These are more recently called additive characters. For these additive characters, the statements (1)-(11) of Corollaries 3.1 and 3.2 hold, e.g., from the last theorem we get the following:

Theorem 4.1 *If $\mathcal{A} \subset \mathbb{Z}_m$ is finite, $r \in \mathbb{Z}$ and $m \in \mathbb{N}$, then writing*

$$f(t) = \sum_{a \in \mathcal{A}} e(at)$$

we have

$$\begin{aligned} |\{a : \ a \in \mathcal{A}, \ a \equiv r \pmod{m}\}| &= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{rk}{m}\right) f\left(\frac{k}{m}\right) \\ &= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{rk}{m}\right) \sum_{a \in \mathcal{A}} e\left(\frac{ak}{m}\right). \end{aligned}$$

Proof of Theorem 4.1. By Theorem 3.1

$$|\{i : \ 1 \le i \le t, \ g_i = g\}| = \frac{1}{|\mathcal{G}|}\sum_{\chi} \overline{\chi}(g) \sum_{i=1}^{t} \chi(g_i). \qquad (4.1)$$

In this theorem, let $\mathcal{G} = \mathbb{Z}_m$, $g \stackrel{\text{def}}{=} r$, $\mathcal{A} = \{a_1, a_2, \ldots, a_s\}$ (that is $t = s$), $g_i \stackrel{\text{def}}{=} a_i$.

If χ is a character on $\mathcal{G} = \mathbb{Z}_m$, then

$$\chi(1) = e\left(\frac{k}{m}\right),$$

where $0 \le k \le m-1$. By (4.1) we get

$$\begin{aligned}
|\{a : a \in \mathcal{A},\ a \equiv r \pmod m\}| &= \frac{1}{m}\sum_{\chi}\overline{\chi}(r)\sum_{i=1}^{s}\chi(a_i) \\
&= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{kr}{m}\right)\sum_{i=1}^{s} e\left(\frac{ka_i}{m}\right) \\
&= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{kr}{m}\right)\sum_{a\in\mathcal{A}} e\left(\frac{ka}{m}\right) \\
&= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{rk}{m}\right) f\left(\frac{k}{m}\right).
\end{aligned}$$

In Theorem 4.1 $f(t)$ is the generator function of the set $\mathcal{A}$, also called Fourier transform.

Now it becomes clear why the function $e(\alpha)$ is so important in number theory:

We know $e(\alpha)$ is periodic with period 1. Thus, $e\left(\frac{n}{m}\right)$ depends only on the residue class $n \pmod m$.

Thus $e\left(a\frac{k}{m}\right)$ for fixed k and m depends only on the residue class $a \pmod m$.

So, if we can control the generator function (Fourier transform) of the sequence $\mathcal{A}$ (which is $f(t) = f_{\mathcal{A}}(t)$), then the distribution of the elements of $\mathcal{A}$ in the residue classes can be controlled.

This principle can also be applied in the opposite direction. Known distribution in the residue classes $\Rightarrow$ control of the generator function $f(t) \Rightarrow$ other arithmetic properties of $\mathcal{A}$ can also be studied.

The applicability of additive characters is based on this.

Of course, the formula in the theorem could be calculated without using characters, but it looks better this way.

4.1 Applications

Theorem 4.2 *If $\ell \in \mathbb{N}$, $f(x_1, \dots, x_\ell) \in \mathbb{Z}[x_1, \dots, x_\ell]$, then the number of solutions of the congruence*

$$f(x_1, \dots, x_\ell) \equiv 0 \pmod{p}$$

is

$$N = \frac{1}{m} \sum_{k=0}^{m-1} \sum_{t_1=0}^{m-1} \cdots \sum_{t_\ell=0}^{m-1} e\left(f(t_1, \dots, t_\ell) \frac{k}{m} \right).$$

Proof of Theorem 4.2. We use the previous theorem with $r = 0$ and

$$\mathcal{A} = \{ f(t_1, \dots, t_\ell) : \ (t_1, \dots, t_\ell) \in \{0, 1, \dots, m-1\}^\ell \}.$$

Then

$$\begin{aligned} N = |\{ f(t_1, \dots, t_\ell) : \quad & (t_1, \dots, t_\ell) \in \{0, 1, \dots, m-1\}^\ell, \\ & f(t_1, \dots, t_\ell) \equiv 0 \pmod{m} \}| \\ = \frac{1}{m} \sum_{k=0}^{m-1} e\left(-\frac{0 \cdot k}{m} \right) & \sum_{t_1=0}^{m-1} \cdots \sum_{t_\ell=0}^{m-1} e\left(f(t_1, \dots, t_\ell) \frac{k}{m} \right). \end{aligned}$$

Here $e\left(-\frac{0\cdot k}{m}\right) = 1$, and with this we proved the statement of the theorem.

Studying the special case of linear congruences:

Theorem 4.3 *Let $\ell \in \mathbb{N}$, $a_1, a_2, \ldots, a_\ell, b \in \mathbb{Z}$ and*

$$d \overset{\text{def}}{=} (a_1, a_2, \ldots, a_\ell, m).$$

Then the number of solutions of the congruence

$$a_1x_1 + \cdots + a_\ell x_\ell \equiv b \pmod{m}$$

is

$$N = \begin{cases} m^{\ell-1}d, & \text{if } d \mid b \\ 0, & \text{if } d \nmid b. \end{cases}$$

Remark. For $\ell = 1$, to solve $ax \equiv b \pmod{m}$ we really get that

$$N = \begin{cases} d = (a, m), & \text{if } d \mid b \\ 0, & \text{if } d \nmid b. \end{cases}$$

Proof of Theorem 4.3. Using the previous theorem with $f(x_1, \ldots, x_\ell) = a_1x_1 + \cdots + a_\ell x_\ell - b$ we get:

$$\begin{aligned} N &= \frac{1}{m} \sum_{k=0}^{m-1} \sum_{t_1=0}^{m-1} \cdots \sum_{t_\ell=0}^{m-1} e\left((a_1t_1 + \cdots + a_\ell t_\ell - b)\frac{k}{m}\right) \\ &= \frac{1}{m} \sum_{k=0}^{m-1} e\left(-b\frac{k}{m}\right) \left(\sum_{t_1=0}^{m-1} e\left(a_1t_1\frac{k}{m}\right)\right) \ldots \left(\sum_{t_\ell=0}^{m-1} e\left(a_\ell t_\ell \frac{k}{m}\right)\right) \\ &\qquad \begin{cases} m, & \text{if } m \mid a_1k \\ 0, & \text{if } m \nmid a_1k \end{cases} \cdots \begin{cases} m, & \text{if } m \mid a_\ell k \\ 0, & \text{if } m \nmid a_\ell k \end{cases} \\ &= \frac{1}{m} \sum_{\substack{0 \le k < m \\ m \mid (a_1k, \ldots, a_\ell k)}} e\left(-b\frac{k}{m}\right) m^\ell \end{aligned}$$

$$= \frac{1}{m} \sum_{\substack{0 \le k < m \\ m \mid (a_1, \ldots, a_\ell)k}} e\left(-b\frac{k}{m}\right) m^\ell.$$

Let $d \stackrel{\text{def}}{=} (a_1, \ldots, a_\ell, m)$, and $m = m^* d$, $(a_1, \ldots, a_\ell) = a^* d$, where $(m^*, a^*) = 1$.

The index of the last sum includes $m \mid (a_1, \ldots, a_\ell)k$, let's analyze this a bit:

$$\begin{aligned} m \mid (a_1, \ldots, a_\ell)k &\Leftrightarrow m^* d \mid a^* dk \\ &\Leftrightarrow m^* \mid a^* k \end{aligned}$$

where by $(m^*, a^*) = 1$ we get

$$\Leftrightarrow m^* \mid k.$$

Therefore, in the limits of the sum, we can write $k = m^* t$, where t runs on the numbers $0, 1, \ldots, \frac{m}{m^*} - 1$, i.e., on $0, 1, \ldots, d-1$. Then $\frac{k}{m} = \frac{m^* t}{m^* d} = \frac{t}{d}$. So

$$\begin{aligned} N &= \frac{1}{m} \sum_{t=0}^{d-1} e\left(-b\frac{t}{d}\right) m^\ell \\ &= \begin{cases} m^{\ell-1} d, & \text{if } d \mid b \\ 0, & \text{if } d \nmid b. \end{cases} \end{aligned}$$

This completes the proof of the theorem.

So far we have studied such exponential sums where the exponent is a linear function of the variable, i.e.,

$$e((r(n)),$$

where $r(n)$ is the first degree polynomial of n. The next step is when there is a quadratic polynomial in the exponent. We will study this case in the next chapter.

5 Gauss sums

Definition 5.1 *Let $m \in \mathbb{N}$, $a \in \mathbb{Z}$. Then the sum*

$$S(a,m) = \sum_{x=0}^{m-1} e\left(x^2 \frac{a}{m}\right)$$

is called the Gauss sum.

Theorem 5.1 *If $p > 2$ is a prime, $(a,p) = 1$, then*

$$S(a,p) = \begin{cases} \pm\sqrt{p}, & \text{if } p \equiv 1 \pmod 4 \\ \pm i\sqrt{p}, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Thus $|S(a,p)| = \sqrt{p}$.

Proof of Theorem 5.1. First, we only determine the value of $|S(a,p)|$.

$$\begin{aligned} |S(a,p)|^2 &= S(a,p)\overline{S(a,p)} \\ &= \sum_{x=0}^{p-1} e\left(x^2\frac{a}{p}\right) \sum_{y=0}^{p-1} e\left(-y^2\frac{a}{p}\right) \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e\left((x^2-y^2)\frac{a}{p}\right) \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e\left((x-y)(x+y)\frac{a}{p}\right). \end{aligned}$$

Now, we introduce new variables according to the value of $x - y$. Let

$$x - y \equiv t \pmod p,$$

where $0 \le t \le p-1$ can be assumed. Here only the residue of $x - y \equiv t \pmod p$ is important. Originally, the sums run on x, y.

The new variables are t, y. Thus:

$$\begin{aligned}
|S(a,p)|^2 &= \sum_{t=0}^{p-1}\sum_{y=0}^{p-1} e\left(\frac{t(t+2y)a}{p}\right) \\
&= \sum_{t=0}^{p-1}\sum_{y=0}^{p-1} e\left(\frac{t^2a}{p}\right) e\left(\frac{2tya}{p}\right) \\
&= \sum_{t=0}^{p-1} e\left(\frac{t^2a}{p}\right) \sum_{y=0}^{p-1} e\left(\frac{2tya}{p}\right) \\
&\qquad\qquad \begin{cases} 0, & \text{if } p \nmid 2at, \text{ that is } t > 0 \\ p, & \text{if } p \mid 2at, \text{ that is } t = 0. \end{cases} \\
&= 1 \cdot p,
\end{aligned}$$

whence

$$S(a,p) = \sqrt{p}.$$

If $p \equiv 1 \pmod 4$, then -1 is a quadratic residue. That is, we list all quadratic residues twice on the left and right sides of the following congruence:

$$\{1^2, 2^2, \ldots, (p-1)^2\} \equiv \{-1^2, -2^2, \ldots, -(p-1)^2\} \pmod p.$$

Thus:

$$\begin{aligned}
\overline{S(a,p)} &= \overline{\sum_{x=0}^{p-1} e\left(x^2\frac{a}{p}\right)} \\
&= \sum_{x=0}^{p-1} e\left(-x^2\frac{a}{p}\right) \\
&= S(a,p).
\end{aligned}$$

That is, $S(a,p)$ is real and its absolute value is $\sqrt{p}$. So $S(a,p) = \pm\sqrt{p}$.

If $p \equiv 3 \pmod 4$ then

$$S(a,p) + \overline{S(a,p)} = \sum_{x=0}^{p-1} e\left(x^2 \frac{a}{p}\right) + \sum_{y=0}^{p-1} e\left(-y^2 \frac{a}{p}\right)$$

$$\uparrow \qquad\qquad \uparrow$$

quadratic residues $2\times$ and "0" $1\times$ — quadratic non-residues $2\times$ and "0" $1\times$

$$= 2\sum_{z=0}^{p-1} e\left(z\frac{a}{p}\right)$$

$$= 0.$$

That is Re $S(a,p) = 0$, but since $|S(a,p)| = \sqrt{p}$ we have

$$S(a,p) = \pm i\sqrt{p}.$$

Theorem 5.2 *If $(a,p) = 1$, then*

$$S(a,p) = \left(\frac{a}{p}\right) S(1,p).$$

Proof of Theorem 5.2. We use the following lemma.

Lemma 5.1 *For $a, b \in \mathbb{Z}_p^*$ we have*

$$S(ab^2,p) = S(a,p).$$

Proof of Lemma 5.1. Indeed

$$S(a,p) = \sum_{x=0}^{p-1} e_p(ax^2) = \sum_{x=0}^{p-1} e(\frac{a}{p}x^2).$$

As x runs on $\mathbb{Z}_p$, obviously bx also runs on $\mathbb{Z}_p$ therefore

$$\begin{aligned} S(a,p) &= \sum_{x=0}^{p-1} e_p(a(bx)^2) \\ &= \sum_{x=0}^{p-1} e_p(ab^2x^2) \\ &= S(ab^2,p), \end{aligned}$$

which is the statement of the lemma.

Let us fix a quadratic non-residue $n \pmod p$. Based on the lemma:

$$S(a,p) = S(1,p),$$

if a is quadratic residue. Thus we get

$$S(a,p) = \left(\frac{a}{p}\right) S(1,p)$$

if $\left(\frac{a}{p}\right) = 1$. The case $\left(\frac{a}{p}\right) = -1$ is missing. Also based on the lemma:

$$S(a,p) = S(n,p),$$

if a is quadratic non-residue. Let's study the sum

$$\sum_{a=0}^{p-1} S(a,p).$$

On the one hand, this is

$$S(0,p) + \frac{p-1}{2} S(1,p) + \frac{p-1}{2} S(n,p),$$

since there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues. On the other hand:

$$\sum_{a=0}^{p-1} S(a,p) = \sum_{a=0}^{p-1} \sum_{x=0}^{p-1} e_p(ax^2)$$

$$= \sum_{x=0}^{p-1} \underbrace{\sum_{a=0}^{p-1} e_p(ax^2)}_{\text{This is } 0 \text{ except for } x=0 \text{ when it is } p}$$

$$= p.$$

That is:

$$\underbrace{S(0,p)}_{\text{This is } p} + \frac{p-1}{2} S(1,p) + \frac{p-1}{2} S(n,p) = p.$$

So

$$S(n,p) = -S(1,p)$$
$$S(n,p) = \left(\frac{n}{p}\right) S(1,p).$$

That is, even in the case $\left(\frac{a}{p}\right) = -1$ we have

$$S(a,p) = S(n,p) = -S(1,p) = \left(\frac{a}{p}\right) S(1,p).$$

The following Theorem can be found e.g. in the "small" Vinogradov book [6, page 67, problem 11b β]. We will not prove it here.

Theorem 5.3 *For $m > 2$, $(a,m) = 1$ we have*

1. $$|S(a,m)| = \begin{cases} \sqrt{m}, & \text{if } m \equiv 1 \pmod 2 \\ 0, & \text{if } m \equiv 2 \pmod 4 \\ \sqrt{2m}, & \text{if } m \equiv 0 \pmod 4. \end{cases}$$

2. $$S(1,m) = \begin{cases} (1+i)\sqrt{m}, & \text{if } m \equiv 0 \pmod 4 \\ \sqrt{m}, & \text{if } m \equiv 1 \pmod 4 \\ 0, & \text{if } m \equiv 2 \pmod 4 \\ i\sqrt{m}, & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

Consider the following as an example:

Theorem 5.4 *The number of solutions of the congruence* $x^2+y^2 \equiv a \pmod p$ *is*

$$N = \begin{cases} 2p-1, & \text{if } a \equiv 0 \pmod p,\ p \equiv 1 \pmod 4 \\ p-1, & \text{if } a \not\equiv 0 \pmod p,\ p \equiv 1 \pmod 4 \\ 1, & \text{if } a \equiv 0 \pmod p,\ p \equiv -1 \pmod 4 \\ p+1, & \text{if } a \not\equiv 0 \pmod p,\ p \equiv -1 \pmod 4 \end{cases}$$

The proof of Theorem 5.4. Due to the studied theorem, the number of solutions of $f(x_1,x_2) \overset{\text{def}}{=} x^2+y^2-a \equiv 0 \pmod m$ is

$$\begin{aligned} N &= \frac{1}{p}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{k=0}^{p-1} e\left((x^2+y^2-a)\frac{k}{p}\right) \\ &= \frac{1}{p}\sum_{k=0}^{p-1} e\left(-a\frac{k}{p}\right)\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e\left((x^2+y^2)\frac{k}{p}\right). \end{aligned}$$

Separating the term $k=0$:

$$N = \frac{1}{p^2}\cdot p^2 + \frac{1}{p}\underbrace{\sum_{k=1}^{p-1} S(k,p)^2}$$

$$\text{This is } \begin{cases} p, & \text{if } p \equiv 1 \pmod 4 \\ -p, & \text{if } p \equiv -1 \pmod 4 \end{cases}$$

$$= \delta_p \cdot p, \text{ where } \delta_p = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Thus:

$$N = p + \delta_p \sum_{k=1}^{p-1} e\left(-a\frac{k}{p}\right)$$

$$= p + \delta_p \cdot \begin{cases} p-1, & \text{if } a = 0 \\ -1, & \text{if } a \neq 0 \end{cases}$$

$$= \begin{cases} p + (p-1) = 2p - 1, & \text{if } a \equiv 0 \pmod{p},\ p \equiv 1 \pmod{4} \\ p + 1 \cdot (-1) = p - 1, & \text{if } a \not\equiv 0 \pmod{p},\ p \equiv 1 \pmod{4} \\ p - (p-1) = 1, & \text{if } a \equiv 0 \pmod{p},\ p \equiv -1 \pmod{4} \\ p - 1 \cdot (-1) = p + 1, & \text{if } a \not\equiv 0 \pmod{p},\ p \equiv -1 \pmod{4}. \end{cases}$$

Corollary 5.1 *For each prime* $p \exists\ a, b \in \mathbb{Z}$ *such that*

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

This was used in the proof of the Lagrange's four-square theorem.

Proof of Corollary 5.1. We state that the congruence

$$x^2 + y^2 \equiv -1 \pmod{p}$$

is solvable. This is trivial for $p = 2$ ($x = 0,\ y = 1$). If $p > 2$, then, according to Theorem 5.4, the number of solutions is:

$$N = \begin{cases} p - 1 > 0 & \text{if } p \equiv 1 \pmod{4} \\ p + 1 > 0 & \text{if } p \equiv -1 \pmod{4}. \end{cases}$$

6 Vinogradov's lemma

Next we present an important inequality about additive characters.

Roth noted in the preface to Vinogradov's book [2] that the basis of Vinogradov's method is that the problem in question is derived to estimating of sums of the form

$$\sum_u \sum_v e(\alpha uv).$$

The first step in this direction:

Lemma 6.1 (Vinogradov) *Let* $(a,q)=1$, $q>1$ *and*

$$S \stackrel{\text{def}}{=} \sum_{x=0}^{q-1}\sum_{y=0}^{q-1} \xi(x)\eta(y)e\left(xy\frac{a}{q}\right)$$

(i.e., if we write the additive character $\Psi(n) = e\left(\frac{a}{q}n\right) \mod q$*, then* $S=\sum_x\sum_y \xi(x)\eta(y)\Psi(xy)$*), and let*

$$\sum_{x=0}^{q-1}|\xi(x)|^2 = X_0, \qquad \sum_{y=0}^{q-1}|\eta(y)|^2 = Y_0.$$

Then

$$|S| \le (X_0Y_0q)^{1/2}.$$

The proof of Lemma 6.1. By the Cauchy-Schwarz inequality:

$$\begin{aligned} |S|^2 &= \left|\sum_{x=0}^{q-1}\sum_{y=0}^{q-1} \xi(x)\eta(y)e\left(xy\frac{a}{q}\right)\right| \\ &= \left|\sum_{x=0}^{q-1} \underbrace{\xi(x)}_{a(x)} \underbrace{\sum_{y=0}^{q-1}\eta(y)e\left(xy\frac{a}{q}\right)}_{b(x)}\right| \end{aligned}$$

$$\leq \underbrace{\left(\sum_{x=0}^{q-1}|\xi(x)|^2\right)}_{X_0} \cdot \underbrace{\left(\sum_{x=0}^{q-1}\left|\sum_{y=0}^{q-1}\eta(x)e\left(xy\frac{a}{q}\right)\right|^2\right)}_{\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}\eta(y)e\left(xy\frac{a}{q}\right)\sum_{y'=0}^{q-1}\overline{\eta(y')}e\left(-xy'\frac{a}{q}.\right)}$$

That is

$$|S|^2 \leq X_0 \sum_{y=0}^{q-1}\sum_{y'=0}^{q-1}\eta(y)\overline{\eta(y')}\underbrace{\sum_{x=0}^{q-1}e\left(\frac{x(y-y')a}{q}\right)}$$

$$= \begin{cases} q, & \text{if } q \mid (y-y')a \Leftrightarrow y = y' \\ 0, & \text{if } y \neq y' \end{cases}$$

$$= X_0 \sum_{y=0}^{q-1}\sum_{y'=0}^{q-1}\eta(y)\overline{\eta(y')}q$$

$$= X_0 Y_0 q.$$

Whence:

$$|S| \leq (X_0 Y_0 q)^{1/2}.$$

In the following, we will study an application. If the sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ are large, then the congruence

$$a + b = cd, \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}$$

is solvable in $\mathbb{Z}_p$.

Theorem 6.1 (Sárközy [1], 2005) *If p is a prime, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ and we denote the number of solutions of*

$$a + b = cd, \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D} \tag{6.1}$$

by N, then

$$\left|N - \frac{|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|}{p}\right| \leq (|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|)^{1/2} p^{1/2}.$$

Corollary 6.1 *If p is a prime, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ and*

$$|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}| > p^3, \tag{6.2}$$

than (6.1) *is solvable.*

Remark. Corollary 6.1, i.e., (6.2) is the best possible apart from the best constant factor: consider $\mathcal{A} = \mathcal{B} = \{n : 1 \leq n < p/2\}$, $\mathcal{C} = \mathbb{Z}_p$, $\mathcal{D} = \{0\}$, then

$$|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}| = \left(\frac{1}{4} + o(1)\right) p^3,$$

and (6.1) is not solvable.

The theorem cannot be extended from a prime modulus to a composite one, i.e. from $\mathbb{Z}_p$ to $\mathbb{Z}_m$: If $m = 2k$, $\mathcal{A} = \mathcal{C} = \{2, 4, \ldots, 2k\}$, $\mathcal{B} = \{1, 3, \ldots, 2k-1\}$, $\mathcal{D} = \mathbb{Z}_m$, then

$$|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}| = \left(\frac{1}{8} + o(1)\right) m^4,$$

and (6.1) is not solvable.

Many interesting corollaries exist, e.g. for

$$\mathcal{C} = \mathcal{D} = \{x^k : x \in \mathbb{Z}_p^*\}$$

we have

$$\{cd : c \in \mathcal{C},\ d \in \mathcal{D}\} = \{z^k : z \in \mathbb{Z}_p^*\},$$

thus for $|\mathcal{A}| \cdot |\mathcal{B}| \geq \left(k^2 + o(1)\right) p$ we know that the congruence

$$a + b = x^k \quad a \in \mathcal{A},\ b \in \mathcal{B}$$

is solvable.

So if, for example, $\mathcal{A} = \{x^m : x \in \mathbb{Z}_p^*\}$, $\mathcal{B} = \{y^n : y \in \mathbb{Z}_p^*\}$, then we get that the congruence

$$x^m + y^n \equiv z^k \pmod{p}, \qquad xyz \not\equiv 0 \pmod{p}$$

is solvable. Particularly, the congruence $x^n + y^n \equiv z^n \pmod{p}$, $xyz \not\equiv 0 \pmod{p}$ is solvable (this is the Fermat congruence).

The following corollaries are also important: if $\mathcal{C} = \mathcal{D} = \{z^2 : z \in \mathbb{Z}_p^*\}$ and $|\mathcal{A}| \cdot |\mathcal{B}| \geq (4 + o(1))p$, then

$$\left(\frac{a+b}{p}\right) = 1, \qquad a \in \mathcal{A},\ b \in \mathcal{B}$$

is solvable. Obviously, it also follows that if $|\mathcal{A}| \cdot |\mathcal{B}| \geq (4 + o(1))p$, then

$$\left(\frac{a+b}{p}\right) = -1, \qquad a \in \mathcal{A},\ b \in \mathcal{B}$$

is solvable. Furthermore, the value of the least quadratic non-residue is related to his problem.

Proof of Theorem 6.1. Let $F(a,b,c,d) = a + b - cd$, then by Theorem 4.2 the number of solutions of the congruence

$$F(a,b,c,d) = a + b - cd \equiv 0 \pmod{p}$$

is

$$N = \frac{1}{p} \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \sum_{c \in \mathcal{C}} \sum_{d \in \mathcal{D}} \underbrace{\sum_{k=0}^{p-1} e\left((a+b-cd)\frac{k}{p}\right)}_{\begin{cases} p, & \text{if } a,b,c,d \text{ are solutions} \\ 0, & \text{if } a,b,c,d \text{ are not solutions.} \end{cases}}$$

Usually, the main character, the case $k = 0$ gives the main term, the rest can go to the error term. So that we separate the term $k = 0$:

$$N = \frac{|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|}{p}$$

$$+\frac{1}{p}\sum_{k=1}^{p-1}\sum_{a\in\mathcal{A}} e\left(a\frac{k}{p}\right)\sum_{b\in\mathcal{B}} e\left(b\frac{k}{p}\right)\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}} e\left(-cd\frac{k}{p}\right).$$

Thus

$$\left|N-\frac{|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|\cdot|\mathcal{D}|}{p}\right| \leq \frac{1}{p}\sum_{k=1}^{p-1}\left|\sum_{a\in\mathcal{A}} e\left(a\frac{k}{p}\right)\right|\left|\sum_{b\in\mathcal{B}} e\left(b\frac{k}{p}\right)\right|\left|\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}} e\left(-cd\frac{k}{p}\right)\right|.$$

By Vinogradov's lemma (see Lemma 6.1):

$$\left|\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}} e\left(-cd\frac{k}{p}\right)\right| \leq (|\mathcal{C}||\mathcal{D}|p)^{1/2}.$$

That is

$$\left|N-\frac{|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|\cdot|\mathcal{D}|}{p}\right| \leq \frac{1}{p^{1/2}}(|\mathcal{C}||\mathcal{D}|)^{1/2}\underbrace{\sum_{k=1}^{p-1}\left|\sum_{a\in\mathcal{A}} e\left(a\frac{k}{p}\right)\right|\left|\sum_{b\in\mathcal{B}} e\left(b\frac{k}{p}\right)\right|}_{\text{Cauchy-Schwarz}}$$

$$\leq \frac{1}{p^{1/2}}(|\mathcal{C}||\mathcal{D}|)^{1/2}\left(\sum_{k=1}^{p-1}\left|\sum_{a\in\mathcal{A}} e\left(a\frac{k}{p}\right)\right|^2\right)^{1/2}\left(\sum_{k=1}^{p-1}\left|\sum_{b\in\mathcal{B}} e\left(b\frac{k}{p}\right)\right|^2\right)^{1/2}$$

We know that if $F(\alpha)=\sum_{j=0}^{p-1} a_j e(j\alpha)$ then

$$\sum_{k=0}^{p-1}\left|F\left(\frac{k}{p}\right)\right|^2 = p\sum_{k=0}^{p-1}|a_k|^2. \tag{6.3}$$

(This is a Parseval-type inequality, HW.) Thus:

$$\left|N-\frac{|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|\cdot|\mathcal{D}|}{p}\right| \leq \frac{1}{p^{1/2}}(|\mathcal{C}||\mathcal{D}|)^{1/2}(p|\mathcal{A}|)^{1/2}(p|\mathcal{B}|)^{1/2}$$
$$= p^{1/2}(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|\cdot|\mathcal{D}|)^{1/2}.$$

Proof of Corollary 6.1.

$$\begin{aligned} N &\geq \frac{|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|}{p} - p^{1/2} \left(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|\right)^{1/2} \\ &= p^{1/2} \left(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|\right)^{1/2} \left(\frac{\left(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|\right)^{1/2}}{p^{3/2}} - 1 \right) \\ &> 0. \end{aligned}$$

References

[1] A. Sárközy, *On sums and products of residues modulo p*, Acta Arith. 118 (4) (2005), 403-409.

[2] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, Dover Publications, Revised edition 2004.

7 Weyl sums and Weil theorem

We saw

$$\underbrace{\left|\sum_{x=0}^{p-1} e\left(\frac{ax^2}{p}\right)\right|}_{\text{Gauss sum}} = \sqrt{p}$$

By the method of the proof:

$$\begin{aligned}\left|\sum_x e\left(\frac{f(x)}{p}\right)\right|^2 &= \sum_x e\left(\frac{f(x)}{p}\right)\overline{\sum_y e\left(\frac{f(y)}{p}\right)} \\ &= \sum_x \sum_y e\left(\underbrace{(f(x)-f(y))}_{\underbrace{(x-y)}_{t}\, g(x,y)}/p\right) \\ &= \sum_t \sum_y e\left(tg(t+y,y)/p\right),\end{aligned}$$

here, the degree of $g(t+x,y)$ in y is one less than the degree of f, and thus we reduced the estimation to polynomials of one degree less. Sums of the type $\sum_{x=M}^{N} e\left(f(x)\right)$ are called Weyl sums.

With this idea, Weyl [3] e.g., proved the following:

Theorem 7.1 *If M, N, a and q are integers, where $(a,q)=1$, $q>0$ and f is a polynomial of degree k with real coefficients, where for the leading coefficient a_k holds the inequality*

$$\left|a_k - \frac{a}{q}\right| \leq \frac{t}{q^2},$$

with some $t \geq 1$, then $\forall\, \varepsilon > 0$ we have

$$\sum_{x=M}^{M+N} e(f(x)) = O\left(N^{1+\varepsilon}\left(\frac{t}{q}+\frac{1}{N}+\frac{t}{N^{k-1}}+\frac{q}{N^k}\right)^{2^{1-k}}\right)$$

as $N \to \infty$.

This estimate is non-trivial only if $q < N^k$.

There is another related general theorem:

Theorem 7.2 (Weil [2], 1941) *Let p be a prime, $f(x) \in \mathbb{F}_p[x]$, is a polynomial of degree d, where $1 \le d < p$. Ekkor*

$$\left| \sum_{x=0}^{p-1} e\left(\frac{f(x)}{p} \right) \right| \le (d-1)\sqrt{p}.$$

Sharp: if $f(x) = x^2$.

We do not prove the theorem, since it is based on very deep algebraic geometry. (Later, Stepanov + Schmidt [1] gave an elementary but lengthy proof.)

References

[1] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Lecture Notes in Mathematics, Vol. 536, Springer, 2006.

[2] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.

[3] H. Weyl, *Über die Gleichverteilung von Zahlen mod Eins*, Math. Ann. 77 (1916).

8 Erdős and Moser's problem

Another illustration. Diophantus asked:

How many integers $a_1, a_2, \ldots, a_t$ can be given such that $a_i a_j + 1$ is always a square number if $i \neq j$?

Euler, Fermat, Dujella and many others worked on the problem (including me).

Erdős and Moser asked the following problem independently in 1963:

Let $\mathcal{A} = \{a_1, a_2, \ldots, a_t\}$ such that

$$a_i + a_j$$

is always a square if $i \neq j$. (The sum of different a_i's is always a square.) How large can t be? Can it be arbitrarily large?

Remark: here i and j must be different because otherwise the criterion that

$$a_i + a_i = 2a_i = n^2$$
$$a_i = \frac{n^2}{2}$$

is too strong, in this case, we would get a Pythagorean triple-like problem.

Lagrange [4] and Nicolas [5] gave an example with $t = 6$:

$$\mathcal{A} = \{-15863902, 17798783, 21126338, 49064546, 82221218, 447422978\}.$$

Since then, there is no other example with $t = 6$.

It is possible that $\max t = 6$ and it is very likely that $\max t = O(1)$, but this seems hopeless. Therefore, in the case of sets in the interval $[1, x]$, we estimate the value of t as a function of x.

Theorem 8.1 (Rivat, Stewart, Sárközy [6]) *There exist an integer x_0 such that $x_0 < x \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, 3, \dots, x\}$, and for $a, a' \in \mathcal{A}$ we know that $a + a'$ is a square, then*

$$|\mathcal{A}| < 37 \log x.$$

Proof of Theorem 8.1. Now here is the lemma, which is the essential part, the rest is easy (sieve application)... So the lemma, which is perhaps of independent interest:

Lemma 8.1 *If p is a prime, $p > 2$, $\mathcal{B} \subseteq \mathbb{Z}_p$ and for $b, b' \in \mathcal{B}$, $b \not\equiv b' \pmod p$ we have*

$$\left(\frac{b + b'}{p}\right) = 1 \quad \text{or} \quad b + b' \equiv 0 \pmod p,$$

then

$$|\mathcal{B}| \leq 6\sqrt{p}.$$

Before we go any further, why does it help us?

Consider a "good" $\mathcal{A}$ sequence. If $a, a' \in \mathcal{A}$, $a \neq a'$, then

$$a + a' = n^2,$$

that is

$$\left(\frac{a + a'}{p}\right) = 1 \quad \text{or} \quad a + a' \equiv 0 \pmod p,$$

Thus, due to the lemma, for $\forall\ p$ the set $\mathcal{A}$ intersects only a few $< 6p^{1/2}$ residue classes modulo p.

This shows that $\mathcal{A} \subseteq \{1, 2, \ldots, x\}$ is "sparse" ($|\mathcal{A}|$ "small") as a function of x .

Lemma 8.1 also follows from Sárközy's theorem (Theorem 6.1), but now let's see the original proof.

Proof of Lemma 8.1. Let

$$\mathcal{G}(h,p) = \sum_{x=0}^{p-1} e\left(\frac{hx^2}{p}\right) \quad \text{(Gauss sum)}$$
$$\mathcal{G}_0 = \mathcal{G}(1,p), \quad |\mathcal{G}_0| = \sqrt{p}.$$

Then by Theorem 5.2 we have

$$\mathcal{G}(h,p) = \left(\frac{h}{p}\right)\mathcal{G}(1,p), \quad \text{if } (h,p) = 1.$$

So

$$\mathcal{G}(h,p) = \begin{cases} \mathcal{G}_0, & \text{if } \left(\frac{h}{p}\right) = 1 \\ -\mathcal{G}_0, & \text{if } \left(\frac{h}{p}\right) = -1 \\ p, & \text{if } p \mid h. \end{cases} \tag{8.1}$$

Now consider

$$S \stackrel{\text{def}}{=} \sum_{x=0}^{p-1} \left(\sum_{b \in \mathcal{B}} e\left(\frac{bx^2}{p}\right)\right)^2.$$

Then, by giving an upper-lower estimate for $|S|$, the statement of the lemma follows.

Let's look at the lower estimate first.

$$|S| = \left| \sum_{x=0}^{p-1} \sum_{b \in \mathcal{B}} \sum_{b' \in \mathcal{B}} e\left(\frac{(b+b')x^2}{p}\right)\right|$$
$$= \left| \sum_{b \in \mathcal{B}} \sum_{b' \in \mathcal{B}} \mathcal{G}(b+b', p)\right|$$

$$= \left| \sum_{b \in \mathcal{B}} \sum_{b' \in \mathcal{B}} \mathcal{G}_0 + \sum_{b \in \mathcal{B}} \sum_{b' \in \mathcal{B}} (G(b+b', p) - \mathcal{G}_0) \right|$$

Here in the second term, $\mathcal{G}(b+b', p) - \mathcal{G}_0$ is almost always 0, since $b + b'$ is a quadratic residue for different b, b' or 0, and here we can use (8.1). The only exceptions are the cases when $b \equiv b' \pmod{p}$ or $p \mid b + b'$.

Thus, by the triangle inequality:

$$\begin{aligned} |S| &\geq |\mathcal{B}|^2 |\mathcal{G}_0| - \sum_{b \in \mathcal{B}} |\mathcal{G}(2b, p) - \mathcal{G}_0| - \sum_{\substack{b, b' \in \mathcal{B}, b \neq b' \\ p \mid b + b'}} |\mathcal{G}(0, p) - \mathcal{G}_0| \\ &\geq |\mathcal{B}|^2 \sqrt{p} - \sum_{b \in \mathcal{B}} 2p - \sum_{\substack{b, b' \in \mathcal{B}, b \neq b' \\ p \mid b + b' \\ \uparrow \\ \forall\ b \text{ at least one } b'\ \exists}} 2p \\ &\geq |\mathcal{B}|^2 \sqrt{p} - \sum_{b \in \mathcal{B}} 2p - \sum_{b \in \mathcal{B}} 2p \\ &\geq |\mathcal{B}|^2 \sqrt{p} - 4p|\mathcal{B}|. \end{aligned}$$

On the other hand:

$$|S| \leq \sum_{x=0}^{p-1} \left| \sum_{b \in \mathcal{B}} e\left(\frac{bx^2}{p}\right) \right|^2.$$

As x runs on the residue classes $0, 1, \ldots, p-1$ modulo p, x^2 takes each residue class at most 2 times. So:

$$\begin{aligned} |S| &\leq 2 \sum_{y=0}^{p-1} \left| \sum_{b \in \mathcal{B}} e\left(\frac{by}{p}\right) \right|^2 \\ &\leq 2 \sum_{y=0}^{p-1} \sum_{b \in \mathcal{B}} \sum_{b' \in \mathcal{B}} e\left(\frac{(b-b')y}{p}\right) \end{aligned}$$

$$
\begin{aligned}
&= 2 \sum_{b \in \mathcal{B}} \sum_{b' \in \mathcal{B}} \sum_{y=0}^{p-1} e\left(\frac{(b-b')y}{p}\right) \\
&= 2 \sum_{\substack{b,b' \in \mathcal{B} \\ b-b' \equiv 0 \pmod p \\ \uparrow \\ \text{only for } b=b'}} p \\
&= 2|\mathcal{B}|p.
\end{aligned}
$$

Thus:

$$
\begin{aligned}
|\mathcal{B}|^2\sqrt{p} - 4p|\mathcal{B}| \leq |S| &\leq 2|\mathcal{B}|p \\
|\mathcal{B}|^2\sqrt{p} &\leq 6|\mathcal{B}|p \\
|\mathcal{B}| &\leq 6\sqrt{p}.
\end{aligned}
$$

In the following, we will study the other tool used, Gallagher's larger sieve [2].

The present version was stated by Erdős, Stewart and Sárközy [1] in 1994.

Theorem 8.2 (Gallagher's larger sieve) *Suppose $m, n \in \mathbb{N}$, $\mathcal{A} \subset \{m+1, m+2, \ldots, m+n\}$ and $\mathcal{P} \subset \mathbb{N}$ is a finite set whose elements are pairwise relative primes. For each $p \in \mathcal{P}$, denote by $\nu(p)$ the number of residue classes $\bmod b$ that intersect $\mathcal{A}$. Then*

$$
|\mathcal{A}| \leq \frac{\sum_{p \in \mathcal{P}} \log p - \log n}{\sum_{p \in \mathcal{P}} \frac{\log p}{\nu(p)} - \log n}, \tag{8.2}
$$

provided that the denominator is positive.

First Gallagher formulated this statement in the case when $\mathcal{P}$ contains only primes.

Why do we call such a theorem a sieve? In this case the number of elements of the set $\mathcal{A}$ is estimated using the $\nu(p)$ functions. If $\mathcal{A}$ does not contain elements from many residue classes $\mod p$, then $\nu(p)$ is small, so the fraction in the denominator of (8.2) is large, which gives a strong upper estimate for $|\mathcal{A}|$.

We proved the theorem in the course "Combinatorial Number Theory", see [3].

Theorem 8.1 follows from Gallagher's larger sieve.

Let $m = 1$, $n = x$ and

$$\mathcal{P} = \{p : \ p \text{ is a prime and } p < 36(\log x)^2\}.$$

Denote by $\mathcal{B}_p \subseteq \mathbb{Z}_p$ the set of residue classes mod p for which there exists a congruent $a \in \mathcal{A}$ modulo p:

$$\mathcal{B}_p \stackrel{\text{def}}{=} \{b \in \mathbb{Z}_p : \ \exists a \in \mathcal{A}, b \equiv a \pmod p\}.$$

Since $a + a'$ is always a square, thus $b, b' \in \mathcal{B}_p$-re:

$$\left(\frac{b + b'}{p}\right) = 1 \quad \text{or} \quad b + b' \equiv 0 \pmod p.$$

By Lemma 8.1:

$$\mu(p) = |\mathcal{B}_p| \leq 6p^{1/2}.$$

Using this:

$$|\mathcal{A}| \leq \frac{\sum\limits_{p \leq 36(\log x)^2} \log p - \log x}{\sum\limits_{p \leq 36(\log x)^2} \frac{\log p}{6\sqrt{p}} - \log x}. \tag{8.3}$$

After calculating sums in this formula, we get the following estimate:

$$|\mathcal{A}| \leq 37 \log x.$$

But how do we handle the two sums running on primes: $\sum_{p \leq 36(\log x)^2} \log p$ and $\sum_{p \leq 36(\log x)^2} \frac{\log p}{6\sqrt{p}}$?

There are two options for handling sums running on primes:

Option 1: with the Lebesgue-Stieltjes integral (of the two options, this gives a more accurate estimate). We will say a few words about this option at the end of the chapter, but now we will proceed according to Option 2.

Option 2: with prime number theorem. By this, the expression in the numerator is:

$$\sum_{p \leq 36(\log x)^2} \log p - \log x = \log \left(\prod_{p \leq 36(\log x)^2} p \right) - \log x.$$

According to the Wikipedia page "Primorial" [7] we have $\prod_{p \leq n} = e^{(1+o(1))n}$, thus

$$\begin{aligned} \sum_{p \leq 36(\log x)^2} \log p - \log x &= \log \left(e^{(1+o(1))36(\log x)^2} - \log x \right) \\ &= (1 + o(1))36 \left(\log x \right)^2 - \log x \\ &= (1 + o(1))36 \left(\log x \right)^2 . \end{aligned}$$

Unfortunately, for the denominator, we are not lucky enough to find the sum running on the primes in question on Wikipedia. This must be calculated...

So, now follows the estimate of the denominator. We immediately merged what we could into $o(1)$. Our sum is:

$$\sum_{p \leq 36(\log x)^2} \frac{\log p}{6\sqrt{p}} - \log x.$$

In the interval $[1.36(\log x)^2]$, the primes in increasing order are: $p_1 = 2,\ p_2 = 3, p_3 = 5, \ldots, p_t$. Then

$$\begin{aligned} t &= \pi(36\,(\log x)^2) \\ &= (1+o(1))\frac{36(\log x)^2}{\log\,(36(\log x)^2)} \\ &= (1+o(1))18\frac{(\log x)^2}{\log\log x}. \end{aligned}$$

The sum in the denominator is

$$\sum_{i=1}^{t}\frac{\log p_i}{6\sqrt{p_i}} - \log x = \sum_{i=1}^{(1+o(1))18\frac{(\log x)^2}{\log\log x}}\frac{\log p_i}{6\sqrt{p_i}} - \log x.$$

By prime number theorem:

$$\begin{aligned} p_i &= (1+o(1))i\log i \\ \log p_i &= (1+o(1))\log i \\ \sqrt{p_i} &= (1+o(1))\sqrt{i\log i}. \end{aligned}$$

Thus the sum n the denominator is

$$\sum_{i=1}^{(1+o(1))18\frac{(\log x)^2}{\log\log x}}(1+o(1))\frac{\sqrt{\log i}}{6\sqrt{i}} - \log x.$$

We approximate this with an integral:

$$\int_{i=1}^{(1+o(1))18\frac{(\log x)^2}{\log\log x}}(1+o(1))\frac{\sqrt{\log i}}{6\sqrt{i}} - \log x.$$

The primitive function of $(1+o(1))\frac{\sqrt{\log i}}{6\sqrt{i}}$ is $(1+o(1))\frac{1}{3}\sqrt{i\log i}$ (this is not an exact value, but one in which we allow an error term with ordo. Derive the latter function and get the former function such a way that we keep the main term, and all the other terms can go to the ordo.)

So now

$$\sum_{p\le 36(\log x)^2}\frac{\log p}{6\sqrt{p}}-\log x$$

$$=(1+o(1))\frac{1}{3}\sqrt{i\log i}\Big]_2^{(1+o(1))18\frac{(\log x)^2}{\log\log x}}-\log x$$

$$=(1+o(1))\frac{1}{3}\sqrt{18\frac{(\log x)^2}{\log\log x}\cdot 2\log\log x}-\log x$$

$$=2(1+o(1))\log x-\log x$$

$$=(1+o(1))\log x.$$

That is

$$|\mathcal{A}|\le\frac{(1+o(1))36(\log x)^2}{(1+o(1))\log x}<37\log x.$$

We mentioned that (8.3) can be estimated in a different way (this was the first of the 2 options mentioned), namely with the Lebesgue-Stieltjes integral. These estimates are based on:

$$\sum_{p\le x}f(p)=\int_2^x f(t)d\,pi(t)$$

$$=f(t)\pi(t)\Big|_2^x-\int_2^x f'(t)\pi(t)dt$$

It is your turn to work out this approach. In this regard, those interested can also view the following: link.

It would follow:

$$\sum_{x=1}^{q}e\left(\frac{x^k a}{q}\right),\sum_{x=1}^{q}e\left(f(x)\frac{a}{q}\right),\sum_{x=m}^{n}e\left(f(x)\frac{a}{q}\right),$$

Waring, Weil sum... Later... However, now in the next chapter there is one more sum with additive characters, after which we will move on to multiplicative characters.

References

[1] P. Erdős, A. Sárközy, C.L. Stewart, *On prime factors of subset sums*, Journal of the London Math. Soc. 49 (2) (1994), 209-218.

[2] P. X. Gallagher, *A larger sieve*, Acta Arithmetica 18 (1971), 77-81.

[3] K. Gyarmati, *Elementary Methods to Combinatorial Number Theory*, prelimenary version.

[4] J. Lagrange, *Six entiers dont les sommes deux à deux sont des carrés*, Acta Arithmetica, 40 (1981), 91–96.

[5] J.-L. Nicolas, *Six nombres dont les sommes deux à deux sont des carrés*, in Utilisation des calculateurs en mathématiques pures (1975, Limoges), Mémoires de la Société Mathématique de France 49-50 (1977), 141-143.

[6] J. Rivat, A. Sárközy and C.L. Stewart, *Congruence properties of the Omega-function on sumsets*, Illinois J. Math., 43 (1999), 1-18.

[7] Wikipedia, *Primorial*, link.

9 Kloosterman sums

Two definitions:

Definition 9.1 *If $q \in \mathbb{N}$, $q > 1$, $a, b \in \mathbb{Z}$, then the sum*

$$U(a,b;q) \stackrel{\text{def}}{=} \sum_{\substack{0 \le x < q \\ (x,q)=1}} e\left(\frac{ax + bx^*}{q}\right)$$

(where x^* is defined by $xx^* \equiv 1 \pmod{q}$) is called Kloosterman sum.

Definition 9.2 *A sum of type*

$$\sum_{x=1}^{q} e\left(f(x)\frac{a}{q}\right) \quad \text{or} \quad \sum_{\substack{1 \le x \le q \\ (x,q)=1}} e\left(f(x)\frac{a}{q}\right)$$

is called complete, while a sum of type

$$\sum_{u < x < v} e\left(f(x)\frac{a}{q}\right) \quad \text{or} \quad \sum_{\substack{u < x < v \\ (x,q)=1}} e\left(f(x)\frac{a}{q}\right)$$

is called incomplete.

So far we have studied complete sums (Ramanujan sums, Gauss sums); the above Kloosterman sums are also complete, but incomplete sums can also be defined by

$$U(a,b;q) \stackrel{\text{def}}{=} \sum_{\substack{u < x < q \\ (x,q)=1}} e\left(\frac{ax + bx^*}{q}\right).$$

Incomplete Kloosterman sums will be discussed later.

First complete Kloosterman sums. Some basic properties (see "small" Vinogradov [2, page 51] or Hooley [1]):

Theorem 9.1

a) $U(a,b;q) \quad \forall\, a,b,q$ *is real.*

b) $U(a,b;q) = U(b,a;q) \quad \forall\, a,b,q$.

c) *If* $(h,q) = 1$ *then*

$$U(a,bh;q) = U(ah,b;q).$$

d) *Multiplicative property: If* $q_1, q_2 \in \mathbb{N}$, $q_1, q_2 > 1$, $(q_1,q_2) = 1$ *and for given* a, b, q_1, q_2 *we define* b_1, b_2 *such that*

$$b_1 q_2^2 + b_2 q_1^2 \equiv b \pmod{q_1 q_2} \tag{9.1}$$

holds, then

$$U(a,b;q_1q_2) = U(a,b;q_1)U(a,b;q_2).$$

Proof of Theorem 9.1.

a) It's enough to prove: $\overline{U(a,b;q)} = U(b,a;q)$.

Indeed:

$$\begin{aligned}
\overline{U(a,b;q)} &= \sum_{\substack{0\le x<q\\(x,q)=1}} \overline{e\left(\frac{ax+bx^*}{q}\right)} \\
&= \sum_{\substack{0\le x<q\\(x,q)=1}} e\left(\frac{a(-x)+b\overbrace{(-x^*)}^{(-x)^*}}{q}\right) \\
&= \sum_{\substack{0\le y<q\\(y,q)=1}} e\left(\frac{ay+by^*}{y}\right) \\
&= U(a,b;q)
\end{aligned}$$

b), c) Similarly easy, HW.

d) Here the key is: With this property d), the study of Kloosterman sums can be reduced to the case $q = p^\alpha$.

During the proof, we start from the following: if

$$x(u,v) \stackrel{\text{def}}{=} uq_2 + vq_1$$

and u runs on a reduced residue system mod q_1, and v runs on a reduced residue system mod q_2, then $x(u,v)$ runs on a reduced residue system mod q_1q_2.

So on the left-hand side

$$U(a,b;q) = \sum_{\substack{1\le x\le q\\(x,q)=1}} e\left(\frac{ax+bx^*}{q}\right)$$

is included, where the summation for x means that x runs over reduced residue system $\mod q_1q_2$. Instead of x we may take $\to x(u,v)$, where u,v runs as above:

$$U(a,b;q_1q_2) = \sum_{\substack{1\le u\le q_1\\(u,q_1)=1}} \sum_{\substack{1\le v\le q_2\\(v,q_2)=1}} e\left(\frac{ax(u,v)+bx(u,v)^*}{q_1q_2}\right)$$

Here, by to the definition of $*$, $x^*(u,v)$ is such that

$$\begin{aligned} \underbrace{x(u,v)}_{uq_2+vq_1}\ x^*(u,v) &\equiv 1 \pmod{q_1q_2}\\ uq_2x^*(u,v) + vq_1x^*(u,v) &\equiv 1 \pmod{q_1q_2}\\ uq_2x^*(u,v) &\equiv 1 \pmod{q_1}\\ vq_1x^*(u,v) &\equiv 1 \pmod{q_2}. \end{aligned} \tag{9.2}$$

Thus, using this and $b \equiv b_1 q_2^2 + b_2 q_1^2 \pmod{q_1 q_2}$

$$e\left(\frac{ax(u,v) + bx(u,v)^*}{q_1 q_2}\right) = \\ = e\left(\frac{a(uq_2 + vq_1) + (b_1 q_2^2 + b_2 q_1^2)x^*(u,v)}{q_1 q_2}\right) \\ = e\left(\frac{au}{q_1} + \frac{av}{q_2} + \frac{b_1 q_2 x^*(u,v)}{q_1} + \frac{b_2 q_1 x^*(u,v)}{q_2}\right).$$

Here by (9.2):

$$q_2 x^*(u,v) \equiv u^* \pmod{q_1}$$
$$q_1 x^*(u,v) \equiv v^* \pmod{q_2},$$

that is

$$e\left(\frac{ax(u,v) + bx(u,v)^*}{q_1 q_2}\right) = e\left(\frac{au}{q_1} + \frac{av}{q_2} + \frac{b_1 u^*}{q_1} + \frac{b_2 v^*}{q_2}\right) \\ = e\left(\frac{au + b_1 u^*}{q_1}\right) e\left(\frac{av + b_1 v^*}{q_2}\right).$$

So

$$U(a,b;q_1 q_2) = \sum_{\substack{0 \le u < q_1 \\ (u,q_1)=1}} e\left(\frac{au + b_1 u^*}{q_1}\right) \sum_{\substack{0 \le v < q_2 \\ (v,q_2)=1}} e\left(\frac{av + b_2 v^*}{q_2}\right) \\ = U(a,b;q_1)U(a,b;q_2).$$

After this, what is known about the absolute value of a Kloosterman sum?

Theorem 9.2

a) For $(a,p) = (b,p) = 1$ we have $|U(a,b;p)| \le 2\sqrt{p}$.

b) $\forall\ a, b$ we have $|U(a,b;p)| \le 2\sqrt{p(b,p)}$.

c) *In case of* $\alpha \in \mathbb{N}$, $\alpha > 1$, $(a,p) = (b,p) = 1$ *we have*

$$|U(a,b;p^\alpha)| \leq 3\sqrt{p^\alpha}.$$

d) $\forall\ a, b$*:*

$$|U(a,b;p^\alpha)| \leq d(p^\alpha)\sqrt{p(b,p^\alpha)}.$$

e) $\forall\ a, b, q$*:*

$$|U(a,b;q)| \leq d(q)\sqrt{p(b,q)}.$$

Proof of Theorem 9.2.

a) This is due to Weil, who used very deep, algebraic geometry, we will not prove it.

b) 3 cases:

1. $(a,p) = (b,p) = 1$: same as a).
2. $p \mid b$: Then $|U(a,b;p)| \leq p$ trivially. Right-hand side $2\sqrt{p(b,p)} = 2p$.
3. $p \mid a$, $(b,p) = 1$:

$$\begin{aligned} U(a,b;p) &= \left| \sum_{\substack{0 \leq x < p \\ (x,p)=1}} e\left(\frac{bx^*}{p}\right) \right| \\ &= \left| \sum_{y=1}^{p-1} e\left(\frac{y}{p}\right) \right| \\ &= 1. \end{aligned}$$

c) Salié proved it elementary, we will not prove.

d) This follows from b) and c). HW.

e) The multiplicative property of Theorem 9.1 + d). HW.

So far we have studied complete Kloosterman sums. Usually handling incomplete exponential sums, estimation is much more difficult; usually only much weaker estimates can be given. 2 important exceptions: Gauss sums (we will return this) and Kloosterman sums; this is partly their importance.

Theorem 9.3 *If* $\varepsilon > 0$, $q \in \mathbb{N}$, $q > q_0(\varepsilon)$, $a, b \in \mathbb{Z}$ *and* $0 \leq v - u \leq 2q$, *then*

$$\left| \sum_{\substack{u \leq x \leq v \\ (x,q)=1}} e\left(\frac{ax + bx^*}{q}\right) \right| < q^{1/2+\varepsilon}\sqrt{(b,q)}.$$

Proof of Theorem 9.3. It can be deduced from the previous theorem; we will use similar technique in case of Pólya-Vinogradov's theorem (see also Hooley [1, page 36].)

References

[1] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, (Cambridge Tracts in Mathematics, Series Number 70, Cambridge University Press, 1976.

[2] I. M. Vinogradov, *Elements of Number Theory*, Dover Publications, Reprint edition 2016.

10 Multiplicative characters

We have seen that there are two important finite groups in number theory: $\mathbb{Z}_m$ and Z_m^* (= multiplicative group of reduced residue classes mod m.)

We discussed the former; now we will study the group characters defined on the latter. But for technical reasons, we will slightly modify (extend) the original definition.

Definition 10.1 *If $m \in \mathbb{N}$, then a function $\chi(n) : \mathbb{Z} \to \mathbb{C}$ is called multiplicative character if $\exists$ a group character χ_1 defined on $\mathbb{Z}_m^*$ such that*

$$\chi(n) = \begin{cases} \chi_1(n), & \text{if } (n,m) = 1 \\ 0, & \text{if } (n,m) > 1. \end{cases}$$

(So, actually, the only difference is that if $(n,m) > 1$ then $\chi(n)$ is taken as 0.)

It could also be defined without group characters:

Definition 10.2 *For $m \in \mathbb{N}$, a function $\chi(n) : \mathbb{Z} \to \mathbb{C}$ is called a multiplicative character if*

a) $u, v \in \mathbb{Z}$, $u \equiv v \pmod{m} \Rightarrow \chi(u) = \chi(v)$.

b) $u, v \in \mathbb{Z} \Rightarrow \chi(uv) = \chi(u)\chi(v)$.

c) $(n,m) > 1 \Rightarrow \chi(n) = 0$.

d) $\chi(n) \not\equiv 0$.

The equivalence of the two definitions is HW.

Example. Let p be a prime. Then

$$\chi(n) = \begin{cases} \left(\frac{a}{p}\right), & \text{if } (a,p) = 1 \\ 0, & \text{if } p \mid a. \end{cases}$$

The following basic properties of the multiplicative characters mod m follow from the studied properties of group characters (see Corollary 3.1).

1. $\chi(1) = 1$.

2. For $(a, m) = 1$, $\chi(a)$ is a $\varphi(m)$ $(= |Z_m^*|)$-th root of unity.

3. The character

$$\chi_0(a) = \begin{cases} 1, & \text{if } (a, n) = 1 \\ 0, & \text{if } (a, n) > 1 \end{cases}$$

   is the so-called main character.
   χ is a character $\Rightarrow$ $\overline{\chi}$ is also a character, where $\overline{\chi}(a) = \overline{\chi(a)}$ $(= \chi(a^{-1}))$
   χ_1, χ_2 are characters $\Rightarrow$ $\chi_1\chi_2$ is also a character, where $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$.

4. The number of characters mod m is $\varphi(m)$.

5.
$$\sum_{a=1}^{m} \chi(a) = \begin{cases} \varphi(m), & \text{if } \chi = \chi_0 \\ 0, & \text{if } \chi \neq \chi_0. \end{cases}$$

6.
$$\sum_{\chi \pmod m} \chi(a) = \begin{cases} \varphi(m), & \text{if } a = 1 \\ 0, & \text{if } a \neq 1. \end{cases}$$

Theorem 10.1 *If $a, n_1, n_2, \ldots, n_t \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$, then*

$$|\{i : 1 \leq i \leq t,\ n_i \equiv a \pmod m\}| = \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi}(a) \sum_{i=1}^{t} \chi(n_i).$$

Because of the studied properties of group characters, it is enough to write $\mathbb{Z}_m^*$ as a direct product of cyclic groups. By the Chinese remainder theorem, for $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ we have

$$\mathbb{Z}_m^* = \mathbb{Z}_{p_1^{\alpha_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}^*.$$

If $\mathbb{Z}_{p_i^{\alpha_i}}^*$ were always cyclic, i.e., there would be a primitive root for $\forall\ p_i^{\alpha_i}$, we would be ready. Unfortunately, this is not the case. Two number theory theorems follow:

Theorem 10.2 *There $\exists$ a primitive root mod m if and only if $m = 2, 4, p^\alpha$ or $2p^\alpha$, where $p > 2$ is a prime.*

Theorem 10.3 *For $\alpha > 2$ we have*

$$\mathbb{Z}_{2^\alpha}^* = \{-1\}_2 \times \{5\}_{2^{\alpha-2}}$$

Proof of Theorems 10.2 and 10.3. See "small" Vinogradov [2, 76-78. page].

Using these two auxiliary theorems of number theory it follows that the explicit form of mod m multiplicative characters is the following:

Theorem 10.4 *Let $m = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where $2 < p_1 < \cdots < p_k$, $0 \le \beta, 0 < \beta_1, \ldots, \beta_k$. Moreover let g_i be a primitive root* mod $p_i^{\alpha_i}$. *Then $\chi : \mathbb{Z}_m \to \mathbb{C}$ is a multiplicative character modulo m if and only if $\exists$ integers $a_1, a_2, b_1, \ldots, b_k$ such that*

$$0 \le a_1 < c_1 \overset{\text{def}}{=} \begin{cases} 1, & \text{if } \alpha = 0 \text{ or } 1 \\ 2, & \text{if } \alpha \ge 2, \end{cases}$$

$$0 \le a_2 \le c_2 \overset{\text{def}}{=} \begin{cases} 1, & \text{if } \alpha = 0 \text{ or } 1 \\ 2^{\alpha-2}, & \text{if } \alpha \ge 2 \end{cases}$$

and

$$0 \le b_i \le \varphi(p_i^{\alpha_i}) - 1,$$

moreover

a) *for* $(n, m) = 1$ *define the integers* $k_1, k_2, \ell_1, \dots, \ell_k$ *by*

$$n \equiv (-1)^{k_1} 5^{k_2} \pmod{2^\beta}, \quad 0 \le k_1 < c_1,\ 0 \le k_2 < c_2$$
$$n \equiv g_i^{\ell_i} \pmod{p_i^{\alpha_i}}, \quad 0 \le \ell_i < \varphi(p_i^{\alpha_i}),$$

then

$$\chi(n) = e\left(k_1 \frac{a_1}{c_1} + k_2 \frac{a_2}{c_2} + \ell_1 \frac{b_1}{\varphi(p_1^{\alpha_1})} + \dots + \ell_k \frac{b_k}{\varphi(p_k^{\alpha_k})}\right)$$

b) *For* $(n, m) > 1$, $\chi(n) = 0$.

Proof of Theorem 10.4. Davenport [1, 29. page], "small" Vinogradov [2, 80. page].

Definition 10.3 *We call the character* χ mod m *primitive, if* $\nexists$ *integer* m_1 *such that* χ_1 *is a character* mod m_1, *where* $m_1 \mid m$, $m_1 < m$ *and for* $n \in \mathbb{Z}$, $(n, m) = 1$ *we have* $\chi(n) = \chi_1(n)$. *If, on the other hand, such* m_1, χ_1 *exists, then* χ *is imprimitive, and the smallest* m_1 *with this property called the "conductor" of* χ, *and* χ *itself is said to be induced by character* χ_1.

Remark.

1. According to Davenport, χ_0 is neither primitive nor imprimitive.
2. If p is prime, then every mod p character $\chi \neq \chi_0$ is primitive.
3. Another possible definition: χ imprimitive, if $\exists\ m_1 \mid m$, $1 < m_1 < m$ such that the values of $\chi(n)$ for n satisfying $(n.m) = 1$ are periodic with period m_1.

References

[1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics 74, Springer New York, 2013, Originally published by Markham Publishing Co., 1967.

[2] I. M. Vinogradov, *Elements of Number Theory*, Dover Publications, Reprint edition 2016.

11 Gauss sums (part 2)

Definition 11.1 *if $q \in \mathbb{N}$ and χ is a character mod m, then the sum*

$$\tau(\chi) = \sum_{m=0}^{q-1} \chi(m) e\left(\frac{a}{m}\right)$$

is also called the Gauss sum.

Why?

We first proved that if p is prime and $(a, p) = 1$, then the absolute value of the Gauss sum

$$S(a, p) = \sum_{x=0}^{p-1} e\left(x^2 \frac{a}{p}\right)$$

is

$$|S(a, p)| = \sqrt{p}.$$

Consider the following Gauss sum $S(a, p)$:

$$\begin{aligned} S(a,p) &= \sum_{x=0}^{p-1} e\left(x^2\frac{a}{p}\right) \\ &= 1 + \sum_{x=1}^{p-1} \underbrace{e\left(x^2\frac{a}{p}\right)}_{\substack{x^2 \equiv (-x)^2 \equiv y \\ \text{counted 2x if } \left(\frac{y}{p}\right)=1, \\ \text{counted 0x if} \left(\frac{y}{p}\right)=-1}} \\ &= 1 + \sum_{y=1}^{p-1} \left(\left(\frac{y}{p}\right) + 1\right) e\left(y\frac{a}{p}\right) \\ &= \underbrace{\sum_{y=0}^{p-1} e\left(y\frac{a}{p}\right)}_{=0, \text{ by } (a,p)=1} + \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) e\left(y\frac{a}{p}\right) \end{aligned}$$

$$= \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) e\left(y\frac{a}{p}\right)$$

Let

$$\chi(n) = \begin{cases} \left(\frac{n}{p}\right), & \text{if } (n,p) = 1 \\ 0 & \text{if } (n,p) > 1. \end{cases}$$

Then $S(a,p)$ is of the form

$$S(a,p) = \sum_{y=0}^{p-1} \chi(y) e\left(\frac{ya}{p}\right).$$

Here substituting $ya \equiv t \pmod p$ we get $y \equiv ta^* \pmod p$, where a^* is the multiplicative inverse of a. That is:

$$\begin{aligned} S(a,p) &= \sum_{t=0}^{p-1} \chi(ta^*) e\left(\frac{t}{p}\right) \\ &= \chi(a^*) \sum_{t=0}^{p-1} \chi(t) e\left(\frac{t}{p}\right) \\ &= \overline{\chi(a)} \underbrace{\sum_{t=0}^{p-1} \chi(t) e\left(\frac{t}{p}\right)}_{\text{Considering this the definition is clear.}} \end{aligned}$$

Theorem 11.1 *If $m \in \mathbb{N}$, χ is a primitive character mod m, then*

$$|\tau(\chi)| = \sqrt{m}.$$

Proof of Theorem 11.1. We only prove if m is a prime p. Then χ being primitive means $\chi \neq \chi_0$. Thus

$$\begin{aligned} |\tau(\chi)|^2 &= \sum_{a=1}^{p-1} \chi(a) e\left(\frac{a}{p}\right) \sum_{b=1}^{p-1} \overline{\chi(b) e\left(\frac{b}{p}\right)} \\ &= \sum_{a=1}^{p-1} \chi(a) e\left(\frac{a}{p}\right) \sum_{b=1}^{p-1} \underbrace{\overline{\chi(b)}}_{\chi(b^*)} e\left(-\frac{b}{p}\right) \end{aligned}$$

$$= \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(ab^*) e\left(\frac{a-b}{p}\right)$$

Let $ab^* \equiv t \pmod{p}$, so $a \equiv tb \pmod{p}$. Then

$$\begin{aligned}
|\tau(\chi)|^2 &= \sum_{t=1}^{p-1} \sum_{b=1}^{p-1} \chi(t) e\left(\frac{bt-b}{p}\right) \\
&= \sum_{t=1}^{p-1} \left(\underbrace{\sum_{b=0}^{t-1} e\left(\frac{b(t-1)}{p}\right)}_{\begin{cases} p, & \text{if } t=1 \\ 0, & \text{if } t \neq 1 \end{cases}} - 1 \right) \\
&= \chi(1)(p-1) + \sum_{t=2}^{p-1} \chi(t)(-1) \\
&= p - 1 + \sum_{t=1}^{p-1} \chi(t) + \chi(1) \\
&= 0.
\end{aligned}$$

In the following, we study a transition formula from a multiplicative to an additive character.

Theorem 11.2 *If $q \in \mathbb{N}$, $n \in \mathbb{Z}$, χ is multiplicative character mod p and*

a) $(n, q) = 1$

or

b) χ *is a primitive character, then*

$$\chi(n)\tau(\overline{\chi}) = \sum_{h=0}^{q-1} \overline{\chi}(h) e\left(n\frac{h}{p}\right).$$

Proof of Theorem 11.2. a)

$$\begin{aligned}\chi(n)\tau(\overline{\chi}) &= \underbrace{\chi(n)}_{\overline{\chi}(n^*)} \sum_{m=0}^{q-1} \overline{\chi}(m) e\left(\frac{m}{q}\right) \\ &= \sum_{m=0}^{q-1} \overline{\chi}(mn^*) e\left(\frac{m}{q}\right) \\ &= \sum_{h=0}^{q-1} \overline{\chi}(h) e\left(\frac{hn}{q}\right),\end{aligned}$$

where in the last line $h \equiv mn^* \pmod{q} \Leftrightarrow m \equiv hn \pmod{q}$. b) More complicated, see Davenport [1, 65. page].

References

[1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics 74, Springer New York, 2013, Originally published by Markham Publishing Co., 1967.

12 The dual of Vinogradov's lemma

Applying the transition formula studied in the previous chapter, i.e., Theorem 11.2, we will prove the dual of Vinogradov lemma (see Lemma 6.1).

For, as follows, there is a duality principle according to which, in the case of certain theorems, additive characters can be replaced by multiplicative characters, and products by sums, and vice versa, and proofs are often convertible. Now we will see an example of this.

In Chapter 6, we proved the following in Lemma 6.1:

Theorem 12.1 (Vinogradov) *Let* $(a,q)=1$, $q>1$ *and*

$$S \stackrel{\text{def}}{=} \sum_{x=0}^{q-1}\sum_{y=0}^{q-1} \xi(x)\eta(y)e\left(xy\frac{a}{q}\right)$$

(i.e., if we write the additive character $\Psi(n) = e\left(\frac{a}{q}n\right) \mod q$*, then* $S=\sum_x\sum_y \xi(x)\eta(y)\Psi(xy)$*), and let*

$$\sum_{x=0}^{q-1}|\xi(x)|^2 = X_0, \qquad \sum_{y=0}^{q-1}|\eta(y)|^2 = Y_0.$$

Then

$$|S| \le (X_0Y_0q)^{1/2}.$$

Particularly, if $q=p$ is prime, then the condition $(a,q)=(a,p)=1$ in the theorem states that $\Psi \neq \Psi_0$ (here, $\Psi(n)=e\left(\frac{a}{q}n\right)$). Thus, in this special case, we get:

The dual of the above theorem is::

Theorem 12.2 (Gyarmati - Sárközy [7]) *If p is a prime and $\chi \neq \chi_0$ is a multiplicative character modulo p, then*

$$|S| = \left| \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x)\eta(y)\chi(x+y) \right| \leq (X_0 Y_0 p)^{1/2},$$

where

$$\sum_{x=0}^{p-1} |\xi(x)|^2 = X_0, \qquad \sum_{y=0}^{p-1} |\eta(y)|^2 = Y_0.$$

Remark. Both Vinogradov's lemma and its dual above can be easily extended from $\mathbb{F}_p$ to any finite field.

Corollary 12.1 *If p is prime and $\xi(x)$ and $\eta(y)$ are characteristic functions of certain sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$, i.e.,*

$$\xi(x) = \begin{cases} 1, & \text{if } x \in \mathcal{A} \\ 0, & \text{if } x \notin \mathcal{A} \end{cases} \qquad \eta(y) = \begin{cases} 1, & \text{if } y \in \mathcal{B} \\ 0, & \text{if } y \notin \mathcal{B}, \end{cases}$$

then

$$\left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(a+b) \right| \leq (|\mathcal{A}||\mathcal{B}|p)^{1/2}.$$

This theorem was proved by Erdős and Shapiro [4] in 1957.

We note that if χ is the quadratic character, i.e., $\chi(n) = \left(\frac{n}{p}\right)$ if $(n,p) = 1$ and $\chi(n) = 0$, if $(n.p) > 1$, then we get the following:

$$\left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \left(\frac{a+b}{p}\right) \right| \leq (|\mathcal{A}||\mathcal{B}|p)^{1/2}.$$

The proof of Theorem 12.2. Since p is prime and $\chi \neq \chi_0$, χ is a primitive character. Thus, the transformation formula, i.e., Theorem

11.2 can be applied:

$$\chi(n)\tau(\overline{\chi}) = \sum_{h=0}^{p-1} \overline{\chi}(h) e\left(n\frac{h}{p}\right).$$

Since χ is primitive $\tau(\overline{\chi}) = \sqrt{p} \neq 0$, so we can divide it by:

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{p-1} \overline{\chi}(h) e\left(n\frac{h}{p}\right).$$

That is, $|S|$ can be estimated as follows:

$$\begin{aligned}
|S| &= \left| \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x)\eta(y) \left(\frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{p-1} \overline{\chi}(h) e\left((x+y)\frac{h}{p}\right) \right) \right| \\
&= \frac{1}{|\tau(\overline{\chi})|} \left| \sum_{h=0}^{p-1} \overline{\chi}(h) \sum_{x=0}^{p-1} \xi(x) e\left(x\frac{h}{p}\right) \sum_{y=0}^{p-1} \eta(y) e\left(y\frac{h}{p}\right) \right| \\
&\leq \frac{1}{\sqrt{p}} \sum_{h=0}^{p-1} \left| \sum_{x=0}^{p-1} \xi(x) e\left(x\frac{h}{p}\right) \right| \left| \sum_{y=0}^{p-1} \eta(y) e\left(y\frac{h}{p}\right) \right|
\end{aligned}$$

By the Cauchy-Schwarz inequality:

$$|S| \leq \frac{1}{\sqrt{p}} \left(\sum_{h=0}^{p-1} \left| \sum_{x=0}^{p-1} \xi(x) e\left(x\frac{h}{p}\right) \right|^2 \right)^{1/2} \left(\sum_{h=0}^{p-1} \left| \sum_{y=0}^{p-1} \eta(y) e\left(y\frac{h}{p}\right) \right|^2 \right)^{1/2}$$

According to a previously studied Parseval formula (see (6.3)):

$$\begin{aligned}
|S| &\leq \frac{1}{\sqrt{p}} \left(p \sum_{x=0}^{p-1} |\xi(x)|^2 \right)^{1/2} \left(p \sum_{y=0}^{p-1} |\eta(y)|^2 \right)^{1/2} \\
&= \frac{1}{\sqrt{p}} \left(pX_0\right)^{1/2} \left(pY_0\right)^{1/2} \\
&= \left(pX_0Y_0\right)^{1/2}.
\end{aligned}$$

As we saw, for example, related to Diophantus' problem (Chapter 8), a multiplicative problem (e.g. $aa' + 1$ is always a square number

if $a \neq a'$ and $a, a' \in \mathcal{A}$) has an additive analog ($a + a'$ is always a square number if $a \neq a'$ and $a, a' \in \mathcal{A}$), and vice versa.

So if we have a statement for sums of type $a + b$, an interesting question is whether the same can be said for $ab + 1$.

Thus, for example, it is an interesting question whether the estimate of $\left|\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\eta(y)\chi(x+y)\right|$ can be converted to the estimate of $\left|\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\eta(y)\chi(xy+1)\right|$? The answer to this question is affirmative, i.e. the following is true:

Corollary 12.2 (Gyarmati - Sárközy) *If p is a prime and $\chi \neq \chi_0$ is a multiplicative character modulo p, then*

$$|S| = \left|\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\eta(y)\chi(xy+1)\right| \leq (pX_0)^{1/2}\left(Y_1^{1/2} + |\eta(0)|\right),$$

where

$$\sum_{x=0}^{p-1}|\xi(x)|^2 = X_0, \qquad \sum_{y=1}^{p-1}|\eta(y)|^2 = Y_1.$$

Proof of Corollary 12.2. Basically, the proof is just that we apply Theorem 12.2 with $\eta(y^{-1})\chi(y^{-1})$ in place of $\eta(y)$ and then introducing the new variable $z = x^{-1}$ in the sum, we get the desired result:

$$\begin{aligned}|S| &= \left|\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\eta(y)\chi(xy+1)\right| \\ &\leq \left|\sum_{x=0}^{p-1}\sum_{y=1}^{p-1}\xi(x)\underbrace{\eta(y)\chi(y)}_{=\eta'(y^{-1})=\eta'(z)}\chi(x+\underbrace{y^{-1}}_{=z})\right| + \left|\sum_{x=0}^{p-1}\xi(x)\eta(0)\underbrace{\chi(1)}_{=1}\right|\end{aligned}$$

$$\leq \left(pX_0 \underbrace{\sum_{z=1}^{p-1} |\eta'(z)|^2}_{\text{Cauchy-Shwarz}} \right)^{1/2} + \underbrace{\left| \sum_{x=0}^{p-1} \xi(x) \right|}_{\text{Cauchy-Shwarz}} |\eta(0)|$$

$$\sum_{z=1}^{p-1} |\eta(z^{-1})|^2 \underbrace{\left|\chi(z^{-1})\right|^2}_{=1} = Y_1$$

$$\leq (pX_0Y_1)^{1/2} + |\eta(0)| \, (X_0 p)^{1/2}$$

$$= (pX_0)^{1/2} \left(Y_1^{1/2} + |\eta(0)| \right).$$

Corollary 12.3 *If p is a prime, $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$, $0 \notin \mathcal{B}$, $\xi(x)$ and $\eta(y)$ are the characteristic functions of $\mathcal{A}$ and $\mathcal{B}$, then:*

$$\left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(ab+1) \right| \leq (|\mathcal{A}||\mathcal{B}|p)^{1/2}.$$

I proved this last corollary in [6], and even earlier Vinogradov studied the case $\chi(n) = \left(\frac{n}{p}\right)$.

Speaking of additive and multiplicative analogies (the cases $a+b$ and $ab+1$), we mention that Sárközy in Theorem 6.1 studied the solvability of the equation

$$a + b = cd, \ a \in \mathcal{A}, \ b \in \mathcal{B}, \ c \in \mathcal{C}, \ d \in \mathcal{D}, \tag{12.1}$$

if $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ are large sets.

An interesting problem is the multiplicative analogue of the above:

Theorem 12.3 (Sárközy [9], 2005) *If p is a prime, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ and we denote the number of solutions of*

$$ab + 1 = cd, \quad a \in \mathcal{A}, \ b \in \mathcal{B}, \ c \in \mathcal{C}, \ d \in \mathcal{D} \tag{12.2}$$

by N, then

$$\left| N - \frac{|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}|}{p} \right| \leq 8 \left(|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| \right)^{1/2} p^{1/2} + 4p^2.$$

Corollary 12.4 *If p is a prime, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ and*

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > 100p^3,$$

then (12.2) *is solvable.*

Proof of Theorem 12.3. The proof is HW, we only mention that it is similar to the proof of Theorem 6.1, with the difference that for the estimation of $|\sum_a \sum_b \chi(ab+1)|$ we use Corollary 12.3.

Remark. Both (12.1) and (12.2) are special case of an algebraic equation of type

$$f(a_1, a_2, \dots, a_k) = 0, \quad a_1 \in \mathcal{A}_1,\ a_2 \in \mathcal{A}_2, \dots,\ a_k \in \mathcal{A}_k,$$

where $f(a_1, \dots, a_k) \in \mathbb{Z}_p[a_1, \dots, a_k]$ and $\mathcal{A}_1, \dots, \mathcal{A}_k$ are large subsets of $\mathbb{Z}_p$. Jointly with András Sárközy, we studied the solvability of equations of the this type in [8].

The Weil theorem plays a key role in these results. The form of Weil's theorem for multiplicative characters is the following:

Theorem 12.4 (Weil) *Let p be a prime, χ is a multiplicative character of order d modulo p, where $d > 1$ and the polynomial $f(x) \in \mathbb{F}_p[x]$ has s distinct roots over the algebraic closure of $\mathbb{F}_p$ moreover $f(x)$ is not of the form $cg(x)^d$, where $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$. Then*

$$\left|\sum_{x \in \mathbb{F}_p} \chi(f(x))\right| \le (s-1)p^{1/2} \le (\deg f - 1)p^{1/2}.$$

Definition 12.1 *The order of a character is the smallest positive integer d for which $\chi^d = \chi_0$*

It follows from the Euler-Fermat theorem that if χ is an arbitrary character modulo m and $(n, m) = 1$, then

$$\chi(n)^{\varphi(m)} = \chi(n^{\varphi(m)}) = \chi(1) = 1 = \chi_0(n).$$

We also know that for $(n, m) > 1$ we have $\chi(n) = 0 = \chi_0(n)$. So $\chi^{\varphi(m)} = \chi_0$ always holds, i.e., the order of a character is always $\leq \varphi(m)$.

In Weil's theorem, the condition $f(x) \neq cg(x)^d$ is important, since if $f(x) = cg(x)^d$ and χ is a character of order d, then

$$\begin{aligned}\left|\sum_{x\in\mathbb{F}_p} \chi(f(x))\right| &= \left|\sum_{x\in\mathbb{F}_p} \chi(cg(x)^d)\right| \\ &= \left|\sum_{x\in\mathbb{F}_p} \chi(c)\chi^d(g(x))\right| \\ &= \left|\sum_{\substack{x\in\mathbb{F}_p \\ g(x)\neq 0}} \chi(c)\right| \\ &\geq p - \deg g.\end{aligned}$$

We also note that in Weil's theorem, the polynomial $f(x)$ can be replaced by a fractional function $\frac{f(x)}{g(x)}$, namely, if $g(x) \neq 0$, then $\frac{1}{g(x)} \stackrel{\text{def}}{=} g^*(x) = g(x)^{p-2}$, and so

$$\begin{aligned}\left|\sum_{\substack{x\in\mathbb{F}_p \\ g(x)\neq 0}} \chi\left(\frac{f(x)}{g(x)}\right)\right| &= \left|\sum_{x\in\mathbb{F}_p} \chi\left(f(x)g(x)^{p-2}\right)\right| \\ &\leq (\#\text{number of distinct roots of } f(x)g(x))\, p^{1/2},\end{aligned}$$

provided that $f(x)g(x)^{p-2}$ is not of the form $ch(x)^d$ (which is equivalent with $f(x)$ or $g(x)$ is not of the form $ch(x)^d$ in the case of

$(f, g) = 1$).

In our joint papers with András Sárközy [7] and [8] we needed to estimate the following character sums: $|\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\Psi(f(x,y))|$, where Ψ is an additive character, and $|\sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\chi(f(x,y))|$, where χ is a multiplicative character and f is a two-variable polynomial .

Sums of this type are most strongly estimated by Delinge [2], [3], then Fouvry and Katz [5], however, during these estimations there is a condition that $f(x,y)$ is not singular, which unfortunately not always holds in our special applications... As a result we had to use weaker estimates where the conditions of the used theorem is more flexible...

We also note that in our joint triple paper with Csikvári [1] we extended the problem from $\mathbb{F}_p$ to $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, but combinatorial tools dominate in these cases.

References

[1] P. Csikvári, A. Sárközy, K. Gyarmati, *Density and Ramsey type results on algebraic equations with restricted solution sets*, Combinatorica 32 (2012), 425-449,

[2] P. Delinge, *La conjecture de Weil, I*, Pub. Math. I. H. E. S. 43 (1974), 273-307.

[3] P. Delinge, *La conjecture de Weil, II*, Pub. Math. I. H. E. S. 43 (1980), 137-250.

[4] P. Erdős, N. H. Shapiro, *On the least primitive root of a prime*, Pacific J. Math. 7 (1957), 861-865.

[5] E. Fouvry, N. Katz, *A general stratification theorem for exponential sums, and applications*, J. Reine Angew. Math. 540 (2001), 115-166.

[6] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97 (1) (2001), 53-65.

[7] K. Gyarmati, A. Sárközy, *Equations in finite fields with restricted solution sets, I. (Character sums.)*, Acta Math. Hungar. 118 (2008), 129-148.

[8] K. Gyarmati, A. Sárközy, *Equations in finite fields with restricted solution sets, II. (Algebraic equations.)*, Acta Math. Hungar. 119 (2008), 259-280.

[9] A. Sárközy, *On sums and products of residues modulo p*, Acta Arith. 118 (4) (2005), 403-409.

13 Is Weil's theorem sharp?

Winterhof (slightly more general than below) proved the following in [1, Lemma 2]:

Lemma 13.1 *Let $\mathcal{A} \subseteq \mathbb{F}_p$ be an arbitrary set. Then*

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathcal{A}}\chi(x+a)\right|^2 = p|\mathcal{A}| - |\mathcal{A}|^2.$$

Proof of Lemma 13.1. Indeed,

$$\begin{aligned}\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathcal{A}}\chi(x+a)\right|^2 &= \sum_{x\in\mathbb{F}_p}\sum_{a,b\in\mathcal{A}}\chi(x+a)\overline{\chi}(x+b)\\ &= \sum_{x\in\mathbb{F}_p}\sum_{a\in\mathcal{A}}\underbrace{\left|\chi(x+a)\right|^2}_{\begin{cases}1, & \text{ha } x\neq -a\\ 0, & \text{ha } x=-a\end{cases}} + \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}\sum_{x\in\mathbb{F}_p}\chi(x+a)\overline{\chi}(x+b)\\ &= (p-1)|\mathcal{A}| + \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}\sum_{x\in\mathbb{F}_p}\chi(x+a)\overline{\chi}(x+b)\\ &= (p-1)|\mathcal{A}| \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}\sum_{\substack{x\in\mathbb{F}_p\\ x\neq -b}}\chi\left(\frac{x+a}{x+b}\right).\end{aligned}$$

It is easy to see that as x runs over the elements of the set $\mathbb{F}_p\setminus\{b\}$, $\frac{x+a}{x+b}$ takes on all values except 1. Thus:

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathcal{A}}\chi(x+a)\right|^2 = (p-1)|\mathcal{A}| + \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}\sum_{\substack{y\in\mathbb{F}_p\\ y\neq 1}}\chi(y)$$

$$= (p-1)|\mathcal{A}| + \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}} (-1)$$
$$= (p-1)|\mathcal{A}| - |\mathcal{A}|\,(|\mathcal{A}|-1)$$
$$= p|\mathcal{A}| - |\mathcal{A}|^2.$$

The above theorem immediately has an interesting consequence. In Lemma 13.1, take the set $\mathcal{A}$ of consecutive numbers: $\mathcal{A} = \{1, 2, \ldots, N\}$. Then by Lemma 13.1:

$$\sum_{x\in\mathbb{F}_p} \left|\sum_{a=1}^{N} \chi(x+a)\right|^2 = pN - N^2.$$

That is, there exists an $x \in \mathbb{F}_p$, say $x = M$, for which

$$\left|\sum_{a=1}^{N} \chi(M+a)\right|^2 \geq N - \frac{N^2}{p}$$
$$\left|\sum_{a=1}^{N} \chi(M+a)\right| \geq \sqrt{N - \frac{N^2}{p}}$$
$$\left|\sum_{x=M+1}^{M+N} \chi(x)\right| \geq \sqrt{N - \frac{N^2}{p}}.$$

If $p \geq 3$, choosing N to be $(p-1)/2$, we get the following:

Corollary 13.1 *If $p \geq 3$ is a prime, then $\exists\ M \in \mathbb{F}_p$, for which*

$$\left|\sum_{x=M+1}^{M+(p-1)/2} \chi(x)\right| \geq \sqrt{\frac{p-1}{2} - \frac{1}{4p}} > \frac{\sqrt{p}}{\sqrt{2}} - 1.$$

In the next chapter we will study how sharp this result is.

There is an even more exciting application when we test how sharp the Weil's theorem in case of multiplicative characters (12.4 Theorem) is.

For the sake of simplicity, let the order of the character χ now be $p-1$ and $f(x)=x^k+m$, where the degree of the polynomial is $k \mid p-1$ and $k<p-1$ holds. Then $f(x)$ is obviously not a polynomial of the form $cg(x)^{p-1}$. We will prove the following:

Corollary 13.2 *Let p be an odd prime, $k \mid p-1$, $k<p-1$ and χ be a multiplicative character of order $p-1$. Then $\exists\, m \in \mathbb{F}_p^*$ such that for the polynomial $f(x)=x^k+m$ we have*

$$\sum_{x\in\mathbb{F}_p} \chi(f(x)) > \sqrt{(k-1)p}.$$

In order to prove the theorem, it is only necessary to slightly modify the proof of Lemma 13.1.

Proof of Corollary 13.2. Let us now study the sum $\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathbb{F}_p^*}\chi(x+a^k)\right|^2$.

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathbb{F}_p^*}\chi(x+a^k)\right|^2 = \sum_{x\in\mathbb{F}_p}\sum_{a,b\in\mathbb{F}_p^*}\chi(x+a^k)\overline{\chi}(x+b^k)$$

$$= \sum_{x\in\mathbb{F}_p}\sum_{\substack{a,b\in\mathbb{F}_p^*\\ a^k=b^k}} \underbrace{\left|\chi(x+a^k)\right|^2}_{\begin{cases}1, & \text{ha } x\neq -a^k\\ 0, & \text{ha } x=-a^k\end{cases}} + \sum_{\substack{a,b\in\mathbb{F}_p^*\\ a^k\neq b^k}}\sum_{x\in\mathbb{F}_p}\chi(x+a^k)\overline{\chi}(x+b^k)$$

For a fixed $b \not\equiv 0 \pmod p$, there are always exactly k pieces a for which $a^k \equiv b^k \pmod p$. (Here we use that in the case of $(c,p)=1$, congruence $x^k \equiv c \pmod p$ can be solved if $c^{(k-1)/(k-1,p)} \equiv 1 \pmod p$ and then the number of solutions is $(k,p-1)$.) Thus:

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathbb{F}_p^*}\chi(x+a^k)\right|^2 = (p-1)^2k + \sum_{\substack{a,b\in\mathbb{F}_p^*\\ a^k\neq b^k}}\sum_{x\in\mathbb{F}_p}\chi(x+a^k)\overline{\chi}(x+b^k)$$
$$= (p-1)^2k + \sum_{\substack{a,b\in\mathbb{F}_p^*\\ a^k\neq b^k}}\sum_{\substack{x\in\mathbb{F}_p\\ x\neq -b^k}}\chi\left(\frac{x+a^k}{x+b^k}\right).$$

It is easy to see that as x runs, $\frac{x+a^k}{x+b^k}$ takes all values on the elements of the set $\mathbb{F}_p\setminus\{-b^k\}$ except for 1. Thus:

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathbb{F}_p^*}\chi(x+a^k)\right|^2 = (p-1)^2k + \sum_{\substack{a,b\in\mathbb{F}_p^*\\ a^k\neq b^k}}\sum_{\substack{y\in\mathbb{F}_p\\ y\neq 1}}\chi(y)$$
$$= (p-1)^2k - (p-1)(p-1-k)$$
$$= (p-1)(pk-p+1)$$
$$\geq (p-1)p(k-1)+2. \tag{13.1}$$

Note that for $x=0$ we have

$$\sum_{a\in\mathbb{F}_p^*}\chi(x+a^k) = \sum_{a\in\mathbb{F}_p^*}\chi(a^k) = \sum_{a\in\mathbb{F}_p^*}\chi^k(a) = -1,$$

since χ^k is a multiplicative character. Thus by (13.1):

$$\sum_{x\in\mathbb{F}_p^*}\left|\sum_{a\in\mathbb{F}_p^*}\chi(x+a^k)\right|^2 \geq (p-1)p(k-1)+1.$$

That is, there exists an $x\in\mathbb{F}_p^*$, say $x=m$, for which

$$\left|\sum_{a\in\mathbb{F}_p^*}\chi(m+a^k)\right|^2 > (k-1)p$$

$$\sum_{a \in \mathbb{F}_p^*} \chi(m + a^k) > \sqrt{(k-1)p}.$$

By writing x instead of a in this, the statement of Corollary 13.2 immediately follows.

References

[1] A. Winterhof, *Some estimates for character sums and applications*, Designs, Codes and Cryptography 22 (2001), 123-131.

14 Pólya-Vinogradov inequality and Vinogradov's method for estimating imcomplete character sums

In 1918, Pólya and Vinogradov independently proved the following:

Theorem 14.1 (Pólya-Vinogradov inequality) *$\exists$ positive absolute constant c such that if $m \in \mathbb{N}$, $m > 2$, χ is a multiplicative character* mod m, *$\chi \neq \chi_0$, $M \in \mathbb{Z}$ and $N \in \mathbb{N}$ then*

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < c\sqrt{m} \log m.$$

Remark. The trivial upper bound for the sum is N. Thus, the Pólya-Vinogradov inequality is not trivial if $N \gg \sqrt{m} \log m$.

We prove the theorem using Vinogradov's principle, which reduces the estimation of imcomplete sums to the estimation of complete sums.

Theorem 14.2 (Vinogradov) *If $m \in \mathbb{N}$, $x, y \in \mathbb{N}$, $(0 <) x < y \leq m$ and $a_1, a_2, \ldots, a_m \in \mathbb{C}$, then writing*

$$F(t) = \sum_{j=1}^{m} a_j e\left(\frac{jt}{m}\right)$$

and

$$A = \sum_{j=1}^{m} a_j,$$

we get

$$\left| \sum_{n=x}^{y} a_n - \frac{y-x+1}{m} A \right| \leq \frac{1}{2m} \sum_{\ell=1}^{m-1} \frac{|F(\ell)|}{||\frac{\ell}{m}||},$$

where $||s||$ denotes the distance of s to the nearest integer.

Corollary 14.1 (Vinogradov)

$$\left|\sum_{n=x}^{y} a_n - \frac{y-x+1}{m}A\right| \leq (\log m + 1) \max_{1\leq \ell \leq m-1} |F(\ell)|.$$

Proof of Theorem 14.2.

$$\begin{aligned}
S &= \sum_{n=x}^{y} a_n \\
&= \sum_{n=x}^{y} \sum_{j=1}^{m} \frac{1}{m} \sum_{\ell=0}^{m-1} e\left(\frac{\ell(j-n)}{m}\right) a_j \\
&= \frac{1}{m} \sum_{\ell=0}^{m-1} \sum_{n=x}^{y} \sum_{j=1}^{m} \underbrace{a_j e\left(\frac{\ell(j-n)}{m}\right)}_{a_j e\left(-\frac{\ell n}{m}\right) e\left(\frac{\ell j}{m}\right)} \underbrace{=}_{\substack{\text{We separate} \\ \text{the term } \ell=0}} \\
&= \underbrace{\frac{1}{m} \sum_{n=x}^{y} \overbrace{\sum_{j=1}^{m} a_j}^{A}}_{\frac{y-x+1}{m}A} + \frac{1}{m} \sum_{\ell=1}^{m} \left(\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right) \left(\underbrace{\sum_{j=1}^{m} a_j e\left(\frac{\ell j}{m}\right)}_{F(\ell)}\right).
\end{aligned}$$

So:

$$\left|S - \frac{y-x+1}{m}A\right| \leq \frac{1}{m} \sum_{\ell=1}^{m} \left|\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right| |F(\ell)|.$$

Here:

$$\left|\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right| = \left|\frac{1 - e\left(-\frac{(y-x+1)\ell}{m}\right)}{1 - e\left(-\frac{\ell}{m}\right)}\right| \leq \frac{2}{\left|1 - e\left(\frac{\ell}{m}\right)\right|}.$$

↑ arithmetic progression with common difference $e\left(-\frac{\ell}{n}\right)$

Then using $|1 - e(\alpha)| \geq 4\,||\alpha||$ (see 2.1 Lemma):

$$\left|\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right| \geq \frac{2}{4\left|\left|\frac{\ell}{m}\right|\right|} = \frac{1}{2\left|\left|\frac{\ell}{m}\right|\right|}.$$

That is

$$\left|S - \frac{y-x+1}{m}A\right| \leq \frac{1}{m}\sum_{\ell=1}^{m}\left|\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right| |F(\ell)|$$
$$\leq \frac{1}{2m}\sum_{\ell=1}^{m-1}\frac{|F(\ell)|}{\left|\left|\frac{\ell}{m}\right|\right|},$$

which is the statement of the theorem.

Proof of Corollary 14.1.

$$\frac{1}{2m}\sum_{\ell=1}^{m-1}\frac{|F(\ell)|}{\left|\left|\frac{\ell}{m}\right|\right|} \leq \left(\max_{1\leq\ell\leq m-1}|F(\ell)|\right)\frac{1}{2m}\sum_{\ell=1}^{m-1}\frac{1}{\left|\left|\frac{\ell}{m}\right|\right|}. \tag{14.1}$$

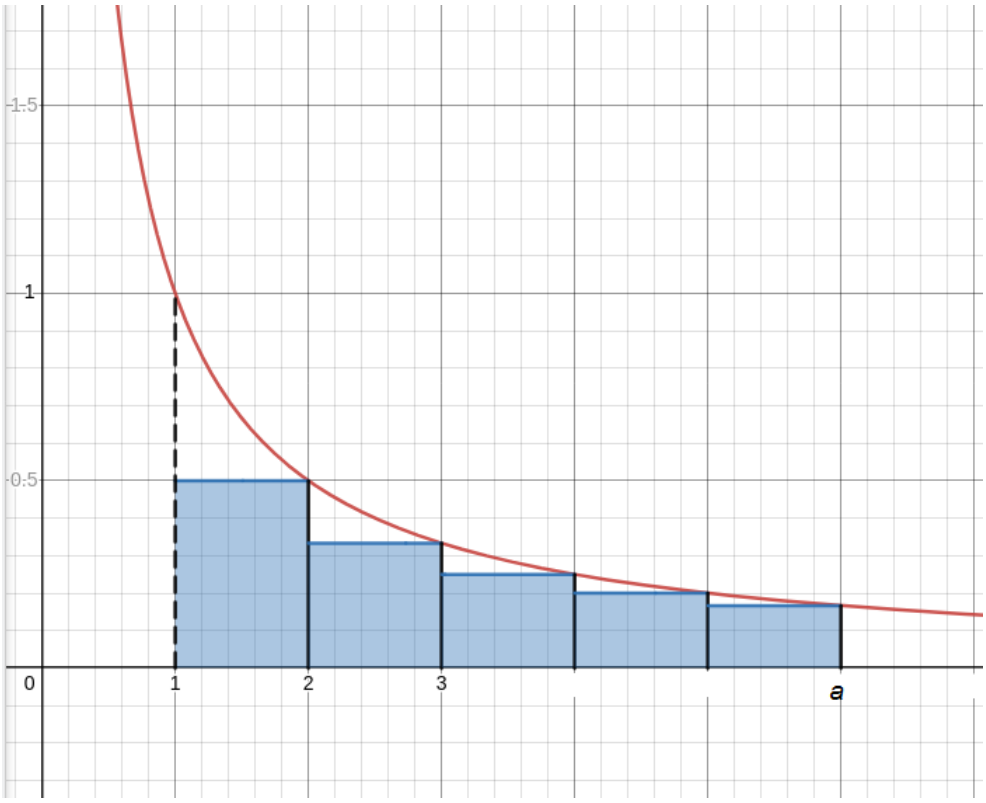
Here:

$$\sum_{\ell=1}^{m-1}\frac{1}{\left|\left|\frac{\ell}{m}\right|\right|} \leq 2\sum_{1\leq\ell\leq[m/2]}\frac{1}{\frac{\ell}{m}} = 2m\sum_{1\leq\ell\leq[m/2]}\frac{1}{\ell}, \tag{14.2}$$

where

$$\sum_{1\leq\ell\leq a}\frac{1}{\ell} = 1 + \sum_{2\leq\ell\leq a}\frac{1}{\ell} \leq 1 + \int_1^a \frac{1}{x}dx = 1 + \log a.$$

This last inequality can be illustrated with the following figure:



Writing this in (14.2):

$$\sum_{\ell=1}^{m-1} \frac{1}{\left|\left|\frac{\ell}{m}\right|\right|} \leq 2m(1+\log[m/2]) \leq 2m(1+\log m).$$

Thus, based on (14.1):

$$\begin{aligned}\frac{1}{2m}\sum_{\ell=1}^{m-1}\frac{|F(\ell)|}{\left|\left|\frac{\ell}{m}\right|\right|} &\leq \left(\max_{1\leq \ell\leq m-1}|F(\ell)|\right)\frac{1}{2m}\cdot 2m(1+\log m)\\ &= (\log m+1)\left(\max_{1\leq \ell\leq m-1}|F(\ell)|\right).\end{aligned}$$

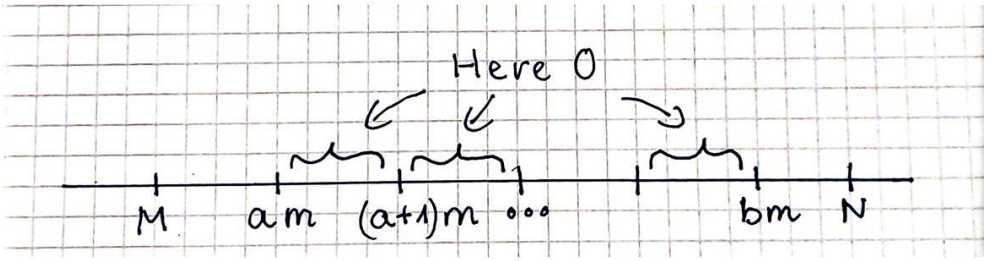
Proof of Theorem 14.1.

Case A. Assume that χ is a primitive character mod m. Consider those n's for which

$$M \leq n \leq M+N.$$

Then by $\sum_{n=1}^{m}\chi(n)=0$ and the periodicity we get that the studied sum on the middle intervals in the following figure is 0, while the

terms in the first and last short interval can be shifted to the interval $(0, p]$:



Thus the task is to estimate a following type sum:

$$\left| \sum_{n=x}^{y} \chi(n) \right|,$$

where $0 \le x \le y$, $y - x \le p$ (If the interval $(0, p]$ has two disjoint subintervals at the very beginning and at the very end, then we estimate the sum on the complementary interval, while if the above two intervals intersect, then it is enough to estimate on the intersection sum, since $\sum_{n=1}^{m} \chi(n) = 0$.)

Using Corollary 14.1 with $a_n = \chi(n)$ we get that

$$A = \sum_{n=1}^{m} \chi(n) = 0$$

and

$$\left| \sum_{n=x}^{y} \chi(n) \right| \le (\log m + 1) \max |F(\ell)|,$$

where, based on the properties of Gaussian sums (see chapter 5):

$$|F(\ell)| = \left| \sum_{j=1}^{m} \chi(j) e\left(\frac{j\ell}{m}\right) \right| = |\overline{\chi}(\ell)\tau(\chi)| \le \sqrt{m}.$$

So indeed:

$$\left| \sum_{n=x}^{y} \chi(n) \right| \le (\log m + 1)\sqrt{m}$$

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| \leq (\log m + 1)\sqrt{m}.$$

Case B. For imprimitive characters χ: This can be reduced to case A, see Davenport [1, 136. page].

Remarks. Pólya-Vinogradov is almost sharp: $\log m$ cannot be completely omitted (see e.g. Corollary 13.1), at best it can be replaced by a $\log \log m$. The first result was obtained by Schur in 1918, who proved that for every primitive character χ

$$\max_{M,N} \left| \sum_{n=N}^{N+M} \chi(N) \right| > \frac{1}{2\pi}\sqrt{m}.$$

Here, we managed to reduce the constant $\frac{1}{2\pi}$ almost to $\frac{1}{\sqrt{2}}$ in the case of a prime modulus in Corollary 13.1.

There are infinitely many characters with even sharper estimates. Payley [3] proved the following in 1932:

Theorem 14.3 (Payley) *There are infinitely many characters m and $\chi \neq \chi_0 \bmod m$ for which*

$$\max_{M,N} \left| \sum_{n=N}^{N+M} \chi(N) \right| > c\sqrt{m} \log \log m.$$

Assuming the generalized Riemann hypothesis in 1977, Montgomery and Vaughan [2] proved the following:

Theorem 14.4 (Montgomery-Vaughan) *$\exists$ absolute positive constant c such that if the generalized Riemann hypothesis holds, then for $m, N \in \mathbb{N}$, $m > 2$ and multiplicative character $\chi \bmod m$, $\chi \neq \chi_0$, $M \in \mathbb{Z}$ we have*

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < c\sqrt{m} \log \log m.$$

References

[1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics 74, Springer New York, 2013, Originally published by Markham Publishing Co., 1967.

[2] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math.43 (1) (1977), 69–82.

[3] R. E. A. C. Paley, *A theorem on characters*, J. Lond. Math. Soc. 7 (1932), 28–32.

15 Short multiplicative character sums and the least quadratic non-residue.

The Pólya-Vinogradov inequality: if $\chi \neq \chi_0$ is a multiplicative character mod m and $M \in \mathbb{Z}$, $N \in \mathbb{N}$, then

$$\left| \sum_{n=M+1}^{N} \chi(n) \right| < c\sqrt{m} \log m. \tag{15.1}$$

Trivially

$$\left| \sum_{n=M+1}^{N} \chi(n) \right| < N$$

(since the absolute value of each term is ≤ 1 and there are M terms in total). Thus, (15.1) is non-trivial only if the upper estimate in (15.1) is $< N$, i.e.,

$$c\sqrt{m} \log m < M.$$

What happens if this doesn't hold, i.e., short character sums are considered for which

$$N = o(\sqrt{m} \log m)?$$

It is very important to be able to give a non-trivial estimate in these cases, say a

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| = o(N)$$

type estimate.

In the following, we present an application of this type of estimate, namely we will study the estimate of the least quadratic non-residue. This is one of the $5 - 6$ most important problems in number theory.

Definition 15.1 *If p is prime, then the smallest positive integer $q = q(p)$, with $\left(\frac{q}{p}\right) = -1$ is called the least quadratic non-residue.*

The Pólya-Vinogradov inequality immediately gives an estimate for $q(p)$. Indeed, applying (15.1) to $\chi(n) = \left(\frac{n}{p}\right)$, $M = 0$, $N = q(p) - 1$ we get that

$$\left| \sum_{n=1}^{q(p)-1} \left(\frac{n}{p}\right) \right| \leq c\sqrt{p}\log p,$$

but for $1 \leq n \leq q(p) - 1$ we have $\left(\frac{n}{p}\right) = 1$, so

$$q(p) - 1 < c\sqrt{p}\log p$$
$$q(p) = O(\sqrt{p}\log p).$$

This estimate can be further improved by Burgess' theorem [1].

But, before we get started, it's important to consider which type of elementary estimate can be given for $q(p)$.

Suppose that $q(p) \geq \sqrt{p}+1$. Then $\left\lceil \frac{p}{q(p)} \right\rceil \leq \frac{p}{q(p)}+1 < q(p)$, so $\left\lceil \frac{p}{q(p)} \right\rceil$ is a quadratic non-residue, since every positive integer value smaller than $q(p)$ is a quadratic residue mod p.

So $\left\lceil \frac{p}{q(p)} \right\rceil q(p)$ is a quadratic non-residue. However

$$p = \frac{p}{q(p)}q(p) < \left\lceil \frac{p}{q(p)} \right\rceil q(p) < \left(\frac{p}{q(p)} + 1\right) q(p) = p + q(p)$$

(here we used that $\frac{p}{q(p)}$ is not an integer, i.e., $\left\lceil \frac{p}{q(p)} \right\rceil$ is strictly between $\frac{p}{q(p)}$ and $\frac{p}{q(p)} + 1$).

That is, the residue of $\left\lceil \frac{p}{q(p)} \right\rceil q(p)$ (which is quadratic non-residue) modulo p is strictly less than $q(p)$, which contradicts of the definition of $q(p)$. So

$$q(p) < \sqrt{p} + 1.$$

Even in an elementary method, we can go a little lower if we also suppose that p is a prime of the form $4k + 1$. Let

$$\mathcal{A} = \{0, 1, 2, \ldots, q(p) - 1\},$$

and n be a fixed quadratic non-residue. Then in the set

$$\mathcal{A} + n\mathcal{A} = \{a + na' : \ a, a' \in \mathcal{A}\}$$

each element is represented only once. Indeed for

$$\begin{aligned} a_1 + na_1' &\equiv a_2 + na_2' \pmod{p} \\ a_1 - a_2 &\equiv n(a_2' - a_1') \pmod{p}, \end{aligned}$$

but here

$$a_1 - a_2, \ a_2' - a_1' \in \{-q(p)+1, -q(p)+2, \ldots, q(p)-2, q(p)-1\},$$

in which set all numbers except 0 are quadratic residues.

By the multiplicative property of the Legendre symbol

$$\begin{aligned} \left(\frac{a_1 - a_2}{p}\right) &= \left(\frac{n}{p}\right)\left(\frac{a_2' - a_1'}{p}\right) \\ 1 &= (-1) \cdot 1, \end{aligned}$$

which is a contradiction. There is only one exception, namely $a_1 - a_2 = 0$ and $a_2' - a_1' = 0$, i.e., $a_1 = a_2$ and $a_1' = a_2'$.

That is, in the set

$$\mathcal{A} + n\mathcal{A} = \{a + na' : \ a, a' \in \mathcal{A}\}$$

each element is represented only once. So $|\mathcal{A} + n\mathcal{A}| = |\mathcal{A}|^2$. On the other hand

$$\mathcal{A} + n\mathcal{A} \subseteq \mathbb{Z}_p^2,$$

thus

$$\begin{aligned} |\mathcal{A}|^2 &\leq p \\ |\mathcal{A}| &\leq \sqrt{p} \\ q(p) &\leq \sqrt{p}. \end{aligned}$$

This concludes the section on the elementary estimation of the least quadratic non-residue. But is it possible to say more than the above with deeper tools? Then Burgess' theorem helps:

Theorem 15.1 (Burgess) *$\exists\ c > 0$, such that if p is a prime and $N, r \in \mathbb{N}$, $N \in \mathbb{Z}$, then*

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < cN^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

We do not prove this theorem here. The proof is based on Weil's theorem, i.e., the estimate of $\left|\sum_{x \in \mathbb{F}_p} \chi(x)\right|$.

Using this theorem we get:

$$\begin{aligned} q(p) - 1 &< cq(p)^{1-1/r} p^{(r+1)/4r^2} (\log p)^{1/r} \\ q(p)^{1/r} &\ll p^{(r+1)/4r^2} (\log p)^{1/r} \\ q(p) &\ll p^{(r+1)/4r} \log p), \end{aligned}$$

so $\forall\ \varepsilon > 0$ we have

$$q(p) = o\left(p^{1/4+\varepsilon}\right).$$

This estimate can be improved using Vinogradov's method [3].

Theorem 15.2 (Vinogradov) *If* $\left|\sum_{n=M+1}^{M+N} \chi(n)\right| = o(N)$ *hols for some* N*, then for* $\varepsilon > 0$*,* $M > M_0(\varepsilon)$ *we have*

$$q(p) < M^{\frac{1}{4\sqrt{e}}}.$$

Corollary 15.1

Pólya-Vinogradov: $M = p^{1/2+\delta} \Rightarrow q(p) \ll p^{\frac{1}{2\sqrt{e}}+\varepsilon}.$

Burgess: $M = p^{1/4+\delta} \Rightarrow q(p) \ll p^{\frac{1}{4\sqrt{e}}+\varepsilon}$

for all $\varepsilon > 0$*.*

Proof of Theorem 15.2.

Lemma 15.1

$$\sum_{p \le x} \frac{1}{p} = \log\log x + c + o(1),$$

where c *is the Meissel–Mertens constant.*

Proof of Lemma 15.1. This lemma is the Mertens' second theorem [2], we will not prove it here.

Similarly to the Pólya-Vinogradov inequality, we estimate a short character sum with

$$\chi(n) \begin{cases} \left(\frac{n}{p}\right) & \text{if } (n,p) = 1 \\ 0 & \text{if } p \mid n. \end{cases}$$

By the conditions of the theorem we have

$$\begin{aligned}
o(M) &= \sum_{n=1}^{M} \left(\frac{n}{p}\right) \\
&= \sum_{n=1}^{M} 1 + \sum_{n=1}^{M} \left(\left(\frac{n}{p}\right) - 1\right) \\
&= M - 2\Big|\underbrace{\{n:\ 1 \le n \le M,\ \left(\frac{n}{p}\right) = -1\}}_{\substack{\exists\ r \text{ prime such that } r \le n, \\ \left(\frac{r}{p}\right) = -1,\ r \mid n, \\ \text{by the definition of } q(p) \\ q(p) \le r \le n \le M}}\Big| \\
&\ge M - 2 \sum_{\substack{q(p) \le r \le n \\ r \text{ prime}}} |\{n:\ 1 \le n \le M,\ r \mid n\}| \\
&\ge M - 2 \sum_{\substack{q(p) \le r \le n \\ r \text{ prime}}} \frac{M}{r} \\
&= M\left(1 - 2\left(\sum_{\substack{r \le M \\ r \text{ prime}}} \frac{1}{r} - \sum_{\substack{r < q(p) \\ r \text{ prime}}} \frac{1}{r}\right)\right) \\
&= 2M\left(\frac{1}{2} - (\log\log M + c + o(1)) + (\log\log q(p) + c + o(1))\right) \\
&= 2M\left(\frac{1}{2} - \log\frac{\log M}{\log q(p)} + o(1)\right).
\end{aligned}$$

Then we prove the theorem indirectly. We assume that

$$q(p) \ge M^{1/\sqrt{e}+\varepsilon}.$$

Then

$$o(M) \ge 2M\left(\frac{1}{2} - \log\frac{\log M}{\log q(p)} + o(1)\right)$$

$$
\begin{aligned}
&\geq 2M\left(\frac{1}{2}-\log\frac{\log M}{\log q(p)}\right)\\
&\geq 2M\left(\frac{1}{2}-\log\frac{\log M}{\log M^{1/\sqrt{e}+\varepsilon}}\right)\\
&\geq 2M\left(\frac{1}{2}-\log\frac{1}{1/\sqrt{e}+\varepsilon}\right)\\
&\geq 2M\left(\frac{1}{2}+\log\left(1/\sqrt{e}+\varepsilon\right)\right)\\
&\geq 2M\left(\frac{1}{2}+\log(1/\sqrt{e})+\log\left(1+\varepsilon\sqrt{e}\right)\right)\\
&= 2M\underbrace{\log\left(1+\varepsilon\sqrt{e}\right)}_{\text{constant}>0}\\
&\neq o(M).
\end{aligned}
$$

References

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. 12 (3) (1962), 179–192.

[2] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine angew. Math. 78 (1874), 46–62.

[3] I. M. Vinogradov, *Sur la distribution des résidus et des non-résidus des puissances*, Journal Physico-Math. Soc. Univ. Perm, (1)(1918), 94–96.

16 Large sieve

This method was discovered by Linnik in 1941 while studying the distribution of quadratic non-residues. Later, Rényi (1947-1950) generalized Linnik's method, systematically studied and proved the following famous result:

Theorem 16.1 (Rényi) *$\exists$ an integer k such that $\forall\ n \in \mathbb{N}$ can be written of the form*

$$p + P_k = n$$

where p is a prime and P_k is a product of $\leq k$ pieces of primes.

This theorem is a partial result on the way to solving the Goldbach conjecture. Rényi did not calculate an explicit k, but it was later determined: Barban $k = 4$, Bombieri $k = 3$, and finally Chen [3] $k = 2$ for $\forall\ n > n_0$.

During the development of the large sieve, Roth, Bombieri, Davenport, Halberstam, Montgomery and Gallagher made significant progress.

The analytic form the large sieve was first formulated by Davenport and Halberstam.

Theorem 16.2 (Analytic form of large sieve) *Suppose $M \in \mathbb{Z}$, $N \in \mathbb{N}$, $a_{M+1}, a_{M+2}, \ldots, a_{M+N} \in \mathbb{C}$, $\mathbf{X} = \{x_1, \ldots, x_R\} \in \mathbb{R}$ such that for $1 \leq i < j \leq R$ $||x_i - x_j|| \geq delta >$0. Let*

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha), \tag{16.1}$$

then

$$\sum_{i=1}^{R} |S(x_i)|^2 \leq \left(\frac{1}{\delta} + \pi N\right) \sum_{n=M+1}^{M+N} |a_n|^2. \tag{16.2}$$

Remark. If the $\{x_i\}$ is uniformly distributed on the interval $[0,1]$ such that $\delta = \frac{1}{R}$ and $N \ll R$, then (16.2) says:

$$\underbrace{\frac{1}{R}\sum_{i=1}^{R}|S(x_i)|^2}_{\substack{\text{Riemann sum for} \\ \int_0^1 |S(\alpha)|^2 d\alpha}} \ll \underbrace{\sum_{n=M+1}^{M+N}|a_n|^2}_{\substack{\text{by Parseval formula} \\ = \int_0^1 |S(\alpha)|^2 d\alpha}}.$$

The theorem states the following: a "quite fine" Riemann sum can be estimated from above by the constant multiple of the integral.

Selberg (see e.g. [8]) improved the estimate of the large sieve by a constant factor, proving that

$$\sum_{i=1}^{R}|S(x_i)|^2 \leq \left(\frac{1}{\delta}+N-1\right)\sum_{n=M+1}^{M+N}|a_n|^2. \tag{16.3}$$

is also true.

Proof of Theorem 16.2. Gallagher's idea [5] is the following: $|S(\alpha)|^2$ is close to $\frac{1}{\delta}\int_{\alpha-\delta/2}^{\alpha+\delta/2}|S(\beta)|^2\,d\beta$.

The relation between the two expressions can be expressed using $S(\beta)$ and $S'(\beta)$. In order to do so, we use a "Sobolev-type" inequality [10]:

Lemma 16.1 *If $f(x) : [0,1] \to \mathbb{C}$ has a continuous first derivative, then for $0 \leq x \leq 1$*

$$|f(x)| \leq \int_0^1 (|f(y)| + |f'(y)|)\,dy \tag{16.4}$$

and

$$\left|f\left(\frac{1}{2}\right)\right| \leq \int_0^1 \left(|f(x)| + \frac{1}{2}|f'(x)|\right)dx \tag{16.5}$$

Proof of Lemma 16.1.

Statement 1.

$$f(x) = \int_0^1 f(u)du + \int_0^x uf'(u)du + \int_x^1 (u-1)f'(u)du.$$

Indeed, written the last integral in two parts:

$$\begin{aligned}
&\int_0^1 f(u)du + \underbrace{\int_0^x uf'(u)du + \int_x^1 uf'(u)du}_{\int_0^1 uf'(u)du = [uf(u)]_0^1 - \int_0^1 f(u)du} - \int_x^1 f'(u)du \\
&= \int_0^1 f(u)du + [uf(u)]_0^1 - \int_0^1 f(u)du - \int_x^1 f'(u)du \\
&= [uf(u)]_0^1 - \int_x^1 f'(u)du \\
&= f(1) - (f(1) - f(x)) \\
&= f(x).
\end{aligned}$$

In order to prove (16.4):

$$\begin{aligned}
|f(x)| &\le \left|\int_0^1 f(u)du\right| + \left|\int_0^x uf'(u)du\right| + \left|\int_x^1 (u-1)f'(u)du\right| \\
&\le \int_0^1 |f(u)|\,du + \int_0^x |u|\,|f'(u)|\,du + \int_x^1 |u-1|\,|f'(u)|\,du.
\end{aligned} \tag{16.6}$$

First of all, we note that on the interval $[0,1]$ $|u|$ and $|u-1| \le 1$, so due to (16.6)

$$\begin{aligned}
|f(x)| &\le \int_0^1 |f(u)|\,du + \int_0^x |f'(u)|\,du + \int_x^1 |f'(u)|\,du \\
&= \int_0^1 |f(u)|\,du + \int_0^1 |f'(u)|\,du,
\end{aligned}$$

which proves (16.4).

To prove (16.5), let's substitute $x = \frac{1}{2}$ in (16.6). Then

$$\begin{aligned}\left|f\left(\frac{1}{2}\right)\right| &\le \int_0^1 |f(u)|\,du + \int_0^{1/2} \frac{1}{2}\,|f'(u)|\,du + \int_{1/2}^1 \frac{1}{2}\,|f'(u)|\,du \\ &= \int_0^1 |f(u)|\,du + \int_0^1 \frac{1}{2}\,|f'(u)|\,du,\end{aligned}$$

which completes the proof of the lemma.

In the proof of Theorem 16.2, we can assume that $M = \left[-\frac{1}{2}(N+1)\right]$.

To see this let $M' \stackrel{\text{def}}{=} \left[-\frac{1}{2}(N+1)\right]$, and $a'_{M'+i} \stackrel{\text{def}}{=} a_{M+i}$. Then

$$\begin{aligned}|S(x_r)| &= \left|\sum_{n=M+1}^{M+N} a_n e(nx_r)\right| \\ &= \left|\sum_{i=1}^{N} a_{M+i} e((M+i)x_r)\right| \\ &= \left|\sum_{i=1}^{N} a_{M+i} e((M'+i)x_r)\right| \\ &= \left|\sum_{i=1}^{N} a'_{M'+i} e((M'+i)x_r)\right| \\ &= \left|\sum_{n=M'+1}^{M'+N} a'_n e(nx_r)\right|.\end{aligned}$$

Furthermore:

$$\sum_{n=M+1}^{M+N} |a_n|^2 = \sum_{n=M'+1}^{M'+N} |a'_n|^2$$

That is, if we prove the theorem for this $M' = \left[-\frac{1}{2}(N+1)\right]$ and arbitrary a'_n's, then by the above re-indexing we also proved it for all M and a_n's.

Next, we would like to estimate $|S(x_i)|^2$ on the interval $I_r = [x_r - \delta/2, x_r + \delta/2]$. Let

$$g(x) : [x_r - \delta/2, x_r + \delta/2] \to \mathbb{C}$$

be a function that has a continuous derivative. Write

$$f(x) = g(\delta x + (x_r - \delta/2)),$$

where $x \in [0, 1]$. Then

$$\begin{aligned}
\left| f\left(\frac{1}{2}\right) \right| &= \left| g\left(\frac{\delta}{2} + \left(x_r - \frac{\delta}{2}\right)\right) \right| = g(x_r) \\
&\leq \int_0^1 |f(x)|\, dx + \int_0^1 \frac{1}{2} |f'(x)|\, dx \\
&= \int_0^1 \left| g\left(\delta x + x_r - \frac{\delta}{2}\right) \right| dx + \int_0^1 \frac{1}{2} \left| \delta g'\left(\delta x + x_r - \frac{\delta}{2}\right) \right| dx.
\end{aligned}$$

Substitute $y = \delta x + x_r - \frac{\delta}{2}$:

$$\frac{dy}{dx} = \delta, \quad dx = \frac{dy}{\delta}.$$

Limits of the integrand:

$$\begin{aligned}
x = 0 &\Rightarrow \; y = x_r - \frac{\delta}{2} \\
x = 1 &\Rightarrow \; y = x_r + \frac{\delta}{2}.
\end{aligned}$$

Thus:

$$\begin{aligned}
g(x_r) &\leq \int_{x_r - \delta/2}^{x_r + \delta/2} |g(y)| \frac{1}{\delta} dy + \int_{x_r - \delta/2}^{x_r + \delta/2} \frac{1}{2} |\delta g'(y)| \frac{1}{\delta} dy \\
&= \frac{1}{\delta} \int_{x_r - \delta/2}^{x_r + \delta/2} |g(y)|\, dy + \frac{1}{2} \int_{x_r - \delta/2}^{x_r + \delta/2} |\delta g'(y)|\, dy.
\end{aligned}$$

Using this inequality for $g(x) = S^2(x)$:

$$|S(x_r)|^2 \leq \frac{1}{\delta} \int_{x_r - \delta/2}^{x_r + \delta/2} |S(\alpha)|^2\, d\alpha + \int_{x_r - \delta/2}^{x_r + \delta/2} |S(\alpha) S'(\alpha)|\, d\alpha. \tag{16.7}$$

According to the condition of the theorem, the intervals $[x_r - \delta/2, x_r + \delta/2]$ are disjoint modulo 1. Using that $S(\alpha)$ is periodic with period 1, we get that

$$\sum_{r=1}^{R}\left(\frac{1}{\delta}\int_{x_r-\delta/2}^{x_r+\delta/2}|S(\alpha)|^2\,d\alpha+\int_{x_r-\delta/2}^{x_r+\delta/2}|S(\alpha)S'(\alpha)|\,d\alpha\right)$$
$$\le\frac{1}{\delta}\int_0^1|S(\alpha)|^2\,d\alpha+\int_0^1|S(\alpha)S'(\alpha)|\,d\alpha.$$

That is, adding the inequalities in (16.7) for $r=0,1,2,\dots,R$:

$$\sum_{r=1}^{R}|S(x_r)|^2\le\frac{1}{\delta}\underbrace{\int_0^1|S(\alpha)|^2\,d\alpha}_{\text{Parseval formula}}+\underbrace{\int_0^1|S(\alpha)S'(\alpha)|\,d\alpha}_{\text{Cauchy-Schwarz}}$$
$$\le\frac{1}{\delta}\sum_{n=M+1}^{M+N}|a_n|^2+\left(\underbrace{\int_0^1|S(\alpha)|^2\,d\alpha}_{\text{Parseval formula}}\right)^{1/2}\left(\underbrace{\int_0^1|S'(\alpha)|^2\,d\alpha}_{\text{Parseval formula}}\right)^{1/2}$$
$$\le\frac{1}{\delta}\sum_{n=M+1}^{M+N}|a_n|^2+\left(\sum_{n=M+1}^{M+N}|a_n|^2\right)^{1/2}\left(\sum_{n=M+1}^{M+N}|2\pi i n a_n|^2\right)^{1/2}.$$

We use here that we may assume $M=\left[-\frac{1}{2}(N+1)\right]$. In this case $n\in[M+1,M+N]\subseteq[-N/2,N/2]$, $|n|\le N/2$, so in the last parenthesis:

$$\sum_{n=M+1}^{M+N}|2\pi i n a_n|^2\le\sum_{n=M+1}^{M+N}|2\pi|^2\left|\frac{N}{2}\right|^2|a_n|^2$$
$$=\pi^2N^2\sum_{n=M+1}^{M+N}|a_n|^2,$$

that is

$$\sum_{r=1}^{R}|S(x_r)|^2\le\frac{1}{\delta}\sum_{n=M+1}^{M+N}|a_n|^2+\left(\sum_{n=M+1}^{M+N}|a_n|^2\right)^{1/2}\left(\pi^2N^2\sum_{n=M+1}^{M+N}|a_n|^2\right)^{1/2}$$

$$\leq \left(\frac{1}{\delta} + \pi N\right) \sum_{n=M+1}^{M+N} |a_n|^2 .$$

This proves the theorem.

Corollary 16.1 *We define $S(\alpha)$ as in Theorem 16.2. Then for all $Q \in \mathbb{N}$, $Q \geq 2$*

$$\sum_{q \leq Q} \sum_{1 \leq a \leq q} |S(a/q)|^2 \leq (Q^2 + \pi N) \sum_{n=M+1}^{M+N} |a_n|^2 .$$

Proof of Corollary 16.1. We prove that the conditions of the theorem holds for the set

$$\mathbf{X} = \left\{ \frac{a}{q} : \ a, q \in \mathbb{N}^+, \ q \leq Q, \ 1 \leq a \leq q, \ (a, q) = 1 \right\}$$

and $\delta = \frac{1}{Q^2}$ since this set $\mathbf{X}$ is $\delta = \frac{1}{Q^2}$-"spaced": i.e., let $\frac{a}{q}, \frac{b}{r} \in \mathbf{X}$, $(a, q) = (b, r) = 1$, $\frac{a}{q} \neq \frac{b}{r}$. Then we know

$$0 < \left| \frac{a}{q} - \frac{b}{r} \right|$$

and $0 < \frac{a}{q}, \frac{b}{r} \leq 1$, thus

$$\left| \frac{a}{q} - \frac{b}{r} \right| < 1.$$

On the other hand define $c \in \mathbb{Z}$ by

$$\left| \frac{a}{q} - \frac{b}{r} \right| = \frac{|ar - qb|}{qr} = \frac{c}{qr},$$

then

$$\left| \frac{a}{q} - \frac{b}{r} \right| \in \left\{ \frac{1}{qr}, \frac{2}{qr}, \frac{3}{qr}, \cdots \frac{qr-1}{qr}, \right\}.$$

So

$$\left\|\frac{a}{q}-\frac{b}{r}\right\| = \left\| \left|\frac{a}{q}-\frac{b}{r}\right| \right\| \in \left\{\frac{1}{qr}, \frac{2}{qr}, \frac{3}{qr}, \cdots \frac{qr-1}{qr}, \right\}$$

thus

$$\left\|\frac{a}{q}-\frac{b}{r}\right\| \geq \frac{1}{qr} \geq \frac{1}{QQ} = \frac{1}{Q^2}.$$

Applying the theorem to $\mathbf{X}$ and δ, we get that

$$\begin{aligned}\sum_{x\in\mathbf{X}} |S(x)|^2 &= \sum_{q\leq Q} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \left|S\left(\frac{a}{q}\right)\right|^2 \\ &\leq \left(\frac{1}{\delta}+\pi N\right) \sum_{n=M+1}^{M+N} |a_n|^2 \\ &\leq \left(Q^2+\pi N\right) \sum_{n=M+1}^{M+N} |a_n|^2 .\end{aligned}$$

Theorem 16.3 (Arithmetic form of the large sieve) *Let $M \in \mathbb{Z}$, $Q, N \in \mathbb{N}$, $\mathcal{M} \subseteq \{1, 2, \ldots, Q\}$ such that $m, m' \in \mathcal{M}$, $m \neq m' \Rightarrow (m, m') = 1$, and let $\mathcal{A} \subseteq \{M+1, M+2, \ldots, M+N\}$, $Z \stackrel{\text{def}}{=} |\mathcal{A}|$,*

$$Z(m,h) = \sum_{\substack{a\equiv h \pmod m\\ a\in\mathcal{A}}} 1.$$

Then

$$\sum_{m\in\mathcal{M}} m\left(\sum_{h=1}^{m} Z(m,h) - \frac{Z}{m}\right) \leq (Q^2+\pi N)Z.$$

If we choose $\mathcal{M} = \{p : \ p \text{ prime}, p \leq Q\}$ in the theorem, we get the following:

Corollary 16.2 *If $M \in \mathbb{Z}$, $Q, N \in \mathbb{N}$, $\mathcal{A} \subseteq \{M+1, M+2, \ldots, M+N\}$, Z, $Z(m,h)$ are defined as in Theorem 16.3 then*

$$\sum_{p\leq Q} p\left(\sum_{h=1}^{p} Z(p,h) - \frac{Z}{p}\right) \leq (Q^2+\pi N)Z.$$

Remark. Suppose that for a positive percentage of the primes $p \le Q$ and a positive percentage of these residue classes modulo p are forbidden.

If h is a forbidden residue class modulo p, then

$$\left(Z(p,h) - \frac{Z}{p}\right) = \frac{Z^2}{p^2},$$

from which

$$\begin{aligned}\sum_{p\le Q} p\left(\sum_{h=1}^{p} Z(p,h) - \frac{Z}{p}\right) &\gg \sum_{p\le Q}^{*} p \sum_{h}^{*} \frac{Z^2}{p^2} \\ &\gg \sum_{p\le Q}^{*} p\frac{Z^2}{p} \\ &\gg Z^2 \sum_{p\le Q}^{*} 1 \\ &\gg Z^2\pi(Q).\end{aligned}$$

Thus it follows from Corollary 16.2 that

$$\begin{aligned}Z^2\pi(Q) &\ll (Q^2 + \pi N)Z \\ z \ll \frac{Q^2+\pi N}{\pi(Q)} &\ll \frac{Q^2+N}{\pi(Q)}.\end{aligned}$$

Montgomery [7] proved a slightly sharper form of the large sieve.

Theorem 16.4 (Montgomery, 1968) *Let $M \in \mathbb{Z}$, $Q, N \in \mathbb{N}$, $Q \ge 2$ $\mathcal{A} \subseteq \{M+1, M+2, \dots, M+N\}$, and let $|\mathcal{A}| = Z$. Assume that $\forall\, p \le Q$ $\exists\, \omega(p)$ pieces of residue classes modulo p that does not intersect $\mathcal{A}$. Suppose $\omega(p) < p$. Then*

$$Z \le \frac{Q^2+\pi N}{L},$$

where

$$L = \sum_{q\le Q} \mu^2(q) \prod_{p\le Q} \frac{\omega(p)}{p-\omega(p)}.$$

We do not prove Theorem 16.4, but we do prove Theorem 16.3.

Proof of Theorem 16.3. We will use the following identity of Parseval type.

Lemma 16.2 *If* $m \in \mathbb{N}$, $b_1, b_2, \ldots, b_m \in \mathbb{C}$, $F(\alpha) = \sum_{h=1}^{m} b_h e(h\alpha)$, *then*

$$\sum_{k=1}^{m} \left| F\left(\frac{k}{m}\right) \right|^2 = m \sum_{h=1}^{m} |b_h|^2.$$

Proof of Lemma 16.2.

$$\begin{aligned}
\sum_{k=1}^{m} \left| F\left(\frac{k}{m}\right) \right|^2 &= \sum_{k=1}^{m} \sum_{h=1}^{m} b_h e\left(h\frac{k}{m}\right) \sum_{j=1}^{m} \overline{b_j} e\left(-j\frac{k}{m}\right) \\
&= \sum_{h=1}^{m} \sum_{j=1}^{m} b_h \overline{b_j} \underbrace{\sum_{k=1}^{m} e\left((h-j)\frac{k}{m}\right)}_{\begin{cases} m, & \text{if } h = j \\ 0, & \text{if } h \neq j \end{cases}} \\
&= m \sum_{h=1}^{m} |b_h|^2,
\end{aligned}$$

which completes the proof of the lemma.

Apply the lemma with $b_h = Z(m,h) - \frac{Z}{m}$ and let $S(\alpha) = \sum_{a \in \mathcal{A}} e(a\alpha)$. Then by the lemma

$$m \sum_{h=1}^{m} \left(Z(m,h) - \frac{Z}{m} \right)^2 = \sum_{k=1}^{m} \left| F\left(\frac{k}{m}\right) \right|^2. \tag{16.8}$$

Here

$$F\left(\frac{k}{m}\right) = \sum_{h=1}^{m} \left(Z(m,h) - \frac{Z}{m} \right) e\left(h\frac{k}{m}\right)$$

$$= \sum_{h=1}^{m} Z(m,h) e\left(h\frac{k}{m}\right) - \frac{Z}{m}\sum_{h=1}^{m} e\left(h\frac{k}{m}\right)$$
$$= \sum_{a\in\mathcal{A}} e\left(a\frac{k}{m}\right) - \frac{Z}{m}\begin{cases} m, & \text{if } m \mid k \\ 0, & \text{if } m \nmid k \end{cases}$$
$$= \begin{cases} |\mathcal{A}| - Z = 0, & \text{ha } m \mid k \\ S\left(\frac{k}{m}\right), & \text{ha } m \nmid k. \end{cases}$$

Thus, by (16.8):

$$m\sum_{h=1}^{m}\left(Z(m,h) - \frac{Z}{m}\right)^2 = \sum_{m\in\mathcal{M}}\sum_{k=1}^{m-1}\left|S\left(\frac{k}{m}\right)\right|^2. \tag{16.9}$$

Since if $m \neq m' \in \mathcal{M}$ we have $(m,m') = 1$, then for $m \neq m'$ or $k \neq k'$ we have $\frac{k}{m} \neq \frac{k'}{m'}$. Thus, writing $\frac{a}{q}$ (where $(a,q) = 1$) in place of $\frac{k}{m}$ on the right-hand side of (16.9), we get that

$$m\sum_{h=1}^{m}\left(Z(m,h) - \frac{Z}{m}\right)^2 \leq \sum_{q\leq Q}\sum_{\substack{1\leq a\leq q\\(a,q)=1}} |S(a/q)|^2$$

By Corollary 16.1

$$m\sum_{h=1}^{m}\left(Z(m,h) - \frac{Z}{m}\right)^2 \leq (Q^2+\pi N)\sum_{n=M+1}^{M+n}|a_n|^2,$$

where now

$$a_n = \begin{cases} 1, & \text{ha } a_n \in \mathcal{A} \\ 0, & \text{ha } a_n \notin \mathcal{A}. \end{cases}$$

Thus

$$m\sum_{h=1}^{m}\left(Z(m,h) - \frac{Z}{m}\right)^2 \leq (Q^2+\pi N)Z,$$

which completes the proof.

It can be deduced from Selberg's estimate (16.3) that the con-

stant factor π in 16.1, 16.3, 16.2 and 16.4 can be omitted from these theorems and corollaries. However, within the framework of this lecture note, we only use the present (slightly weaker) versions of these theorems and corollaries because of their shorter proofs.

A simple application: let

$$P(n) \stackrel{\text{def}}{=} \max_{\substack{p|n \\ p \text{ prím}}} p.$$

Theorem 16.5 (Balog-Sárközy [2]) *If* $N > N_0$, $\mathcal{A} \subseteq \{1, 2, \dots, N\}$ *and*

$$|\mathcal{A}| > 33N^{1/2} \log N, \tag{16.10}$$

then $\exists\, a, a' \in \mathcal{A}$, *such that*

$$P(a + a') > \frac{|\mathcal{A}|}{33 \log N}. \tag{16.11}$$

Remark. What does this theorem state? For such an $a + a'$, write $P(a + a') = p$, $\frac{a+a'}{p} = m$. Then

$$m = \frac{a + a'}{p} < \frac{N + N}{\frac{|\mathcal{A}|}{33 \log N}} = 66 \frac{N}{|\mathcal{A}|} \log N.$$

If, say, (16.10) is true in the much sharper form, i.e., $|\mathcal{A}| > \varepsilon N$, then

$$m < 66 \frac{N}{|\mathcal{A}|} \log N < \frac{66}{\varepsilon} \log N$$

and

$$p > \frac{|\mathcal{A}|}{33 \log N} > \frac{\varepsilon}{33} \frac{N}{\log N}.$$

That is, then $a + a' = mp$, where p is "very large" and m is "very small", so the sum $a + a'$ is "close" to a prime.

An interesting question might be the case $a+a' =$ prime, it turns out there is no such theorem, let $\mathcal{A} = \{n : n \text{ even}, n \leq N\}$. Then $\forall\ a + a'$ is even, $\forall\ a + a'$ is composite.

Proof of Theorem 16.5. We prove this indirectly. Suppose that in contrast with (16.11), $\forall\ a + a'$ we have

$$P(a + a') \leq \left\lceil \frac{|\mathcal{A}|}{33 \log N} \right\rceil \stackrel{\text{def}}{=} t.$$

Then $\forall\ p > t$ for $a, a' \in \mathcal{A}\ p \nmid a + a'$, so that

$$a + a' \not\equiv 0 \pmod{p} \quad (\forall a, a' \in \mathcal{A},\ p > t)$$
$$a \not\equiv -a' \pmod{p}.$$

Let $\nu(p)$ denote the number of residue classes mod p intersecting $\mathcal{A}$:

$$\nu(p) = |\{r : 0 \leq r < p, \exists a \in \mathcal{A}, \text{ where } a \equiv r \pmod{p}\}|.$$

Then

$$\left.\begin{array}{ll} \mathcal{A}: & \nu(p) \text{ different residue classes} \\ -\mathcal{A}: & \nu(p) \text{ different residue classes} \end{array}\right\} \begin{array}{l}\text{Together, they} \\ \text{are all different.}\end{array}$$

Thus

$$\nu(p) + \nu(p) \leq p$$
$$\nu(p) \leq \frac{p}{2}.$$

So $\mathcal{A}$ does not intersect at least $p - \nu(p) \geq \frac{p}{2}$ residue classes mod p. Thus for $\forall\ p > t$:

$$S = \sum_{t < p \leq 2t} p \sum_{h=1}^{p} \left(Z(p, h) - \frac{Z}{p} \right)^2$$

$$\geq \sum_{t<p\leq 2t} p \sum_{\substack{1\leq h\leq p \\ Z(p,h)=0}} \left(0-\frac{Z}{p}\right)^2$$

$$= \sum_{t<p\leq 2t} p\frac{Z^2}{p^2} \underbrace{\sum_{\substack{1\leq h\leq p \\ Z(p,h)=0}} 1}_{\geq \frac{p}{2}} \tag{16.12}$$

$$\geq \frac{Z^2}{2} \sum_{t<p\leq 2t} 1$$

$$= \frac{Z^2}{2}\left(\pi(2t)-\pi(t)\right). \tag{16.13}$$

Here by (16.10)

$$t = \left\lceil \frac{|\mathcal{A}|}{33\log N} \right\rceil > \frac{33N^{1/2}\log N}{33\log N} = N^{1/2} \to \infty,$$

as $N \to \infty$.

By the prime number theorem, $\pi(x) \sim \frac{x}{\log x}$ as $x \to \infty$. So

$$\pi(2t)-\pi(t) = (1+o(1))\frac{2t}{\log 2t} - (1+o(1))\frac{t}{\log t}$$
$$= (1+o(1))\frac{t}{\log t},$$

that is

$$\pi(2t)-\pi(t) > \frac{t}{2\log t}, \quad \text{if } N > N_0. \tag{16.14}$$

Then by (16.13) and (16.14) we have

$$S > \frac{Z^2}{2}\cdot\frac{t}{2\log t}. \tag{16.15}$$

On the other hand, by the arithmetic form of the large sieve (see Theorem 16.3):

$$\begin{aligned} S &= \sum_{t<p\le 2t} p \sum_{h=1}^{p} \left(Z(p,h) - \frac{Z}{p} \right)^2 \\ &\le \sum_{p \le 2t \stackrel{\text{def}}{=} Q} p \sum_{h=1}^{p} \left(Z(p,h) - \frac{Z}{p} \right)^2 \\ &\le (Q^2 + \pi N) Z \\ &< 4(t^2 + N) Z. \end{aligned} \tag{16.16}$$

Thus by (16.15) and (16.16):

$$\begin{aligned} \frac{1}{4} Z^2 \frac{t}{\log t} < S < 4(t^2 + N) Z \\ Z < 16 \frac{\log N}{t} (t^2 + N). \end{aligned} \tag{16.17}$$

By (16.10):

$$t^2 = \left\lceil \frac{|\mathcal{A}|}{33 \log N} \right\rceil^2 \ge \left\lceil \frac{1}{33} \frac{33 N^{1/2} \log N}{\log N} \right\rceil^2 = \left\lceil N^{1/2} \right\rceil^2 = N \tag{16.18}$$

By (16.17) and (16.18):

$$\begin{aligned} Z < 16 \frac{\log N}{t} \cdot 2t^2 = 32 t \log N = 32 \left\lceil \frac{|\mathcal{A}|}{33 \log N} \log N \right\rceil \\ < 32 \left(1 + \frac{|\mathcal{A}|}{33 \log N} \log N \right) = \frac{32}{33} |\mathcal{A}| + \log N < |\mathcal{A}| = Z, \end{aligned}$$

which is contradiction.

Remark. The theorem can be extended from sums $a + a'$ to sums $a + b$, and then a similar theorem can be proved. The following results also due to Balog and Sárközy [1], [2]:

If $\varepsilon > 0$, $N > N_0(\varepsilon)$, $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \dots, N\}$, $|\mathcal{A}|, |\mathcal{B}| > \varepsilon N$, then $\exists a \in \mathcal{A},\ b \in \mathcal{B}$, such that

1. $P(a+b) > c(\varepsilon)N \quad (\Rightarrow \ a+b = pO(1))$.

2. $\exists p: \ p^2 \mid a+b, \ p^2 > c'(\varepsilon)N$

3. $P(a+b) < \exp\left(c''(\varepsilon)\sqrt{\log N \log\log N}\right)$ i.e., "small" $= N^{o(1)}$.

There exist many similar theorems for dense sets $\mathcal{A}$, $\mathcal{B}$, where by the statements there is a sum $a+b$ that has certain arithmetic properties.

Recall the following corollary of the analytical form of the large sieve:

$$\sum_{q\le Q}\sum_{1\le a\le q}\Big|\underbrace{S(a/q)}_{\sum_n a_n e\left(n\frac{a}{q}\right)}\Big|^2 \le (Q^2+\pi N)\sum_{n=M+1}^{M+N}|a_n|^2. \tag{16.19}$$

Since there is a duality between additive and multiplicative characters, we hope that $\exists$ a multiplicative analogue of the above corollary. Indeed:

Theorem 16.6 (Gallagher [6]) *If $Q \in \mathbb{N}$, $Q \ge 2$ then*

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sum_{\substack{\chi \text{ primitive}\\ \text{character mod} q}}^{*}\left|\sum_{n=M+1}^{M+N}a_n\chi(n)\right|^2 \le (Q^2+\pi N)\sum_{n=M+1}^{M+N}|a_n|^2. \tag{16.20}$$

Proof of Theorem 16.6. We would like to derive (16.20) from (16.19). Thus, we have to switch from additive characters to multiplicative characters, for which we use a translation formula, see Theroem 11.2. By this theorem, if χ is a primitive character mod q, then

$$\chi(n)\tau(\overline{\chi}) = \sum_{h=0}^{q-1}\overline{\chi}(h)e\left(n\frac{h}{q}\right), \tag{16.21}$$

where $\tau(\chi)$ is a Gauss sum:

$$\tau(\chi) = \sum_{1 \le a \le q} \chi(a) e\left(\frac{a}{q}\right).$$

We also studied (see Theorem 11.1) that for a primitive character

$$|\tau(\chi)| = \sqrt{q}.$$

So by (16.21):

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{q-1} \overline{\chi}(h) e\left(n\frac{h}{q}\right).$$

Thus, for a primitive character χ:

$$\begin{aligned}\sum_{n=M+1}^{M+N} a_n \chi(n) &= \sum_{n=M+1}^{M+N} a_n \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{q-1} \overline{\chi}(h) e\left(n\frac{h}{q}\right) \\ &= \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{q-1} \overline{\chi}(h) \sum_{n=M+1}^{M+N} a_n e\left(n\frac{h}{q}\right) \\ &= \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{q-1} \overline{\chi}(h) S\left(\frac{h}{q}\right).\end{aligned}$$

That is, the left-hand side of (16.20):

$$\begin{aligned}&\sum_{q \le Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \text{ primitive} \\ \text{character mod} q}}^{*} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \\ &\quad = \sum_{q \le Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \text{ primitive} \\ \text{character mod} q}}^{*} \underbrace{\frac{1}{|\tau(\overline{\chi})|^2}}_{\substack{=q \text{ since} \\ \chi \text{ is primitive}}} \left| \sum_{h=0}^{q-1} \overline{\chi}(h) S\left(\frac{h}{q}\right) \right|^2.\end{aligned}$$

Here on the right, $\forall$ term is ≥ 0, so we get an upper estimate if we also take the non-primitive characters, i.e.,

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \text{ primitive} \\ \text{character mod} q}}^{*} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2$$

$$\leq \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\chi}\left|\sum_{h=0}^{q-1}\overline{\chi}(h)S\left(\frac{h}{q}\right)\right|^2$$

$$= \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\chi}\sum_{h=0}^{q-1}\overline{\chi}(h)S\left(\frac{h}{q}\right)\sum_{k=0}^{q-1}\chi(k)\overline{S\left(\frac{k}{q}\right)}$$

since $\chi(k)=0$, if $(k,q)=1$ and $\overline{\chi}(h)=0$, if $(h,q)=1$ így

$$= \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\chi}\sum_{\substack{0\leq h<q\\(h,q)=1}}\sum_{\substack{0\leq k<q\\(k,q)=1}}\underbrace{\overline{\chi}(h)\chi(k)}_{\chi(h^*k)}S\left(\frac{h}{q}\right)\overline{S\left(\frac{k}{q}\right)}$$

$$= \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\substack{0\leq h<q\\(h,q)=1}}\sum_{\substack{0\leq k<q\\(k,q)=1}}S\left(\frac{h}{q}\right)\overline{S\left(\frac{k}{q}\right)}\underbrace{\sum_{\chi}\chi(h^*k)}$$

$$\begin{cases}\varphi(q), & \text{if } h^*k\equiv 1\ (q)\\ & \Leftrightarrow h=k\\ 0, & \text{if } h\neq k.\end{cases}$$

$$= \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\substack{0\leq h<q\\(h,q)=1}}\left|S\left(\frac{h}{q}\right)\right|^2\varphi(q)$$

$$= \sum_{q\leq Q}\sum_{\substack{0\leq h<q\\(h,q)=1}}\left|S\left(\frac{h}{q}\right)\right|^2$$

$$\leq (Q^2+\pi N)\sum_{n=M+1}^{M+N}.$$

This completes the proof of the theorem.

References

[1] A. Balog, A. Sárközy, *On sums of sequences of integers I.*, Acta Arithmetica 44 (1984), 73-84.

[2] A. Balog, A. Sárközy, *On sums of sequences of integers II.*, Acta Math. Acad. Sci.Hungar. 44 (1984), 169-179.

[3] J. R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica. 16 (1973) 157–176.

[4] H. Davenport, H. Halberstam, *The values of a trigonometric polynomial at well spaced points*, Mathematika 13 (1966), 91-96. *Corrigendum and addendum*, Mathematika 14 (1967), 229-232.

[5] P. X. Gallagher, *The large sieve*, Mathematika 14 (1967), 14-20.

[6] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math. 11, 329-339 (1970).

[7] H. L. Montgomery, *A note on the large sieve*, J. London Math. Soc. 43 (1968), 93-98.

[8] H. L. Montgomery, *The analytic principle of the large sieve*, Bulletin of the American Mathematical Society 84 (4) (1978), 547-567.

[9] A. Rényi, *On the representation of an even number as the sum of a prime and an almost prime*. Izvestiya Akademii Nauk SSSR Seriya Matematicheskaya 12 (1948), 57–78 (oroszul).

[10] S. L. Sobolev, *Applications of functional analysis in mathematical physics*, TransL Math. Monographs, vol. 7, 1963.

17 The reverse of the large sieve

Recall the large sieve: A dense set of integers is uniformly distributed in almost every residue class for almost every modulus.

On the other hand, Roth [4] proved that this distribution cannot be excessively uniform, i.e., $\exists$ is a residue class whose elements are either much more or much less in the studied set than expected.

Later, Roth [5] also proved the following:

Theorem 17.1 *Let k be a positive integer and suppose that $N > (10k)^7$. Then, for the sequence of real numbers $s_1, s_2, \dots, s_N$ we know $\exists n, q \in \mathbb{Z}^+$, for which*

$$1 \le n \le n + (k-1)q \le N$$

and

$$\left| \sum_{i=0}^{k-1} s_{n+iq} \right| \ge \left(\frac{k}{10N} \sum_{j=1}^{N} |s_j|^2 \right)^{1/2}.$$

In [6], Sárközy developed some modular analogues of of Roth's general results. However, in these generalizations, a slightly modified and more precise form of the above theorem was required. This more general theorem was the following:

Theorem 17.2 *Let $N, Q \in \mathbb{N}$, $Q \ge 2$, $s_1, s_2, \dots, s_N \in \mathbb{C}$, $Q_1 = \left[\frac{Q}{2}\right]$ and $s_j \stackrel{\text{def}}{=} 0$ if $j \le 0$ or $j > N$, moreover for $\forall n \in \mathbb{Z}$, $q, k \in \mathbb{Z}^+$ let*

$$D(n, q, k) \stackrel{\text{def}}{=} s_n + s_{n+q} + s_{n+2q} + \cdots + s_{n+(k-1)q}.$$

Then

$$\sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} |D(n, q, Q_1)|^2 \ge \left(\frac{2}{\pi} Q_1\right)^2 \sum_{m=1}^{N} |s_m|^2. \qquad (17.1)$$

In this chapter, following Sárközy's original calculations, we prove Theorem 17.2 and also see how Roth's original first question (see later Corollary 17.3) follows from this theorem. But before this, we see some important remarks and corollaries.

Remark. Typically $s_1 + s_2 + \cdots + s_N = 0 \Rightarrow s_n + s_{n+q} + \cdots + s_{n+(k-1)q}$ is also expected to be 0, or at least ' 'small" $\Rightarrow |D(n,q,k)|$ measures its standard deviation from the expected value, this is the discrepancy. So the theorem says: the standard deviation of the discrepancy is large.

Some corollaries:

Corollary 17.1 *$\exists\, n \in \mathbb{Z},\ q \in \mathbb{N}$ such that $q \le Q$ and*

$$|D(n,q,Q_1)| \ge \frac{2}{\pi}\left[\frac{Q}{2}\right] Q^{-1/2}\left(N+\frac{Q^2}{4}\right)^{-1/2}\left(\sum_{m=1}^{N}|s_m|^2\right)^{1/2}. \tag{17.2}$$

Proof of Corollary 17.1. Write

$$M \overset{\text{def}}{=} \max_{m,q} |D(n,q,Q_1)|.$$

Here we have to prove that $M \ge$ than the right-hand side of (17.2).

For the left-hand side of (17.1):

$$\begin{aligned} &\le \sum_{q=1}^{Q}\sum_{n=1-(Q_1-1)q}^{N} M^2 \\ &= M^2 \sum_{q=1}^{Q}\sum_{n=1-(Q_1-1)q}^{N} 1 \\ &= M^2 \sum_{q=1}^{Q}(N+(Q_1-1)q) \end{aligned}$$

$$
\begin{aligned}
&= M^2 \left(NQ + (Q_1 - 1) \sum_{q=1}^{Q} q \right) \\
&= M^2 \left(NQ + \left(\left[\frac{Q}{2} \right] - 1 \right) \frac{Q(Q+1)}{2} \right) \\
&\le M^2 Q \left(N + \left(\frac{Q}{2} - \underbrace{1}_{<\frac{1}{2}} \right) \left(\frac{Q}{2} + \frac{1}{2} \right) \right) \\
&< M^2 Q \left(N + \frac{Q^2}{4} - \frac{1}{4} \right) \\
&< M^2 Q \left(N + \frac{Q^2}{4} \right). \qquad (17.3)
\end{aligned}
$$

(17.1) and (17.3):

$$
M^2 Q \left(N + \frac{Q^2}{4} \right) \ge \frac{2}{\pi} \left[\frac{Q}{2} \right]^2 \sum_{m=1}^{N} |s_m|^2 .
$$

Dividing this by $Q\left(N + \frac{Q^2}{4}\right)$ and taking the square root, we get (17.2).

We get the best estimate for $\max_{n,q,Q} |D(n,q,Q_1)|$ if $Q \asymp \sqrt{N}$. Namely, if $Q = \left[\sqrt{N}\right]$, then by Corollary 17.1:

Corollary 17.2 *If $\varepsilon > 0$, $N > N_0(\varepsilon)$, $N \in \mathbb{N}$, $s_1, s_2, \ldots, s_N \in \mathbb{C}$ $\Rightarrow \exists\, n \in \mathbb{Z},\ q \in \mathbb{Z}^+$ such that $q \le \sqrt{N}$ and*

$$
|D(n,q,[\sqrt{N}/2])| \ge \left(\frac{2}{\pi\sqrt{5}} - \varepsilon \right) \left(\frac{\sum_{m=1}^{N} |s_m|^2}{N} \right)^{1/2} N^{1/4}. \qquad (17.4)
$$

Proof of Corollary 17.2. Now $Q = \left[\sqrt{N}\right]$. Then the right-hand side of (17.2) in Corollary 17.1:

$$
(1 + o(1)) \left(\frac{2}{\pi} \frac{\sqrt{N}}{2} N^{-1/4} \left(N + \frac{N}{4} \right)^{-1/2} \left(\sum_{m=1}^{N} |s_m|^2 \right) \right)^{1/2}
$$

$$= (1+o(1))\left(\frac{1}{\pi}\left(\frac{4}{5}\right)^{1/2} N^{1/4}\left(\frac{\sum_{m=1}^{N}|s_m|^2}{N}\right)^{1/2}\right)$$

$$\geq \left(\frac{2}{\pi\sqrt{5}}-\varepsilon\right) N^{1/4}\left(\frac{\sum_{m=1}^{N}|s_m|^2}{N}\right)^{1/2}. \tag{17.5}$$

Then from (17.2) and (17.4) follows (17.5).

After this, we will study the special case originally studied by Roth [4].

Corollary 17.3 *For* $\varepsilon > 0$, $N > N_0(\varepsilon)$, $\mathcal{A} \subseteq \{1,2,\dots,N\}$, *write* $\eta = \frac{|\mathcal{A}|}{N}$ *and* $\mathcal{A}(u,q,t) \stackrel{\text{def}}{=} |\{u, u+q, \dots, u+(t-1)q\} \cap \mathcal{A}|$, *then* $\exists\, u, q, t$ *such that* $\{u, u+q, \dots, u+(t-1)q\} \subseteq \{1,2,\dots,N\}$, $q \leq N$ *and*

$$|\mathcal{A}(u,q,t) - \eta t| \geq \left(\frac{2}{\pi\sqrt{5}}-\varepsilon\right)\sqrt{\eta(1-\eta)}N^{1/4}. \tag{17.6}$$

Remark. This is a reverse of the large sieve: at least one arithmetic sequence exists with the irregularity of order $\sqrt[4]{N}$.

Proof of Corollary 17.3. We use Corollary 17.2 with

$$s_n = \begin{cases} \eta, & \text{ha } n \notin \mathcal{A},\ 1 \leq n \leq N \\ -(1-\eta), & \text{ha } n \in \mathcal{A},\ 1 \leq n \leq N \\ 0, & \text{ha } n < 1 \text{ vagy } n > N. \end{cases}$$

Then, by Corollary 17.2 $\exists\, n,\ q,\ q \leq N$, for which

$$|D(n,q,[\sqrt{N}/2])| = |s_n + s_{n+q} + \dots + s_{n+([\sqrt{N}/2]-1)q}|$$
$$\geq \left(\frac{2}{\pi\sqrt{5}}-\varepsilon\right)\left(\frac{\sum_{m=1}^{N}|s_m|^2}{N}\right)^{1/2} N^{1/4}. \tag{17.7}$$

In principle, it may happen here that our arithmetic sequence $n, n+q, \ldots, n+([\sqrt{N}/2]-1)q$ extends beyond the interval $[1, N]$, in which case we discard those s_i's, for which $i \notin [1, N]$ (then $s_i = 0$), i.e., only 0 are discarded. We keep the intersection.

$$\{u, u+q, \ldots, u+(t-1)q\} \stackrel{\text{def}}{=} \\ \{n, n+q, \ldots, n+([\sqrt{N}/2]-1)q\} \cap \{1, 2, \ldots, N\}.$$

Then

$$\begin{aligned} D(n, q, [\sqrt{N}/2]) &= \sum_{j=0}^{[\sqrt{N}/2]-1} s_{n+jq} \\ &= \sum_{j=0}^{t-1} s_{u+jq} \\ &= \sum_{\substack{0 \le j < t \\ u+jq \notin \mathcal{A}}} \eta + \sum_{\substack{0 \le j < t \\ u+jq \in \mathcal{A}}} -(1-\eta) \\ &= \eta t - A(u, q, t). \end{aligned} \tag{17.8}$$

While the right-hand side of (17.7)

$$\begin{aligned} \frac{1}{N} \sum_{m=1}^{N} |s_m|^2 &= \frac{1}{N} \left(\sum_{\substack{n \notin \mathcal{A} \\ 1 \le n \le N}} \eta^2 + \sum_{\substack{n \in \mathcal{A} \\ 1 \le n \le N}} (1-\eta)^2 \right) \\ &= \frac{1}{N} \left(\eta^2 (N - \eta N) + (1-\eta)^2 \eta N \right) \\ &= \eta(1-\eta) \left(\eta + (1-\eta) \right) \\ &= \eta(1-\eta). \end{aligned} \tag{17.9}$$

Thus from (17.7), (17.8) and (17.9) follows (17.6).

Proof of Theorem 17.2. We will use the generator function method, which was introduced by Euler.

In the case of generator function methods, we usually assign a function $S(\alpha)$ to a sequence $s_1, s_2, \dots$ (here $S(\alpha)$ is typically a polynomial or power series). Next, we study the analytic properties of $S(\alpha)$ and derive certain arithmetic properties of the original sequence from this:

$$\text{sequence} \to \text{generator function} \overset{\text{analysis}}{\to} \text{analytic properties} \to$$
$$\to \text{ arithmetic properties of the sequence}$$

So let's look at the studied squence in the theorem: $s_1, s_2, \dots, s_N$ and assign a polynomial

$$S(\alpha) \overset{\text{def}}{=} \sum_{n=1}^{N} s_n e(n\alpha)$$

to the sequence. Then we use the complex version of the so-called Fejér kernel: for $M \in \mathbb{N}$ let

$$F_M(\alpha) \overset{\text{def}}{=} \sum_{j=0}^{M-1} e(j\alpha).$$

Then the (complex) Fejér kernel is $|F_M(\alpha)|^2$.

Lemma 17.1 *If $\alpha \in \mathbb{R}$, $|\alpha| \le \frac{1}{2M}$, then $|F_M(\alpha)| \ge \frac{2}{\pi}M$.*

Proof of Lemma 17.1. If $\alpha = 0$, then the lemma is trivial since $F_M(0) = M > \frac{2}{\pi}M$.

We also know that $F_M(-\alpha) = \overline{F_M(\alpha)}$, i.e., $|F_M(-\alpha)| = |F_M(\alpha)|$. So, during the proof, we can assume that $0 < \alpha \le \frac{1}{2M}$. Then $F_M(\alpha)$ is a geometric sequence with quotient $e(\alpha) \ne 1$, so

$$|F_M(\alpha)|^2 = \left|\frac{1 - e(M\alpha)}{1 - e(\alpha)}\right|^2.$$

Here, both the denominator and the numerator are the form $|1 - e(\beta)|^2$, where

$$\begin{aligned} |1 - e(\beta)|^2 &= (1 - e(\beta))\overline{(1 - e(\beta))} \\ &= (1 - e(\beta))(1 - e(-\beta)) \\ &= 2 - (e(\beta) + e(-\beta)) \\ &= 2 - 2\mathrm{Re}\, e(\beta) \\ &= 2 - 2\cos 2\pi\beta \\ &= 4\sin^2 \pi\beta, \end{aligned}$$

that is

$$|F_M(\alpha)|^2 = \frac{4\sin^2 M\pi\alpha}{4\sin^2 \pi\alpha} = \left|\frac{\sin M\pi\alpha}{\sin \pi\alpha}\right|^2.$$

Next write

$$f(x) = \frac{\sin Mx}{\sin x}$$

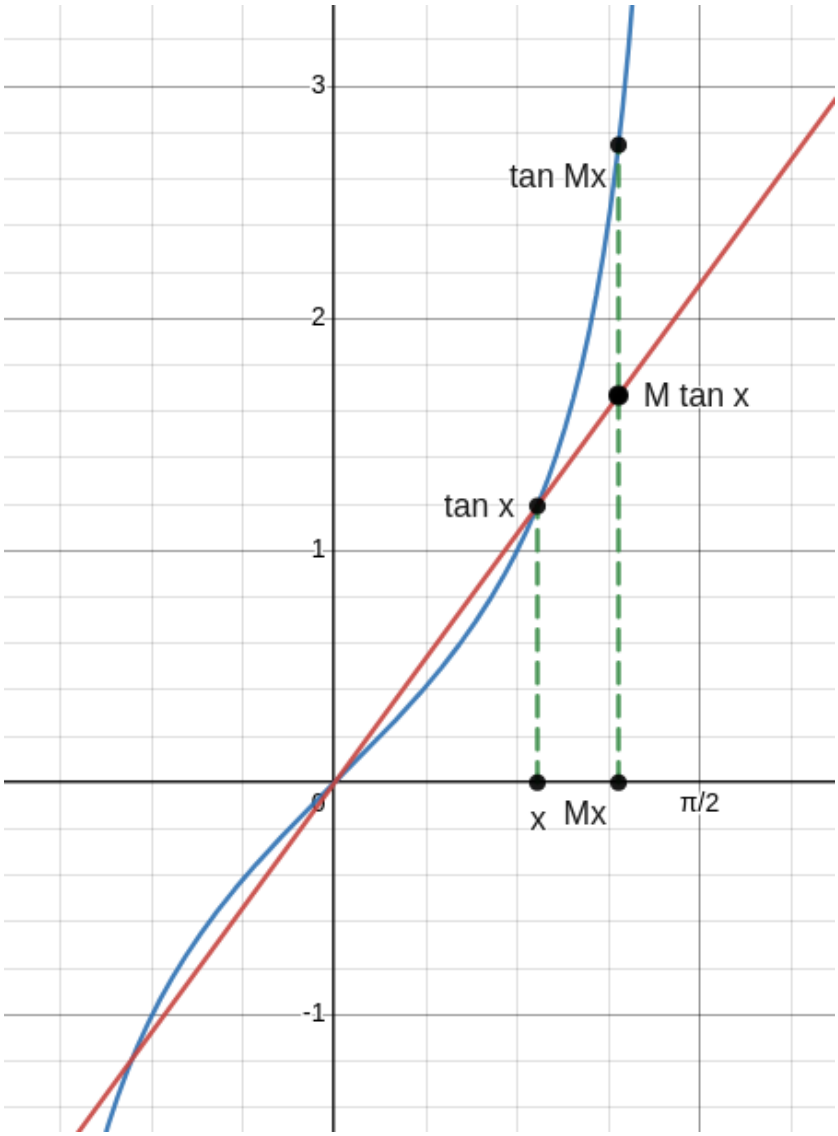
(where now M is fixed).

Statement. The function $f(x)$ is monotonically decreasing on the interval $\left(0, \frac{\pi}{2M}\right]$.

Then we have to show that $f'(x) < 0$. Indeed, for $x = \frac{\pi}{2M}$ this is trivial, and for $0 < x < \frac{\pi}{2M}$:

$$\begin{aligned} f'(x) &= \frac{M\cos Mx \sin x - \sin Mx \cos x}{\sin^2 x} \\ &= \frac{\cos x \cos Mx}{\sin^2 x}\left(M\frac{\sin x}{\cos x} - \frac{\sin Mx}{\cos Mx}\right) \\ &= \frac{\cos x \cos Mx}{\sin^2 x}\left(M\tan x - \tan Mx\right). \end{aligned}$$

Here the first factor is $\frac{\cos x \cos Mx}{\sin^2 x} > 0$, since $0 < x \leq Mx < \frac{\pi}{2}$, while $M\tan x - \tan Mx < 0$, since if we plot the tangent function we get the following figure:



By the convexity, the function $x = \tan x$ (blue curve) is above the line connecting the origin with the point $(x, \tan x)$ (red line) on the interval $\left[x, \frac{\pi}{2}\right)$. (By the convexity we have $\frac{\tan x - \tan 0}{x-0} \leq \tan' x \leq \frac{\tan Mx - \tan x}{Mx - x}$.)

So $M \tan x < \tan Mx$, which completes the proof of the statement.

By this statement for $0 < x \leq \frac{\pi}{2M}$ we have

$$f(x) \geq f\left(\frac{\pi}{2M}\right) = \frac{\sin M\frac{\pi}{2M}}{\sin \frac{\pi}{2M}} = \frac{1}{\sin \frac{\pi}{2M}} > \frac{1}{\frac{\pi}{2M}} = \frac{2}{\pi}M.$$

$$\uparrow$$
$$\sin x < x$$

That is

$$|F_M(\alpha)| = |f(\underbrace{\pi|\alpha|}_{\text{here } 0 \le \pi|\alpha| \le \frac{\pi}{2M}})| \ge \frac{2}{\pi}M,$$

which completes the proof of Lemma 17.1.

Let $Q_1 \overset{\text{def}}{=} \left[\frac{Q}{2}\right]$ (as defined in the theorem) and

$$G(\alpha) \overset{\text{def}}{=} \sum_{q=1}^{Q} |F_{Q_1}(q\alpha)|^2 . \tag{17.10}$$

Lemma 17.2 *For all $\alpha \in \mathbb{R}$ we have*

$$G(\alpha) \ge \left(\frac{2}{\pi}Q_1\right)^2 .$$

Proof of Lemma 17.2. By Dirichlet's approximation theorem, if $\alpha \in \mathbb{R}$, $Q \in \mathbb{N}$, then $\exists\, p \in \mathbb{Z}$, $q \in \mathbb{N}$, for which $q \le Q$, $(p, q) = 1$ and

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ},$$

from which

$$|q\alpha - p| < \frac{1}{Q} \le \frac{1}{2[Q/2]} = \frac{1}{2Q_1}. \tag{17.11}$$

By Lemma 17.1:

$$G(\alpha) = \sum_{q=1}^{Q} |F_{Q_1}(q\alpha)|^2 .$$

We keep a single q from the sum, the one for which (17.11) holds. Then

$$G(\alpha) \geq |F_{Q_1}(q\alpha)|^2 = |F_{Q_1}(q\alpha - p)|^2 .$$

Here we can use Lemma 17.1 with $M = Q_1$, since $|q\alpha - p| < \frac{1}{2Q_1}$. So:

$$G(\alpha) \geq \left(\frac{2}{\pi} Q_1\right)^2 .$$

Then consider the function

$$\mathcal{J} \stackrel{\text{def}}{=} \int_0^1 |S(\alpha)|^2 G(\alpha) d\alpha,$$

where $|S(\alpha)|^2$ is the Jensen function, and $G(\alpha)$ is the weight function defined in (17.10). Then we can give the following lower estimate for $\mathcal{J}$:

$$\mathcal{J} \geq \underbrace{(\min G(\alpha))}_{\text{Lemma 17.2}} \int_0^1 |S(\alpha)|^2 d\alpha \geq \left(\frac{2}{\pi} Q_1\right)^2 \sum_{m=1}^{N} |s_m|^2. \quad (17.12)$$

On the other hand, $\mathcal{J}$ can be calculated using the Parseval formula:

$$\begin{aligned}
\mathcal{J} &= \int_0^1 |S(\alpha)|^2 G(\alpha) d\alpha \\
&= \int_0^1 |S(\alpha)|^2 \sum_{q=1}^{Q} |F_{Q_1}(q\alpha)|^2 d\alpha \\
&= \sum_{q=1}^{Q} \int_0^1 |S(\alpha) F_{Q_1}(q\alpha)|^2 d\alpha \\
&= \sum_{q=1}^{Q} \int_0^1 \left| \sum_{n=1}^{N} s_n e(n\alpha) \sum_{j=0}^{Q_1 - 1} e(jq\alpha) \right|^2 d\alpha
\end{aligned}$$

$$= \sum_{q=1}^{Q} \int_0^1 \left| \sum_{n=1}^{N} s_n \sum_{j=0}^{Q_1-1} e((n+jq)\alpha) \right|^2 d\alpha.$$

Substitute $m = (n + jq)$ in this formula. Then $n = m - jq$, i.e.,

$$\mathcal{J} = \sum_{q=1}^{Q} \int_0^1 \left| \sum_{m=1}^{N+(Q_1-1)q} \underbrace{\left(\sum_{j=0}^{Q_1-1} s_{m-jq} \right)}_{D(m-q(Q_1-1),q,Q_1)} e(m\alpha) \right|^2 d\alpha.$$

By the Parseval formula:

$$\mathcal{J} = \sum_{q=1}^{Q} \sum_{m=1}^{N+(Q_1-1)q} |D(m - q(Q_1 - 1), q, Q_1)|^2 .$$

Then we substitute $n = m - q(Q_1 - 1)$:

$$\mathcal{J} = \sum_{q=1}^{Q} \sum_{n=1-q(Q_1-1)}^{N} |D(n, q, Q_1)|^2 .$$

So by (17.12):

$$\sum_{q=1}^{Q} \sum_{n=1-q(Q_1-1)}^{N} |D(n, q, Q_1)|^2 \geq \left(\frac{2}{\pi} Q_1 \right)^2 \sum_{m=1}^{N} |s_m|^2, \quad (17.13)$$

which completes the proof of the theorem.

Question. How far is Roth's inequality, i.e., (17.13) from the best possible estimate?

For simplicity, consider Corollary 17.2 in the case of $s_1, s_2, \ldots, s_N \in \{-1, +1\}$. Then we know that $\exists\, n \in \mathbb{Z},\ q \in \mathbb{Z}^+$, for which

$$\left| D(n, q, [\sqrt{N}/2)] \right| \gg N^{1/4}.$$

From the other direction, Roth noticed that, using probabilistic methods, one can see that there is an N-long ± 1 sequence for which $\max |D(n,q,k)| \ll N^{1/2}(\log N)^{1/2}$ and guessed that this result cannot be significantly improved, i.e.,

$$\max |D(n,q,k)| \gg N^{1/2-\varepsilon}.$$

holds for every N-long ± 1 sequence and positive ε (where the applied constant factor in $\gg$ depends only on ε).

This conjecture was disproved by Sárközy ([2, §8]), proving the existence of a sequence for which

$$\max |D(n,q,k| \ll N^{1/3}(\log N)^{2/3}. \tag{17.14}$$

Beck [1] proved a smaller upper bound $N^{1/4}(\log N)^{5/2}$. Finally, Matoušek and Spencer [3] proved the sharpest possible estimate, i.e. they showed the existence of a sequence for which

$$\max |D(n,q,k)| \ll N^{1/4}.$$

Here we only prove (17.14), i.e., the following:

Theorem 17.3 (Sárközy) *For all positive integer N, $\exists$ a sequence $s_1, s_2, \dots, s_N \in \{-1, +1\}$ for which*

$$\max_{n,q,t} \left|s_n + s_{n+q} + \cdots + s_{n+(t-1)q}\right| \ll N^{1/3}(\log N)^{2/3}.$$

Proof of Theorem 17.3. By Chebyshev's theorem, there is always a prime between n and $2n$, so let us now fix a prime p such that

$$\left(\frac{N}{\log N}\right)^{2/3} < p < 2\left(\frac{N}{\log N}\right)^{2/3}.$$

We define the sequence s_n as follows

$$s_n = \begin{cases} \left(\frac{n}{p}\right), & \text{ha } p \nmid n \\ 1, & \text{ha } p \mid n. \end{cases}$$

Then $D = \sum_{j=0}^{t-1} s_{n+jq}$ can be estimated as follows:

Case I.: $p \mid q$. Then

$$\begin{aligned} n + (t-1)q &\le N \\ (t-1)q &\le N - n \le N - 1 \\ t &\le \frac{N-1}{q} + 1 \le \frac{N-1}{p} + 1 \ll \frac{N}{\left(\frac{N}{\log N}\right)^{2/3}} \\ t &\ll N^{1/3}(\log N)^{2/3}. \end{aligned}$$

That is, $t \ll N^{1/3}(\log N)^{2/3}$ holds for the difference of the arithmetic progression, and then the theorem is trivial.

Case II.: $p \nmid q$. Denote by χ the quadratic character, i.e.,

$$\chi(n) = \begin{cases} \left(\frac{n}{p}\right), & \text{if } p \nmid n, \\ 0, & \text{if } p \mid n, \end{cases}$$

then

$$s_n = \begin{cases} \chi(n), & \text{if } p \nmid n, \\ 0, & \text{if } p \mid n. \end{cases}$$

So:

$$|D| = \left| \sum_{j=0}^{t-1} \chi(n+jq) + \sum_{\substack{0 \le j \le t \\ p \mid n+jq}} 1 \right|.$$

By the triangle inequality:

$$|D| \le \left| \sum_{j=0}^{t-1} \chi(n+jq) \right| + \left| \sum_{\substack{0 \le m \le N \\ p \mid m}} 1 \right|.$$

In this case $p \nmid q$, i.e., there exists q^* for which $qq^* \equiv 1 \pmod{p}$. So:

$$\begin{aligned} |D| &\le \left| \chi(q^*) \sum_{j=0}^{t-1} \chi(n+jq) \right| + \left[\frac{N}{p} \right] \\ &\le \left| \sum_{j=0}^{t-1} \chi(nq^*+j) \right| + \frac{N}{p}. \end{aligned}$$

By the Pólya-Vinogradov inequality (Theorem 14.1):

$$\begin{aligned} |D| &\le \sqrt{p} \log p + \frac{N}{p} \\ &\ll \left(\frac{N}{\log N} \right)^{1/3} \log \left(\frac{N}{\log N} \right)^{2/3} + \frac{N}{\left(\frac{N}{\log N} \right)^{2/3}} \\ &\ll N^{1/3} (\log N)^{2/3}. \end{aligned}$$

Thus, in both cases, we proved the statement of the theorem.

References

[1] J. Beck, *Roth's estimate of the discrepancy of integer sequences is nearly sharp*, Combinatorica 1 (4) (1981), 319-325.

[2] P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest, 1974.

[3] J. Matoušek, J. Spencer, *Discrepancy in arithmetic progression*, Jornal of the American Mathematical Society 9 (1) (1996), 195-204.

[4] K. F. Roth, *Remark concerning integer sequences*, Acta Arithmetica, 9 (1964), 257-260.

[5] K. F. Roth, *Irregularities of sequences relative to arithmetic progressions, I*, Math. Ann., 169 (1967), 1-25.

[6] A. Sárközy, *Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions. IV*, Acta Math. Academiae Scientiarum Hungaricae 30 (1977), 155–162.