Elementary Methods to Combinatorial Number Theory

Katalin Gyarmati

katalin.gyarmati@ttk.elte.hu

Eötvös Loránd University

Lecture Note

ELTE TTK, Mathematical Institute

Contents

Introduction

Combinatorial number theory commonly employs combinatorial methods, such as counting or graphs, in combination with well-known number theoretical tools.

Let us have a look at an example of a simple exercise for illustration purposes. It must be shown that the $n+1 \mid \binom{2n}{n}$ always holds.

This appears to be a challenging task when using elementary number theory approaches, but when we realize that $\frac{1}{n+1}\binom{2n}{n}$ is a well-known Catalan number from combinatorics, which is actually an integer related to the number of arrangements (for example, how many ways can we arrange n brackets), the proof becomes considerably simpler.

My favorite combinatorial number theory proofs are usually related to graph theory applications (Ramsey theory or extreme combinatorics). I tried to choose proofs in the notes that are as simple as possible, and the knowledge from the introductory combinatorics and number theory BSc courses is sufficient for their understanding.

I used a wide range of literature and provided the entire bibliography as carefully as I could at the end of each chapter. Among these, I would like to mention that a few chapters were written based on András Sárközy's classroom university lectures (where it is relevant I included this in the bibliography).

I began writing the note in the spring course of the 2020/21 online semester to adapt to the difficult circumstances and replace the well-known blackboard in traditional education.

1 Fermat congruence

Perhaps, you have heard about Hilbert's problems. Hilbert proposed 23 problems, and ten of them were presented at the Second International Congress of Mathematicians in Paris on August 8th, 1900.

Hilbert's problems lead to a substantial advance in mathematics. The 10th problem of his was the following:

Does there exist a universal (finite) algorithm for solving Diophantine equations? (An equation is called Diophantine if we are looking for its integer solutions.)

We will look at Diophantine equations from a combinatorial viewpoint in this chapter.

Before we move on, let us look at some of the most well-known Diophantine equations.

$ax + by = c$	Linear Diophantine equation.
$x^n + y^n = z^n$ for $n \geq 3$	Fermat's "last theorem"
$x^2 + y^2 = z^2$	Pythagorean triple

$x^4 + y^4 + z^4 = w^4$	Euler [6] conjectured this equation has only trivial solutions. Elkies [1] proved this is not true in 1988.

Typical questions about Diophantine equations:

1. Are there any solutions?
2. Are there any further solutions beyond than the ones found easily?
3. Are there finitely or infinitely many solutions?
4. Can one describe all the solutions?
5. Can one in practice determine a full list of solutions?

About the first question, there is sometimes (if we are lucky) an easy way to show that there is no solution to the Diophantine equation at all.

Examples:

1. $x^2 + y^2 = 3z^2$ has no solution in $\mathbb{N}$. Consider the equation modulo 3.
2. There exist infinitely many $m \in \mathbb{Z}$ such that $x^3 + y^3 + z^3 = m$ has no solution in $\mathbb{Z}$ (related to Waring problem [7]). Let $m \equiv \pm 4 \pmod 9$ and consider the equation modulo 9.

Returning to Hilbert's 10th Problem:

Does there exist a universal algorithm for solving all Diophantine equations?

This was unsolved for a long period. Finally, Martin Davis, Yuri Matiyasevich, Hilary Putnam, and Julia Robinson proved that there is no universal algorithm of this type (for further details see [8]).

As seen in Example 1 and 2, reducing the equation modulo m sometimes reveals that there is no solution at all.

Furthermore, there may have been historical assumptions that modulo m studies may lead to a goal in the case of nearly all Diophantine equations.

Let us consider the famous Fermat's last theorem:

$$x^n + y^n = z^n$$

has only trivial solutions for $n \geq 3$.

The trivial solutions are $x = 0$ or $y = 0$ or $z = 0$.

Fermat proposed this conjecture in 1637. He noted in the margin of a book that he found a beautiful and brief proof, but it was too large to fit in the margin.

Several mathematicians attempted but failed to find Fermat's original beautiful proof.

Finally, Wiles [4], [5] proved the conjecture in 1994, but his proof was more than 120 pages long.

But the conjecture had been open for more than 350 years.

In the past, I believe many mathematicians attempted to solve this Diophantine equation by reducing it modulo m.

Show that there exist infinitely many prime p such that the congruence

$$x^n + y^n \equiv z^n \pmod{p}$$

has no solution. What do you think: Is it true or not?

It is not true, e.g.

$$x \equiv 0 \ (p) \qquad y \equiv z \ (p)$$

is always a solution. The followings are called trivial solution:

$$x \equiv 0 \ (p) \quad \text{or} \quad y \equiv 0 \ (p) \quad \text{or} \quad z \equiv 0 \ (p)$$
$$\Updownarrow$$
$$xyz \equiv 0 \ (p).$$

Thus one might correct the idea:

Does there exist infinitely many prime p such that the congruence

$$x^n + y^n \equiv z^n \pmod{p}.$$

has only trivial solutions?

I believe several mathematicians tried to find such primes...

How would this statement imply Fermat's last theorem?

Suppose that $p_1 < p_2 < p_3 < \dots$ is an increasing sequence of primes such that

$$x^n + y^n \equiv z^n \pmod{p_i},$$

and this equation has only trivial solutions. Then $x \equiv 0 \ (p_i)$ or $y \equiv 0 \ (p_i)$ or $z \equiv 0 \ (p_i)$. But then $p_i \mid xyz$.

That means xyz has an infinite number of prime divisors while being finite, which is a contradiction.

It turned out that this method does not work, namely in 1916 Schur [3] proved the following (here the parentheses $\lceil \cdot \rceil$ will denote the ceiling function).

Theorem 1.1 (Schur) *If $p \geq \lceil en! \rceil + 1$, then the congruence*

$$x^n + y^n \equiv z^n \pmod{p}.$$

always has a non-trivial solution.

The proof uses combinatorial number theory.

Several erroneous proofs of famous conjectures, such as Goldbach's or Fermat's, have already been sent to mathematical institutes for examination...

This theorem destroyed several attempts to solve Fermat's problem using basic congruence processes, making reviewers' jobs easier.

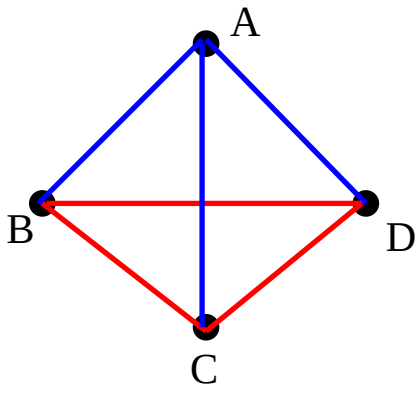
The proof uses graph theory, specifically Ramsey theory. The necessary tools are described in the following chapter.

1.1 Ramsey theory

Suppose that in a group of 6 people every two people either know each other or do not know each other but the relationship is always symmetric. Then there exist 3 people among them such that everybody knows everybody or nobody knows the others.

This can be illustrated by a graph of 6 vertices. The people are represented by the vertices. If two people know each other, we draw a blue edge. If they do not know each other, we draw a red edge.

Statement: In this graph always exists a monochromatic triangle. Fix a vertex A. Then there exist 3 other vertices B, C, D such that AB, AC, AD have the same color, say blue.

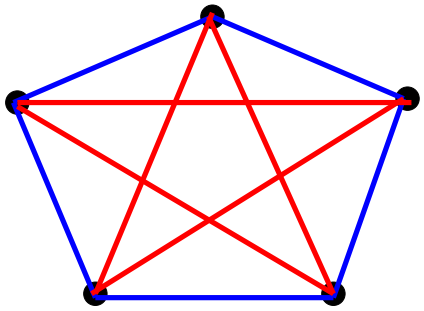


If the edge BC is blue, ABC is a blue triangle. As a result, we can assume that BC is red. Similarly, we can assume the edges BD and CD are also red. But if the edges BC, BD, CD are all red, then BCD is a red triangle.

Let $R_t(3)$ be the smallest integer n such that every complete graph on n (or more) vertices colored by t colors has a monochromatic triangle. If we color the edges of a complete graph on 3 vertices with only one color, then obviously it contains a monochromatic triangle. Thus

$$R_1(3) = 3.$$

In the example seen earlier, we have seen that $R_2(3) \leq 6$. On the other hand $R_2(3) > 5$ because in the next figure you will see a graph on 5 vertices colored by two colors, which does not contain a monochromatic triangle.



Thus

$$R_2(3) = 6.$$

Generalizing the previous ideas, we get that

$$R_t(3) \leq t\,(R_{t-1}(3) - 1) + 2. \tag{1.1}$$

Let us see the proof in details: Let $\mathcal{G}$ be a complete graph on n vertices.

Suppose that $n \geq t\,(R_{t-1}(3) - 1) + 2$. We will prove that if we color the edges of $\mathcal{G}$ by t colors, then it always contains a monochromatic triangle. From this (1.1) follows.

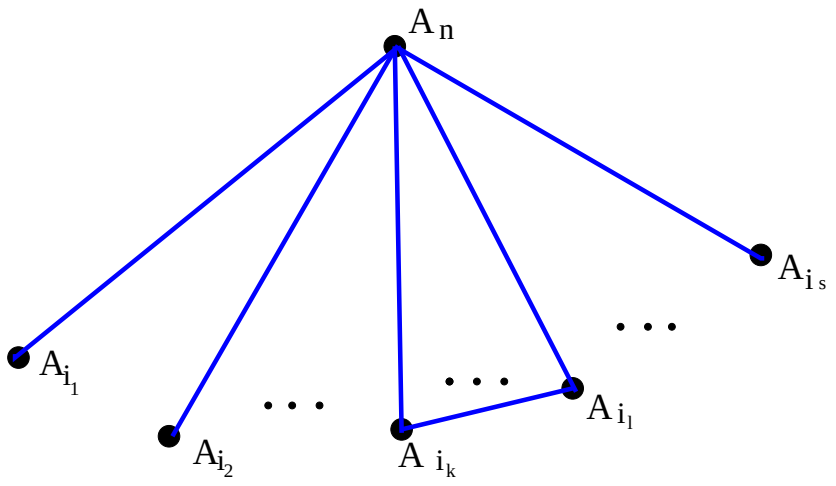
Let denote the vertices of $\mathcal{G}$ by $A_1, A_2, \ldots, A_n$. For a while we fix the vertex A_n, and consider the vertices $A_1, A_2, \ldots, A_{n-1}$. Since

$$n - 1 \geq t\,(R_{t-1}(3) - 1) + 1,$$

by the pigeon-hole principle, there exist $s = R_{t-1}(3)$ vertices $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$ such that the edges

$$A_nA_{i_1}, A_nA_{i_2}, \ldots, A_nA_{i_s}$$

are colored by the same color. Say, this color is blue. If among the vertices $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$ there is a blue edge, say $A_{i_k}A_{i_\ell}$, then there is a blue triangle: $A_nA_{i_k}A_{i_\ell}$:



If among the vertices $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$ there is no blue edge, then consider the subgraph $\mathcal{G}_0$ formed by these vertices. The edges of $\mathcal{G}_0$ are not colored by blue, so they are colored only by $t-1$ colors. Denote the number of vertices of $\mathcal{G}_0$ by $V(\mathcal{G}_0)$. Since

$$V(\mathcal{G}_0) = s = R_{t-1}(3),$$

by the definition of $R_{t-1}(3)$, we have $\mathcal{G}_0$ contains a monochromatic triangle.

By induction on t, it is easy to show that

$$R_t(3) \leq t!\left(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{t!}\right)+1. \tag{1.2}$$

Indeed, for $t=1$

$$R_1(3) = 3 \leq 1!\left(1+\frac{1}{1!}\right)+1.$$

If the statement is true for $t=k-1$, then it is also true for $t=k$. By (1.1) we have

$$\begin{aligned} R_k(3) &\leq k\left(R_{k-1}(3)-1\right)+2 \\ &\leq k\cdot(k-1)!\left(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{(k-1)!}\right)+2 \end{aligned}$$

$$= k! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{k!}\right) + 1.$$

This proves (1.2). Since

$$t! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{t!}\right) \leq t! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots\right) = t!e,$$

we obtain the following.

Theorem 1.2 (Schur)

$$R_t(3) \leq \lceil t!e \rceil.$$

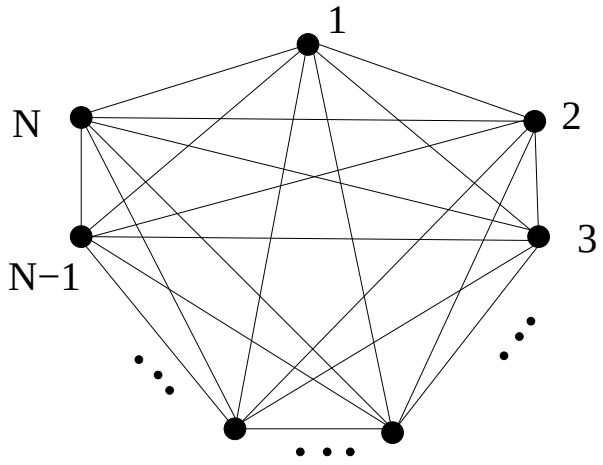
You can read more about $R_t(3)$ Ramsey numbers, e.g., on the following page: link.

Using Theorem 1.2 we will prove

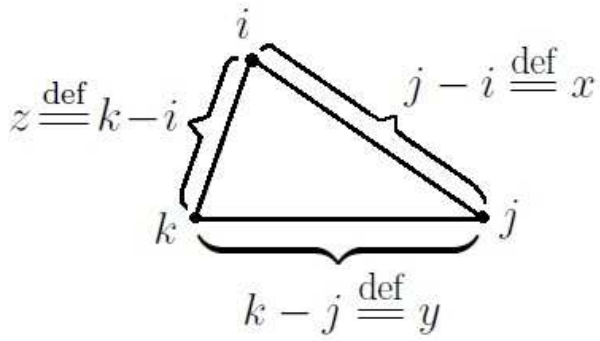
Theorem 1.3 (Schur) *If $N \geq \lceil t!e \rceil$ and the numbers $\{1, 2, \ldots, N\}$ are colored with t colors, then there always exists a monochromatic solution of*

$$x + y = z.$$

Proof of Theorem 1.3. Let $\mathcal{G}$ be a complete graph whose vertices are integer numbers between 1 and N.



We color the edges of $\mathcal{G}$ by t color by the following way: We assign a value to each edge. The value of the edge between i and j will be the integer number $|i-j|$. Since for this value we have $|i-j| \in \{1,2,\dots,N\}$ the number $|i-j|$ has a color. This color will be the color of the edge $\{i,j\}$. Since $R_t(3) \leq \lceil t!e \rceil \leq N$, the graph $\mathcal{G}$ contains a monochromatic triangle: $\{i,j,k\}$. We may assume $i<j<k$. Then:



By the definition of the coloring x, y and z have the same color. Moreover $x+y=z$ since $(j-i)+(k-j)=k-i$. Thus we have proved Schur's theorem.

Exercise. How does Schur theorem imply that the Fermat congruence $x^n+y^n \equiv z^n \pmod p$ always has a non-trivial solution for primes p large enough?

Hint: Use primitive roots!

Solution. Let p be a prime, $p \geq \lceil n!e \rceil + 1$. Let g be a primitive root $\bmod p$. Then

$$\{g^0, g^1, g^2, \dots, g^{p-2}\}$$

is a reduced residue system $\bmod p$. Thus the reminders of $g^0, g^1, \dots, g^{p-2}$ modulo p are the integers $1, 2, \dots, p-2$ (but not in this order). We write

$$\{g^0, g^1, g^2, \dots, g^{p-2}\} \equiv \{1, 2, \dots, p-1\} \pmod p.$$

Color $\{1, 2, 3, \ldots, p-1\}$ by n different colors.

An $s \in \{1, 2, \ldots, p-1\}$ is colored by the r-th color if there exists an integer k such that

$$s \equiv g^{kn+r} \pmod{p}.$$

We illustrate this by the following:

$$\begin{aligned}
\mathbf{1}\text{-st color} &\equiv \{g, g^{n+1}, g^{2n+1}, \ldots\} \pmod{p} \\
\mathbf{2}\text{-nd color} &\equiv \{g^2, g^{n+2}, g^{2n+2}, \ldots\} \pmod{p} \\
\mathbf{3}\text{-rd color} &\equiv \{g^3, g^{n+3}, g^{2n+3}, \ldots\} \pmod{p} \\
&\vdots \\
n\text{-th color} &\equiv \{g^0, g^n, g^{2n}, \ldots\} \pmod{p}
\end{aligned}$$

We will use Schur's theorem for this coloring. Then there exist x, y and z such that

$$x + y = z$$

and x, y, z have the same color. Denote this monochromatic solution by x_0, y_0, z_0. Then

$$x_0 + y_0 = z_0.$$

Since x_0, y_0, z_0 have the same color, then by the definition of coloring we have there exist integers r, k, ℓ and m such that

$$\begin{aligned}
x_0 &\equiv g^{kn+r} \pmod{p} \\
y_0 &\equiv g^{\ell n+r} \pmod{p} \\
z_0 &\equiv g^{mn+r} \pmod{p}.
\end{aligned}$$

Then

$$x_0 + y_0 = z_0$$

$$x_0 + y_0 \equiv z_0 \pmod{p}$$
$$g^{kn+r} + g^{\ell n+r} \equiv g^{mn+r} \pmod{p}$$
$$g^{kn} + g^{\ell n} \equiv g^{mn} \pmod{p}$$

Thus for $a \equiv g^k,\ b \equiv g^\ell,\ c \equiv g^m \pmod{p}$ we have

$$a^n + b^n \equiv c^n \pmod{p},$$

which was to be proved.

References

[1] N. Elkies, *On $A^4 + B^4 + C^4 = D^4$*, Mathematics of Computation. 51 (184) (1988), 825–835.

[2] P. Erdős, J. Surányi, *Topics in the Theory of Numbers*, 2003rd Edition, Springer, Undergraduate Texts in Mathematics.

[3] I. Schur, *Über die Kongruenz $x^m + y^m \equiv z^m \mod p$*, Jahresber. Deutsche Math.-Verein. 25, 114-116, 1916.

[4] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics. 141 (3) (1995), 443–551.

[5] R. Taylor, A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Mathematics. 141 (3) (1995), 553–572.

[6] Wikipedia, Euler's sum of powers conjecture, link.

[7] Wikipedia, Waring's problem, link.

[8] Wikipedia, Hilbert's tenth problem, link.

[9] Photo, David Hilbert, Wikipedia, link.

[10] Photo of Léonard Cotte, Paris, link.

[11] Figures to this section, home-made.

2 Further Ramsey theory applications

We saw a tricky application of the Ramsey theory in the first chapter. We will now present two other applications in number theory. But, before we go any further, a word about the creator of the theory. Ramsey was fascinated not only by mathematics, but also by many other fields, particularly economics. He was, nonetheless, interested in psychoanalysis.

Ramsey theory is well-known in mathematics for its aplicability; it is used not just in number theory but also in harmonic analysis, ergodic theory, geometry, information theory, logic, and so on.

The following example due to Sárközy [4].

Theorem 2.1 (Sárközy) *Let p be a prime of form $4k+1$. There exists a set $\mathcal{A} \subseteq \mathbb{Z}_p$ such that*

$$|\mathcal{A}| \geq \left\lceil \frac{1}{4} \log p \right\rceil$$

and all differences $a - a'$ with $a, a' \in \mathcal{A}$ are quadratic residues modulo p or zeros.

Proof of Theorem 2.1. Graph theory is needed for proving this theorem. We will use Ramsey's theory again.

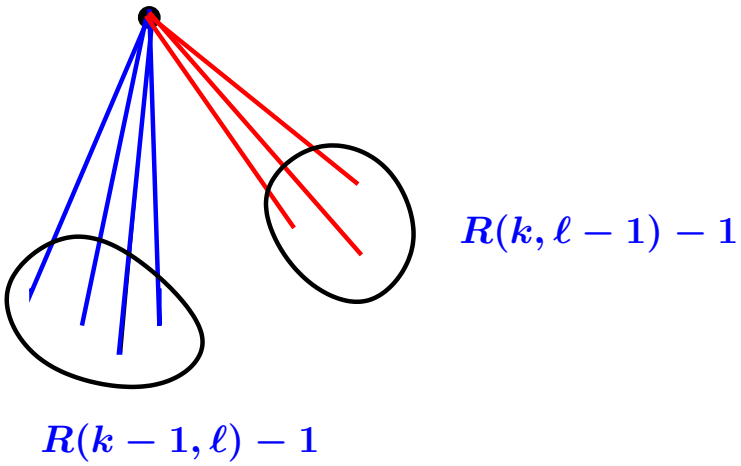
For a graph $\mathcal{G}$, let $V(\mathcal{G})$ denote the set of vertices of $\mathcal{G}$ and $E(\mathcal{G})$ denote the set of edges of $\mathcal{G}$.

Let K_n denote the complete graph on n vertices.

Moreover, let $R(k,\ell)$ denote the smallest integer such that every complete graph $\mathcal{G}$ with $|V(\mathcal{G})| \geq R(k,\ell)$ has the following property: If we color the edges of $\mathcal{G}$ with two colors: red and blue, then there always exists a monochromatic K_k colored with blue or a monochromatic K_ℓ colored with red. Then

$$R(k,\ell) \leq R(k-1,\ell) + R(k,\ell-1). \tag{2.1}$$

The proof of this can be illustrated by the following figure:



Indeed, suppose that $\mathcal{G}$ is a graph for which

$$|V(\mathcal{G})| \geq R(k-1,\ell) + R(k,\ell-1). \tag{2.2}$$

We will prove either G contains a blue K_k, either G contains a red K_ℓ. By this we get (2.1).

So suppose that $\mathcal{G}$ is graph for which (2.2) holds, and contrary to the statement, $\mathcal{G}$ does not contain blue K_k and red K_ℓ. Fix a vertex

A of $\mathcal{G}$. We divide all other vertices of $\mathcal{G}$ into two groups: V_0 is the set of the vertices B for which the edge AB is blue, V_1 is the set of vertices C, for which the edge AC is red.

Let $\mathcal{G}_0$ be the complete graph formed by the vertices in V_1 and $\mathcal{G}_1$ be the complete graph formed by the vertices in V_2.

If $\mathcal{G}_0$ contains a blue K_{k-1}, then $\mathcal{G}$ contains a blue K_k, since adding the vertex A to the blue subgraph K_{k-1} of $\mathcal{G}_0$, we obtain a blue subgraph K_k of $\mathcal{G}$. Thus if $\mathcal{G}$ does not contain blue K_k and red K_ℓ, then $\mathcal{G}_0$ does not contain blue K_{k-1} and red K_ℓ. Thus

$$|V(\mathcal{G}_0)| \leq R(k-1,\ell) - 1.$$

Similarly,

$$|V(\mathcal{G}_1)| \leq R(k,\ell-1) - 1.$$

Thus

$$\begin{aligned} |V(\mathcal{G})| &= |V(\mathcal{G}_0)| + |V(\mathcal{G}_1)| + 1 \\ &\leq (R(k-1,\ell) - 1) + (R(k,\ell-1) - 1) + 1 \\ &= R(k-1,\ell) + R(k,\ell-1) - 1, \end{aligned}$$

which contradicts to (2.2). Thus we proved (2.1).

Then by induction it is easy to show that

Theorem 2.2

$$R(k,\ell) \leq \binom{k+\ell-2}{\ell-1}.$$

Proof of Theorem 2.2. We will prove by induction First we prove $R(2,\ell) = \ell$ and $R(k,2) = k$.

Indeed if a graph has ℓ vertices, then either it contains a blue edge (so it contains a blue K_2), either its every edges are red (so it contains a red K_ℓ). Similarly, we may get $R(k,2) = k$.

Secondly, we show that if the theorem holds for all k's and ℓ's where $n = k+\ell$, then it also holds for all k's and ℓ's where $n+1 = k+\ell$.

Indeed, let $n+1 = k+\ell$. By (2.1) and the induction

$$\begin{aligned} R(k,\ell) &\leq R(k-1,\ell) + R(k,\ell-1) \\ &\leq \binom{k+\ell-3}{\ell-1} + \binom{k+\ell-3}{\ell-2} \\ &= \binom{k+\ell-2}{\ell-1}, \end{aligned}$$

which was to be proved.

The binomial theorem provides the following corollary:

Corollary 2.3

$$R(k,k) \leq \binom{2k-2}{k-1} < (1+1)^{2k-2} < 4^k.$$

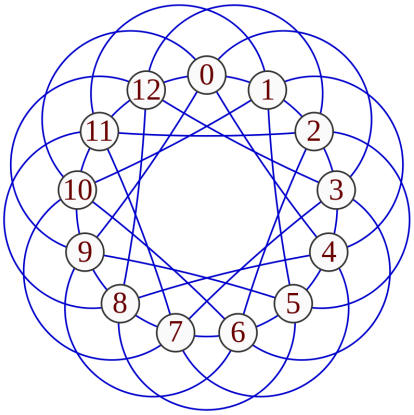
Proof of Theorem 2.1. Define a complete graph G whose vertices are the elements of $\mathbb{Z}_p$. We will use the following coloring:

For $a \neq a'$ the edge (a,a') is blue if $a-a'$ is a quadratic residue. The edge (a,a') is red if $a-a'$ is a quadratic non-residue. That is an appropriate definition because

$$\left(\frac{a-a'}{p}\right) = \left(\frac{a'-a}{p}\right). \tag{2.3}$$

Indeed, p is a prime of form $4k+1$, thus $\left(\frac{-1}{p}\right) = 1$, from which by the multiplicativity of Legendre symbol we get (2.3).

We note that the subgraph created by the blue edges is known as the Payley graph, after Raymond Payley. The figure illustrates the case $p = 13$:



We now return to the proof of the theorem. Let $k = \left[\frac{1}{4}\log p\right]$. Then

$$R(k,k) \le \binom{2k}{k} < 4^k < p.$$

So the graph (colored by blue and red) consists of a monochromatic K_k where $k = \left[\frac{1}{4}\log p\right]$.

If this color is blue, then let the vertices of the blue K_k are $a_1, a_2, \ldots, a_k$. By the definition of the coloring, all differences $a_i - a_j$ are quadratic residues.

If this color is red, we fix a quadratic non-residue $n \in \mathbb{Z}_p$. Let again the vertices of the red K_k are $a_1, a_2 \ldots, a_k$. Then all differences $a_i - a_j$ are quadratic non-residue. Define S_k by

$$S_k \stackrel{\text{def}}{=} \{na_1, na_2, \ldots, na_k\}.$$

Then $na_i - na_j$ is always a quadratic residue since:

$$\left(\frac{na_i - na_j}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{a_i - a_j}{p}\right) = (-1)(-1) = 1,$$

which proves the theorem.

Exercises

1. Does this proof work for sums $a + a'$ in place of $a - a'$?
2. Does there exist a similar proof for shifted products $aa' + 1$?
3. Could you give a non-trivial upper bound for $|\mathcal{A}|$ if $\mathcal{A} \subseteq \mathbb{Z}_p$ and $a - a'$ is always a quadratic residue modulo p?

Solutions of the exercises.

1.) The answer is yes, and the proof is very similar to the original. We will prove the following:

Theorem 2.4 *Let p be a prime. There exists a set $\mathcal{A} \subseteq \mathbb{Z}_p$ such that*

$$|\mathcal{A}| \geq \left[\frac{1}{4}\log p\right]$$

and all sums $a + a'$ with $a \neq a'$, $a, a' \in \mathcal{A}$ are quadratic residues modulo p or zeros.

Proof of Theorem 2.4. We define a complete graph $\mathcal{G}$ whose vertices are the elements of $\mathbb{Z}_p$. We will use the following coloring: For $a \neq a'$ the edge (a, a') is blue if $a + a'$ is a quadratic residue or 0. The edge (a, a') is red if $a + a'$ is a quadratic non-residue. It is a good definition since

$$\left(\frac{a + a'}{p}\right) = \left(\frac{a' + a}{p}\right).$$

Let $k = \left[\frac{1}{4}\log p\right]$. Then again

$$R(k, k) \leq \binom{2k}{k} < 4^k < p.$$

So the graph consists of a monochromatic K_k where $k = \left[\frac{1}{4}\log p\right]$.

If this color is blue, then let the vertices of the blue K_k are $a_1, a_2, \ldots, a_k$. By the definition of the coloring, all sums $a_i + a_j$ are quadratic residues or zeros.

If this color is red, we fix a quadratic non-residue $n \in \mathbb{Z}_p$. Let again the vertices of the red K_k are $a_1, a_2 \ldots, a_k$. Then all sums $a_i + a_j$ are quadratic non-residue. Define S_k by

$$S_k \stackrel{\text{def}}{=} \{na_1, na_2, \ldots, na_k\}.$$

Then $na_i + na_j$ is always a quadratic residue since:

$$\left(\frac{na_i + na_j}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{a_i + a_j}{p}\right) = (-1)(-1) = 1,$$

which proves the theorem.

2.) We will prove the following:

Theorem 2.5 (Gyarmati [2]) *There is a constant p_0 such that if p is a prime of the form $4k + 1$ and $p > p_0$ then there exists $\mathcal{A} \subseteq \mathbb{Z}_p$ so that $|\mathcal{A}| \geq \frac{1}{6\log 3}\log p$ and $aa' + 1$ is a quadratic residue or $0 \mod p$ for all $a, a' \in \mathcal{A}$, $a \neq a'$.*

The proof of Theorem 2.5. The theorem will follow from the following Ramsey type result:

Lemma 2.6 *If s_1, s_2, s_3 are non-negative integers then there exists an integer r with the following property: If G is a complete graph, $|G| \geq r$ and C is any 3-coloring of the edges of G with colors c_1, c_2, c_3, then for some $1 \leq i \leq 3$ the graph G has a subgraph G' which is monochromatic with color c_i and $|G'| \geq s_i$.*

Furthermore, denoting the least integer r *with this property by* $R(s_1, s_2, s_3)$ *we have:*

$$R(s_1, s_2, s_3) \leq \frac{(s_1 + s_2 + s_3)!}{s_1! s_2! s_3!}.$$

Proof of Lemma 2.6. If any of the numbers s_1, s_2, s_3 is 0 then the lemma is trivial because $R(s_1, s_2, s_3) = 0$. We may assume that $s_1, s_2, s_3 > 0$. The following inequality is well-known [1, p. 75] (and can be verified with a typical Ramsey theoretical proof):

$$R(s_1, s_2, s_3) \leq$$
$$R(s_1 - 1, s_2, s_3) + R(s_1, s_2 - 1, s_3) + R(s_1, s_2, s_3 - 1)$$

for $s_1, s_2, s_3 > 0$. Using induction we get:

$$R(s_1, s_2, s_3) \leq \frac{(s_1 + s_2 + s_3)!}{s_1! s_2! s_3!}.$$

Consider the graph whose vertices are the residue classes modulo p. Since p is a prime of the form $4k + 1$ there exists an integer i such that $i^2 \equiv -1 \pmod{p}$.

Let the edge e join the classes a and b. We color e with c_1 if $\left(\frac{ab+1}{p}\right) = 1$ or 0. Furthermore we color e with c_2 if $\left(\frac{-ab+1}{p}\right) = 1$ or 0 and $\left(\frac{ab+1}{p}\right) = -1$. Finally we color e with c_3 if $\left(\frac{-a^2b^2+1}{p}\right) = 1$ or 0 and $\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = -1$ (we set $\left(\frac{0}{p}\right) = 0$).

We color all edges because otherwise:

$$\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = \left(\frac{-a^2b^2+1}{p}\right) = -1.$$

So:

$$-1 = \left(\frac{(ab+1)(-ab+1)(-a^2b^2+1)}{p}\right) = \left(\frac{(a^2b^2-1)^2}{p}\right).$$

But this contradicts the obvious fact that $\left(\frac{\left(a^2b^2-1\right)^2}{p}\right) = 1$ or 0.

Take $c = \left[\frac{1}{3\log 3}\log p\right] + 1$. Applying the lemma we obtain:

$$R(c,c,c) \leq \frac{(3c)!}{c!c!c!}.$$

By Stirling formula, for $c \to \infty$ we have:

$$\frac{(3c)!}{c!c!c!} \leq (1+o(1))\frac{\left(\frac{3c}{e}\right)^{3c}\sqrt{2\pi 3c}}{\left(\left(\frac{c}{e}\right)^{c}\sqrt{2\pi c}\right)^3} \leq 3^{3c-3} \leq p.$$

Thus if p is large enough then $R(c,c,c) \leq p$. Therefore the graph has a subgraph X which is monochromatic c_j for some $1 \leq j \leq 3$ and $|X| \geq c$.

Let $\mathcal{A}$ be the set of the vertices of X if we colored the edges of X with c_1. Let $\mathcal{A}$ be $\{ix : x \in V(X)\}$ if we colored the edges of X with c_2. Let $\mathcal{A}$ be $\{ix^2 : x \in V(X)\}$ if we colored the edges of X with c_3.

Now $|\mathcal{A}| \geq \frac{1}{2}|X|$. Using the definition of coloring, we obtain that the product of any two elements of $\mathcal{A}$ increased by 1 is a quadratic residue or $0 \mod p$.

3.) We will prove the following:

Theorem 2.7 (folklore) *Let p be a prime. If $\mathcal{A} \subset \mathbb{Z}_p$ is a set such that for all $a \neq a'$, $a, a' \in \mathcal{A}$ we have that $a - a'$ is quadratic residue modulo p then*

$$|\mathcal{A}| \leq \sqrt{p}.$$

Proof of Theorem 2.7.

Suppose that $A - A$ contains only quadratic residues and 0. Let $n \in \mathbb{Z}_p$ be a quadratic non-residue. Then all sums of the form

$$a - na', \qquad a, a' \in A$$

are distinct. Indeed, if

$$a_0 - na_0{}' \equiv a_1 - na_1{}' \pmod{p},$$

then

$$a_0 - a_1 \equiv n(a_0{}' - a_1{}') \pmod{p}.$$

There is a quadratic residue on the left-hand side, and a quadratic non-residue on the right-hand side. The only exception is $a_0 = a_1$, $a_0{}' = a_1{}'$. So indeed, all sums

$$a - na', \qquad a, a' \in A$$

are distinct.

The number of pairs $a, a' \in A$ is $|\mathcal{A}|^2$, thus

$$|\mathcal{A}|^2 \leq p,$$
$$|\mathcal{A}| \leq \sqrt{p}.$$

The best result differs from this theorem only by a constant factor, namely Hanson and Pertidis [3] proved that $|\mathcal{A}| \leq \sqrt{p/2} + 1$.

References

[1] , R.L. Graham, B.L. Rothschild, J.H. Spencer, *Ramsey Theory*, Wiley 1980.

[2] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97.1 (2001), 53-65.

[3] B. Hanson, G. Pertidis, *Refined estimates concerning sumsets contained in the roots of unity*, available at https://arxiv.org/abs/1905.09134

[4] A. Sárközy, *On difference sets of integers II*, Ann. Univ. Sci. Budapest. 21 (1978).

[5] Photo, Frank Plumpton Ramsey, Wikipedia, link.

[6] Figure, Payley graph, Wikipedia, link.

[7] Figure, Ramsey-theory, home-made.

3 Gallagher's larger sieve

The sieve described here, by Patrik Ximenes Gallagher, is perhaps the simplest to prove.

Its proof relies solely on the Cauchy-Schwarz inequality and elementary considerations.

The idea behind sieve formulae is that if we know the modular structure of a subset of the natural numbers (for many m, the set intersects only a few residue classes $\mod m$), we may estimate the number of elements in the set.

Before we describe the larger sieve, we will present a theorem derived from its application:

Theorem 3.1 (Rivat, Stewart, Sárközy [7]) *There exists an integer x_0 such that if $x_0 < x \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, 3, \ldots, x\}$ and for all $a, a' \in \mathcal{A}$ we have that $a + a'$ is always a square, then*

$$|\mathcal{A}| < 37 \log x. \tag{3.1}$$

We have no idea how sharp this theorem is. J. Lagrange [5] and J.-L. Nicolas [6] found a 6-element set A satisfying the above property, namely

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

Since then, it has been a conjecture that there is no set $\mathcal{A}$ greater than this.

Instead of Rivat, Stewart, and Sárközy's result, we prove a slightly simpler statement.

Theorem 3.2 (Gyarmati [4]) *There exists an integer x_0 such that if $x_0 < x \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, 3, \dots, x\}$ and for all $a > a' \in \mathcal{A}$ we have that $a - a'$ is always a square, then*

$$|\mathcal{A}| < 2.01 \log x. \tag{3.2}$$

The proof is exactly the same as in the $a + a'$ case, the only difference is that the used lemma (see Theorem 2.7 of this note) is not based on exponential sums.

The main idea of the proof is Gallagher's larger sieve [7]. The form of the sieve shown here was verified by Erdős, Stewart and Sárközy [2] in 1994.

Theorem 3.3 (Gallagher's larger sieve) *Suppose that $m, n \in \mathbb{N}$, $\mathcal{A} \subset \{m + 1, m + 2, \dots, m + n\}$ and $\mathcal{B} \subset \mathbb{N}$ is a finite set, such that its elements are pairwise relatively primes. For all $b \in \mathcal{B}$ denote*

by $\nu(b)$ the number of such residue classes $\mod b$ which intersect $\mathcal{A}$. Then

$$|\mathcal{A}| \le \frac{\sum\limits_{b\in\mathcal{B}} \log b - \log n}{\sum\limits_{b\in\mathcal{B}} \frac{\log b}{\nu(b)} - \log n}, \tag{3.3}$$

provided that the denominator is positive.

Gallagher stated the theorem for the subset of primes $\mathcal{B} = \mathcal{P}$.

Why this theorem called as a sieve? Here, we estimate $\mathcal{A}$ in terms of functions $\nu(b)$. If $\mathcal{A}$ contains no element from many residue classes $\mod b$, the value of $\nu(b)$ is small, and so the denominator in (3.3) is large, resulting in a small $|\mathcal{A}|$.

Proof of Theorem 3.3. Let

$$n_k \stackrel{\text{def}}{=} \left|\{a:\ a\in\mathcal{A},\ a\equiv k \pmod b\}\right|.$$

Then by the Cauchy-Schwarz inequality for fixed b we have:

$$\sum_{k=1}^{b} n_k^2 \ge \frac{\left(\sum_{k=1}^{b} n_k\right)^2}{\nu(b)} = \frac{|\mathcal{A}|^2}{\nu(b)}.$$

On the other hand:

$$\sum_{k=1}^{b} n_k^2 = \sum_{k=1}^{b} \sum_{\substack{a,a'\in\mathcal{A}\\ a\equiv a'\equiv k \pmod b}} 1$$

$$= \sum_{\substack{a,a'\in\mathcal{A}\\ a\equiv a' \pmod b}} 1$$

$$= |\mathcal{A}| + \sum_{\substack{a,a'\in\mathcal{A},\ a\ne a'\\ b\mid a-a'}} 1.$$

Thus

$$\frac{|\mathcal{A}|^2}{\nu(b)} \leq |\mathcal{A}| + \sum_{\substack{a,a' \in \mathcal{A},\ a \neq a' \\ b \mid a-a'}} 1.$$

Then by multiplying $\log b$:

$$|\mathcal{A}|^2 \frac{\log b}{\nu(b)} \leq |\mathcal{A}| \log b + \sum_{\substack{a,a' \in \mathcal{A},\ a \neq a' \\ b \mid a-a'}} \log b.$$

Summing up for b:

$$|\mathcal{A}|^2 \sum_{b \in \mathcal{B}} \frac{\log b}{\nu(b)} \leq |\mathcal{A}| \sum_{b \in \mathcal{B}} \log b + \sum_{\substack{a,a' \in \mathcal{A} \\ a \neq a'}} \sum_{\substack{b \mid a-a' \\ b \in \mathcal{B}}} \log b.$$

Here in the final sum:

$$\sum_{\substack{b \mid a-a' \\ b \in \mathcal{B}}} \log b = \log \prod_{\substack{b \mid a-a' \\ b \in \mathcal{B}}} b \leq \log n.$$

Thus:

$$|\mathcal{A}|^2 \sum_{b \in \mathcal{B}} \frac{\log b}{\nu(b)} \leq |\mathcal{A}| \sum_{b \in \mathcal{B}} \log b + \sum_{\substack{a,a' \in \mathcal{A} \\ a \neq a'}} \log n$$

$$|\mathcal{A}| \sum_{b \in \mathcal{B}} \frac{\log b}{\nu(b)} \leq \sum_{b \in \mathcal{B}} \log b + (|\mathcal{A}| - 1) \log n$$

$$|\mathcal{A}| \left(\sum_{b \in \mathcal{B}} \frac{\log b}{\nu(b)} - \log n \right) \leq \sum_{b \in \mathcal{B}} \log b - \log n.$$

If the multiplier following $|\mathcal{A}|$ is positive, we could prove the theorem by dividing by it.

Proof of Theorem 3.2. We know that for $a, a' \in \mathcal{A},\ a > a'$, the difference $a - a'$ is always a square. That is, for $a, a' \in \mathcal{A},\ a > a'$ we have that $a - a'$ is a quadratic residue $\mod p$ or 0 for every prime p.

If -1 is quadratic residue $\mod p$, then $a' - a$ is also a quadratic residue $\mod p$ or 0, not only $a - a'$.

We know that -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$.

That is, if $p \equiv 1 \pmod 4$, then for all $a, a' \in \mathcal{A}$ we have $a - a'$ is a quadratic residue $\mod p$ or 0 (then the condition $a > a'$ is no longer needed).

Next we use Theorem 2.7 as a lemma.

Lemma 3.4 *Let p be a prime. If $\mathcal{C} \subset \mathbb{Z}_p$ is a set such that for all $a \neq a'$, $a, a' \in \mathcal{C}$ we have that $a - a'$ is quadratic residue modulo p then*

$$|\mathcal{C}| \leq \sqrt{p}.$$

Let $\mathcal{C}$ denote the set of $\mod p$ residual classes that contain an element in $\mathcal{A}$. Then $\mathcal{C} \leq \sqrt{p}$.

That is, using the notation of Theorem 3.3 from the previous lemma $\nu(p) \leq \sqrt{p}$ follows.

Then we simply use Gallagher's larger sieve. For this let:

$$\mathcal{B} = \{p :\ p \text{ is a prime},\ p \equiv 1 \pmod 4,\ 2 \leq p \leq c(\log x)^2\},$$

where the value of the constant c will be chosen later, for now the only important thing is that c is a constant greater than 1.

By using Gallagher's larger sieve:

$$|\mathcal{A}| \leq \frac{\sum\limits_{p\equiv 1 \pmod 4,\ p\leq c(\log x)^2} \log p - \log x}{\sum\limits_{p\equiv 1 \pmod 4,\ p\leq c(\log x)^2} \frac{\log p}{\sqrt{p}} - \log x}. \tag{3.4}$$

Next, we estimate the value of the expression on the right. Introduce the following notations:

$$\pi(y,4,1) \stackrel{\text{def}}{=} \sum_{p\equiv 1 \pmod 4,\ p\leq y} 1$$

$$\theta(y,4,1) \stackrel{\text{def}}{=} \sum_{p\equiv 1 \pmod 4,\ p\leq y} \log p$$

$p_n(4,1)$ is the n-th smallest positive prime that is $\equiv 1 \pmod 4$.

Luckily, these terms are increasingly being estimated more accurately. For example, by Bennet, Martin, O'Bryan, and Rechnitzer's result [1] we get the following:

$$\begin{aligned}
\pi(y,4,1) &= (1+o(1))\frac{y}{2\log y} && \text{see Theorem 1.4 in [1],}\\
\theta(y,4,1) &= (1+o(1))\frac{y}{2} && \text{see Corollary 1.7 in [1],}\\
p_n(4,1) &= (1+o(1))2n\log n && \text{see Theorem 1.5 in [1].}
\end{aligned}$$

It follows directly from the estimate for $\theta(y,4,1)$ that for the expression in the numerator of the fraction holds the following:

$$\sum_{p\equiv 1 \pmod 4,\ p\le c(\log x)^2} \log p - \log x$$

$$= \theta(c(\log x)^2, 4, 1) - \log x$$

$$= (1+o(1))\frac{c}{2}(\log x)^2 - \log x$$

$$= (1+o(1))\frac{c}{2}(\log x)^2. \tag{3.5}$$

Estimating the denominator of the fraction (3.4) is more complicated:

$$\sum_{p\equiv 1 \pmod 4,\ p\le c(\log x)^2} \frac{\log p}{\sqrt{p}} - \log x$$

$$= \sum_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\log p_n(4,1)}{\sqrt{p_n(4,1)}} - \log x$$

$$= (1+o(1)) \sum_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\log(2n\log n)}{\sqrt{2n\log n}} - \log x$$

$$= (1+o(1))\frac{1}{\sqrt{2}} \sum_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\log n}{\sqrt{n\log n}} - \log x$$

$$= (1+o(1))\frac{1}{\sqrt{2}} \sum_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\sqrt{\log n}}{\sqrt{n}} - \log x$$

$$= (1+o(1))\frac{1}{\sqrt{2}} \int_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\sqrt{\log n}}{\sqrt{n}} dn - \log x$$

$$= (1+o(1))\sqrt{2}\ \sqrt{n\log n}\Big]_1^{\pi(c(\log x)^2,4,1)} - \log x$$

$$= (1+o(1))\sqrt{2}\sqrt{\pi(c(\log x)^2,4,1)\log\left(\pi(c(\log x)^2,4,1)\right)} - \log x$$

$$= (1+o(1))\sqrt{2}\sqrt{\frac{c(\log x)^2}{2\log\left(c(\log x)^2\right)}\log\left(\frac{c(\log x)^2}{2\log\left(c(\log x)^2\right)}\right)} - \log x$$

$$= (1+o(1))\sqrt{2}\sqrt{\frac{c(\log x)^2}{4\log\log x}2\log\log x} - \log x$$

$$= (1+o(1))\sqrt{c}\log x - \log x$$

$$= (1+o(1))(\sqrt{c}-1)\log x.$$

Writing this estimate and (3.5) into (3.4) yields the following:

$$|\mathcal{A}| \leq (1+o(1))\frac{c}{2\left(\sqrt{c}-1\right)}\log x,$$

if $c > 1$. By choosing $c = 4$ we get

$$|\mathcal{A}| \leq 2.01\log x,$$

for $x > x_0$, and this completes the proof.

References

[1] M. A. Bennet, G. Martin, K. O'Bryant, A. Rechnitzer, *Explicit bounds for primes in arithmetic progressions*, Illinois J. Math. 62 (2018), no. 1-4, 427–532.

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

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

[4] K. Gyarmati, *On Diophantine square tuples*, Int. J. Number Theory, submitted.

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

[6] J.-L. Nicolas, *Six nombres dont les sommes deux à deux sont des carrés*, Calculateuren Math. (1975, Limoges), Bulletin de la Société Mathématique de France, mémoire 49-50, (1977), pp. 141–143.

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

[8] Photo, Archeologist clip art, link.

4 On a problem of Diophantus

Diophantus of Alexandria, a Greek mathematician, observed that the rational numbers $\frac{1}{16}$, $\frac{33}{16}$, $\frac{17}{4}$, and $\frac{105}{16}$ have the following property: the product of any two of them increased by one is a square of rational number.

Later Fermat found a set of four positive integers with the above property: {1,3,8,120}.

Phil Gibbs has found a set of six rational numbers having this property: $\left\{\frac{11}{192}, \frac{32}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$ (see [4]).

In 2004 Andrej Dujella proved [3] the following.

Theorem 4.1 (Dujella) *There are no 6 numbers with the property that whenever any two are multiplied and increased by one, the result is always a square number.*

This result, however, is too complex to prove within the scope of this note. Those who are interested may visit the following web page of Dujella: link.

Dujella's result was improved in a more than forty-page long paper by He, Togbé and Ziegler [6], who proved the following.

Theorem 4.2 (He-Togbé-Ziegler) *There are no 5 numbers with the property that whenever any two are multiplied and increased by one, the result is always a square number.*

Using this result, however, the following pleasant theorem can be proved:

Theorem 4.3 (Bugeaud, Gyarmati [2]) *Let $\mathcal{A}$ be a set of positive integers with $|\mathcal{A}| \geq 5$. Then the set*

$$\{(a, a') : a, a' \in \mathcal{A},\ a > a',\ aa' + 1 \text{ is a square}\}$$

has at most $\frac{3}{8}|\mathcal{A}|^2$ elements.

In fact, since Theorem 4.2 had not yet been proved then, we proved a slightly weaker result in [2].

Proof of Theorem 4.3. The proof is based on Turán's well-known theorem [8]:

Lemma 4.4 (Turán) *Let G be a graph on n vertices having at least*

$$\frac{r-2}{2(r-1)}n^2$$

edges for some positive integer $r \geq 3$. Then G contains a complete subgraph on r edges.

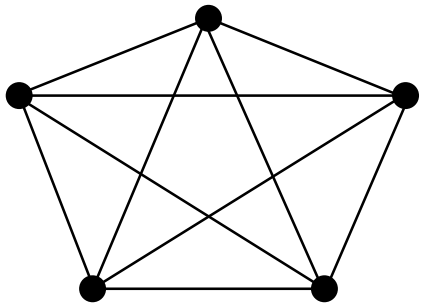
Proof of Lemma 4.4. Pál Turán's original proof is obtainable in [8] in Hungarian. Since then, many proofs of the theorem have been established; for example, [1] contains five distinct proofs.

We now turn to the proof of Theorem 4.3.

Let $a_1, a_2, \ldots, a_n$ denote the elements of $\mathcal{A}$.

Denote the vertices of the graph G by $a_1, a_2, \ldots, a_n$ and there is an edge between two vertices a_i and a_j if and only if $a_i a_j + 1$ is a square.

By Theorem 4.2, the graph G does not contain K_5 as a subgraph.



Lemma 4.4 then implies that G has at most $\frac{3}{8}n^2 = \frac{3}{8}|\mathcal{A}|^2$ edges. This proves Theorem 4.3.

We can justify a little better than the above if we know that the elements of the set $\mathcal{A}$ fall within a not too long interval. Namely:

Theorem 4.5 (Gyarmati) *Let $\mathcal{A} \subset \{N, N+1, N+2, \ldots, M\}$ be a set of positive integers, such that $N < M < \sqrt{3}N$. Then the set*

$$\{(a, a') : \ a, a' \in \mathcal{A},\ a > a',\ aa' + 1 \ \textit{is a square}\}$$

has at most $\frac{1}{2}|\mathcal{A}|^{3/2} + \frac{1}{4}|\mathcal{A}|$ elements.

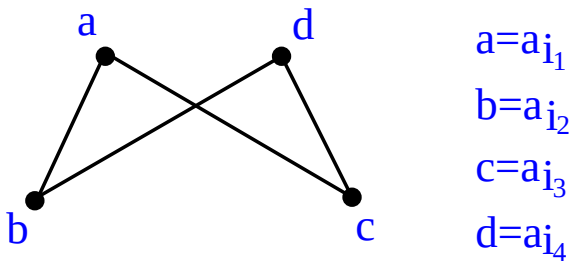
Proof of Theorem 4.5. The graph $\mathcal{G}$ is defined in the same way as in Theorem 4.3. The set of vertices is simply denoted by $V = \{a_1, a_2, \cdots, a_n\}$, where a_i's are the elements of the set $\mathcal{A}$. There is an edge between a_i and a_j if and only if $a_i a_j + 1$ is a square.

(Usually, the set of vertices in a graph is denoted by V, while the set of edges is denoted by E.)

We will prove the following.

Lemma 4.6 *The graph $\mathcal{G}$ does not contain 4-cycles.*

Proof of Lemma 4.6 Assume that the graph contains a 4-cycle. The smallest element of this 4-cycle is denoted by $a = a_{i_1}$. In this 4-cycle, the vertex a has two neighbors, the smaller one will be denoted by $b = a_{i_2}$ and the larger one by $c = a_{i_3}$. The final element of the 4-cycle is $d = a_{i_4}$.



We know $a < d$ (since a was the smallest element) and $b < c$ (since b was smaller among a's neighbors). Then:

$$(ac + 1)(bd + 1) < (ab + 1)(cd + 1), \tag{4.1}$$

since, breaking apart the parentheses, we get that

$$abcd + ac + bd + 1 < abcd + ab + cd + 1.$$

Therefore, by equivalent transformations:

$$\begin{aligned} ac + bd &< ab + cd \\ 0 &< ab + cd - ac - bd \\ 0 &< (d - a)(c - b), \end{aligned}$$

where the last statement is true because of $a < d$ and $b < c$. By (4.1):

$$\sqrt{(ac + 1)(bd + 1)} < \sqrt{(ab + 1)(cd + 1)},$$

but $\sqrt{ac+1}, \sqrt{bd+1}, \sqrt{ab+1}$ and $\sqrt{cd+1}$ are integers, since there is an edge between the vertices a_i and a_j if $a_i a_j + 1$ is a square.

That is $\sqrt{(ac+1)(bd+1)}$ and $\sqrt{(ab+1)(cd+1)}$ are integers, and the former is smaller than the latter, so

$$\sqrt{(ac+1)(bd+1)} + 1 \leq \sqrt{(ab+1)(cd+1)}.$$

By squaring:

$$(ac+1)(bd+1) + 2\sqrt{(ac+1)(bd+1)} + 1 \leq (ab+1)(cd+1)$$
$$abcd + ac + bd + 1 + 2\sqrt{(ac+1)(bd+1)} + 1 \leq abcd + ab + cd + 1$$
$$ac + bd + 1 + 2\sqrt{abcd} < ab + cd.$$

According to the inequality between the arithmetic and geometric means $ac + bd \geq 2\sqrt{abcd} \geq 2ab$. Thus

$$2ab + 2\sqrt{abcd} < ab + cd$$
$$4ab < ab + cd$$
$$3ab < cd.$$

Yes, but it holds for the elements of the set $\mathcal{A} \subset \{N, N+1, \ldots, M\}$ that $N \leq a, b$ and $c, d \leq M < \sqrt{3}N$. Thus

$$3N^2 \leq 3ab < cd < 3N^2,$$

which is contradiction. Thus we proved the lemma.

This proof is also available in [5], with a few minor changes that clarify that it also works for k-th powers.

Next we use the following lemma.

Lemma 4.7 (Reiman [7]) *If $G = (V, E)$ is a graph on n vertices, which has no 4-cycles, then*

$$|E| \leq \frac{n}{4}\left(1 + \sqrt{4n - 3}\right).$$

Since the graph $\mathcal{G}$ does not contain C_4 by Lemma 4.6, it has no more edges than

$$\frac{|\mathcal{A}|}{4}\left(1 + \sqrt{4\,|\mathcal{A}| - 3}\right) < \frac{|\mathcal{A}|^{3/2}}{2} + \frac{|\mathcal{A}|}{4}.$$

This completes the proof of Theorem 4.5.

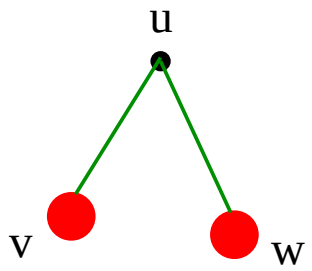
For the sake of completeness, we also present the proof of Lemma 4.7.

Proof of Lemma 4.7 Let $G = (V, E)$ be a C_4-free graph with vertex-set $V = v_1, \ldots, v_n$ and the degrees of its vertices are $d_1, d_2, \ldots, d_n$.

The set S is made up of all (ordered) pairings $(u, \{v, w\})$ where u, v, w are vertices of G, $v \neq w$ and u is adjacent to both v and w in G.

We now count the number of elements in S in two methods.

That is, we count all occurrences of "cherries" in G in two ways.



For each vertex u, we have $\binom{d}{2}$ options for selecting a 2-element subset of its d neighbors. Hence, when we sum over u, we get

$$S = \sum_{i=1}^{n} \binom{d_i}{2}.$$

Since G does not contain C_4, it follows that no pair of vertices v, w can have more than one common neighbor. As a result, when we sum up all the pairs, we get

$$|S| \leq \binom{n}{2}.$$

That is

$$\sum_{i=1}^{n} \binom{d_i}{2} \leq \binom{n}{2},$$

or equivalently

$$\sum_{i=1}^{n} d_i^2 - \sum_{i=1}^{n} d_i \leq n(n-1).$$

Here $\sum_{i=1}^{n} d_i = 2\,|E|$, thus

$$\sum_{i=1}^{n} d_i^2 - 2\,|E| \leq n(n-1). \tag{4.2}$$

According to the arithmetic and quadratic means inequality:

$$\sum_{i=1}^{n} d_i^2 \geq n \left(\frac{\sum_{i=1}^{n} d_i}{n} \right)^2 = \frac{4\,|E|^2}{n}.$$

Writing this into (4.2) we get

$$\frac{4\,|E|^2}{n} - 2\,|E| \leq n(n-1)$$

$$|E|^2 - \frac{n}{2}\,|E| - \frac{n^2(n-1)}{2} \leq 0.$$

The required upper bound on E is obtained by solving the related quadratic equation.

References

[1] M. Aigner, G. M. Ziegler, *Proofs from THE BOOK* (6th ed.) (2018), Springer-Verlag, pp. 285–289,

[2] Y. Bugeaud, K. Gyarmati, *On generalizations of a problem of Diophantus*, Illinois J. Math. 48 (2004), 1105-1115.

[3] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183–214.

[4] P. Gibbs, *Some Rational Diophantine Sixtuples*, arXiv:math/9902081.

[5] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97.1 (2001), 53-65.

[6] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. 371 (2019), 6665-6709.

[7] I. Reiman, *Über ein Problem von K. Zarankiewicz*, Acta Math. Acad. Sci. Hungar. 9 (1958), 269-273.

[8] P. Turán, *On an extremal problem in graph theory*, Matematikai és Fizikai Lapok 48 (1941), 436–452.

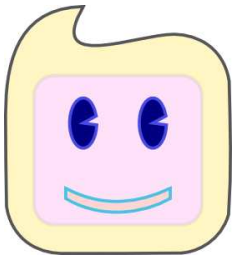
[9] Photo, Diophantus of Alexandria, Wikipedia, link.

5 Difference sets without sqaures

So far, we have mostly concentrated on sets in which $A - A$ or $A + A$, or even $A \cdot A + 1$ exclusively contains square values. Here $A - A$, $A + A$ and $A \cdot A + 1$ denote the following sets:

$$A - A = \{a - a' : \ a > a', \ a, a' \in \mathcal{A}\},$$
$$A + A = \{a + a' : \ a > a', \ a, a' \in \mathcal{A}\},$$
$$A \cdot A + 1 = \{aa' + 1 : \ a > a', \ a, a' \in \mathcal{A}\}.$$

We have an interesting question when we invert our reasoning and ask what estimates can be made for $|A|$ if e.g., $A - A$ never contains a square number.



In such a circumstance, we would expect to be given a very large set A with the aforementioned property, but this is not the case.

On the other hand, Imre Ruzsa [3] gave a tricky construction with this feature and a reasonably large number of elements, disproving the preceding conjectures. His result is described below; he studied the issue more generally for k-th powers, but we only study the case of square numbers.

But first let's see what happened in chronological order:

Lovász proposed and Sárközy [4] showed that if S is any sequence of natural numbers with positive asymptotic density, then $S - S$ must contain a square.

Let $D(x)$ indicate the maximum number of integers that may be chosen from $[1, x]$ with no difference being a square. Sárközy even proved that

$$D(x) = O(x(\log x)^{-1/3}).$$

We do not offer the proof since it uses the Hardy-Littlewood circle method, which goes beyond the scope of this note.

The following is the first natural construction for a set S in which $S - S$ does not contain a square. Fix a prime p for which $\frac{\sqrt{x}}{2} \le p \le \sqrt{x}$. Let

$$S = \{p, 2p, 3p, \dots, p^2\}.$$

Then

$$S - S = \{p, 2p, 3p, \dots, p^2 - p\}.$$

That is, $p \mid m$, but $p^2 \nmid m$ for every $m \in S - S$, i.e., m cannot be a square.

This construction shows that $D(x) \ge \frac{\sqrt{x}}{2}$.

Erdős proposed the conjecture that

$$D(x) = O(x^{1/2}(\log x)^k)$$

holds with some constant k.

Sárközy [5] disproved this but still conjectured

$$D(x) = O(x^{1/2+\varepsilon}).$$

Ruzsa disproved this conjecture, confirming the following.

Theorem 5.1 *$D(x) > \frac{1}{65}x^\gamma$, where*

$$\gamma = \frac{1}{2}\left(1 + \frac{\log 7}{\log 65}\right) = 0.733077\dots .$$

Actually, he proved a little more than that, namely let $r(m)$ denote the maximal number of residues (mod m) that can be selected so that no difference between them is a square modulo m. Then:

Theorem 5.2 *For every squarefree m we have*

$$D(x) \geq \frac{1}{m} x^{\gamma(m)},$$

where

$$\gamma(m) = \frac{1}{2} + \frac{\log r(m)}{2 \log m}.$$

First we prove Theorem 5.2.

Proof of Theorem 5.2. Let $R \subseteq [1, m]$ be a set of integers with no difference that is a square modulo m and $|R| = r(m)$.

Let S be a set of natural numbers of the form

$$s = \sum_{j=0}^{n-1} r_j m^j + 1,$$

where $r_j \in R$ if j is even, and $0 \leq r_j < m$ is arbitrary otherwise. Clearly

$$\begin{aligned} S(m^n) &\stackrel{\text{def}}{=} |S \cap \{1, 2, 3, \ldots, m^n\}| \\ &= r(m)^{1+[(n-1)/2]} m^{(n-1)-[(n-1)/2]}. \end{aligned}$$

Let $m^n \leq x < m^{n+1}$. A simple calculation shows:

$$\begin{aligned} S(x) &\geq S(m^n) \\ &= r(m)^{1+[(n-1)/2]} m^{(n-1)-[(n-1)/2]} \\ &= m^{(1+[(n-1)/2])\frac{\log r(m)}{\log m} + n - 1 - [(n-1)/2]} \\ &= m^{\frac{\log r(m)}{\log m} + n - 1 + [(n-1)/2]\left(\frac{\log r(m)}{\log m} - 1\right)} \\ &\geq m^{\frac{\log r(m)}{\log m} + n - 1 + \frac{n-1}{2}\left(\frac{\log r(m)}{\log m} - 1\right)} \end{aligned}$$

$$
\begin{aligned}
&= m^{\frac{\log r(m)}{\log m}+\frac{n-1}{2}+\frac{n-1}{2}\frac{\log r(m)}{\log m}} \\
&= \frac{1}{m} m^{\frac{n+1}{2}+\frac{n+1}{2}\frac{\log r(m)}{\log m}} \\
&\geq \frac{1}{m} x^{\frac{1}{2}+\frac{\log r(m)}{2\log m}} \\
&= \frac{1}{m} x^{\gamma(m)}.
\end{aligned}
$$

Next we prove $S - S$ does not contain a square. Suppose that $s - s' = t^2$ where $s, s' \in S$. Write

$$
s = \sum_{j=0}^{n-1} r_j m^j + 1, \quad s' = \sum_{j=0}^{n-1} r'_j m^j + 1.
$$

Let k denote the first suffix for which $r_k \neq r'_k$. Now we have

$$
t^2 = s - s' = (r_k - r'_k) m^k + z m^{k+1}.
$$

If k is odd then $m^k \mid t^2$, but $m^{k+1} \nmid t^2$ which is impossible for squarefree m. If k is even then $k = 2\ell$ and

$$
\left(t/m^{\ell}\right)^2 \equiv r_k - r'_k \pmod{m} \quad \text{with } r_k,\ r'_k \in R,
$$

in contrary with the definition of R. This completes the proof.

Theorem 5.1 can be easily derived from Theorem 5.2.

To prove Theorem 5.1 we show that

$$
r(65) \geq 7.
$$

Consider the numbers

$$
(0,0),\ (0,2),\ (1,8),\ (2,1),\ (2,3),\ (3,9),\ (4,7),
$$

where the first component is the residue modulo 5 and the second modulo 13. All of the differences derived from this set are quadratic non-residue mod 3 or mod 5, proving the statement.

Following that, we describe how much these results have improved in a few sentences.

Pintz, Steiger, and Szemerédi [6] refined Sárközy's argument, by proving the upper bound on $D(x) \leq \frac{x}{(\log x)^{c \log\log\log\log x}}$.

Bloom and Maynard [1] improved on this, namely

$$D(x) \leq \frac{x}{(\log x)^{c \log\log\log x}}.$$

Lewko [2] improved Ruzsa's lower bound to

$$D(x) \gg x^{\delta},$$

where $\delta = \frac{1}{2} + \frac{\log 12}{\log 205} = 0.733412\cdots$.

References

[1] T. F. Bloom, J. Maynard, *A new upper bound for sets with no square differences*, Compos. Math. 158 (2022), no. 8, 1777–1798.

[2] M. Lewko, *An improved lower bound related to the Furstenberg-SárkÖzy theorem*, Electron. J. Combin. 22 (2015), no. 1, Paper 1.32, 6 pp.

[3] I. Ruzsa, *Difference sets without squares*, Periodica Mathematica Hungarica 15 (1984), 205–209.

[4] A. Sárközy, *On difference sets of sequences of integers, I*, Acta Math. Acad. Sci. Hungar. 31 (1978), 125-149.

[5] A. Sárközy, *On difference sets of sequences of integers, II*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 21 (1978), 45-53.

[6] J. Pintz, W. L. Steiger, E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. Lond. Math. Soc. (2)37(1988), 219–231.

[7] Photo, Smiley square face, link.

6 Sidon Sequences

Simon Sidon posed a question to fellow student Erdős in 1932. Their advisor was Fejér, a creative mathematician, who was working on the summability of infinite series.

Sidon formulated his question when analyzing the L_p norm of certain Fourier series. This problem is described in modern terminology below.

In number theory, a Sidon sequence (or Sidon set) is a sequence $\mathcal{A} = \{a_0, a_1, a_2, ...\}$ of natural numbers in which all pairwise sums $a_i + a_j \; for i \leq j$ are different.

Excercise Provide examples of constructions of Sidon sequences.

For example, powers of 2.

Definition 6.1 *Denote by $S(N)$ the maximum number of elements of a Sidon sequence which is a subset of $\{1, 2, 3, \ldots, N\}$:*

$$S(N) = \max_{\substack{\mathcal{A} \subseteq \{1,2,\ldots,N\} \\ \mathcal{A} \text{ is Sidon}}} |\mathcal{A}| \tag{6.1}$$

Erdős immediately observed that the greedy algorithm gives $S(N) > (2N)^{1/3}$. This result will be discussed shortly, but first some upper estimates will be given.

The simplest upper estimate is the following.

Theorem 6.2

$$S(N) \leq 2\sqrt{N}.$$

Proof of Theorem 6.2. Consider a Sidon sequence

$$\mathcal{A} = \{a_1, a_2, \ldots, a_S\} \subseteq \{1, 2, \ldots, N\}.$$

We will prove

$$S = |\mathcal{A}| \leq 2\sqrt{N}.$$

Consider the number line and the integers $1, 2, \ldots, 2N$ on it.

Put an X on the integers which can be written on the form $a+a'$, where $a, a' \in \mathcal{A}$. Here the number of X's is

$$\begin{array}{c} \binom{S}{2} + S \longleftarrow a_i = a_j, \\ \uparrow \\ (a_i, a_j) \quad a_i \neq a_j. \end{array}$$

All sums are different and for each sum

$$2 \leq a + a' \leq 2N.$$

Thus

$$\begin{aligned} \binom{S}{2} + S &\leq 2N, \\ \frac{S(S+1)}{2} &\leq 2N, \\ S^2 < S(S+1) &\leq 4N, \\ S &< 2\sqrt{N}, \end{aligned}$$

which proves the theorem.

This estimate can be slightly improved if in place of sums we consider differences.

$$a_0 + a_0{}' = a_1 + a_1{}'$$

$$\Updownarrow$$

$$a_0 - a_1 = a_1' - a_0'$$

Thus $\mathcal{A}$ is a Sidon sequence if all (non-zero) differences $a - a'$, $a, a' \in \mathcal{A}$, $a \neq a'$ are different.

Consider again the number line and the integers $1, 2, \ldots, N-1$ on it.

Put an X on the integers which can be written on the form $a - a'$ where $a, a' \in \mathcal{A}$, and $a - a'$ is positive.

Here the number of X's is $\binom{S}{2}$.

Every difference $a - a'$ is different and

$$1 \leq a - a' \leq N - 1,$$

thus

$$\begin{aligned}
\binom{S}{2} &\leq N - 1, \\
S(S-1) &\leq 2N - 2, \\
S^2 - S + \frac{1}{4} &\leq 2N - \frac{7}{4}, \\
\left(S - \frac{1}{2}\right)^2 &\leq 2N - \frac{7}{4}, \\
S - \frac{1}{2} &\leq \sqrt{2N - \frac{7}{4}} < \sqrt{2}\sqrt{N}, \\
S &< \sqrt{2} \cdot \sqrt{N} + \frac{1}{2}.
\end{aligned}$$

Using even cleverer ideas we can get rid of the factor $\sqrt{2}$. Erdős and Turán [5] provided the following tricky proof.

Theorem 6.3

$$S(N) < \sqrt{N} + \sqrt[4]{N} + 1.$$

The terminology used in the following proof was taken from Erdős, Surányi's book, Topics in the Theory of Numbers [4].

Proof of Theorem 6.3.

We will fix the value t later.

We divide $[0, N]$ into intervals. More exactly consider the following $N + t$ intervals:

$$[-t + 1, 0], [-t + 2, 1], \ldots, [N, N + t - 1].$$

Let $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ a Sidon sequence, and from $\mathcal{A}$

$$A_1, \quad A_2, \quad \ldots \quad A_{N+t}$$

pieces of elements fall in these intervals.

Each element of $\mathcal{A}$ falls into t consecutive intervals, thus

$$\sum_{i=1}^{N+t} A_i = ts.$$

Now, count how many times the pair (a_i, a_j) (for $i > j$) falls within the above-mentioned intervals.

Let the total number of these be D.

Then, on the one hand, it is clear that

$$D = \sum_{i=1}^{n+t} \binom{A_i}{2} = \frac{1}{2} \sum_{i=1}^{n+t} A_i^2 - \frac{1}{2} \sum_{i=1}^{n+t} A_i.$$

On the other hand, if the difference of a pair of elements is d, then this pair falls within $t - d$ intervals.

Since all the differences are distinct, then each d can occur at most once. Therefore,

$$D \le \sum_{d=1}^{t-1}(t-d) = \frac{t(t-1)}{2}.$$

Comparing the above two relations for D, we have

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \le t(t-1).$$

We saw that the second sum on the left-hand side equals ts.

Now we apply the inequality for arithmetic and quadratic means to the first sum on the left-hand side:

$$\sum_{i=1}^{n+t} A_i^2 \ge \frac{\left(\sum_{i=1}^{n+t} A_i\right)^2}{n+t} = \frac{t^2 s^2}{n+t}.$$

Writing these into the above inequality, reducing it to zero, and multiplying both sides by $(n+t)/t^2$ we get that

$$s^2 - s\left(\frac{n}{t}+1\right) - \left(\frac{n}{t}+1\right)(t-1) \le 0.$$

For the values of s satisfying this second-degree inequality we have

$$\begin{aligned} s &\le \frac{n}{2t} + \frac{1}{2} + \sqrt{n+t+\frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4}} \\ &= \frac{n}{2t} + \frac{1}{2} + \sqrt{n+t+\left(\frac{n}{2t}-\frac{1}{2}\right)^2 - 1}. \end{aligned}$$

Now, if we choose $t = \left[\sqrt[4]{n^3}\right] + 1$, then the first term on the right-hand side is less than $\frac{1}{2}\sqrt[4]{n}$, while the last term is less than the square of $\sqrt{n} + \frac{1}{2}\sqrt[4]{n} + \frac{1}{2}$.

This yields the desired inequality.

Balogh, Füredi, and Roy [2] improved the obtained result slightly, however only the error term is improved by 0.2%:

$$S(N) \leq \sqrt{N} + 0.998N^{1/4}.$$

Next we give lower bounds on $S(N)$.

At first, we will discuss Erdős' observation regarding the greedy algorithm.

Theorem 6.4 *For every N, there is a Sidon set $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ such that $|\mathcal{A}| \geq [(2N)^{1/3}]$.*

Proof of Theorem 6.4. Clearly it suffices to show that if

$$\{a_1, a_2, \ldots, a_t\} \subseteq \{1, 2, \ldots, N\}$$

is a Sidon set of cardinality t and $t \leq (2N)^{1/3} - 1$, then there is an integer b such that

$$1 \leq b \leq N \quad \text{and} \quad b \notin \{a_1, a_2, \ldots, a_t\} \tag{6.2}$$

and

$$\{a_1, a_2, \ldots, a_t\} \cup \{b\}$$

is a Sidon set. A number b is called "bad" if $\{a_1, a_2, \ldots, a_t\} \cup \{b\}$ is not a Sidon set, and it is called "good" if $\{a_1, a_2, \ldots, a_t\} \cup \{b\}$ is Sidon set.

Thus in order to complete the proof it is sufficient to prove that if $t \leq (2N)^{1/3} - 1$ then there exists a good b for which (6.2) holds.

First we count the number of bad b's. Since $\{a_1, a_2, \ldots, a_t\}$ is a Sidon set, if b is bad (so $\{a_1, a_2, \ldots, a_t\} \cup \{b\}$ is not a Sidon set) then there are a_i, a_j, a_k with

$$a_i + a_j = a_k + b \tag{6.3}$$

or there are a_u, a_v with

$$a_u + a_v = b + b. \tag{6.4}$$

The number of bad b's for which (6.3) holds is

$$\leq \left(\binom{t}{2} + t\right)(t-1) = \frac{t(t^2-1)}{2}.$$

The number of bad b's for which (6.4) holds is

$$\leq \binom{t}{2} = \frac{t(t-1)}{2}.$$

Thus the number of "bad" b's is $\leq \frac{t(t^2-1)}{2} + \frac{t(t-1)}{2} = \frac{t(t-1)(t+3)}{2}$. Finally the number of b's for which $b \in \{a_1, a_2, \ldots, a_t\}$ is t If

$$\frac{t(t-1)(t+3)}{2} + t < N,$$

then there is a good b with (6.2). For $t \leq (2N)^{1/3} - 1$, this clearly holds since

$$\frac{t(t-1)(t+1)}{2} + t < \frac{(t+1)^3}{2} < N,$$

and this completes the proof.

Next we show two tricky constructions for Sidon sets.

To begin, we will discuss a slightly modified version of Erdős and Turán's [5] construction.

Theorem 6.5 *There is a Sidon set $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ with*

$$|\mathcal{A}| \geq \frac{\sqrt{N}}{4}.$$

Proof of Theorem 6.5. We may suppose that $N \geq 16$.

According to Chebyshev's theorem, for every $n \geq 2$ there exists a prime number between n and $2n$. (You can read more about this theorem on the related Wikipedia page: link. Pál Erdős also gave an elementary proof of the theorem, see e.g. here link.)

By Chebyshev's theorem for every integer $n \geq 2$, there is a prime between n and $2n$. Using Chebyshev's theorem we get there is a prime p for which

$$\frac{\sqrt{N}}{2} < p < \sqrt{N}.$$

Since $N \geq 16$, this prime is odd. Denote by $r_p(x)$ the least non-negative residue of x modulo p, so

$$x \equiv r_p(x) \pmod{p} \quad \text{and } 0 \leq r_p(x) \leq p-1.$$

Define the set $\mathcal{A}$ by

$$\mathcal{A} \stackrel{\text{def}}{=} \{a : \ a = x + pr_p(x^2),\ 0 \leq x \leq \frac{p-1}{2}\}.$$

We will prove this set is a Sidon set.

Clearly, $\mathcal{A}$ contains $\frac{p+1}{2}$ elements, since for diferrent x's the elements $x + pr_p(x^2)$'s have different residues modulo p.

Next we prove $\mathcal{A}$ is Sidon set. Suppose that

$$a_1 + a_2 = b_1 + b_2, \tag{6.5}$$

where $a_1, a_2, b_1, b_2 \in \mathcal{A}$. Then there are $0 \leq x_1, x_2, y_1, y_2 \leq \frac{p-1}{2}$ such that

$$\begin{aligned} a_1 &= x_1 + pr_p(x_1^2) \\ a_2 &= x_2 + pr_p(x_2^2) \\ b_1 &= y_1 + pr_p(y_1^2) \\ b_2 &= y_2 + pr_p(y_2^2). \end{aligned}$$

By (6.5) we have

$$x_1 + x_2 + p\left(r_p(x_1^2) + r_p(x_2^2)\right) = y_1 + y_2 + p\left(r_p(y_1^2) + r_p(y_2^2)\right). \tag{6.6}$$

Then

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{p}.$$

Since $0 \leq x_1 + x_2, y_1 + y_2 \leq p - 1$ we have

$$x_1 + x_2 = y_1 + y_2. \tag{6.7}$$

By this and (6.6) we get

$$\begin{aligned} r_p(x_1^2) + r_p(x_2^2) &= r_p(y_1^2) + r_p(y_2^2) \\ x_1^2 + x_2^2 &\equiv y_1^2 + y_2^2 \pmod{p}. \end{aligned} \tag{6.8}$$

By considering the difference of the square of (6.7) and (6.8) we get

$$\begin{aligned} 2x_1x_2 &\equiv 2y_1y_2 \pmod{p} \\ x_1x_2 &\equiv y_1y_2 \pmod{p} \end{aligned} \tag{6.9}$$

By the relationship between roots and coefficients, from (6.7) and (6.9) we get x_1, x_2 and y_1, y_2 are the roots of the same quadratic congruence.

By Lagrange's degree theorem, the quadratic congruence has at most 2 roots, thus

$$\{x_1, x_2\} = \{y_1, y_2\}$$

and so

$$\{a_1, a_2\} = \{b_1, b_2\}.$$

Thus $\mathcal{A}$ is a Sidon set with $|\mathcal{A}| \geq \frac{\sqrt{N}}{4}$, and this completes the proof.

The following tricky construction comes from Ruzsa [3], who managed to eliminate the factor 1/4 in this manner.

Theorem 6.6 *Let p be an odd prime. There exist $p-1$ numbers a_i for which the differences $a_i - a_j$ $(i \neq j)$ are incongruent modulo $p^2 - p$.*

Proof of Theorem 6.6. Let g be a primitve root, modulo p, and let the a_i's be the unique solution modulo $p^2 - p$, to the simultaneous congruences

$$\begin{aligned} x &\equiv i \pmod{p-1}, \\ x &\equiv g^i \pmod{p}. \end{aligned}$$

(By the Chinese remainder theorem, such a solution exists and is unique.) We need to show that the congruence

$$a_i - a_j \equiv a_r - a_s \pmod{p^2 - p},$$

or written in the equivalent form

$$a_i + a_s \equiv a_r + a_j \pmod{p^2 - p},$$

is satisfied only by the trivial solutions. In other words, this means that for any number c there is at most one pair of numbers i, j that

satisfies the congruence

$$c \equiv a_i + a_j \pmod{p^2 - p}.$$

Based on the definition of the a_i's, this is equivalent to the congruences

$$c \equiv i + j \pmod{p-1},$$
$$c \equiv g^i + g^j \pmod{p}.$$

being simultaneously satisfied. The first congruence we may rewrite as

$$g^c \equiv g^i g^j \pmod{p}.$$

The relationship between the roots of a quadratic equation and its coefficients implies that the residue classes $(g^i)_p$ and $(g^j)_p$ are uniquely defined as the two roots of the second-degree congruence

$$x^2 - cx + g^c \equiv 0 \pmod{p}.$$

Since the modulus is prime, the pair of roots is uniquely determined, and thus the pair i, j is uniquely defined.

The sequence of a_i's constructed above forms a Sidon set in $\mathbb{Z}_{p^2-p}$. This completes the proof of the theorem.

By assigning a congruent natural number to each residue class mod $p^2 - p$, we may get a Sidon set in $\{1, 2, ..., p^2 - p\}$.

Thus if N of the form $p^2 - p$, we see that

$$S(N) \geq p - 1 = \frac{1}{2}(\sqrt{4N+1} + 1) - 1 > \sqrt{N} - 1.$$

For arbitrary N, we choose a prime such that $p^2 - p$ is close to N.

There is a famous conjecture that for every positive δ there is a prime between n and $n + n^{\delta}$ (if n is large enough depending on δ), but the proof of this looks to be without hope.

However, the conjecture was verified for some positive δ.

Note that the value of proved δ is constantly being improved. Currently, the sharpest estimate comes from Baker, Harman and Pintz [1], namely $\delta = 0.525$.

Thus we can choose a prime p between $\sqrt{N} - N^{0.2625}$ and $\sqrt{N}$, and hence

$$S(N) \geq S(p^2 - p) \geq p - 1 \geq \sqrt{N} - O(N^{0.2625}).$$

Erdős proposed numerous conjectures concerning the Sidon sequences, of which you can read more about here: link. Unfortunately, today (to the best of my knowledge) there is no monetary reward for solving these problems...

References

[1] R. C. Baker, G. Harman, J. Pintz, *The difference between consecutive primes, II*, Proceedings of the London Mathematical Society. 83 (3) (2001), 532–562.

[2] J. Balogh, Z. Füredi, S. Roy, *An Upper Bound on the Size of Sidon Sets*, The American Mathematical Monthly, DOI: 10.1080/00029890.2023.2176667.

[3] I. Z. Ruzsa, *Solving a linear equation in a set of integers. I*, Acta Arith.65 (1993), 259–282.

[4] P. Erdős, J. Surányi, *Topics in the Theory of Numbers*, 2003rd Edition, Springer, Undergraduate Texts in Mathematics.

[5] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory and related problems*, Journ. London Math. Soc.16 (1941), 212—215.

7 Cauchy-Davenport theorem

A basic problem in group theory is to obtain a lower bound for $|\mathcal{A}+\mathcal{B}|$ in terms of $|\mathcal{A}|$ and $|\mathcal{B}|$. In the case of finite groups, the following simple theorem provides an obvious solution when $|\mathcal{A}|+|\mathcal{B}|$ is sufficiently large.

Theorem 7.1 *If $\mathcal{G}$ is a finite abelian group, and $\mathcal{A}, \mathcal{B}$ are nonempty subsets of $\mathcal{G}$ such that*

$$|\mathcal{A}|+|\mathcal{B}|>|\mathcal{G}|,$$

then

$$\mathcal{A}+\mathcal{B}=\mathcal{G}.$$

Proof of Theorem 7.1. Let $g \in \mathcal{G}$ be arbitrary. We will prove g can be written of the form $g=a+b$ where $a \in \mathcal{A}$, $b \in \mathcal{B}$. In order to prove this consider the set

$$g-\mathcal{B}=\{g-b : b \in \mathcal{B}\}.$$

Then $|g-\mathcal{B}|=|\mathcal{B}|$, so

$$|\mathcal{A}|+|g-\mathcal{B}|>|\mathcal{G}|,$$

which implies $\mathcal{A} \cap (g-\mathcal{B}) \neq \emptyset$. Therefore there exists $a \in \mathcal{A}$ and $b \in \mathcal{B}$ such that $a=g-b \Longrightarrow g=a+b$.

The first theorem in additive group theory is the famous Cauchy-Davenport theorem, which will be the subject of this chapter.

Cauchy [1] established the theorem in 1813, and Davenport [3] rediscovered it in 1935. (also see [4]).

This theorem provides a lower bound for $|\mathcal{A}+\mathcal{B}|$ in terms of $|\mathcal{A}|$ and $|\mathcal{B}|$ when $\mathcal{A}$ and $\mathcal{B}$ are nonempty subsets of $\mathbb{Z}_p$ for a prime p.

Theorem 7.2 (Cauchy–Davenport) *Let p be a prime number $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$ be nonempty sets. Then*

$$|\mathcal{A}+\mathcal{B}| \geq \min\{p, |\mathcal{A}|+|\mathcal{B}|-1\}.$$

Proof of Theorem 7.2. First, we prove the following lemma:

Lemma 7.3 *Let $\mathcal{A} \subseteq \mathbb{Z}_p$, $d \in \mathbb{Z}_p$, $d \neq 0$. If*

$$\mathcal{A}+d \subseteq \mathcal{A},$$

then

$$\mathcal{A} = \mathbb{Z}_p.$$

Proof of Lemma 7.3. If $\mathcal{A}+d \subseteq \mathcal{A}$, then for $a \in \mathcal{A} \Longrightarrow a+d \in \mathcal{A}$. By repeating this argument we get

$$a, a+d, a+2d, \ldots, a+(p-1)d \in \mathcal{A}. \tag{7.1}$$

Here $a, a+d, a+2d, \ldots, a+(p-1)d$ is a complete residue system modulo p, since this set contains p elements and every two are incongruent modulo p. Indeed, if

$$a+id \equiv a+jd \pmod{p}$$

for $0 \le i, j \le p-1$, then

$$\begin{aligned} id &\equiv jd \pmod{p} \quad / : d \\ i &\equiv j \pmod{p} \\ i &= j. \end{aligned}$$

Thus by (7.1) we have

$$\mathbb{Z}_p \subseteq \mathcal{A}.$$

Since $\mathcal{A} \subseteq \mathbb{Z}_p$ also holds, we get

$$\mathcal{A} = \mathbb{Z}_p.$$

Lemma 7.4 *Let $\mathcal{A} \subseteq \mathbb{Z}_p$, $x, y \in \mathbb{Z}_p$, $x \neq y$. Then if*

$$\mathcal{A} + x \subseteq \mathcal{A} + y,$$

then

$$\mathcal{A} = \mathbb{Z}_p.$$

Proof of Lemma 7.4. If $\mathcal{A} + x \subseteq \mathcal{A} + y$, then

$$\mathcal{A} + (x - y) \subseteq \mathcal{A}.$$

Write $x - y = d$, then

$$\mathcal{A} + d \subseteq \mathcal{A}.$$

Using Lemma 7.3 we get $\mathcal{A} = \mathbb{Z}_p$.

Exercise

Prove the Cauchy–Davenport theorem for $|\mathcal{B}| = 1$ and $|\mathcal{B}| = 2$.

Solution

Let

$$\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\},$$
$$\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\}$$

If $n = 1$, then

$$|\mathcal{A} + \mathcal{B}| = |\mathcal{A} + \beta_1| = |\mathcal{A}| = m$$
$$= m + 1 - 1 = m + n - 1.$$

Thus for $n = 1$ we have proved the Cauchy-Davenport theorem.

Next we study the case $n = 2$. Let $\mathcal{B} = \{\beta_1, \beta_2\}$ and denote their difference by d, so $d = \beta_2 - \beta_1$.

$$\beta_1 \not\equiv \beta_2 \pmod{p} \implies (d, p) = 1.$$

Next we distinguish two cases.

Case I: $\mathcal{A} + d \subseteq \mathcal{A}$.

By Lemma 7.3 then $\mathcal{A} = \mathbb{Z}_p$, so $\mathcal{A} + \mathcal{B} = \mathbb{Z}_p$, thus

$$|\mathcal{A} + \mathcal{B}| = |Z_p| = p \geq \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\},$$

which means that in Case I the theorem holds.

Case II: $\mathcal{A} + d \not\subseteq \mathcal{A}$.

Then $\exists\ \alpha \in \mathcal{A}$ such that $\alpha + d \notin \mathcal{A}$.
We may suppose that $\alpha = \alpha_1$. So

$$\alpha_1 + d \notin \mathcal{A},$$
$$\alpha_1 + \beta_2 - \beta_1 \notin \mathcal{A},$$
$$\alpha_1 + \beta_2 - \beta_1 \neq \alpha_i \text{ for } 1 \leq i \leq m,$$

$$\alpha_1 + \beta_2 \neq \alpha_i + \beta_1 \text{ for } 1 \leq i \leq m,$$

Then:

$$\{\alpha_1 + \beta_2\} \cap \{\alpha_i + \beta_1,\ 1 \leq i \leq m\} = \emptyset,$$
$$|\mathcal{A} + \mathcal{B}| \geq 1 + m = m + 2 - 1 = m + n - 1.$$

Thus we have proved the Cauchy-Davenport theorem for $n = 1$ and $n = 2$.

When $|\mathcal{A}| = p$ or $|\mathcal{B}| = p$ (so $\mathcal{A} = \mathbb{Z}_p$ or $\mathcal{B} = \mathbb{Z}_p$) the theorem is trivial.

Next we prove the Cauchy-Davenport theorem by induction on n.

For $n = 1$ and $n = 2$ we have seen the proof.

By the induction, we may suppose that we proved the theorem for every $\mathcal{A}'$ and $\mathcal{B}'$ with

$$1 \leq |\mathcal{B}'| < n,$$

and we would like to prove it for a pair $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$ with $|\mathcal{B}| = n < p$ and $|\mathcal{A}| < p$. (This is the induction step.)

First, consider the following special case.

Case I: When $\mathcal{A} \cap \mathcal{B}$ is a nonempty, proper subset of $\mathcal{B}$.

Let

$$\mathcal{A}' \stackrel{\text{def}}{=} \mathcal{A} \cup \mathcal{B},$$
$$\mathcal{B}' \stackrel{\text{def}}{=} \mathcal{A} \cap \mathcal{B}.$$

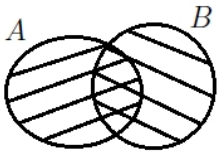
In this case $\mathcal{B}'$ is a nonempty proper subset of $\mathcal{B}$, so

$$1 \leq |\mathcal{B}'| < |\mathcal{B}| = n.$$

By the induction hypothesis:

$$|\mathcal{A}' + \mathcal{B}'| \geq \min\{p, |\mathcal{A}'| + |\mathcal{B}'| - 1\}, \tag{7.2}$$

Clearly, for every pair of sets $\mathcal{A}$ and $\mathcal{B}$ we have



$$\begin{aligned} |\mathcal{A}| + |\mathcal{B}| &= |\mathcal{A} \cup \mathcal{B}| + |\mathcal{A} \cap \mathcal{B}| \\ &= |\mathcal{A}'| + |\mathcal{B}'|. \end{aligned}$$

On the other hand we will see that

$$\mathcal{A}' + \mathcal{B}' \subseteq \mathcal{A} + \mathcal{B}. \tag{7.3}$$

Indeed, suppose that $x \in \mathcal{A}' = \mathcal{A} \cup \mathcal{B}$ and $y \in \mathcal{B}' = \mathcal{A} \cap \mathcal{B}$. We will prove that $x + y \in \mathcal{A} + \mathcal{B}$.

If $x \in \mathcal{A}$ then by $y \in \mathcal{B}$ we get $x + y \in \mathcal{A} + \mathcal{B}$. If $x \in \mathcal{B}$ then by $y \in \mathcal{A}$ we get $x + y \in \mathcal{A} + \mathcal{B}$. Thus we proved (7.3).

By (7.2) and (7.3) we get

$$\begin{aligned} |\mathcal{A} + \mathcal{B}| &\geq |\mathcal{A}' + \mathcal{B}'| \geq \min\{p, |\mathcal{A}'| + |\mathcal{B}'| - 1\} \\ &= \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\}. \end{aligned}$$

This completes the proof of Cauchy-Davenport theorem in Case I.

The general case (when $\mathcal{A} \cap \mathcal{B}$ is not necessarily a nonempty, proper subset of $\mathcal{B}$) will be studied in the following section. Then we will use the following.

Lemma 7.5 *If $|\mathcal{A}| < p$, then exists a $c \in \mathbb{Z}_p$ such that $\mathcal{B} \cap (\mathcal{A} + c)$ is a nonempty proper subset of $\mathcal{B}$.*

Proof of Lemma 7.5. Let

$$\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\},$$
$$\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\}.$$

If c is of the form $\beta_i - \alpha_j$, then $\mathcal{B} \cap (\mathcal{A} + c) = \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j)$ is nonempty since

$$\beta_i \in \mathcal{B} \quad \text{and} \quad \beta_i = \alpha_j + \beta_i - \alpha_j \in \mathcal{A} + (\beta_i - \alpha_j).$$

First we fix two elements from $\mathcal{B}$: β_k and β_i where $\beta_k \neq \beta_i$. We may suppose that

$$\mathcal{A} + (\beta_k - \beta_i) \not\subseteq \mathcal{A},$$

since otherwise by the Lemma 7.3 we get $\mathcal{A} = \mathbb{Z}_p$, and then the theorem is trivial.

Let α_j such that $\alpha_j + (\beta_k - \beta_i) \notin \mathcal{A}$. Then

$$\beta_k \notin \mathcal{A} + \beta_i - \alpha_j,$$
$$\beta_k \notin \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j).$$

So $\mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j) \neq \mathcal{B}$ and it is nonempty $(\beta_i \in \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j))$, thus it is a proper subset of $\mathcal{B}$. This proves the lemma.

Now we will return to the proof of Cauchy-Davenport theorem. Fix an element $c \in \mathbb{Z}_p$ for which Lemma 7.5 holds. Using Case I for the sets $\mathcal{A} + c$ and $\mathcal{B}$ we get

$$\begin{aligned} |\mathcal{A} + \mathcal{B}| &= |(\mathcal{A} + c) + \mathcal{B}| \\ &\geq \min\{p, |\mathcal{A} + c| + |\mathcal{B}| - 1\} \end{aligned}$$

$$= \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\}.$$

Following that, we will look at certain generalizations of the Cauchy–Davenport theorem but without proofs.

The first result is due to Chowla [2] (see also [6], [7]) and generalizes the Cauchy-Davenport theorem to composite numbers.

Theorem 7.6 (Chowla) *Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_n$ be nonempty sets. If $0 \in \mathcal{B}$ and $(b, n) = 1$ for all $b \in \mathcal{B} \setminus \{0\}$, then*

$$|\mathcal{A} + \mathcal{B}| \geq \min\{n, |\mathcal{A}| + |\mathcal{B}| - 1\}.$$

Pillai [8] found an additional generalization of the Cauchy-Davenport theorem for $\mathbb{Z}_n$ with composite n.

Theorem 7.7 (Pillai) *Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_n$ be non-empty sets. Writing $\mathcal{B} = \{\beta_1, \ldots, \beta_m\}$ and*

$$d = \max_{i \neq j}(n, \beta_i - \beta_j)$$

we have

$$|\mathcal{A} + \mathcal{B}| \geq \min\left\{\frac{n}{d},\ |\mathcal{A}| + |\mathcal{B}| - 1\right\}.$$

Kneser's [5] theorem, which generalizes the Cauchy-Davenport theorem for infinite abelian groups, is now classical. Here we will need the concept of the stabilizer, which in the case of $\mathcal{C} \subseteq G$ (where G is an abelian group and $\mathcal{C}$ is an arbitrary subset of G) is given by the formula

$$\text{stab}(\mathcal{C}) = \{g \in \mathcal{G},\ g + \mathcal{C} = \mathcal{C}\}.$$

Theorem 7.8 (Kneser) *Let G be an additive abelian group (possibly infinite), $\mathcal{A}, \mathcal{B} \subseteq \mathcal{G}$ be finite and nonempty. Then writing*

$$H = \text{stab}(\mathcal{A} + \mathcal{B}) = \{g \in \mathcal{G},\ g + (\mathcal{A} + \mathcal{B}) = \mathcal{A} + \mathcal{B}\}$$

we have

$$|\mathcal{A} + \mathcal{B}| \geq |\mathcal{A} + H| + |\mathcal{B} + H| - |H|.$$

References

[1] A. L. Cauchy, *Recherches sur les nombres*, J. École Polytech. 9 (1813), 99–123.

[2] I. Chowla, *A theorem on the addition of residue classes: application to the number $\Gamma(k)$ in Waring's problem*, Proc. Indian Acad. Sci.,2 (1935), 242–243.

[3] H. Davenport, *On the addition of residue classes*, J. London Math. Soc.,10 (1935), 30–32.

[4] H. Davenport, *A historical note*, J. London Math. Soc. 22 (1947), 100–101.

[5] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z., 58 (1953), 459–484.

[6] H. B. Mann, *Addition Theorems in Group Theory and Number Theory*, R. E. Krieger Publishing Company, Huntington, New York, 1976.

[7] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[8] S. S. Pillai, *Generalization of a theorem of Davenport on the addition of residue classes*, Proc. Indian Acad. Sci. A, 6 (1937), 179–180.

[9] Photo, Augustin Louis Cauchy, Wikipedia, link.

[10] Photo, Harold Davenport, Wikimedia Commons, link.

8 The Combinatorial Nullstellensatz

This chapter will discuss Alon's Combinatorial Nullstellensatz [1] as well as an useful application that slightly extends the Cauchy-Davenport theorem.

Theorem 8.1 (Combinatorial Nullstellensatz) *Let F be any arbitrary field and $P(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Assume that P has a degree $\deg P = \sum_{i=1}^{n} k_i$, where k_i is a non-negative integer, and the coefficient of $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ in P is non-zero. Then for any subsets $A_1, \ldots, A_n$ of F satisfying $|A_i| \geq k_i + 1$ for all $i = 1, 2, \ldots, n$, there are $a_1 \in A_1, \ldots, a_n \in A_n$ such that $P(a_1, \ldots, a_n) \neq 0$.*

The following brief proof of the theorem is based on Michalek's paper [6].

Proof of Theorem 8.1. The proof is via induction on the degree of P. If $\deg P = 1$, the theorem is trivial.

Then we assume, that $\deg P = n > 1$, and we have already proved the theorem for all polynomial of degree less than n. We would like to prove the statement for P. We continue the proof indirectly.

Assume $\deg P > 1$ and P satisfies the theorem's assumptions, but the statement is false, that is, $P(x) = 0$ for all $x \in A_1 \times \cdots \times A_n$.

We may suppose $k_1 > 0$ without losing generality. Fix $a \in A_1$ and write

$$P = (x_1 - a)Q + R, \tag{8.1}$$

using the polynomial long division algorithm.

Equation (8.1) is a formal identity in the ring of polynomials in one variable x_1 with coefficients in the ring $F[x_2, \ldots, x_n]$.

Since the degree of R in the variable x_1 is strictly less than $\deg(x_1 - a)$, the polynomial R contains no x_1.

According to our assumption on P, which states that P has a nonvanishing monomial of maximum degree of the form $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, it follows that Q must have a nonvanishing monomial of maximum degree of the form $x_1^{k_1 - 1} x_2^{k_2} \cdots x_n^{k_n}$, where $\deg Q = \sum_{i=1}^{n} k_i - 1 = \deg P - 1$.

Pick any $x \in \{a\} \times A_2 \times \cdots \times A_n$ and substitute it into the equation (8.1).

Since $P(x) = 0$ we have $R(x) = 0$.

But, because R does not contain x_1, R vanishes on $(A_1 \setminus \{a\}) \times A_2 \times \cdots \times A_n$.

Now substitute any $x \in (A_1 \setminus \{a\}) \times A_2 \times \cdots \times A_n$ to (8.1). Since $x_1 - a$ is non-zero, $Q(x) = 0$.

As a result, Q vanishes on $(A_1 \setminus \{a\}) \times A_2 \times \cdots \times A_n$, which contradicts the inductive assumption.

Erdős and Heilbronn [4] conjectured the following in 1964.

Conjecture 8.2 (Erdős-Heilbronn) *If p is a prime, and $\mathcal{A}$ is a nonempty subset of $\mathbb{Z}_p$, then*

$$|\{a + a' : a, a' \in \mathcal{A},\ a \neq a'\}| \geq \min\{p,\ 2|\mathcal{A}| - 3\}.$$

Dias Da Silva and Hamidoune [3] proved this conjecture using tools from linear algebra and the representation theory of the symmetric group.

Alon, Nathanson, and Ruzsa [2] simplified the proof by using the Combinatorial Nullstellensatz.

Their theorem for the case of two sets is as follows:

Theorem 8.3 *Let p be a prime, $\mathcal{A}$ and $\mathcal{B}$ be two non-empty subset of $\mathbb{Z}_p$. Then if $|\mathcal{A}| \neq |\mathcal{B}|$ we have*

$$|\{a+b:\ a\in\mathcal{A},\ b\in\mathcal{B},\ a\neq b\}| \geq \min\{p,\ |\mathcal{A}|+|\mathcal{B}|-2\}.$$

If the condition $|A| \neq |B|$ is not assumed, the following follows as an immediate conclusion.

Theorem 8.4 *Let p be a prime, $\mathcal{A}$ and $\mathcal{B}$ be two non-empty subset of $\mathbb{Z}_p$. Then*

$$|\{a+b:\ a\in\mathcal{A},\ b\in\mathcal{B},\ a\neq b\}| \geq \min\{p,\ |\mathcal{A}|+|\mathcal{B}|-3\}.$$

This estimate is marginally (but only marginally) worse than the previous one. Gyula Károlyi [5] was able to precisely specify the sets that only have this weaker estimate.

Theorem 8.5 *Let p be a prime, $\mathcal{A}$ and $\mathcal{B}$ be two non-empty subset of $\mathbb{Z}_p$. Then*

$$|\{a+b:\ a\in\mathcal{A},\ b\in\mathcal{B},\ a\neq b\}| \geq \min\{p, |\mathcal{A}|+|\mathcal{B}|-2\},$$

unless $\mathcal{A}=\mathcal{B}$ and one of the following holds:

(i) $|\mathcal{A}| = 2$ *or* $|\mathcal{A}| = 3$*;*

(ii) $|\mathcal{A}| = 4$ *and* $\mathcal{A} = \{a, a+d, c, c+d\}$*;*

(iii) $|\mathcal{A}| \geq 5$ *and* $\mathcal{A}$ *is an arithmetic progression.*

Based on Michalek's paper [6], we only show Theorem 8.4 here.

Proof of Theorem 8.4. Write

$$\mathcal{C} = \{a + b : \ a \in \mathcal{A}, \ b \in \mathcal{B}, \ a \neq b\}.$$

Our goal is to prove

$$|\mathcal{C}| \geq \min\{p, |\mathcal{A}| + |\mathcal{B}| - 3\}.$$

For $p = 2$ the theorem is trivial. Assume that $p > 2$.

If $\min\{p, \ |\mathcal{A}| + |\mathcal{B}| - 3\} = p$, then the sets $\mathcal{A}$ and $g - \mathcal{B}$ have at least two different elements in common for any $g \in \mathbb{Z}_p$.

If a differs from $\frac{g}{2}$, then $g = a + b$ for some $b \in \mathcal{B}$ that differs from a.

This proves that $g \in \mathcal{C}$, and so $\mathcal{C} = \mathbb{Z}_p$.

Assume that $|\mathcal{A}| + |\mathcal{B}| - 3 < p$ and the theorem do not hold.

In that case, a set $\mathcal{D}$ exists in which $C \subseteq D$ and $|\mathcal{D}| = |\mathcal{A}| + |\mathcal{B}| - 4$.

We define two polynomials:

$$P(x, y) = \prod_{d \in \mathcal{D}} (x + y - d) \quad \text{and} \quad Q(x, y) = P(x, y)(x - y).$$

Clearly $P(a, b) = 0$ for all $a \in \mathcal{A}, \ b \in \mathcal{B}, a \neq b$, hence $Q(a, b) = 0$ for any $a \in \mathcal{A}$, $b \in \mathcal{B}$.

If $i+j=|\mathcal{D}|$ then the coefficient of x^iy^j in $P(x,y)$ is equal to $\binom{|\mathcal{D}|}{i}$.

As a result, if $i+j=|\mathcal{D}|+1$, the coefficient of x^iy^j in $Q(x,y)$ is equal to $\binom{|\mathcal{D}|}{i-1}-\binom{|\mathcal{D}|}{i}=\frac{|\mathcal{D}|!}{i!(|\mathcal{D}|-i+1)!}(i-(|\mathcal{D}|-i+1))$.

This coefficient is equal to 0 in $\mathbb{Z}_p$, if and only if $i=\frac{|\mathcal{D}|+1}{2}$.

Since $|\mathcal{D}|+1=|\mathcal{A}|+|\mathcal{B}|-3$, one of the coefficients of $x^{|\mathcal{A}|-1}y^{|\mathcal{B}|-2}$ or $x^{|\mathcal{A}|-2}y^{|\mathcal{B}|-1}$ is nonzero.

We get a contradiction using Theorem 8.1 and the fact that $\deg Q=|\mathcal{A}|+|\mathcal{B}|-3$.

References

[1] N. Alon, *Combinatorial Nullstellensatz*, Combin. Prob.Comput. 8 (1999), 7-29.

[2] N. Alon, M. B. Nathanson, I. Ruzsa, *The Polynomial Method and Restricted Sums of Congruence Classes*, Journal of Number Theory 56 (2), (1996), 404-417.

[3] J. A. Dias da Silva, Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory,* Bull. London Math. Soc. 26 (1994), 140-146.

[4] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory,*, L'Enseignement Mathématique, Geneva, 1980.

[5] Gy. Károlyi, *Restricted set addition: The exceptional case of the Erdős–Heilbronn conjecture*, Journal of Combinatorial Theory, Series A 116 (3), (2009), 741-746.

[6] M. Michalek, *A Short Proof of Combinatorial Nullstellensatz*, The American Mathematical Monthly 117 (9), (2010), 821-823.

9 Erdős-Ginzburg-Ziv Theorem

The Erdős-Ginzburg-Ziv theorem is a good illustration of the applicability of the Cauchy-Davenport theorem, which its authors (Erdős, Ginzburg and Ziv) developed in 1961 [1].In the following, we describe the proof of the theorem based on [1] and the related Wikipedia page [2].

Theorem 9.1 (Erdős–Ginzburg–Ziv) *If m is a positive integer and $2m-1$ arbitrary integers are given, there will always be m pieces among them whose sum is divisible by m.*

Proof of Theorem 9.1 First, we prove the statement for primes.

Let p be a prime and denote the elements by $a_1, a_2, \ldots, a_{2p-1}$. We may assume

$$0 \leq a_1 \leq a_2 \leq \ldots \leq a_{2p-1} < p.$$

If $a_i = a_{i+p-1}$ for some $1 \leq i \leq p-1$, then

$$a_i + a_{i+1} + \ldots + a_{i+p-1} = pa_i = 0 \quad \text{(in } \mathbb{Z}_p\text{)}$$

and the desired result follows. Otherwise define

$$A_i = \{a_i, a_{i+p-1}\}.$$

By repeated application of the Cauchy–Davenport theorem we get

$$\{A_1+A_2+\ldots+A_{p-1}\} \geq \min\{p, |A_1|+\ldots+|A_{p-1}|-(p-2)\} = p.$$

As a result, we discovered that every residue class $\mod p$ can be written as a sum of $p-1$ elements from the set $a_1, a_2, \ldots, a_{2p-2}$,

particularly $-a_{2p-1}$. We get the theorem statement by arranging the congruence.

In the future, we will abbreviate the Erdős-Ginzburg-Ziv theorem to EGZT.

Lemma 9.2 *EGZT is true for primes.*

We have just proved this.

Lemma 9.3 *If EGZT is true for the integers m and n, it is true for mn.*

Proof of Lemma 9.3. First we will prove by induction on k such that from $k \cdot m + m - 1$ pieces of integers we can choose integers $a_1, a_2, \ldots, a_{km}$ such that for all $0 \leq i \leq k-1$

$$a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m} \tag{9.1}$$

is divisible by m.

This is true for $k = 1$ since it is EGZT for the integer m by the condition of Lemma 9.3.

Suppose that we proved the statement for $k \cdot m + (m-1)$ pieces of integers and we will prove it for $k \cdot m + (2m-1) = (k+1)m + m - 1$ pieces of integers.

By the inductive hypothesis there exist integers $a_1, a_2, \ldots, a_{km}$ such that

$$a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m}$$

is divisible by m for $0 \leq i \leq k-1$.

For a while, we remove the integers $a_1, a_2, \ldots, a_{km}$ from the list.

Then there are $2m-1$ integers left, and we can choose m whose sum is divisible by m. These are

$$a_{km+1}, a_{km+2}, \ldots, a_{km+m}.$$

(This is EGZT for m.) Thus we proved (9.1).

Using (9.1) for $k = 2n-1$ we get that among

$$(2n-1)m + m - 1 = 2nm - 1$$

pieces of integers, there exist integers $a_1, a_2, \ldots, a_{(2n-1)m}$ such that

$$b_i \stackrel{\text{def}}{=} \frac{a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m}}{m} \tag{9.2}$$

is always an integer for $0 \le i \le 2n-2$.

If we use EGZT for n and $b_0, b_1, \ldots, b_{2n-2}$ we get among b_i's there exist n pieces such that their sum is divisible by n.

If we consider those a_j's whose sums (see (9.2)) give us these n pieces of b_i's, we get the statement of EGZT for the modulus nm.

References

[1] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*. Bull. Res. Council Israel. 10F (1961), 41–43.

[2] Wikipedia, Erdős-Ginzburg-Ziv theorem, link.

10 Coloring and density theorems with applications

Van der Waerden proved his famous theorem (by solving a conjecture of Baudet) while he was only 24 years old, establishing a joint field of number theory and combinatorics [12] .

Theorem 10.1 (van der Waerden) *For any given positive integer r and k there is a number N such that if the integers $1, 2, ..., N$ are colored, each with one of r different colors, then there are at least k integers in arithmetic progression whose elements are of the same color. The least such N is now called the van der Waerden number $W(r, k)$.*

When $r = 2$, for example, we have two colors, say red and blue. Then $W(2, 3)$ is greater than 8, because the integers from 1 to 8 can be colored as follows:

When all cases are examined separately (a total of $2^9 = 512$ pieces), it is clear that no matter how we color the numbers

$1, 2, 3, \ldots, 9$ with two colors, they will always contain a three-term arithmetic progression.

In other words $W(2, 3) = 9$.

Unfortunately, we only know the exact value of a few van der Waerden numbers. These can be found in the Wikipedia article linked to above: link.

Gowers [11] found the best upper bound currently known:

$$W(r, k) \leq 2^{2^{r^{2^{2^{k+9}}}}}.$$

Berlekamp [3] gave the following lower estimate for two colors in case of primes p:

$$W(2, p + 1) \geq p \cdot 2^p.$$

In general, the proofs of known upper estimates for van der Waerden numbers are very complicated (similar to the proof of Szemerédi's theorem later), thus we do not prove any upper estimates in this chapter.

On the other hand, a good lower estimate can be provided by a basic, elementary probability computation. The proof that follows is based on [7].

Theorem 10.2 $W(2, k) \geq \sqrt{\frac{k}{3}} \cdot 2^{(k-1)/2}$.

Proof of Theorem 10.2. First, we state that the number of k-term arithmetic progression (k-AP) of $\{1, 2, 3, \ldots, N\}$ is less than $\frac{N^2}{k}$.

If a k-AP begins with a, then $a + (k-1)d \leq N$, yielding in $d \leq \frac{N-a}{k-1}$.

As a result, the total number of k-AP's in $\{1, 2, 3, \ldots, N\}$ is bounded by

$$\sum_{a=1}^{N-1} \frac{N-a}{k-1} = \frac{N(N-1)}{2(k-1)} < \frac{N^2}{k}.$$

Let $N = \sqrt{\frac{k}{3}} \cdot 2^{(k-1)/2}$.

By flipping a coin, color each number x from 1 to N. If the coin is head, color x with blue, if it is tail, color x with red.

Let p denote the probability of existence of a monochromatic k-AP.

We will show that $p < 1$ and hence there are some coin flips that result in a proper 2-coloring of $\{1, 2, 3, \ldots, N\}$.

We know that $\frac{N^2}{k}$ is an upper bound for the number of k-AP's.

Due of the random color selection, each k-AP becomes monochromatic with a chance of exactly $\frac{1}{2^{k-1}}$, and a simple union bound over all k-AP's yields:

$$p \leq \frac{N^2}{k} \cdot \frac{1}{2^{k-1}} = \frac{1}{3}$$

This shows that the probability of obtaining proper coloring (with no monochromatic k-AP) is $\geq 2/3$. This completes the proof.

You might not believe it, but the van der Waerden theorem has an intriguing consequence: there are infinitely many primes.

Although there have been various proofs of this theorem since Euclid, it surprised me that it also follows from van der Waerden's theorem.

The following is a description of Levent Alpoge's paper [1].

Theorem 10.3 *There are infinitely many primes.*

Proof of Theorem 10.3. Let $\nu_p(n)$ denote the largest exponent of the prime p, for which $p^{\nu_p(n)}$ divides the positive integer n. Clearly

$$n = \prod_p p^{\nu_p(n)}.$$

Obviously, $\mu_p(ab) = \nu_p(a) + \nu_p(b)$, and

$$\nu_p(a+b) \geq \min(\nu_p(a), \nu_p(b)), \tag{10.1}$$

where for $\nu_p(a) \neq \nu_p(b)$ there is definitely an equality.

Assume there are a finite number of primes. Color the positive integers according to the list of primes that divide them and the exponents' parities.

So, if P is the finite set of primes, define $f : \mathbb{Z}^+ \to (\{0,1\} \times \{0,1\})^P$ by

$$f(n) = \left(\begin{cases} 1 & p \mid n \\ 0 & p \nmid n \end{cases}, \ \nu_p(n) \pmod 2 \right)_P, \qquad \text{if } n = \prod_p p^{\nu_p(n)}.$$

This coloring employs a finite set of colors, thus by van der Waerden theorem we know there exist arbitrarly long monochromatic arithmetic progressions.

Pick a monochromatic arithmetic progression $a, a+d, \ldots, a+dr$ with r higher than any prime's square.

Suppose that p divides a. Since each integer in the progression has the same prime factors, p divides $a+d$ and so p divides $d = (a+d) - a$.

We state that $\nu_p(a) < \nu_p(d)$.

Indeed, suppose that $\nu_p(a) > \nu_p(d)$. Then by (10.1)

$$\nu_p(a+d) = \nu_p(d). \tag{10.2}$$

Clearly $\nu_p(pd) = \nu_p(d) + 1$. Thus if $\nu_p(a) > \nu_p(pd) = \nu_p(d) + 1$, then

$$\nu_p(a+pd) = \nu_p(pd) = \nu_p(d) + 1 = \nu_p(a+d) + 1,$$

which contradicts $\nu_p(a+pd) \equiv \nu_p(a+d) \pmod 2$ (see the definition of the coloring).

If $\nu_p(a) = \nu_p(d) + 1$ then $\nu_p(a) = \nu_p(a+d) + 1$ (see (10.2)), which now contradicts $\nu_p(a) \equiv \mu_p(a+d) \pmod 2$.

If $\nu_p(a) = \nu_p(d)$ then

$$\nu_p(a+kd) = \nu_p(a) + 1 \not\equiv \nu_p(a) \pmod 2,$$

for a suitable chosen $k < p^2$ (here we must solve the congruence $A + kD \equiv p \pmod{p^2}$, where A and D are those parts of a and d, which are relatively prime to p).

Thus we proved for every prime p dividing a, $\nu_p(a) < \nu_p(d)$. Then (10.1) yields

$$\nu_p(a+d) = \nu_p(a).$$

By the definition of the coloring, a and $a+d$ have the same prime factors, and even their exponents are the same, which contradicts the unique factorization if $d \geq 1$.

The van der Waerden theorem had important consequences in mathematics. In 1936, Turán and Erdős [6] formulated the following conjecture.

Every set of integers $\mathcal{A}$ with positive natural density contains a k-term arithmetic progression for each k.

Endre Szemerédi [10] proved the conjecture in 1975, and he was awarded the Abel Prize for it in 2012.

Theorem 10.4 (Szemerédi) *For every $\varepsilon \in \mathbb{R}^+$ and $k \in \mathbb{N}$ there exists an $N_0 = N_0(\varepsilon, k)$ such that if $N > N_0$, $A \subseteq \{1, 2, 3, \ldots, N\}$ and $|\mathcal{A}| > \varepsilon N$, then $\mathcal{A}$ contains a k-term arithmetic progression.*

There are several types of proofs of Szemerédi theorem, including combinatorial ones (which use the famous Szemerédi regularity lemma), ergodic theoretical, Fourier analytic, and one based on the hypergraph removal lemma.

Moreover there are quantitave versions of Szemerédi's theorem. They mostly use the function $r_k(N)$, which returns the size of the largest subset of $\{1, 2, \ldots, N\}$ without an arithmetic progression of length k.

The best known general bounds are

$$CN\exp\left(-n2^{(n-1)/2}(\log N)^{1/n}+\tfrac{1}{2n}\log\log N\right)\le r_k(N)\le \frac{N}{(\log\log N)^{2-2^{k+9}}},$$

where $n=\lceil \log k\rceil$.

O'Bryant [8] gave the best known lower bound (based on various earlier results, such as Behrend's theorem [2]). The upper bound is due to Gowers [11].

Similarly to van der Warden numbers, we do not prove an upper estimate here because it is beyond the scope of this note. We will, however, justify a lower estimate.

But first, consider an application of Szemerédi's theorem, which was also developed by Szemerédi [9].

Since Fermat, we have known that four square numbers never form an arithmetic progression.

That is, if an N-term arithmetic progression $a, a+d, a+2d, \ldots, a+(N-1)d$ is given, and we color the t's in red, where $a+td$ is a square number, then the red numbers in $0, 1, 2, 3, ..., N-1$ do not contain a 4-term arithmetic progression.

Thus for every $\varepsilon > 0$ if $N > N_0(\varepsilon)$, there are less than εN elements colored in red in $\{0, 1, 2, \ldots, N-1\}$, according to Szemerédi's theorem. Summarizing this we get the following [9].

Theorem 10.5 (Szemerédi) *For every $\varepsilon \in \mathbb{R}^+$ there exists an $N_0 = N_0(\varepsilon)$ such that if $N > N_0$, then every N-term arithmetic progression contains less than εN squares.*

Since then, this result has been improved, e.g., in 1992 Bombieri, Granwille and Pintz [4] proved the following.

Theorem 10.6 *There are at most* $c_1 N^{2/3} (\log N)^{c_2}$ *squares in any arithmetic progression of length* N*, where* c_1 *and* c_2 *are absolue and effectively computable constants.*

In [5] Bombieri and Zannier improved the exponent from $2/3$ to $3/5$.

In the following chapter, we see a nice lower estimate for the number $r_3(n)$, namely Behrend's theorem [2], which is based on geometrical reasoning.

References

[1] L. Alpoge, *van der Waerden and the primes*, The American Mathematical Monthly 122 (8) (2015), 784-785.

[2] F. A. Behrend, *On the sets of integers which contain no three terms in arithmetic progression*, Proceedings of the National Academy of Sciences. 32 (12) (1946) 331–332.

[3] E. Berlekamp, *A construction for partitions which avoid long arithmetic progressions*, Canadian Mathematical Bulletin. 11 (3) (1968), 409–414.

[4] E. Bombieri, A. Granville, J. Pintz, *Squares in arithmetic progressions*, Duke Mathematical Journal 66 (1992), 369–385.

[5] E. Bombieri, U. Zannier, *A Note on squares in arithmetic progressions, II*, Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni 13 (2) (2002), 69-75.

[6] P. Erdős, P. Turán, *On some sequences of integers*, Journal of the London Mathematical Society. 11 (4) (1936) 261–264.

[7] W. Gasarch, B. Haeupler, *Lower Bounds on van der Waerden Numbers: Randomized- and Deterministic-Constructive*, Electronic Journal of Combinatorics Vol 18, 2011.

[8] K. O'Bryant, *Sets of integers that do not contain long arithmetic progressions*. Electronic Journal of Combinatorics. 18 (1) (2011).

[9] 3E. Szemerédi, *The number of squares in arithmetic progressions*, Stud. Sci. Math. Hungar., 9 (1975) p.417.

[10] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arithmetica 27 (1975), 199–245.

[11] G. Timothy, *A new proof of Szemerédi's theorem*, Geometric and Functional Analysis. 11 (3) (2001), 465–588.

[12] B. L. van der Waerden, *Beweis einer baudetschen vermutung*, Nieuw Arch. Wisk. 15 (1927), 212–216.

[13] Photo, Cartoon Businessman Flipping A Coin, link.

[14] Photo, Van der Waerden, Wikipedia, link.

11 Behrend's construction

In this chapter, we are looking for a relatively large subset of $\{1, 2, 3, \ldots, N\}$ that does not contain a three-term arithmetic progression.

The next theorem due to Behrend [1] is based on an amazing geometric construction. We use the terminology of [4] during the presentation.

Theorem 11.1 (Behrend, 1946.) *There exists a positive constant c such that for all N we can give a set*

$$\mathcal{A} \subset \{1, 2, 3, \ldots, N\}$$

for which

$$|\mathcal{A}| \geq N \exp(-c\sqrt{\log N})$$

and $\mathcal{A}$ does not contain a three-term arithmetic progression.

Proof of Theorem 11.1. Behrend's construction is based on the observation that a straight line can intersect a sphere at most 2 points.

If $\mathrm{x}, \mathrm{y}, \mathrm{z}$ is a three-term arithmetic progression then $\mathrm{y} = \frac{\mathrm{x}+\mathrm{z}}{2}$.

First, we give a n dimensional construction (a spherical shell) where in the set it is not included the average of two points, moreover, there are no three points in the set that lies in the same line.

After this we assign the set of these points to a set $\mathcal{A} \subseteq \{1, 2, 3, \ldots, N\}$.

We will fix the exact values of n and M later.

Consider the integer-coordinated points $\mathbf{x} = (x_1, x_2, ..., x_n) \in [1, M]^n$. There are M^n such points, and we assign the square of the distance from the origin to each one, i.e., the number $r^2 = x_1^2 + ... + x_n^2$.

These assigned values are integers from $[n, nM^2]$. That is, there exists a radius r such that the $S_n(r)$ sphere contains at least

$$|S_n(r)| \geq \frac{M^n}{nM^2 - n + 1} \geq \frac{M^n}{nM^2} \geq \frac{M^{n-2}}{n}$$

points.

We want to assign integers to the points of $S_n(r)$. We define the function $P : \mathbb{Z}^n \to \mathbb{Z}$ as follows:

$$P(\mathbf{x}) \stackrel{\text{def}}{=} \frac{1}{2M} \sum_{i=1}^{n} x_i (2M)^i.$$

The basic properties of the above function are the following:

1. P is integer valued.
2. $1 \leq P(\mathbf{x}) \leq (2M)^n$ for all $\mathbf{x} \in [1, M]^n$.
3. P is linear.
4. P is injective in $[1, M]^n$.
5. $P(\mathbf{z}) - P(\mathbf{y}) = P(\mathbf{y}) - P(\mathbf{x}) \Rightarrow \mathbf{z} - \mathbf{y} = \mathbf{y} - \mathbf{x}$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in [1, M]^n$.

Property 1 is obvious, since all terms in the sum are divisible with $2M$.

Property 2 is also true since $P(\mathrm{x})$ is positive and the maximum is attained in the sum when each x_i is chosen to be maximal, i.e., M. Then

$$P(\mathrm{x}) \leq P(M, M, \ldots, M) = \frac{1}{2M} \sum_{i=1}^{n} M(2M)^i$$
$$= M\frac{(2M)^n - 1}{2M - 1} \leq M\frac{(2M)^n}{2M} < (2M)^n.$$

Property 3 is also obvious, since let $\mathrm{x}, \mathrm{y} \in \mathbb{Z}^n$ and $a, b \in \mathbb{Z}$. Then, using the definition of P, it is easy to prove that

$$P(a\mathrm{x} + b\mathrm{y}) = aP(\mathrm{x}) + bP(\mathrm{y}).$$

In order to prove properties 4 and 5, we will need the following lemma.

Lemma 11.2 *Let $\mathrm{x} \in (-2M, 2M)^n$. Then $P(\mathrm{x}) = 0$ if and only if $\mathrm{x} = 0$.*

Proof of Lemma 11.2. If $\mathrm{x} = 0$, then $P(\mathrm{x}) = 0$.

Conversely, suppose there exists $\mathrm{x} \neq 0$ for which $P(\mathrm{x}) = 0$. Among the coordinates of the number $\mathrm{x} = (x_1, x_2, \ldots, x_n)$, take the smallest one, which is not 0, let it be x_j. Then

$$P(\mathrm{x}) = \frac{1}{2M} \sum_{i=j}^{n} x_i(2M)^i = 0.$$

By arranging this, we get

$$-x_j = \sum_{i=j+1}^{n} x_i (2M)^{j-i}$$

where the right-hand side is divisible by $2M$, but on the left-hand side $1 \leq x_j < 2M$, which is a contradiction. This completes the proof of the lemma.

Using the lemma, we will prove properties 4 and 5.

To prove property 4, assume that $P(\mathbf{x}) = P(\mathbf{y})$ holds for a pair of integers $\mathbf{x}, \mathbf{y}$ in $[1, M]^n$.

According to linearity, $\mathbf{0} = P(\mathbf{x}) - P(\mathbf{y}) = P(\mathbf{x} - \mathbf{y})$, but $\mathbf{x} - \mathbf{y} \in (-M, M)^n \subset (-2M, 2M)^n$, so based on the lemma $\mathbf{x} - \mathbf{y} = \mathbf{0}$, i.e., $\mathbf{x} = \mathbf{y}$. As a result, P is injective.

We only have to prove the last, property 5.

Assume that $P(\mathbf{z}) - P(\mathbf{y}) = P(\mathbf{y}) - P(\mathbf{x})$ is satisfied for some number triple $\mathbf{x}, \mathbf{y}, \mathbf{z} \in [1, M]^n$. Then $P(\mathbf{z}) - 2P(\mathbf{y}) + P(\mathbf{x}) = P(\mathbf{z} - 2\mathbf{y} + \mathbf{x}) = \mathbf{0}$, and here $\mathbf{z} - 2\mathbf{y} + \mathbf{x} \in (-2M, 2M)^n$. So again using the lemma we get $\mathbf{z} - 2\mathbf{y} + \mathbf{x} = \mathbf{0}$, i.e., $\mathbf{z} - \mathbf{y} = \mathbf{y} - \mathbf{x}$, which was to be proved.

Now we fix the values of n and M. Let $n = \lceil \sqrt{\log N} \rceil$, $M = [N^{1/n}/2]$.

Then $\mathcal{A} \subset [1, (2M)^n] \subset [1, N]$.

Due to property 5 of the function P, we know that $\mathcal{A}$ does not contain a three-term arithmetic progression.

Now we only need to estimate the number of elements of $\mathcal{A}$.

$$
\begin{aligned}
|\mathcal{A}| &\geq \frac{M^{n-2}}{n} = \frac{[N^{1/n}/2]^{n-2}}{n} \geq \frac{\left(N^{1/n}/e\right)^{n-2}}{n} = e^{2-n}N^{1-2/n} \cdot \frac{1}{n} \\
&= Ne^{2-\lceil\sqrt{\log N}\rceil} \cdot N^{-2/\lceil\sqrt{\log N}\rceil} \cdot \frac{1}{\lceil\sqrt{\log N}\rceil} \\
&\geq Ne^{2-\left(\sqrt{\log N}+1\right)} \cdot N^{-2/\sqrt{\log N}} \cdot \frac{1}{\sqrt{\log N}+1} \\
&\geq Ne^{1-\left(\sqrt{\log N}\right)} \cdot e^{-2\log N/\sqrt{\log N}} \cdot e^{-\sqrt{\log N}} \\
&> Ne^{-4\sqrt{\log N}}.
\end{aligned}
$$

Thus, for the number $r_3(N)$ defined in the previous chapter, we obtained that

$$r_3(N) > Ne^{-4\sqrt{\log N}}.$$

On the contrary, Roth [6] proved in 1953 that if a set $A \subseteq \{1, 2, 3, \ldots, N\}$ does not contain a 3-term arithmetic progression, then $|\mathcal{A}| \ll \frac{N}{\log\log N}$. Since then, this result has been continuously improved. The best current result comes from Bloom and Sisask [2], who proved that there exists a constant $c > 0$ for which $|\mathcal{A}| \ll \frac{N}{(\log N)^{1+c}}$.

The best lower estimate also comes from Bloom and Sisask [3] (in fact they simplified the result of Kelley and Meka [5]), they proved $r_3([N]) \leq \exp(-c(\log N)^{1/11})N$.

References

[1] F. A. Behrend, *On the sets of integers which contain no three in arithmetic progression*, Proceedings of the National Academy of Sciences 23 (1946), 331-332.

[2] T. F. Bloom, O. Sisask, *Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions*, link.

[3] T. F. Bloom, O. Sisask, *The Kelley–Meka bounds for sets free of three-term arithmetic progressions*, link.

[4] B. Gillespie, *Behrend's Construction*, link.

[5] Z. Kelley, R. Meka, *Strong Bounds for 3-Progressions*, link.

[6] K. Roth, *On certain sets of integers*. Journal of the London Mathematical Society. 28 (1) (1953), 104–109.

[7] Photo, Basketball Clip Art, link.

12 On prime factors in a product of sums

The following theorem was discovered by Erdős and Turán when they were university students.

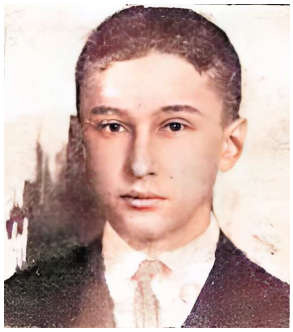
Here $\omega(n)$ denotes the number of distinct prime factors of n.

Theorem 12.1 (Erdős–Turán, [3]) *Let $\mathcal{A} \subseteq \mathbb{N}^+$ a set of positive integers. Suppose that $|A| \geq 2^k + 1$. Then*

$$\omega\Big(\prod_{a,a' \in A} (a + a')\Big) \geq k + 1.$$

Remark 12.2 *From this theorem follows*

$$\omega\Big(\prod_{a,a' \in A} (a + a')\Big) \geq \log_2 |A|.$$



We will use the context from Erdős-Surányi's book [2].

Proof of Theorem 12.1. The main idea is to find many distinct prime divisors of the pairwise sums $a + a'$ such that from

$$p^k \mid a + a' \implies p^k \mid a \text{ and } p^k \mid a'.$$

In order to find such primes p, first we prove the following lemma.

Lemma 12.3 *If p is an odd prime, then among $2\ell+1$ distinct odd integers there are $\ell+1$ such that for pairwise sums $a+a'$ we have*

$$p^k \mid a+a' \implies p^k \mid a \text{ and } p^k \mid a'.$$

Proof of Lemma 12.3. Let these $2\ell+1$ integers be

$$n_1, n_2, \ldots, n_{2\ell+1}.$$

Write all of them of the form

$$n_i = p^{\alpha_i} q_i \quad \text{where} \quad p \nmid q_i.$$

Then for the sum of two of them, say n_i and n_j, assuming $\alpha_i \le \alpha_j$ we have

$$n_i + n_j = p^{\alpha_i}\left(q_i + p^{\alpha_j-\alpha_i} q_j\right).$$

If $\alpha_i \neq \alpha_j$, then

$$p^{\alpha_i} \mid n_i + n_j \quad \text{and} \quad p^{\alpha_i} \mid n_i,\ p^{\alpha_i} \mid n_j,\ p^{\alpha_i+1} \nmid n_i + n_j.$$

If, on the other hand, $\alpha_i = \alpha_j$, we must ensure that $q_i + q_j$ is not divisible by p.

This is guaranteed if both the remainder of $q_i \pmod p$ and the remainder of $q_j \pmod p$ are less than $p/2$ or greater than $p/2$ (since p is odd, they cannot equal $p/2$).

In these cases, the sum of two has a remainder that is strictly between 0 and p, respectively between p and $2p$.

By the pigeon hole principle, the numbers

$$q_1, q_2, \ldots, q_{2\ell+1}$$

contains either $\ell + 1$ pieces with remainders less than $p/2$ or $\ell + 1$ pieces with remainders larger than $p/2$ modulo p. This completes the proof of the lemma.

The proof of the Erdős-Turán theorem is continued below.

Let

$$|A| \geq 2^k + 1 \quad \text{where} \quad k \geq 1.$$

Since $|A| \geq 3$ among the elements of $\mathcal{A}$ there exist two odd or two even, so $\prod_{a,a' \in A} (a + a')$ is divisible by 2.

Let us denote the odd prime divisors of the pairwise sums by

$$p_1, p_2, \ldots, p_i.$$

By using indirect reasoning, we will prove that $i \geq k$.

Assume that $i < k$.

According to Lemma 12.3, from the $2^k + 1$ numbers we can choose $2^{k-1} + 1$ such that if

$$p_1^{\alpha_1} \mid a + a', \quad \text{then} \quad p_1^{\alpha_1} \mid a \quad \text{and} \quad p_1^{\alpha_1} \mid a'.$$

From these $2^{k-1} + 1$ integers we can choose $2^{k-2} + 1$ such that

$$p_2^{\alpha_2} \mid a + a', \quad \text{then} \quad p_2^{\alpha_2} \mid a \quad \text{and} \quad p_2^{\alpha_2} \mid a'.$$

Using this technique again and again, we obtain $2^{k-i} + 1 \geq 3$ integers such that the statement holds for all prime numbers $p_1, p_2, \ldots, p_i$.

Let a_1, a_2, a_3 integers be chosen from among the $2^{k-i} + 1 \geq 3$ integers that remained at the end of the method.

Then (since we have already enumerated all of the odd prime divisors of all pairwise sums) we get:

$$\begin{aligned} a_1 + a_2 &= 2^{u_0} p_1^{u_1} p_2^{u_2} \dots p_i^{u_i}, \\ a_1 + a_3 &= 2^{v_0} p_1^{v_1} p_2^{v_2} \dots p_i^{v_i}, \\ a_2 + a_3 &= 2^{w_0} p_1^{w_1} p_2^{w_2} \dots p_i^{w_i}. \end{aligned}$$

Here $p_1^{u_1} p_2^{u_2} \dots p_i^{u_i} \mid a_1$ and a_2.

Thus it is not possible $2^{u_0} \mid a_1$, since then the sum $a_1 + a_2$ is too large. Similarly: $2^{u_0} \nmid a_2$.

We write $2^\gamma \parallel x$ if $2^\gamma \mid x$ but $2^{\gamma+1} \nmid x$. If the exponent of 2 in a_1 and a_2 are different, then

$$\begin{gathered} 2^\gamma \parallel a_1 \quad 2^\delta \parallel a_2 \quad \gamma < \delta \\ 2^\gamma \parallel a_1 + a_2 \Longrightarrow \gamma = u_0 \Longrightarrow 2^{u_0} \parallel a_1, \end{gathered}$$

which contradicts to $2^{u_0} \nmid a_1$.

The case of $\gamma > \delta$ can be handled similarly. Thus $\gamma = \delta$.

So if $2^\gamma \parallel a_1$,then $2^\gamma \parallel a_2$, $2^\gamma \parallel a_3$.

Write $a_i = 2^\gamma b_i$ where b_i is odd. Then

$$\begin{aligned} b_1 + b_2 &= 2^{r_1} p_1^{u_1} \dots p_i^{u_i}, \\ b_1 + b_3 &= 2^{r_2} p_1^{v_1} \dots p_i^{v_i}, \\ b_2 + b_3 &= 2^{r_3} p_1^{w_1} \dots p_i^{w_i}. \end{aligned}$$

Since it follows from $p^\alpha \mid a_i + a_j$ that $p^\alpha \mid a_i$ and $p^\alpha \mid a_j$ it is also true for b_i and b_j. Thus

$$p_1^{u_1} \dots p_i^{u_i} \mid b_1, b_2, b_3, \quad b_1 \neq b_2, \quad b_1 \neq b_3, \quad b_2 \neq b_3.$$

So that $b_1 + b_2 \geq 3p_1^{u_1} \dots p_i^{u_i} \Longrightarrow r_1 \geq 2$. Similarly, $r_2, r_3 \geq 2$, that $b_1 + b_2 + b_3$ is divisible by 2, which contradicts to that each b_i is odd.

In the case of two different sets Győry, Stewart and Tijdeman [4] proved the following:

Theorem 12.4 *Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}^+$ a set of positive integers. Suppose that $|\mathcal{A}| > |\mathcal{B}|$. Then*

$$\omega\left(\prod_{a \in A, b \in \mathcal{B}} (a+b)\right) \geq c_1 \log |\mathcal{A}|.$$

Erdős, Stewart and Tijdeman [1] showed that the lawer bound $c_1 \log |\mathcal{A}|$ cannot be improved to $\left(\frac{1}{8} + \varepsilon\right) (\log |\mathcal{A}|)^2 \log\log |\mathcal{A}|$.

Győry, Sárközy and Tijdeman [5] proved a similar lawer bound regarding the prime factors of the product of $ab + 1$'s.

References

[1] P. Erdős, C. L. Stewart, R. Tijdeman, *Some diophantine equations with many solutions*, Compositio Math. 66 (1988), 37-56.

[2] P. Erdős, J. Surányi, *Topics in the Theory of Numbers*, 2003rd Edition, Springer, Undergraduate Texts in Mathematics.

[3] P. Erdős, P. Turán, *On a Problem in the Elementary Theory of Numbers*, American Math. Monthly 40 (1934), 608-611.

[4] K. Győry, C. L. Stewart, R. Tijdeman, *On prime factors of sums of integers I*, Compositio Math. 59 (1) (1986), 81-88.

[5] K. Győry, C. L. Stewart, R. Tijdeman, *On the number of prime factors of integers of the form* $ab + 1$, Acta Arith. 74 (4) (1996), 365-385.

[6] Photo, Pál Erdős, KöMaL arcképcsarnok, link.

[7] Photo, Pál Turán, KöMaL arcképcsarnok, link.

13 Squares form an additive basis

A central question in additive number theory is whether a given infinite set is an *asymptotic basic of finite order?*

In other words, for which sets $\mathcal{B}$ exists a positive integer k such that every natural number is the sum of k elements of the set $\mathcal{B}$?

Lagrange's theorem, perhaps the earliest of these types of results, which states:

Theorem 13.1 (Lagrange's four square theorem) *Every integer can be written as the sum of at most* 4 *squares.*

First, we study which numbers can be written as the sum of two squares.

The origin of the problem goes back to Albert Girard, who noticed that every prime of the form $4k+1$ can be written as the sum of two squares. The result was published in 1625 [1].

A variant of the problem was also written by Fermat in a letter to Mersenne. Moreover, Fermat also gave the number of ways a prime power p can be written as the sum of two square numbers.

For composite numbers, the sum of two squares theorem relates the prime decomposition. More exactly:

Theorem 13.2 *An integer $n \geq 2$ can be written as the sum of two squares if and only if its prime decomposition contains no term p^k, where prime $p \equiv 3 \pmod 4$ and k is odd.*

If $n = x^2$ is a perfect square, the statement is trivial setting a (or b) to zero: $n = x^2 = 0^2 + x^2$. (Some perfect squares also have non-trivial decomposition such as $25 = 4^2 + 3^2$ or $100 = 8^2 + 6^2$, also known as Pythagorean triples.)

Examples

The prime decomposition of the number 2450 is given by $2450 = 2 \cdot 5^2 \cdot 7^2$. Among the primes occurring in this decomposition (which are 2. 5 and 7), only 7 is congruent to 3 modulo 4. Its exponent in the prime decomposition, 2, is even. Therefore, the theorem states that it is expressible as the sum of two squares. Indeed, $2450 = 7^2 + 49^2$.

The prime decomposition of the number 3430 is $2 \cdot 5 \cdot 7^3$. This time, the exponent of 7 in the prime decomposition is 3, an odd number. So 3430 cannot be written as the sum of two squares.

In order to prove the theorem first we will prove the following:

Lemma 13.3 *If the integers a and b can be written as the sum of two squares then their product ab can be also written as the sum of two squares.*

Proof of the Lemma 13.3. Let $a = x^2 + y^2$ and $b = u^2 + v^2$. Then

$$ab = (x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv + yu)^2.$$

Using this lemma, we can see that we first need to decide which primes p can be expressed as the sum of two squares.

This is Girard's theorem, also known as Fermat's theorem on sums of two squares.

Theorem 13.4 *Let p be a prime number. Then the equation*

$$x^2 + y^2 = p$$

can be solved in integers if and only $p = 2$ or p is a prime of form $4k + 1$.

First we prove Theorem 13.4 and after we will derive Theorem 13.1 from Theorem 13.4.

Proof of Theorem 13.4. First we will prove that if p is a prime of form $4k + 3$ then it can not be written of the sum of two squares. Contrary, suppose that p is a prime of the form $4k + 3$ and there exit integer x and y such that

$$x^2 + y^2 = p.$$

Then

$$x^2 + y^2 \equiv p \pmod 4.$$

Here p is a prime of the form $4k + 3$, so

$$x^2 + y^2 \equiv 3 \pmod 4.$$

A square is always congruent to 0 or 1 modulo 4. Thus $x^2 + y^2$ is congruent to $0, 1$ or 2 modulo 4, but $x^2 + y^2$ is never congruent to 3 modulo 4.

Next we prove that 2 and the primes of form $4k+1$ can be written as a sum of two squares. For $p = 2$ the statement is trivial:

$$2 = 1^2 + 1^2.$$

Now let p be a prime of form $4k+1$. Then -1 is a quadratic residue modulo p. Thus the congruence

$$x^2 \equiv -1 \pmod{p} \tag{13.1}$$

has a solution. Let s denote a solution of (13.1). Then

$$\begin{aligned} s^2 &\equiv -1 \pmod{p} \\ p &\mid s^2 + 1 \end{aligned}$$

Consider all numbers $a + bs$ where $a, b \in \mathbb{N}$ and

$$0 \leq a < \sqrt{p},\ 0 \leq b < \sqrt{p}.$$

The number of such sums is $\left([\sqrt{p}+1]\right)^2 > p$, so using the pigeonhole principle we get there exist pairs (a_1, b_1) and (a_2, b_2) for which

$$a_1 + b_1 s \equiv a_2 + b_2 s \pmod{p}$$

Writing $a = a_1 - a_2$ and $b = b_1 - b_2$ we get

$$\begin{aligned} a + bs &\equiv 0 \pmod{p} \\ a &\equiv -bs \pmod{p} \\ a^2 &\equiv b^2 s^2 \pmod{p} \\ a^2 &\equiv -b^2 \pmod{p} \\ p &\mid a^2 + b^2. \end{aligned}$$

Since $0 \leq a_1, a_2 < \sqrt{p}$ and $0 \leq b_1, b_2 < \sqrt{p}$ we get $-\sqrt{p} < a < \sqrt{p}$ and $-\sqrt{p} < b < \sqrt{p}$. Thus

$$0 < a^2 + b^2 < 2p.$$

Since $p \mid a^2 + b^2$ we get $a^2 + b^2 = p$.

Next we prove Theorem 13.1. First we remark that Theorem 13.1 is equivalent with the following statement:

If the prime factorization of n

$$n = 2^{\alpha} p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}, \tag{13.2}$$

where the primes p_i *are of the form* $4k+1$ *and the primes* q_i *are of the form* $4k+3$*, then* n *can be written as the sum of two squares if and only if every* β_i *is even.*

First we will prove that the n's which are of the form (13.2) is a sum of two squares. Indeed, by Theorem 13.1 we have 2 and the primes p_i are the sum of two squares. Clearly, $q_i^{\beta_i}$ is the sum of two squares if β_i is even since

$$q_i^{\beta_i} = 0^2 + \left(q_i^{\beta_i/2}\right)^2.$$

Using Lemma 13.3 multiple times we get n is of the form (13.2).

Next we prove if

$$n = q^{\beta} m, \tag{13.3}$$

where $q \nmid m$, q is a prime of form $4k+3$ and β is odd, then n cannot be written as the sum of two squares. This will complete the proof of Theorem 13.4.

We prove this indirect. Suppose that the statement does not hold, so n is of the form (13.3) and n is the sum of two squares. Consider one of these n's for which β is minimal. (Here β is odd, so $\beta \geq 1$.). Then

$$x^2 + y^2 = q^{\beta} m$$

$$x^2 + y^2 \equiv 0 \pmod{q}$$
$$x^2 \equiv -y^2 \pmod{q}. \tag{13.4}$$

If $q \nmid x$ and $q \nmid y$ then by taking $(q-1)/2$-th power of (13.4) we get

$$x^{q-1} \equiv (-1)^{(q-1)/2} y^{q-1} \pmod{q}.$$

Since q is a prime of form $4k+3$ we get $(q-1)/2$ is odd, so

$$x^{q-1} \equiv -y^{q-1} \pmod{q}.$$

By Fermat's little theorem $x^{q-1} \equiv 1 \pmod{q}$ and $y^{q-1} \equiv 1 \pmod{q}$, thus

$$1 \equiv -1 \pmod{q},$$

which is contradiction. So $q \nmid x$ and $q \nmid y$ is not possible. Thus $q \mid x$ or $\mid y$. Both cases by (13.4) we get

$$q \mid x \text{ and } q \mid y$$

hold simultaneously. Then

$$x = qx_0 \text{ and } y = qy_0,$$

where x_0 and y_0 are integers. Using these notation we get

$$\begin{aligned} x^2 + y^2 &= q^\beta m = n \\ (qx_0)^2 + (qy_0)^2 &= q^\beta m \\ x_0^2 + y_0^2 &= q^{\beta-2} m. \end{aligned}$$

This contradicts the fact that we fixed an integer n which is the sum of two squares of the form (13.3) such that β is already minimal. As a result, we proved Theorem 13.4.

Next we study Lagrange's four-square theorem. This theorem states that the squares form an additive basis of order four.

For illustration, 3, 31 and 310 can be represented as the sum of four squares as follows:

$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$31 = 5^2 + 2^2 + 1^2 + 1^2$$
$$310 = 17^2 + 4^2 + 2^2 + 1^2.$$

The examples in the Arithmetica clearly show that Diophantus was aware of the theorem. Finally, Lagrange proved the theorem much later, in 1770.

Carl Gustav Jakob Jacobi later found a simple formula for the number of representations of an integer as the sum of four squares in 1834.

Proof of Theorem 13.1. First we remark that it is sufficient to prove the theorem for every odd prime number p. This immediately follows from Euler's four-square identity (and from the that the theorem is trivially holds for the numbers 1 and 2).

Lemma 13.5 (Euler's four identity) *If a and b can be written as the sum of four squares, then their product ab can be also written as the sum of four squares.*

This identity easily follows from the following:

$$
\begin{aligned}
(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = \\
&(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\
&+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\
&+(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 \\
&+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2. \qquad (13.5)
\end{aligned}
$$

But how one can figure it out? Consider the quaternions

$$
\begin{aligned}
\alpha &= x_1+x_2i+x_3j+x_4k \\
\beta &= y_1-y_2i-y_3j-y_4k
\end{aligned}
$$

Then for the conjugates we have

$$
\begin{aligned}
\overline{\alpha} &= x_1-x_2i-x_3j-x_4k \\
\overline{\beta} &= y_1+y_2i+y_3j+y_4k
\end{aligned}
$$

The norm of a quaternion α is defined by $N(\alpha)=\alpha\cdot\overline{\alpha}$ then

$$
\begin{aligned}
N(\alpha) &= x_1^2+x_2^2+x_3^2+x_4^2 \\
N(\beta) &= y_1^2+y_2^2+y_3^2+y_4^2. \qquad (13.6)
\end{aligned}
$$

Define γ by $\gamma=\alpha\beta$. Then

$$
\begin{aligned}
\gamma = &(x_1y_1+x_2y_2+x_3y_3+x_4y_4) \\
&+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)i \\
&+(x_1y_3-x_2y_4-x_3y_1+x_4y_2)j \\
&+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)k.
\end{aligned}
$$

Thus

$$
N(\gamma)=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2
$$

$$
\begin{aligned}
&+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\
&+ (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 \\
&+ (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2.
\end{aligned}
$$

On the other hand

$$
\begin{aligned}
N(\gamma) &= N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} \\
&= \alpha\beta\overline{\beta}\overline{\alpha} = \alpha N(\beta)\overline{\alpha} = \alpha\overline{\alpha}N(\beta) \\
&= N(\alpha)N(\beta).
\end{aligned}
$$

Using this and (13.6) we get (13.5) which was to be proved.

Next we prove Lagrange theorem. As we have remarked it is sufficient to prove the theorem for every odd prime number p.

First we prove there is a multiple of p, we will denote it by np, which is the sum of four squares and $1 \leq n < p$.

The residues of a^2 modulo p are distinct for every a between 0 and $(p-1)/2$. Indeed, if for $1 \leq x, y \leq p-1$ we have

$$
x^2 \equiv y^2 \pmod{p},
$$

then

$$
\begin{aligned}
&p \mid x^2 - y^2 \\
&p \mid (x-y)(x+y) \\
&p \mid x-y \quad \text{or} \quad p \mid x+y.
\end{aligned}
$$

Since $1 \leq x, y \leq p-1$ this is equivalent with

$$
x = y \quad \text{or} \quad x = p - y.
$$

Similarly, for b taking integral values between 0 and $(p-1)/2$, the numbers $-b^2-1$ are distinct modulo p. By the pigeonhole principle, there are a and b in this range, for which a^2 and $-b^2-1$ are congruent modulo p, that is for which

$$\begin{aligned} a^2 &\equiv -b^2-1 \pmod{p} \\ a^2+b^2+1 &\equiv 0 \pmod{p} \\ a^2+b^2+1^2+0^2 &= np \qquad \text{for a positive integer } n. \end{aligned}$$

By $0 \le a, b \le (p-1)/2$ we get

$$np \le 2\left(\frac{p-1}{2}\right)^2 + 1 < p^2,$$

so $n < p$. This proves our statement.

Now let m be the smallest positive integer such that mp is the sum of four squares, $mp = x_1^2+x_2^2+x_3^2+x_4^2$ (we have just shown that there is some $m < p$ with this property, so among them there is a smallest).

We show by contradiction that m equals 1: supposing it is not the case, we prove the existence of a positive integer r less than m, for which rp is also the sum of four squares (this is in the spirit of the infinite descent method of Fermat).

First we prove m is odd. Suppose that m is even. Then

$$\begin{aligned} mp &= x_1^2+x_2^2+x_3^2+x_4^2 \\ \frac{m}{2}p &= \frac{1}{2}\left(x_1^2+x_2^2+x_3^2+x_4^2\right) \\ \frac{m}{2}p &= \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2, \end{aligned}$$

so the statement holds with $r = m/2$. Next we suppose m is odd.

Now we consider for each x_i the y_i which is in the same residue class modulo m and between $-(m-1)/2$ and $(m-1)/2$. Then

$$0 \equiv mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv y_1^2 + y_2^2 + y_3^2 + y_4^2 \pmod{m}.$$

It follows that $y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr$, for some non-negative integer r.

Next we will prove r is positive and less than m. Indeed, if $r = 0$, then $y_1^2 + y_2^2 + y_3^2 + y_4^2 = 0$, so $y_1 = y_2 = y_2 = y_4 = 0$. Thus $m \mid x_1, x_2, x_2, x_4$. But then $m^2 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$. So $m \mid p$ from which $m = 1$ since $1 < m < p$. On the other hand

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4\left(\frac{m-1}{2}\right)^2 < m^2,$$

thus $r < m$.

Finally, we use Euler's four-square identity again which shows that $mpmr = z_1^2 + z_2^2 + z_3^2 + z_4^2$. But the fact that each x_i is congruent to y_i modulo m implies that all of the z_i are divisible by m. Indeed:

$$\begin{aligned}
z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\
&\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \pmod{m}, \\
z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\
&\equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 = 0 \pmod{m}, \\
z_3 &= x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2 \\
&\equiv x_1x_3 - x_2x_4 - x_3x_1 + x_4x_2 = 0 \pmod{m}, \\
z_4 &= x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1 \\
&\equiv x_1x_4 + x_2x_3 - x_3x_2 - x_4x_1 = 0 \pmod{m}.
\end{aligned}$$

It follows that, for $w_i = z_i/m$, $w_1^2 + w_2^2 + w_3^2 + w_4^2 = rp$ where $r < m$, and this contradicts to the minimality of m.

Finally, we say a few words about Legendre's three-square theorem.

Theorem 13.6 (Legendre's three-square theorem) *Every natural number can be represented as the sum of three squares of integers*

$$n = x^2 + y^2 + z^2$$

if and only if n is not of the form $n = 4^k(8m + 7)$ for nonnegative integers k and m.

Legendre's original proof was incomplete.

Gauss later generalized the theorem and calculated the number of solutions to an integer written as the sum of three squares.

One part of the theorem, which states that if n is the sum of three squares, then it is not of the form $n = 4^k(8m + 7)$ is almost trivial.

First we prove that if n is of the form $8m+7$, then n cannot be written as the sum of three squares.

Indeed, each square is congruent to $0, 1$ or 4 modulo 8, and thus a sum of three squares can be congruent to $0+0+0$, $0+0+1$, $0+1+1$, $1+1+1$, $4+0+0$, $4+0+1$, $4+1+1$, $4+4+0$, $4+4+1$ or $4+4+4$ modulo 8. Among these residues the 7 never occurs, and from this follow that the sum of three squares can not be of the form $8m+7$.

Next suppose that n is of the form

$$n = 4^k(8m+7) \tag{13.7}$$

where k is positive integer and $m \in \mathbb{N}$, and n is the sum of three squares.

We may suppose that in (13.7) n was chosen such that the value of the positive integer k is minimal. Then n is divisible by 4.

Every square is congruent to 0 or 1 modulo 4. It is easy to see that the residue 0 modulo 4 can not be written as the sum of three elements form the set $\{0,1\}$ if and only if each residues are 0. In other words, if

$$n = x^2 + y^2 + z^2,$$

then every squares are divisible by 4. Let $x = 2x_0$, $y = 2y_0$ and $z = 2z_0$ where x_0, y_0 and z_0 are integers. Then

$$\frac{n}{4} = x_0^2 + y_0^2 + z_0^2,$$

so $\frac{n}{4} = 4^{k-1}(8m+7)$ can be also written as the sum of three squares, which contradicts that in (13.7) was chosen so that k is minimal. This proves one direction in Legendre's three square theorem. The other direction is very difficult, we do not prove it here.

References

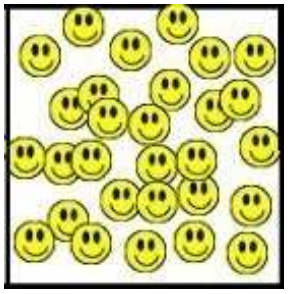
[1] S. Stevin, *l'Arithmétique de Simon Stevin de Bruges, annotated by Albert Girard*, Leyde 1625, p. 622.

[2] Photo, Giuseppe Luigi Lagrangia, link.

[3] Photo, Adrien-Marie Legendre, link.

14 Schnirelmann density

There are several density concepts in number theory, perhaps not the most natural at first, but the so-called Schnirelmann density has many practical applications.



The following definition was discovered by Lev Schnirelmann, a Russian mathematician [1], [2] in 1930.

Definition 14.1 *Let* $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$. *Then the Schnirelmann density of* $\mathcal{A}$ *is*

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}} \frac{\mathcal{A}(n)}{n},$$

where $\mathcal{A}(n) \stackrel{\text{def}}{=} |\mathcal{A} \cap \{1, 2, \ldots, n\}|$.

Clearly, $\sigma(\mathcal{A})$ is always a nonnegative number. First we state two propositions.

Proposition 14.2

$$\sigma(\mathcal{A}) > 0 \Longleftrightarrow 1 \in \mathcal{A} \text{ and } \exists\, c > 0\ \forall n\ \mathcal{A}(n) > cn.$$

Proposition 14.3

$$\sigma(\mathcal{A}) = 1 \iff \mathcal{A} = \mathbb{N}^+ \text{ or } \mathcal{A} = \mathbb{N} \cup \{0\}.$$

Proof of Proposition 14.2 First we prove that if $\sigma(\mathcal{A}) > 0$ then $1 \in \mathcal{A}$ and $\exists\, c > 0$ such that $\mathcal{A}(n) \geq cn$ for all positive integer n. Indeed, then

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} \leq \frac{\mathcal{A}(1)}{1} = \mathcal{A}(1). \tag{14.1}$$

If $1 \notin \mathcal{A}$, then $\mathcal{A}(1) = 0$, so by (14.1) we have $\sigma(\mathcal{A}) \leq 0$. But since $\sigma(\mathcal{A})$ is nonnegative we get $\sigma(\mathcal{A}) = 0$, which is a contradiction. Thus $1 \in \mathcal{A}$. On the other hand, if $\sigma(\mathcal{A}) > 0$, then writing $c = \sigma(\mathcal{A})$ we get

$$c = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} \leq \frac{\mathcal{A}(n)}{n}$$

for every $n \in \mathbb{N}^+$. Thus

$$cn \leq \mathcal{A}(n)$$

for every $n \in \mathbb{N}^+$.

Next we suppose that $1 \in \mathcal{A}$ and $\mathcal{A}(n) > cn$ for every n. Then

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} > \inf_{n \in \mathbb{N}^+} c = c > 0.$$

Proof of Proposition 14.3. Suppose that $\sigma(\mathcal{A}) = 1$. We will prove $\mathcal{A} = \mathbb{N}^+$ or $\mathcal{A} = \mathbb{N}^+ \cup \{0\}$. Indeed, let $n \in \mathbb{N}^+$. Then

$$1 = \sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} \leq \frac{\mathcal{A}(n)}{n}.$$

So

$$n \leq \mathcal{A}(n).$$

By the definition $\mathcal{A}(n)$, we get $1, 2, 3, \ldots, n \in \mathcal{A}$. So we proved for every $n \in \mathbb{N}^+$ that $n \in \mathcal{A}$, from which the statement follow. Clearly if $\mathcal{A} = \mathbb{N}^+$ or $\mathcal{A} = \mathbb{N}^+ \cup \{0\}$ then

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} = \inf_{n \in \mathbb{N}^+} \frac{n}{n} = 1.$$

Following that, we will prove Schnirelmann's main theorems.

Theorem 14.4 (Schnirelmann) *If $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N} \cup \{0\}$ and $0 \in \mathcal{A} \cap \mathcal{B}$, then*

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B}).$$

Proof of Theorem 14.4. If $\sigma(\mathcal{A}) = 0$, then we need to prove the following:

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{B}).$$

But since $0 \in \mathcal{A}$ we have

$$\mathcal{A} + \mathcal{B} \supseteq \mathcal{B},$$

thus the statement is trivial. So we may assume $\sigma(\mathcal{A}) > 0$. By Proposition 14.2 we have $1 \in \mathcal{A}$. Consider an arbitrary $n \in \mathbb{N}$ and denote the elements of $\mathcal{A} \cap [1, n]$ by

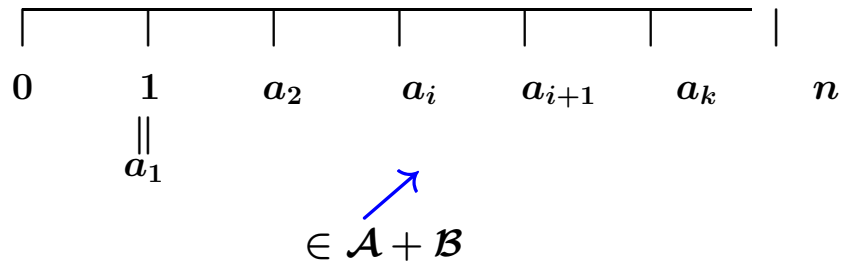
$$1 = a_1 < a_2 < \ldots < a_k \leq n.$$

Now $k = \mathcal{A}(n)$.

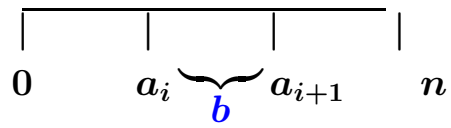
Next we will list some elements of the set $\mathcal{A} + \mathcal{B}$ (not every element!).

Since $0 \in \mathcal{B}$

$$a_i + 0 = a_i \in \mathcal{A} + \mathcal{B} \quad \text{for} \quad i = 1, \ldots, k.$$



There are further elements from $\mathcal{A}+\mathcal{B}$. For $i=1,2,\ldots,k-1$ consider the elements of form a_i+b where $b\in\mathcal{B}$ and $0<b<a_{i+1}-a_i$.

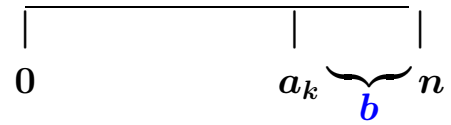


All elements of this form are in (a_i,a_{i+1}) and $\in\mathcal{A}+\mathcal{B}$.

Finally consider the elements of form

$$a_k+b,\quad b\in\mathcal{B},\quad b\le n-a_k.$$

All elements of this form are in $(a_k,n]$ and $\in\mathcal{A}+\mathcal{B}$.



How many elements have we listed so far?

$a_i\in\mathcal{A}+\mathcal{B},\ \ i=1,\ldots,k,\ \ k=\mathcal{A}(n)$ pieces of elements.

$a_i+b\in\mathcal{A}+\mathcal{B},\ \ i=1,\ldots,k-1,\ \ b\in\mathcal{B},\ \ 0<b<a_{i+1}-a_i$ for fixed i,
$\mathcal{B}(a_{i+1}-a_i-1)$ pieces of elements.

$a_k+b\in\mathcal{A}+\mathcal{B},\ \ b\in\mathcal{B},\ \ 0<b\le n-a_k,\ \ \mathcal{B}(n-a_k)$ pieces of elements.

Thus the number of elements in $\mathcal{A}+\mathcal{B}\cap[1,n]$ is at least

$$(\mathcal{A}+\mathcal{B})(n)\geq\mathcal{A}(n)+\sum_{i=1}^{k-1}\mathcal{B}(a_{i+1}-a_i-1)+\mathcal{B}(n-a_k).$$

Then

$$\begin{aligned}(\mathcal{A}+\mathcal{B})(n)&\geq\mathcal{A}(n)+\sigma(\mathcal{B})\cdot\left(\sum_{i=1}^{k-1}(a_{i+1}-a_i-1)\right)+\sigma(\mathcal{B})\cdot(n-a_k)\\&=\mathcal{A}(n)+\sigma(\mathcal{B})\cdot(n-\mathcal{A}(n))\\&=\mathcal{A}(n)(1-\sigma(\mathcal{B}))+\sigma(\mathcal{B})\cdot n.\end{aligned}$$

Here $1-\sigma(\mathcal{B})$ is positive or 0 and $\mathcal{A}(n)\geq\sigma(\mathcal{A})n$, so

$$\begin{aligned}(\mathcal{A}+\mathcal{B})(n)&\geq\sigma(\mathcal{A})\cdot n\cdot(1-\sigma(\mathcal{B}))+\sigma(\mathcal{B})\cdot n\\&=\big(\sigma(\mathcal{A})+\sigma(\mathcal{B})-\sigma(\mathcal{A})\sigma(\mathcal{B})\big)\cdot n.\end{aligned}$$

Using $\mathcal{A}(n)\geq\sigma(\mathcal{A})n$ we get

$$\begin{aligned}\frac{(\mathcal{A}+\mathcal{B})(n)}{n}&\geq\sigma(\mathcal{A})+\sigma(\mathcal{B})-\sigma(\mathcal{A})\sigma(\mathcal{B})\ \text{ for every } n\geq1,\\\sigma(\mathcal{A}+\mathcal{B})&\geq\sigma(\mathcal{A})+\sigma(\mathcal{B})-\sigma(\mathcal{A})\sigma(\mathcal{B}).\end{aligned}$$

Next we prove the following:

Theorem 14.5 (Schnirelmann) *If $\mathcal{A},\mathcal{B}\subseteq\mathbb{N}\cup\{0\}$, $0\in\mathcal{A}\cap\mathcal{B}$ and*

$$\sigma(\mathcal{A})+\sigma(\mathcal{B})\geq1,$$

then

$$\sigma(\mathcal{A}+\mathcal{B})=1.$$

Proof of Theorem 14.5. By Proposition 14.3:

$$\sigma(\mathcal{A}+\mathcal{B})=1\iff\forall n\in\mathbb{N}^+,\ n\in\mathcal{A}+\mathcal{B}.$$

We will prove this.

Case I: $n \in \mathcal{A} \cup \mathcal{B}$.

$$\text{If } n \in \mathcal{A}, \text{ then } n = n + 0 \in \mathcal{A} + \mathcal{B}.$$
$$\cap \quad \cap$$
$$\mathcal{A} \quad \mathcal{B}$$

If $n \in \mathcal{B}$ using similarly ideas we get $n \in \mathcal{A} + \mathcal{B}$.

Case II: $n \notin \mathcal{A} \cup \mathcal{B}$. Then $n > 1$, otherwise

$$1 \notin \mathcal{A} \cup \mathcal{B}$$
$$1 \notin \mathcal{A} \quad 1 \notin \mathcal{B}$$
$$\mathcal{A}(1) = \mathcal{B}(1) = 0$$
$$\sigma(\mathcal{A}) = \sigma(\mathcal{B}) = \frac{\mathcal{A}(1)}{1} = \frac{\mathcal{B}(1)}{1} = 0$$

Then $\sigma(\mathcal{A}) + \sigma(\mathcal{B}) = 0$, but by the condition of the theorem we have $\sigma(\mathcal{A}) + \sigma(\mathcal{B}) \geq 1$. Thus we proved $n > 1$. Then

$$\mathcal{A}(n) + \mathcal{B}(n) \geq \sigma(\mathcal{A}) \cdot n + \sigma(\mathcal{B}) \cdot n = (\sigma(\mathcal{A}) + \sigma(\mathcal{B})) \cdot n \geq n.$$

By this and $n \notin \mathcal{A} \cup \mathcal{B}$ we get

$$\mathcal{A}(n) = \mathcal{A}(n-1), \ \ \mathcal{B}(n) = \mathcal{B}(n-1), \ \ \mathcal{A}(n-1) + \mathcal{B}(n-1) \geq n.$$

For every $a \in \mathcal{A}$, $0 < a \leq n - 1$ consider a, and for every $b \in \mathcal{B}$, $0 < b \leq n - 1$ consider $n - b$. These are all in $\{1, 2, \ldots, n - 1\}$ and the number of them is

$$\mathcal{A}(n - 1) + \mathcal{B}(n - 1) \geq n.$$

By the pigeon-hole principle we get there exist $a \in \mathcal{A}$ and $b \in \mathcal{B}$ for which

$$a = n - b \implies a + b = n, \ \ n \in \mathcal{A} + \mathcal{B},$$

this completes the proof of the theorem.

For many years it was a conjecture whether in

$$\sigma(\mathcal{A}+\mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B})$$

the term "$-\sigma(\mathcal{A})\sigma(\mathcal{B})$" could be removed?

In 1932 Khintchin [3] was able to handle the case $\sigma(\mathcal{A}) = \sigma(\mathcal{B})$. Finally in 1942 Mann [4] proved this conjecture.

Theorem 14.6 (Mann, 1942) *If* $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N} \cup \{0\}$ *and* $0 \in \mathcal{A} \cap \mathcal{B}$, *then*

$$\sigma(\mathcal{A}+\mathcal{B}) \geq \min\{1, \sigma(\mathcal{A}) + \sigma(\mathcal{B})\}.$$

One of the most important theorems in combinatorial number theory. Since it is extremely difficult, we have omitted the proof from this note.

References

[1] L. G. Schnirelmann, *On the additive properties of numbers*, first published in "Proceedings of the Don Polytechnic Institute in Novocherkassk" (in Russian), vol XIV (1930), 3-27, and reprinted in "Uspekhi Matematicheskikh Nauk" (in Russian), 1939, no. 6, 9–25.

[2] L. G. Schnirelmann, First published as "Über additive Eigenschaften von Zahlen" in "Mathematische Annalen" (in German), vol 107 (1933), 649-690, and reprinted as "On the additive properties of numbers" in "Uspekhin. Matematicheskikh Nauk" (in Russian), 1940, no. 7, 7–46.

[3] A. Y. Khinchin, *Zur additiven Zahlentheorie*, Mat. Sb., 39:3 (1932), 27–34.

[4] H. B. Mann, *A Proof of the Fundamental Theorem on the Density of Sets of Positive Integers*, Ann. Math. 43 (1942), 523-527.

[5] A. Sárközy, Combinatorial Number theory, university lecture.

[6] Photo, Lev Schnirelmann, link.

[7] Photo, illustration of density, link.

15 Brun sieve

Viggo Brun developed an extension of Eratosthenes' sieve in the first quarter of the twentieth century that yielded good estimates on the number of elements of a set $\mathcal{A}$ that are not divisible by any of the primes $p_1, ..., p_k$ provided $\mathcal{A}$ is "regularly distributed" modulo these primes (see [1] and [2]).

Using Brun sieve, we can get more notable results related to the Goldbach conjecture. Namely, every integer can be written as the sum of two numbers, each of which has at most nine prime factors in the prime factorization (see [3]).

Furthermore, Schnirelmann proved that all integers can be written as the sum of at most 800000 primes. This last result will be studied in further detail in the following chapter.

The content of the present chapter is mainly given by [5] and [6].

The well-known exclusion-inclusion principle is used as the first step in explaining the Brun sieve.

Lemma 15.1 *Assume we have a finite set $\mathcal{A}$ with N elements, and some elements have the bad properties $T_1, T_2, ..., T_r$. Let $N_{i_1,i_2,...,i_k}$*

be the number of those elements which have the bad properties $T_{i_1}, T_{i_2}, \ldots, T_{i_k}$. *Then for the number of good elements (with no bad properties) we have:*

$$G = N + \sum_{k=1}^{r} (-1)^k \sum_{\leq i_1 < i_2 < \cdots < i_k \leq r} N_{i_1, i_2, \ldots, i_k}. \tag{15.1}$$

Proof of Lemma 15.1. Two facts need to be verified:

1. All good elements are counted just once.
2. All bad elements are counted 0 times.

Here 1. is trivial, since we just count all good elements in the first term.

In order to show 2., suppose a bad element has ℓ bad properties (then $r \geq \ell > 0$).

These are the properties: $T_{j_1}, \ldots, T_{j_\ell}$. The multiplicity is then calculated in (15.1) by taking the number of ways from $i_1, \ldots, i_k$ selected from $j_1, \ldots, j_\ell$ with $(-1)^k$ weight.

There are $\binom{\ell}{k}$ possibilities, which means we counted this bad element

$$\sum_{k=0}^{\ell} (-1)^k \binom{\ell}{k}$$

times in total. However, according to the binomial theorem, this is $(1-1)^\ell = 0$, proving our statement 2.

When we look at (15.1), we can see that it has a large number of members (a total of 2^r), which were too numerous during the development of the Brun sieve. However, with a clever idea, we may significantly decrease the number of members.

Lemma 15.2 *Using the notation of inclusion-exclusion principle for the good elements G, we get that*

$$N + \sum_{k=1}^{2t-1} (-1)^k \sum_{\leq i_1 < i_2 < \cdots < i_k \leq r} N_{i_1, i_2, \ldots, i_k} \leq G$$
$$\leq N + \sum_{k=1}^{2t} (-1)^k \sum_{\leq i_1 < i_2 < \cdots < i_k \leq r} N_{i_1, i_2, \ldots, i_k}.$$

for all $t \in \mathbb{N}^+$.

Roughly: after the "-"s, we estimate from the bottom, after the "+"s, we estimate from the top.

Proof of Lemma 15.2. Again two facts need to be verified:

1. All good elements are counted just once in both sums.
2. All bad elements are counted ≤ 0 times in the sum in left-hand side and ≥ 0 weight in the sum in right-hand side.

Here 1. is trivial.

In order to show 2., we need to prove:

$$\sum_{k=0}^{j} (-1)^k \binom{\ell}{k} = (-1)^j \binom{\ell - 1}{j}.$$

The proof of this is immediate by induction on j and using the relation $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$. This completes the proof of the lemma.

Next, we may describe the Brun sieve.

In the following, we use the principle of inclusion-exclusion (see Lemma 15.2) but with slightly new notations.

Let $\mathcal{A}$ be a set of integers, and let A_d be the number of the those elements of $\mathcal{A}$ which are divisible by d. Moreover $\omega(d)$ denotes the distinct prime divisors of d.

Suppose that we would like to determine the number of elements of A that are not divisible by any of the primes $p_1, p_2, \ldots, p_k$. If T_i denotes the bad property that an element is divisible by the prime p_i, then according to Lemma 15.2:

$$\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\leq 2t-1}} \mu(d)A_d \leq \sum_{a\in\mathcal{A}} \sum_{p_1\nmid a, p_2\nmid a,\ldots,p_k\nmid a} 1 \leq \sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\leq 2t}} \mu(d)A_d. \tag{15.2}$$

In the ideal scenario, the size of A_d can be approximated as follows:

$$X\frac{m(d)}{d} + R_d, \tag{15.3}$$

where $m(d)$ is a multiplicative function, X is a constant depending only on the set $\mathcal{A}$ and R_d is small in comparison to $X\frac{m(d)}{d}$.

Before we go any further, consider one or two examples of estimating A_d.

First, let $\mathcal{A} = \{a : 1 \leq a \leq x\}$. It is clear that then

$$A_d = \frac{x}{d} + R_d, \tag{15.4}$$

where $|R_d| \leq 1$. So in (15.3) one may take $X = x$, $m(d) = 1$.

In the second example $\mathcal{A} = \{n(n+2) : n \in \{y, y+1, \ldots, x\}\}$. Let d a squarefree integer. Then the congruence

$$n(n+2) \equiv 0 \pmod{d}$$

has $m(d)$ solutions by the Chinese remainder theorem, where m is a multiplicative function with $m(2) = 1$ and $m(p) = 2$ for primes $p \geq 3$. Clearly,

$$A_d = (x - y)\frac{m(d)}{d} + R_d, \tag{15.5}$$

where $|R_d| \leq 2^{\omega(d)}$.

Let us return to the general situation. If (15.3) indeed holds, then:

$$\begin{aligned}\sum_{\substack{d|p_1p_2\cdots p_k \\ \omega(d)\leq h}} \mu(d)A_d &= \sum_{\substack{d|p_1p_2\cdots p_k \\ \omega(d)\leq h}} \mu(d)\left(X\frac{m(d)}{d} + R_d\right) \\ &= X\sum_{\substack{d|p_1p_2\cdots p_k \\ \omega(d)\leq h}} \mu(d)\frac{m(d)}{d} + O\left(\sum_{\substack{d|p_1p_2\cdots p_k \\ \omega(d)\leq h}} R_d\right).\end{aligned} \tag{15.6}$$

In the following, we estimate $\sum_{\substack{d|p_1p_2\cdots p_k \\ \omega(d)\leq h}} \mu(d)\frac{m(d)}{d}$. Let $u > 1$ be an arbitrary real number, whose exact value will be fixed later. Then $u^{\omega(d)-h} > 1$ holds if $\omega(d) > h$. Thus:

$$\begin{aligned}\sum_{\substack{d|p_1p_2\cdots p_k \\ \omega(d)\leq h}} \mu(d)\frac{m(d)}{d} &= \sum_{d|p_1p_2\cdots p_k} \mu(d)\frac{m(d)}{d} + O\left(\sum_{\substack{d|p_1p_2\cdots p_k \\ \omega(d)> h}} \frac{m(d)}{d}\right) \\ &= \sum_{d|p_1p_2\cdots p_k} \mu(d)\frac{m(d)}{d} + O\left(\sum_{d|p_1p_2\cdots p_k} \frac{m(d)}{d}u^{\omega(d)-h}\right) \\ &= \sum_{d|p_1p_2\cdots p_k} \mu(d)\frac{m(d)}{d} + O\left(u^{-h}\sum_{d|p_1p_2\cdots p_k} \frac{m(d)}{d}u^{\omega(d)}\right).\end{aligned}$$

Here the sums can be written as an Euler product, thus:

$$\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\le h}} \mu(d)\frac{m(d)}{d} =$$

$$= \prod_{p\in\mathcal{P}}\left(1-\frac{m(p)}{p}\right) + O\left(u^{-h}\prod_{p\in\mathcal{P}}\left(1+u\frac{m(p)}{p}\right)\right)$$

$$= \prod_{p\in\mathcal{P}}\left(1-\frac{m(p)}{p}\right) + O\left(u^{-h}\prod_{p\in\mathcal{P}}\left(1+\frac{m(p)}{p}\right)^u\right),$$

where $\mathcal{P}$ denotes the set of the primes $p_1, p_2, \ldots, p_k$.

Now we fix $u = h/\left(\sum_{p\in\mathcal{P}}\log\left(1+\frac{m(p)}{p}\right)\right)$ in order to reduce the error term and get

$$\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\le h}} \mu(d)\frac{m(d)}{d} = \prod_{p\in\mathcal{P}}\left(1-\frac{m(p)}{p}\right) + O\left(\frac{1}{h}\sum_{p\in\mathcal{P}}\frac{m(p)}{p}\right)^h.$$

Using this, (15.2) and (15.6) we get

$$\sum_{a\in\mathcal{A}}\sum_{p_1\nmid a, p_2\nmid a,\ldots,p_k\nmid a} 1 = X\prod_{p\in\mathcal{P}}\left(1-\frac{m(p)}{p}\right) + X\cdot O\left(\frac{1}{h}\sum_{p\in\mathcal{P}}\frac{m(p)}{p}\right)^h + O\left(\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\le h}} R_d\right) \tag{15.7}$$

if $u = h/\left(\sum_{p\in\mathcal{P}}\log\left(1+\frac{m(p)}{p}\right)\right) \ge 1$.

In the following we show two applications. First we estimate the number of primes less than or equal to x.

If P is a set of all primes less than y and $\mathcal{A} = \{1, 2, ..., x\}$, the right hand side of (15.7) gives an upper bound on the number of primes between y and x.

In (15.4) we see that we may take $m(d) = 1$ and $|R_d| \leq 1$. First we estimate the two error terms. Here we need Mertens theorems [4]. In the following estimates the sums are taken over the set of primes.

Lemma 15.3 (Mertens' first theorem)

$$\left| \sum_{p \leq n} \frac{\log p}{p} - \log n \right| \leq 2$$

for any $n \geq 2$.

Lemma 15.4 (Mertens' second theorem)

$$\lim_{n \to \infty} \left(\sum_{p \leq n} \frac{1}{p} - \log \log n - M \right) = 0.$$

Here M *is the Meissel-Mertens constant (see A077761). Even more precisely, it is true that the expression under the limet does not exceed in absolute value*

$$\frac{4}{\log(n+1)} + \frac{2}{n \log n}$$

for any $n \geq 2$.

Lemma 15.5 (Mertens' third theorem)

$$\lim_{n \to \infty} \log n \prod_{p \leq n} \left(1 - \frac{1}{p} \right) = e^{-\gamma} \approx 0.561459483566885,$$

where γ *is the Euler–Mascheroni constant (see A001620).*

Mertens' theorems are not proved here, but we note that the proofs of the first two theorems can be found, e.g., on the related Wikipedia page: link.

Let's return to estimating the number of primes between y and x. For this, we use (15.7), with a suitable choice of h.

In (15.7), the second error component can be estimated by y^t, and Mertens' theorems are used to estimate the other terms. (Remember that $m(d) = 1$). Then we get:

$$\pi(x) - \pi(y) \le x\frac{e^{-\gamma} + o(1)}{\log y} + x \cdot O(\frac{1}{h}\log\log y)^h + O(y^h).$$

If we are only interested in primes that do not exceed x, we may fix y by $y = x^{1/(2c)\log\log x}$ and $h = c\log\log x$ (thus we obtain a nearly optimal upper estimate in the inequality above), with a sufficiently large constant c. Then we get

$$\pi(x) = O(\frac{x\log\log x}{\log x}),$$

which is worse by a factor of $\log\log x$ than the sharpest estimate but much better than the trivial estimates.

Next we give an upper bound for the number of twin primes.

Let $\mathcal{P}$ again be the set of primes smaller than y, and define $\mathcal{A}$ by $\mathcal{A} = \{n(n+2) : \ n \in [y, x]\}$.

Note that if $p \mid n(n+2)$ for a prime $p \in \mathcal{P}$, then n and $n+2$ cannot be prime at the same time. Then we use the estimate in (15.7), where $m(2) = 1$ and $m(p) = 2$ if $p > 2$. We also have $|R_d| \le 2^{\omega(d)}$. As before, we get that

$$\pi_2(x) - \pi_2(y) \leq x\frac{c}{(\log y)^2} + xO(\frac{1}{h}\log\log y)^h + O((2y)^h),$$

where $\pi_2(x)$ denotes the twin prime numbers not exceeding x. Fix $h = c\log\log x$ and $y = x^{1/(2c)\log\lg x}$. Then we get

$$\pi_2(x) \leq O\left(\frac{x(\log\log x)^2}{(\log x)^2}\right).$$

(Here we also use $1 - \frac{2}{p} \leq e^{-2/p}$ and Mertens' theorems.)

Using this result and summation by parts, Brun proved that the sum $\sum_{p,p+2 \text{ primes}} \frac{1}{p} + \frac{1}{p+2}$ is convergent:

$$\begin{aligned}
\sum_{p,p+2 \text{ primes}} \frac{1}{p} + \frac{1}{p+2} &\ll \sum_{p,p+2 \text{ primes}} \frac{1}{p} \\
&\leq \sum_x \frac{\pi_2(x) - \pi_2(x-1)}{x} \\
&\leq \sum_x \pi_2(x)\left(\frac{1}{x} - \frac{1}{x+1}\right) \\
&\ll \sum_x \frac{\pi_2(x)}{x^2} \\
&\ll \sum_x \frac{(\log\log x)^2}{x(\log x)^2} \\
&\ll \infty.
\end{aligned}$$

The upper estimate given for the twin primes is $(\log\log x)^2$ worse than the expected value. By further developing the above "simple" Brun sieve, as Brun did, the factor $(\log\log x)^2$ can also be eliminated. This "complete" Brun sieve is much more complicated.

The basic idea in short: Our starting formula was

$$\sum_{\substack{d\mid p_1p_2\cdots p_k\\ \omega(d)\le 2t-1}} \mu(d)A_d \le S(\mathcal{A},\mathcal{P}) \le \sum_{\substack{d\mid p_1p_2\cdots p_k\\ \omega(d)\le 2t}} \mu(d)A_d,$$

where $S(\mathcal{A},\mathcal{P}) = \sum_{a\in\mathcal{A}}\sum_{p_1\nmid a, p_2\nmid a,\dots,p_k\nmid a} 1$. This can be written of the form

$$\sum_{d\mid p_1p_2\cdots p_k} \chi_1(d)\mu(d)A_d \le S(\mathcal{A},\mathcal{P}) \le \sum_{d\mid p_1p_2\cdots p_k} \chi_2(d)\mu(d)A_d, \tag{15.8}$$

where

$$\chi_1(d) = \begin{cases} +1 & \text{if } \omega(d)\le 2t-1,\\ 0 & \text{if } \omega(d) > 2t-1,\end{cases} \quad \chi_2(d) = \begin{cases} +1 & \text{if } \omega(d)\le 2t,\\ 0 & \text{if } \omega(d) > 2t.\end{cases} \tag{15.9}$$

The goal is to replace χ_1,χ_2 with other χ_1,χ_2 for which:

a) The functions χ_1,χ_2 still satisfy (15.8).

b) $\chi_1(1)=\chi_2(2)=1$.

c) $\chi_i(d)\in\{0,1\}$ for all $d \mid p_1p_2\cdots p_k$ and $i=1$ or $i=2$.

d) This χ_1,χ_2 gives a better estimate for $S(\mathcal{A},\mathcal{P})$.

Brun found such χ_1,χ_2, but his proof was extremely complicated. Here we present only one particularly important and general theorem that can be proven in this way.

Theorem 15.6 *Let $k\in\mathbb{N}$, $a_1,b_1,\dots,a_k,b_k\in\mathbb{Z}$ and $(a_i,b_i)=1$ for $i=1,2,\dots,k$. Moreover*

$$E \overset{\text{def}}{=} \prod_{i=1}^{k} a_i \prod_{1\le r<s\le k} (a_rb_s - a_sb_r) \neq 0,$$

$0 < \varepsilon < 1$, $y \in \mathbb{R}$, $2 \le y \le x$, $z \stackrel{\text{def}}{=} y^{\varepsilon}$,

$$\mathcal{A} \stackrel{\text{def}}{=} \{\prod_{i=1}^{k}(a_i n + b_1) : \ n \in \mathbb{N}, \ x - y < n \le x\}$$

and

$$\mathcal{P} \stackrel{\text{def}}{=} \{p : \ 0 < p \le z, \ p \text{ is a prime}\}.$$

Suppose that the congruence

$$\prod_{i=1}^{k}(a_i n + b_1) \equiv 0 \pmod{h}$$

has $m(p)$ *pieces of soultions. Then*

$$S(\mathcal{A}, \mathcal{P}) = \left|\{a : \ a \in \mathcal{A}, \ (a, \prod_{p \in \mathcal{P}} p) = 1\}\right|$$
$$\le c \left(\prod_{p|E, \ p \le y} \left(1 - \frac{1}{p}\right)^{m(p)-k}\right) \frac{y}{(\log y)^k},$$

where the constant c *depends only on* k *and* ε.

We do not prove the theorem. We present only two applications. In the first one, choose $k = 2, a_1 = 1, b_1 = 0, a_2 = 1, b_2 = 2, y = x, \varepsilon = 1/2$. Then we get:

Corollary 15.7

$$\pi_2(x) \stackrel{\text{def}}{=} \{p : \ 0 < p \le x, \ p, p+2 \text{ are primes}\} \ll \frac{x}{(\log x)^2}.$$

When we use $k = 2, a_1 = 1, b_1 = 0, a_2 = -1, b_2 = x, y = x, \varepsilon = 1/2$ in the next application, we obtain the following:

Corollary 15.8

$$|\{(p, q) : \ p + q = x, 0 < p, q \text{ primes}\}| \ll \prod_{p|x}\left(1 + \frac{1}{p}\right) \frac{x}{(\log x)^2}.$$

This last corollary will play an important role in the next chapter.

References

[1] V. Brun, *Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare*. Archiv for Mathematik og Naturvidenskab. B34 (8) (1915).

[2] V. Brun, *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ où *les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie*, Bulletin des Sciences Mathématiques. 43 100–104, 124–128 (1919).

[3] V. Brun, *Le crible d'Eratosthène et le théorème de Goldbach*, Christiania Vidensk.Selsk. Skr. 1920, Nr. 3.

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

[5] Planemath, Brun's pure sieve, link.

[6] A. Sárközy, Combinatorial Number theory, university lecture.

[7] Photo, Viggo Brun, link.

[8] Photo, Eratosthenes, link.

16 Partial results to Goldbach conjecture

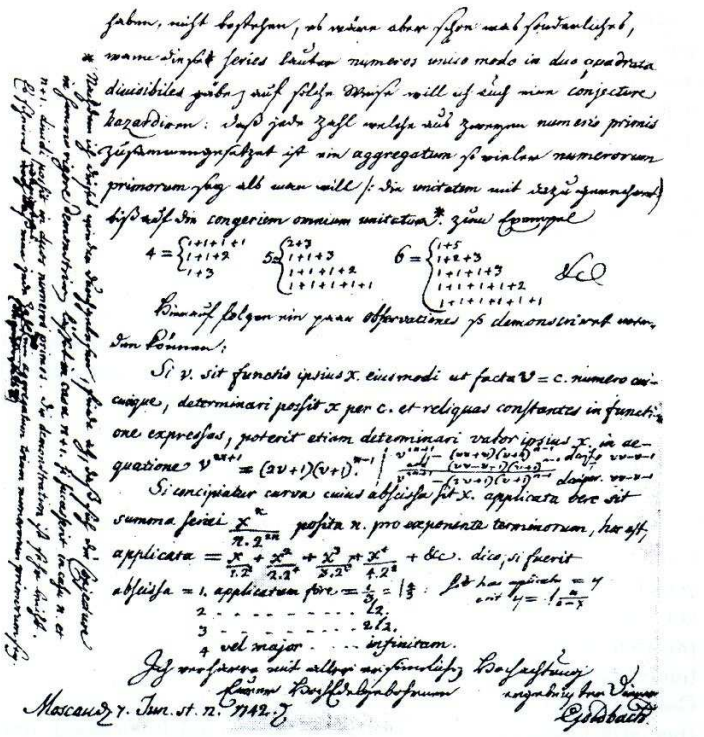
Christian Goldbach, a German mathematician, began studying sums of primes in a letter to Leonhard Euler on June 7, 1742, and proposed the famous Goldbach-conjecture. The following are modern versions of Goldbach's conjecture:

Conjecture 16.1 (strong Goldbach-conjecture) *Every even integer $n \geq 4$ can be written as the sum of two primes.*

Conjecture 16.2 (weak Goldbach-conjecture) *Every integer $n \geq 4$ can be written as the sum of at most 3 primes.*

It is worth noting that the weak conjecture is a consequence of the strong conjecture: If n is even, then the strong version of the conjecture states that n is the sum of two primes. If n is an odd number, then $n-3$ is an even number, hence $n-3$ is the sum of two primes, and n is the sum of three primes.

Below is a letter from Goldbach that he sent to Euler (although he did not formulate his famous conjecture in this letter, but it is certainly of historical interest).



You can read more about the Goldbach conjecture and related partial results on the related Wikipedia page [8]. We only mention here that the weak conjecture was proved by Vinogradov [7] for sufficiently large primes, and then by Helfgott [1], [2] for all numbers not smaller than 4, but his work is still under review.

Although Helfgott's result solved the weak Goldbach conjecture, historically there have been previous steps towards solving the conjecture. Perhaps the most famous of these is the result of Schnirelmann [5], [6] who proved that every number greater than 1 can be formed as the sum of at most $800\,000$ primes.

In this chapter, we describe this result based on [4].

Definition 16.3 *If $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$ is a set such that every element of $\mathbb{N}$ can be written as the sum of at most k elements of $\mathcal{A}$, then $\mathcal{A}$ is called as a basis of order k. If it is true only for large $n \in \mathbb{N}$ $(n \geq n_0)$, then $\mathcal{A}$ is called asymptotic basis of order k.*

Theorem 16.4 (Schnirelmann) *Primes are asymptotic basis. In other words there exists a k such that every large integer n can be written as the sum of at most k primes.*

The proof is based on the following two theorems, which are interesting in themselves.

Theorem 16.5

$$|\{(p,q) : \ p+q = x, 0 < p, q \text{ primes}\}| \ll \prod_{p|x} \left(1 + \frac{1}{p}\right) \frac{x}{(\log x)^2}.$$

This theorem is Corollary 15.8 of Chapter 15, which, although we did not prove it in full detail, the necessary tools were described.

Other important tools will be Schnirelmann's sumsets theorems. First we will prove the following:

Theorem 16.6 (Schnirelmann) *There exist $c > 0 \, \exists \, x_0$ such that if $x > x_0$, then at least cx pieces of integers n exist such that $n \in [1, x]$ and n can be written of the form $n = p + q$ where p and q are positive primes.*

Proof of Theorem 16.6. For $n \in [1, x]$ let $g(n)$ denote the number of solutions

$$p + q = n,$$

where p and q are positive primes. Moreover let

$$\mathcal{A} = \{n : n \leq x, g(n) > 0\}.$$

We need to prove

$$|\mathcal{A}| > cx.$$

Let

$$S = \sum_{n\in\mathcal{A}} g^2(n) \quad \left(= \sum_{n\le x} g^2(n)\right).$$

We will give a lower and an upper bound for S and comparing these two bounds we will get the statement of the theorem.

First we give a lawer bound for S.

Using the Cauchy–Schwarz inequality we get

$$S = \sum_{n\in A} g^2(n) \ge \frac{1}{|A|}\left(\sum_{n\in A} g(n)\right)^2.$$

Here

$$\sum_{n\in A} g(n) = \sum_{n=1}^{x} g(n) = \sum_{n=1}^{x}\sum_{p+q=n} 1 = \sum_{p+q\le x} 1$$
$$\ge \sum_{p,q\le \frac{x}{2}} 1 = \pi^2\left(\frac{x}{2}\right)$$

By the prime number theorem we have $\pi(x) \ge \frac{x}{3\log x}$ thus

$$\sum_{n\in A} g(n) > \left(\frac{x}{3\log x}\right)^2 = \frac{1}{9}\frac{x^2}{(\log x)^2}.$$

From this we get

$$S > \frac{1}{81}\frac{x^4}{(\log x)^4}\frac{1}{|\mathcal{A}|}.$$

Using Theorem 16.5 we get

$$g(n) \ll \prod_{p|n}\left(1+\frac{1}{p}\right)\cdot\frac{n}{(\log n)^2}.$$

Thus

$$S = \sum_{n \le x} g^2(n) \ll \sum_{n \le x} \prod_{p \mid n} \left(1 + \frac{1}{p}\right)^2 \cdot \frac{n^2}{(\log n)^4},$$

Since the function $\frac{n^2}{(\log n)^4}$ is monotone increasing for $n \in [1, x]$ we have $\frac{n^2}{(\log n)^4} \le \frac{x^2}{(\log x)^4}$. Thus

$$S \ll \frac{x^2}{(\log x)^4} \sum_{n \le x} \prod_{p \mid n} \left(1 + \frac{1}{p}\right)^2.$$

Here $\left(1 + \frac{1}{p}\right)^2 \ll \left(1 + \frac{2}{p}\right) e^{1/p^2}$ since

$$\begin{aligned} \frac{\left(1 + \frac{1}{p}\right)^2}{1 + \frac{2}{p}} &= \frac{1 + \frac{2}{p} + \frac{1}{p^2}}{1 + \frac{2}{p}} \\ &= 1 + \frac{1}{p^2} \cdot \frac{1}{1 + \frac{2}{p}} < 1 + \frac{1}{p^2} < e^{1/p^2}. \end{aligned}$$

Thus

$$S \ll \frac{x^2}{(\log x)^4} \sum_{n \le x} \prod_{p \mid n} \left(1 + \frac{2}{p}\right) e^{1/p^2}$$

Next we estimate $\prod_{p \mid n} \left(1 + \frac{2}{p}\right) e^{1/p^2}$:

$$\begin{aligned} \prod_{p \mid n} \left(1 + \frac{2}{p}\right) e^{1/p^2} &= e^{\sum_{p \mid n} \frac{1}{p^2}} \prod_{p \mid n} \left(1 + \frac{2}{p}\right) \\ &\ll \prod_{p \mid n} \left(1 + \frac{2}{p}\right) \\ &= 1 + \sum_{p_{i_1}, \ldots, p_{i_k} \mid n} \frac{2^k}{p_{i_1} \cdots p_{i_k}} \\ &= \sum_{\substack{d \mid n \\ |\mu(d)| = 1}} \frac{2^{\omega(d)}}{d}. \end{aligned}$$

Thus

$$\begin{aligned}
S &\ll \frac{x^2}{(\log x)^4} \sum_{n\le x} \sum_{\substack{d\mid n\\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d} \\
&\ll \frac{x^2}{(\log x)^4} \sum_{\substack{d\le x\\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d} \sum_{\substack{d\mid n\\ n\le x}} 1 \\
&\ll \frac{x^2}{(\log x)^4} \sum_{\substack{d\le x\\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d} \cdot \frac{x}{d} \\
&= \frac{x^3}{(\log x)^4} \sum_{\substack{d\le x\\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d^2} \\
&\ll \frac{x^3}{(\log x)^4} \sum_{d\le x} \frac{2^{\omega(d)}}{d^2} \ll \frac{x^3}{(\log x)^4} \sum_{d=1}^{\infty} \frac{2^{\omega(d)}}{d^2} \\
&= \frac{x^3}{(\log x)^4} \prod_p \left(1+\frac{2}{p^2}\right) = \frac{x^3}{(\log x)^4} \prod_p e^{2/p^2} \\
&\ll \frac{x^3}{(\log x)^4}.
\end{aligned}$$

Comparing the lawer and upper bound for S we get:

$$\begin{gathered}
\frac{x^4}{(\log x)^4} \cdot \frac{1}{|\mathcal{A}|} \ll S \ll \frac{x^3}{(\log x)^4} \\
\Downarrow \\
x \ll |\mathcal{A}|.
\end{gathered}$$

This completes the proof.

Next, a theorem would be needed, according to which, if a set has a positive density, then it is an asymptotic basis under certain conditions. However, before we introduce the asymptotic density, we return for a moment to the Schniralmann density. As a reminder:

The Schnirelmann density of a set $\mathcal{A}$ is defined by

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n}.$$

Next we will prove the following

Theorem 16.7 (Schnirelmann) *If $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$ and $\sigma(\mathcal{A}) > 0$, then $\mathcal{A} \cup \{0\}$ is a basis (of finite order).*

Proof of Theorem 16.7. Let $\mathcal{A}_0 = \mathcal{A} \cup \{0\}$. Then $\sigma(\mathcal{A}_0) > 0$. We will use the following lemma:

Lemma 16.8

$$\sigma(k\mathcal{A}_0) \geq 1 - \big(1 - \sigma(\mathcal{A}_0)\big)^k$$

Proof of Lemma 16.8 We prove by induction. For $k = 1$ the lemma is trivial. Suppose that we proved the lemma for $k = n$ and we would like to prove it for $k = n + 1$. Then by Theorem 14.4:

$$\begin{aligned}
\sigma\big((n+1)\mathcal{A}_0\big) &= \sigma(n\mathcal{A}_0 + \mathcal{A}_0) \\
&\geq \sigma(n\mathcal{A}_0) + \sigma(\mathcal{A}_0) - \sigma(n\mathcal{A}_0)\sigma(\mathcal{A}_0) \\
&= \sigma(\mathcal{A}_0) + \sigma(n\mathcal{A}_0)(1 - \sigma(\mathcal{A}_0)) \\
&\geq \sigma(\mathcal{A}_0) + \big(1 - (1 - \sigma(\mathcal{A}_0))^n\big)(1 - \sigma(\mathcal{A}_0)) \\
&= 1 - (1 - \sigma(\mathcal{A}))^{n+1}.
\end{aligned}$$

Next we return to the proof of Theorem 16.7. Since $\sigma(\mathcal{A}_0) > 0$ we have

$$\exists\, k_0 \quad (1 - \sigma(\mathcal{A}_0))^{k_0} < \frac{1}{2},$$

Then:

$$\sigma(k_0\mathcal{A}_0) \geq 1 - (1 - \sigma(\mathcal{A}_0))^k > 1 - \frac{1}{2} = \frac{1}{2}.$$

By using Theorem 14.5 for $\mathcal{A} = \mathcal{B} = k_0\mathcal{A}_0$ we get

$$\sigma(2k_0\mathcal{A}_0) = 1,$$

which means (see Proposition 14.3) $\mathcal{A}_0$ is a basis, and this completes the proof.

So far we proved that if we denote the set of primes by $\mathcal{P}$, then $P + P = 2P$ contains the positive proportion of natural numbers (see Theorem 16.6). Now we need a theorem such that if $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$ has positive density, then $\mathcal{A}$ is an asymptotic basis.

Asymptotic basis of order k: $\exists\, n_0$ such that

$$k\mathcal{A} = \mathcal{A} + \mathcal{A} + \ldots + \mathcal{A} \supseteq \{n_0, n_0 + 1, n_0 + 2, \ldots\}.$$

If $2P$ is an asymptotic basis of order k, then P is an asymptotic basis of order $2k$:

$$\underbrace{(p_1 + q_1) + (p_2 + q_2) + \ldots + (p_k + q_k)}_{\text{This is the sum of } 2k \text{ primes.}} = n, \quad n > n_0.$$

Unfortunately there is no theorem of type that

$$\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$$

has positive density, then $\mathcal{A}$ is an asymptotic basis.

Let's see some counterexamples.

$$\mathcal{A} = \{a : a \text{ is even}\}.$$

Then $\mathcal{A}$ has positive density, but $k\mathcal{A}$ contains only even numbers. Similarly, for

$$\mathcal{A} = \{a : 3 \mid a\}.$$

we have that $k\mathcal{A}$ contains only those integers which is divisible by 3. In order to avoid such constructions we need certain relative prime condition in $\mathcal{A}$.

The simplest is to require that $\mathcal{A}$ include two consecutive elements. First a definition follows.

Definition 16.9 *For $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$ let*

$$\mathcal{A}(n) \stackrel{\text{def}}{=\!=} \big|\{a : 0 < a \leq n,\ a \in \mathcal{A}\}\big|.$$

This function $\mathcal{A}(n)$ is called counting function. If $\mathcal{A}$ is an infinite sequence, then

$$\underline{d}(\mathcal{A}) \stackrel{\text{def}}{=\!=} \liminf_{n\to\infty} \frac{\mathcal{A}(n)}{n}$$

and

$$\overline{d}(\mathcal{A}) \stackrel{\text{def}}{=\!=} \limsup_{n\to\infty} \frac{\mathcal{A}(n)}{n}.$$

These are the asymptotic lower and upper density. If $\underline{d}(\mathcal{A}) = \overline{d}(\mathcal{A})$, this common value is the asymptotic density.

Theorem 16.10 (Schnirelmann) *If $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$ is such that*

a) $\underline{d}(\mathcal{A}) > 0$,

b) $\exists\ a_0$ *such that* $a_0, a_0 + 1 \in \mathcal{A}$,

then $\mathcal{A}$ is an asymptotic basis.

Corollary 16.11 *The prime numbers are asymptotic basis.*

In other words we get Theorem 16.4 as a consequence of a more general theorem.

Proof of Corollary 16.11 By Theorem 16.6 we have $\underline{d}(2P) > 0$. Clearly $4, 5 \in 2P$ since $4 = 2 + 2$ and $5 = 2 + 3$. Using Theorem 16.10 we get $2P$ is an asymptotic basis. But then P is also an asymptotic basis.

Proof of the Theorem 16.10. By the condition of the theorem we have there exists a_0 such that

$$a_0, a_0 + 1 \in \mathcal{A}.$$

Let

$$\mathcal{B} \stackrel{\text{def}}{=\!=} \{b : b \in \mathbb{N} \cup \{0\}, a_0 + b \in \mathcal{A}\},$$

Then

$$\underline{d}(\mathcal{B}) = \underline{d}(\mathcal{A}),$$
$$\{0, 1\} \in \mathcal{B}$$

Using Proposition 14.2 we get $\sigma(\mathcal{B}) > 0$. Now by Theorem 16.7 we have that $\mathcal{B}$ is a basis of finite order.

Let k denote the order of the basis $\mathcal{B}$. Then $\mathcal{A}$ is an asymptotic basis of order k. Indeed, suppose that $n > ka_0$. Write $n = ka_0 + x$, since $\mathcal{B}$ is a basis of order k, there exist $b_1, b_2, \ldots, b_k \in \mathcal{B}$ such that

$$b_1 + b_2 + \cdots + b_k = x.$$

Then

$$(a_0 + b_1) + (a_0 + b_2) + \cdots + (a_0 + b_k) = ka_0 + x = n.$$

By the definition of $\mathcal{B}$, here we have $a_0 + b_i \in \mathcal{A}$, so n can be written as the sum of k pieces of integers from $\mathcal{A}$. This is true for every positive integer $n > ka_0$, thus $\mathcal{A}$ is an asymptotic basis.

Following Schnirelmann's proof, we may give an upper estimate for the exact applied constants, and in this way we also get that every

natural number greater than 1 can be written as the sum of at most $800\,000$ primes.

Mann's theorem (see Theorem 14.6) is a fundamental theorem in combinatorial number theory.

It's a beautiful theorem, but it employs Schnirelmann density, which is a bit artificial definition.

It would be useful to know a theorem that makes use of asymptotic density.

This is Kneser's theorem [3], a very nice theorem with many applications:

Theorem 16.12 (Kneser) *If* $\mathcal{A}_0, \ldots, \mathcal{A}_k \subseteq \mathbb{N} \cup \{0\}$, *then*

$$d(\mathcal{A}_0 + \ldots + \mathcal{A}_k) \geq \liminf \frac{\mathcal{A}_0(n) + \ldots + \mathcal{A}_k(n)}{n}$$
$$\left(\geq \underline{d}(\mathcal{A}_0) + \ldots + \underline{d}(\mathcal{A}_k)\right)$$

or $\exists\, g, a_0, \ldots, a_k \in \mathbb{N}$ *such that:*

1) *Every* $\mathcal{A}_i$ *is contained in* $\mathcal{A}_i'$ *which is a union of* a_i *pieces of* mod g *residue classes.*

2) *There are finitely many elements of* $\mathcal{A}_0' + \ldots + \mathcal{A}_k'$ *which is not in* $\mathcal{A}_0 + \ldots + \mathcal{A}_k$.

3) $d(\mathcal{A}_0 + \ldots + \mathcal{A}_k) \geq \dfrac{a_0 + \ldots + a_k - k}{g}$.

The proof is extremely complicated, so we omit it in this note.

References

[1] H. A. Helfgott, *Major arcs for Goldbach's theorem*. arXiv:1305.2897 [math.NT] (2013).

[2] H. A. Helfgott, *Minor arcs for Goldbach's problem*. arXiv:1205.5252 [math.NT] (2012).

[3] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*. Math. Z. (in German). 58 (1953), 459–484.

[4] A. Sárközy, Combinatorial Number theory, university lecture.

[5] L. G. Schnirelmann, *On the additive properties of numbers*, first published in "Proceedings of the Don Polytechnic Institute in Novocherkassk" (in Russian), vol 14 (1930), pp. 3–27, and reprinted in "Uspekhi Matematicheskikh Nauk" (in Russian), 1939, no. 6, 9–25.

[6] L. G. Schnirelmann, First published as "Über additive Eigenschaften von Zahlen" in "Mathematische Annalen" (in German), vol. 107 (1933), 649–690, and reprinted as "On the additive properties of numbers" in "Uspekhi Matematicheskikh Nauk" (in Russian), 1940, no. 7, 7–46.

[7] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, 1954, Translated, revised and annotated by K. F. Roth and Anne Davenport.

[8] Wikipedia, Goldbach's conjecture, link

[9] Photo, Christian Goldbach, link.

[10] Photo, *Letter from Goldbach to Euler*, link.

17 Multiplicative problems

As we have seen, there are many theorems in combinatorial number theory with quite different nature. Based on [10] we study problems which have multiplicative nature in some sense.

First we study sets A where the sumset $2A = A + A$ does not increase the size much.

It is easy to give such a set A: e.g., arithmetic progressions are good examples of such a set. But are they the only ones? In 1962, Freiman solved this question.

First, let us see a new definition.

Definition 17.1 *Let $k_1, \dots, k_d \in \mathbb{N}$, $k_1, \dots, k_d \geq 2$, $u, v_1, \dots, v_d \in \mathbb{Z}$ and*

$$\mathcal{M} \stackrel{\text{def}}{=} \left\{ u + \sum_{i=1}^{d} x_i v_i : x_i \in \{1, \dots, k_i\},\ i = 1, \dots, d \right\}.$$

Then $\mathcal{M}$ is called as a generalized arithmetic progression of dimension d.

Freiman proved the following:

Theorem 17.2 (Freiman) *For every $\alpha > 1$ there exists a $c_1 = c_1(\alpha)$ and $c_2 = c_2(\alpha)$ such that if $|2\mathcal{A}| < \alpha|\mathcal{A}|$, then there exists a generalized arithmetic progression of dimension d such that $d < c_1$, $\mathcal{A} \subseteq \mathcal{M}$ and $|\mathcal{M}| < c_2|\mathcal{A}|$.*

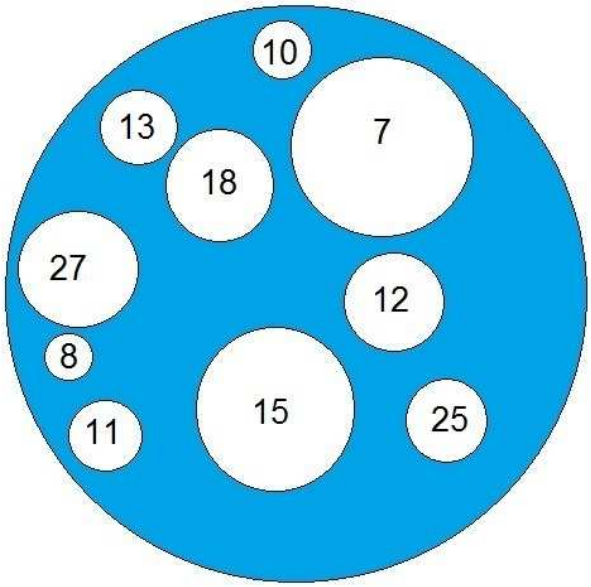
Freiman's original proof used exponential sums and was rather complicated [4], [5].

Later Ruzsa [8] gave another proof based on graph theory and sumset sum's results using the famous Ruzsa-Plünnecke ineqality.

I strongly recommend studying Imre Ruzsa's lecture notes Sum-sets and Structure [9] for those who are interested.

In January 1935, Behrend [1] began to study sets in which no element divides another:

Definition 17.3 *A set $\mathcal{A} \subseteq \mathbb{N}$ is primitive if there is no $a, a' \in \mathcal{A}$, $a \neq a'$ such that $a \mid a'$.*



Question. How dense can be a primitive set?

The answer strongly depends on that what kind of density we use.

A pleasant exercise for the reader is to find a proof of the following theorem:

Theorem 17.4

$$\max_{\substack{\mathcal{A}\subseteq\{1,\dots,2N\},\\ \mathcal{A} \text{ is primitive}}} |\mathcal{A}| = N.$$

The previous theorem was stated as a finite question. The question is more interesting for infinite sets. First we introduce a new type of density:

Definition 17.5 *If $\mathcal{A} \subseteq \mathbb{N}$ and $\mathcal{A}$ is an infinite sequence, we define the logarithmic lower density by*

$$\underline{\delta}(\mathcal{A}) = \liminf \frac{\sum_{a \in A} \frac{1}{a}}{\log N},$$

and the logarithmic upper density is defined by

$$\overline{\delta}(\mathcal{A}) = \limsup \frac{\sum_{a \in A} \frac{1}{a}}{\log N}.$$

If they are equal $\left(\underline{\delta}(\mathcal{A}) = \overline{\delta}(\mathcal{A})\right)$, then $\delta(\mathcal{A}) = \underline{\delta}(\mathcal{A}) = \overline{\delta}(\mathcal{A})$ is the logarithmic density.

Here we have

$$\underline{d}(\mathcal{A}) \leq \underline{\delta}(\mathcal{A}) \leq \overline{\delta}(\mathcal{A}) \leq \overline{d}(A).$$

Behrend [1] was able to prove the following:

Theorem 17.6 (Behrend) *If $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ and $\mathcal{A}$ is primitive, then*

$$\sum_{a \in A} \frac{1}{a} < c \frac{\log N}{\sqrt{\log \log N}} \tag{17.1}$$

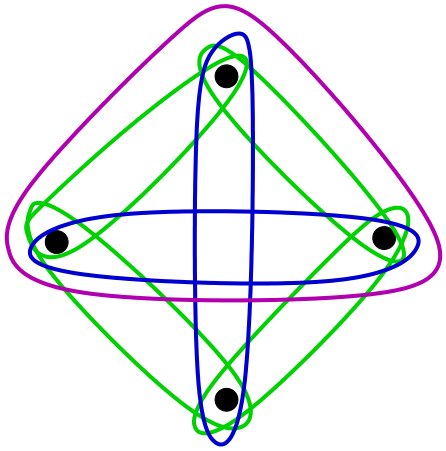
So the logarithmic density of a set A is 0. (This is not true for the normal density, this can be around $1/2$.)

An interesting feature of the proof is that it is not enough to use extremal graph theory, but extremal set theory is needed. One of the main tools is Sperner's theorem [11], which we will not prove here.

Lemma 17.7 (Sperner's theorem) *If S is a finite set, $|S| = r$, $R_1, \dots, R_t$ are subsets of S, and*

$$t > \binom{r}{[r/2]}, \tag{17.2}$$

then there are R_i and R_j subsets of S such that $i \neq j$ and $R_i \subseteq R_j$.



In other words, if a sufficient number (in the (17.2) meaning) of subsets of a given set are considered, there are two of them that have an inclusion relation.

Note that the bound in (17.2) is the best possible: There is no inclusion relation between subsets of S with $[r/2]$ elements.

We will not prove Sperner's theorem, we will use it only.

To prove Behrend's theorem, assume that c is large enough, and $N > N_0$, $\mathcal{A} \subset \{1, 2, 3, \dots, N\}$, moreover

$$\sum_{a \in \mathcal{A}} \frac{1}{a} \geq c \frac{\log N}{\log \log N}.$$

We will prove that there exist $a, a' \in \mathcal{A}$ for which $a < a'$ and $a \mid a'$.

We begin with a reduction step, in which we compress the problem into sequences of squarefree numbers. Every $a \in \mathcal{A}$ can be written as a square number multiplied by a squarefree number.

$$a = m_a^2 q_a, \quad m_a \in \mathbb{N}, \quad |\mu(q_a)| = 1.$$

Then by (17.1) we have

$$c\frac{\log N}{\sqrt{\log\log N}} \leq \sum_{a\in\mathcal{A}} \frac{1}{a} = \sum_{a\in\mathcal{A}} \frac{1}{m_a^2 q_a}$$
$$= \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{\substack{a:\ a\in\mathcal{A} \\ m_a = m}} \frac{1}{q_a}. \tag{17.3}$$

Here we denote the inner sum by $S(m)$:

$$S(m) = \sum_{\substack{a:\ a\in\mathcal{A} \\ m_a = m}} \frac{1}{q_a}.$$

We state that there exists an $m \in \mathbb{N}$ such that

$$S(m) > \frac{c}{2} \cdot \frac{\log N}{\sqrt{\log\log N}}. \tag{17.4}$$

We confirm this indirectly. If there is no such m, then $\forall m \in \mathbb{N}$ we have

$$S(m) \leq \frac{c}{2} \cdot \frac{\log N}{\sqrt{\log\log N}},$$

and then by (17.3) we get

$$c\frac{\log N}{\sqrt{\log\log N}} \leq \sum_{m=1}^{2} \frac{1}{m^2} \frac{c}{2} \frac{\log N}{\sqrt{\log\log N}}$$
$$= \frac{\pi^2}{6} \cdot \frac{c}{2} \frac{\log N}{\sqrt{\log\log N}} < c\frac{\log N}{\sqrt{\log\log N}},$$

which is contradiction. So there really exists m satisfying (17.4).

Let us now fix one such m and let

$$\mathcal{A}(m) = \{a : \ a \in \mathcal{A}, \ m_a = m\}$$
$$Q(m) = \{q : \ m^2 q \in \mathcal{A}(m)\}.$$

So $Q(m)$ is the set of q such that $m^2 q \in \mathcal{A}$, where q is a square-free number. Then in case of

$$q, q' \in \mathcal{Q}(m), \quad q < q', \quad q \mid q', \tag{17.5}$$

we clearly have

$$m^2 q, m^2 q' \in \mathcal{A}(m) \subset \mathcal{A}, \ m^2 q < m^2 q', \ m^2 q \mid m^2 q',$$

so there is a divisibility relation in $\mathcal{A}$ (i.e., $a = m^2 q, a' = m^2 q'$). As a result, proving the existence of q, q' satisfying (17.5) suffices.

Furthermore for $q \in \mathcal{Q}(m)$ we have $m^2 q \in \mathcal{A}(m) \subset A$, and thus

$$m^2 q \leq N,$$

whence

$$q \leq N.$$

Finally for $q \in Q(m)$ we have $|\mu(q)| = 1$.

Thus, by writing $Q = Q(m)$, the following conditions hold:

$$Q \subset \{1, 2, 3, \ldots, N\},$$
$$S(m) = \sum_{q \in Q} \frac{1}{q} > \frac{c}{2} \cdot \frac{\log N}{\sqrt{\log \log N}}, \tag{17.6}$$
$$\forall q \in Q \text{ is squarefree.}$$

Thus in order to prove (17.5), it suffices to prove that if a sequence Q a has the above three properties, then

$$\exists q, q' \in Q,\ q < q',\ q \mid q'. \tag{17.7}$$

This really reduced the problem to squarefree numbers.

Now let us introduce the following notation: for $n \in \mathbb{N}$ let

$$d_Q(n) \stackrel{\text{def}}{=} |\{q :\ q \in Q,\ q \mid n\}|$$

(i.e., $d_Q(n)$ counts how many divisors n has in Q.)

We will use the following:

Lemma 17.8 *For all $N > N_0$ there exists $n \in \mathbb{N}$ such that*

1. $n \leq N$
2. $d(n) > \frac{\log N}{\log\log N}$
3. $d_Q(n) > \frac{d(n)}{\sqrt{\log d(n)}}$

Proof of the Lemma 17.8. We prove it indirectly: suppose that there is no such n. Then for $\forall n \leq N$ we have

$$d(n) \leq \frac{\log N}{\log\log N}$$

or we have

$$d(n) > \frac{\log N}{\log\log N}.$$

However, in the latter case, property 3 is not fulfilled so

$$d_Q(n) \leq \frac{d(n)}{\sqrt{\log d(n)}} < \frac{d(n)}{\sqrt{\log \frac{\log N}{\log\log N}}}$$

$$< 2\frac{d(n)}{\sqrt{\log\log N}}.$$

Thus:

$$\sum_{n=1}^{N} d_Q(n) < \sum_{\substack{n\le N \\ d(n)\le \frac{\log N}{\log\log N}}} d_Q(n) + \sum_{\substack{n\le N \\ d(n)<2\frac{d(n)}{\sqrt{\log\log N}}}} d_Q(n)$$
$$< \sum_{n\le N} \frac{\log N}{\log\log N} + \frac{2}{\sqrt{\log\log N}} \sum_{n\le N} d(n).$$

Now

$$\sum_{n\le N} d(n) = \sum_{n\le N}\sum_{d|n} 1 = \sum_{d\le N}\sum_{\substack{n\le N \\ d|N}}$$
$$< \sum_{d\le N} \frac{N}{d} < 2N\log N.$$

Here:

$$\sum_{n=1}^{N} d_Q(n) < N\frac{\log N}{\log\log N} + \frac{2}{\sqrt{\log\log N}} 2N\log N$$
$$< 5N\frac{\log N}{\sqrt{\log\log N}}. \tag{17.8}$$

On the other hand by (17.6):

$$\sum_{n=1}^{N} d_Q(n) = \sum_{n=1}^{N}\sum_{\substack{q|n \\ q\in Q}} 1 = \sum_{q\in Q}\sum_{\substack{n\le N \\ q|n}} 1$$
$$= \sum_{q\in Q}\left[\frac{N}{q}\right] > \sum_{q\in Q}\frac{1}{2}\frac{N}{q} = \frac{1}{2}N\sum_{q\in Q}\frac{1}{q}$$
$$> \frac{1}{2}N\cdot\frac{c}{2}\frac{\log N}{\sqrt{\log\log N}}$$
$$= \frac{c}{4}N\frac{\log N}{\sqrt{\log\log N}}.$$

If $\frac{c}{4} \geq 5$, i.e., for example $c = 20$, then this contradicts to (17.8), and thus we proved the lemma (i.e., the existence of n with properties 1, 2 and 3).

Let us therefore consider a n with properties 1, 2, 3, denote the product of various prime divisors of n by v and $\frac{n}{v}$ by u, i.e.

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \left(p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}\right)(p_1 \cdots p_r) = uv,$$

where $u \in \mathbb{N}$, $|\mu(v)| = 1$. Clearly if q is a squarefree number, then $q \mid n$ if and only if $q \mid v$. Thus

$$d_Q(n) = d_Q(v). \tag{17.9}$$

Since obviously $d(n) > d(v)$, therefore from properties 2 and 3 and from (17.9) follows that

$$d_Q(n) = d_Q(v) > \frac{d(n)}{\sqrt{\log d(n)}}.$$

But since $\frac{x}{\sqrt{\log x}}$ is monoton, thus

$$d_Q(n) = d_Q(v) > \frac{d(v)}{\sqrt{\log d(v)}} \tag{17.10}$$

is also true.

Since $v = p_1 p_2 \ldots p_r$ we have $d(v) = 2^r$. Writing this to (17.10) we get

$$d_Q(v) > \frac{2^r}{\sqrt{\log 2^r}} = \frac{1}{\sqrt{\log 2}} \frac{2^r}{\sqrt{r}} > \frac{2^r}{\sqrt{r}} > \binom{r}{[r/2]}.$$

Here, the last inequality is a consequence of Stirling's formula.

Now let v have the following divisors in Q: $q_1, q_2, \ldots, q_t$. Then

$$t = d_Q(v) > \binom{r}{[r/2]} \tag{17.11}$$

Denote the set of prime divisors of a squarefree number h by $P(h)$. Then:

Proposition 17.9 *For squarefree numbers, $h \mid h'$ holds if and only if if $P(h) \subset P(h')$.*

With this principle, the examination of divisibility relations can be changed to inclusion relations, that is, it can be reduced to combinatorics, specifically to Sperner's theorem. This is the proof basic idea.

Then by $q_1, \dots, q_t \mid v$ we have

$$P(q_1), P(q_2), \dots, P(q_t) \subset P(v), \tag{17.12}$$

but here for the number of subsets $P(q_i)$ which is t by (17.11) we get

$$t > \binom{r}{[r/2]}, \tag{17.13}$$

where $r = \omega(v) = |P(v)|$. Then by (17.12) and (17.13), Sperner's theorem is applicable with $S, R_1, \dots, R_t$ in place of $P(v), P(q_1), \dots, P(q_t)$. Applying this theorem, we get that

$$\exists i, j,\ i \neq j, \text{ such that } P(q_i) \subset P(q_j).$$

By the proposition, it follows that $q_i \mid q_j$, so indeed there is a divisibility relation in Q, i.e., the desired conclusion is fulfilled.

According to Behrend's theorem, if $\mathcal{A}$ is primitive and $\mathcal{A} \subset \{1, 2, \dots, N\}$, then

$$\sum_{a \in \mathcal{A}} \frac{1}{a} < c \frac{\log N}{\log \log N}.$$

Question. How far is this from the best possible?

Pillai [7] in 1939 proved for $N > N_0(\varepsilon)$ the existence of a primitive sequence $\mathcal{A} \subset \{1, 2, \ldots, N\}$, such that

$$\sum_{a \in \mathcal{A}} \frac{1}{a} > \left(\frac{1}{2\pi} - \varepsilon\right) \frac{\log N}{\log\log N}.$$

The set $\mathcal{A}$ given during the proof was the following:

$$\mathcal{A} = \{a : \ a \leq N, \ \Omega(a) = [\log\log N]\}.$$

It is easy to see that this sequence is primitive, since $a \neq a'$, $a \mid a'$ for $\Omega(a) < \Omega(a')$.

Erdős, Sárközy and Szemerédi [3] also proved that in Behrend's theorem, the constant c can be taken as $\frac{1}{\sqrt{2\pi}} + \varepsilon$.

Finally, we note that Erdős [2] gave an ingenious proof of the following theorem:

Theorem 17.10 *There exists a constant c that for every primitive set $\mathcal{A} \subset \mathbb{N}^+$ we have*

$$\sum_{a \in \mathcal{A}} \frac{1}{a \log a} < c$$

.

In fact, Erdős conjectured that

$$\sum_{a \in \mathcal{A}} \frac{1}{a \log a} < \sum_{p \text{ prime}} \frac{1}{p \log p}.$$

In 2022, Jared Duker Lichtman [6] solved this conjecture absolutely unexpectedly. His paper is currently being reviewed.

Those who are interested in further Erdős's conjectures can find more open problems in the following Wikipedia page: link.

References

[1] F. Behrend, *On sequences of numbers not divisible one by another*, Journal of the London Mathematical Society, s1-10 (1): 42–44,

[2] P. Erdős, *Note on sequences of integers no one of which is divisible by any other*, J. London Math. Soc.10 (1935), 126–128.

[3] P. Erdős, A. Sárközy, E. Szemerédi, *On divisibility properties of sequences of integers*, Collect Math.Soc. J. Bolyai 2 (1970) 35–49.

[4] G. A. Freiman, *Addition of finite sets*, Soviet Mathematics. Doklady. 5 (1964), 1366–1370.

[5] G. A. Freiman, *Foundations of a Structural Theory of Set Addition* (in Russian), Kazan: Kazan Gos. Ped. Inst. (1966) p. 140.

[6] Jared Duker Lichtman, A proof of the Erdős primitive set conjecture, arXiv:2202.02384, link.

[7] S. Pillai, *On numbers which are not multiples of any other in the set*, Proc. Indian Acad. Sci. A10 (1939) 392–394.

[8] I. Z. Ruzsa, *Generalized arithmetical progressions and sumsets*, Acta Mathematica Hungarica. 65 (4) (1994) 379–388.

[9] I. Z. Ruzsa, Sumsets and Structure, link.

[10] A. Sárközy, Combinatorial Number theory, university lecture.

[11] E. Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Mathematische Zeitschrift (in German), 27 (1) (1928) 544–548.

[12] Figure, Primitive set, home-made.

[13] Figure, Sperner's theorem, home-made.