SUMMER SCHOOL IN MATHEMATICS

EÖTVÖS LORÁND UNIVERSITY

BUDAPEST, HUNGARY

27. June − 1. July 2022

Topics in Number Theory: Ancient Problems, Recent Results

Róbert Freud (ELTE):
A problem of Erdős and two proofs from "The Book"

Gyula Károlyi (ELTE − Rényi Institute):
Some applications of the Combinatorial Nullstellensatz

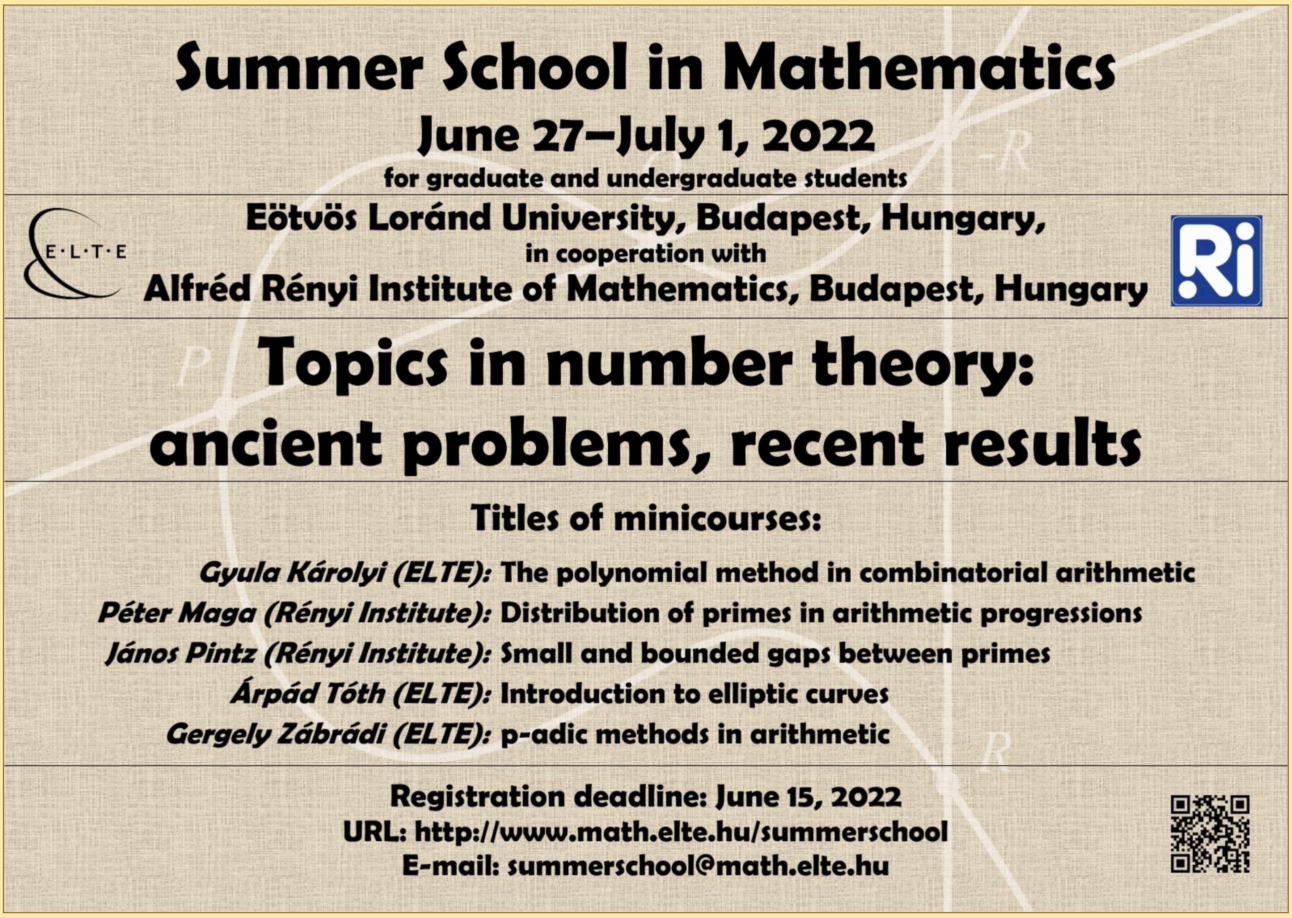
Péter Maga (Rényi Institute):
Distribution of primes in arithmetic progressions

János Pintz (Rényi Institute):
Gaps between consecutive primes

Árpád Tóth (ELTE):
Elliptic curves (minicourse)

Gergely Zábrádi (ELTE):
p-adic methods in arithmetic

Budapest, July 2022



Summer School in Mathematics

June 27–July 1, 2022

for graduate and undergraduate students

Eötvös Loránd University, Budapest, Hungary,
in cooperation with
Alfréd Rényi Institute of Mathematics, Budapest, Hungary

Topics in number theory: ancient problems, recent results

Titles of minicourses:

Gyula Károlyi (ELTE): **The polynomial method in combinatorial arithmetic**
Péter Maga (Rényi Institute): **Distribution of primes in arithmetic progressions**
János Pintz (Rényi Institute): **Small and bounded gaps between primes**
Árpád Tóth (ELTE): **Introduction to elliptic curves**
Gergely Zábrádi (ELTE): **p-adic methods in arithmetic**

Registration deadline: June 15, 2022
URL: http://www.math.elte.hu/summerschool
E-mail: summerschool@math.elte.hu

SSM-2022	Topics in number theory: ancient problems, recent results				ELTE, BUDAPEST
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
09.00 - 10.00	Péter Maga: *Distribution of primes in arithmetic progressions* *9.00-10.30*	Árpád Tóth: *Introduction to elliptic curves* *9.00-10.30*	Péter Maga: *Distribution of primes in arithmetic progressions* *9.00-10.30*	Gergely Zábrádi: *p-adic methods in arithmetic* *9.00-10.30*	Árpád Tóth: *Introduction to elliptc curves* *9.00-10.30*
10.00 - 11.00	COFFEE	COFFEE	COFFEE	COFFEE	COFFEE
11.00 - 12.00	Árpád Tóth: *Introduction to elliptic curves* *11.00-12.30*	Gergely Zábrádi: *p-adic methods in arithmetic* *11.00-12.30*	János Pintz: *Small and bounded gaps between primes* *11.00-12.30*	János Pintz: *Small and bounded gaps between primes* *11.00-12.30*	Róbert Freud: *A problem of Erdős and two proofs from "The Book"* *11.00-12.30*
12.00 - 13.00	LUNCH BREAK	LUNCH BREAK	LUNCH BREAK	LUNCH BREAK	LUNCH BREAK
13.00 - 14.00					
14.00 - 15.00	Gergely Zábrádi: *p-adic methods in arithmetic* *14.00-15.30*	Péter Maga: *Distribution of primes in arithmetic progressions* *14.00-15.30*	CAVE TOUR / BICYCLE TOUR	Árpád Tóth: *Introduction to elliptic curves (practice)* *14.00-15.30*	János Pintz: *Small and bounded gaps between primes* *14.00-15.30*
15.00 - 16.00	Pizza party				
16.00 - 17.00					
17.00 - 18.00					

CONTENTS

LIST OF REGISTERED PARTICIPANTS

1. **Anderlik, Csaba** – Eötvös Loránd University, Budapest (*Hungary*)
2. **Barabás, Eszter** – Eötvös Loránd University, Budapest (*Hungary*)
3. **Barnes, Douglas** – Trinity College, Cambridge University (*UK*)
4. **Eideme, Bentley** – Belgian Université Libre de Bruxelles (ULB) (*Belgium*)
5. **Földesi, András** – Eötvös Loránd University, Budapest (*Hungary*)
6. **Führer, Jakob** – University of Technology Graz (*Austria*)
7. **Gupta, Divij** – Brandeis University, Waltham, MA (*USA*)
8. **He, Chenfeng** – Budapest University of Technology and Economics (*Hungary*)
9. **Horváth, Balázs** – Eötvös Loránd University, Budapest (*Hungary*)
10. **Kouider, Fatna** – Eötvös Loránd University, Budapest (*Hungary*)
11. **Kövér, Blanka** – Eötvös Loránd University, Budapest (*Hungary*)
12. **Krásenský, Jakub** – Charles University, Prague (*Czech Republic*)
13. **Liguori, Maurizio** – Universit degli Studi di Salerno (*Italy*)
14. **Maini, Elena** – University of Florence (*Italy*)
15. **Marques, Ricardo** – Universidade do Porto (*Portugal*)
16. **Martin, Johannes** – Kopernikus-Gymnasium NDK (*Germany*)
17. **Mecacci, Niccol** – University of Florence (*Italy*)
18. **Mogyorsi, Bálint** – Eötvös Loránd University, Budapest (*Hungary*)
19. **Murata, So** – Budapest University of Technology and Economics (*Hungary*)
20. **Nuti, Valentina** – University of Florence (*Italy*)
21. **Pálffy, Patrik** – Eötvös Loránd University, Budapest (*Hungary*)
22. **Pálsson, Breki** – Sorbonne Université (*France*)
23. **Perea, Sinuhe** – King's College London (*UK*)
24. **Poulsen, Karl-Emil Bruhn** – Aarhus University (*Denmark*)
25. **Raunjak, Christoph** – University of Graz (*Austria*)
26. **Robustelli Della Cuna, Andrea** – University of Trieste (*Italy*)
27. **Sciammacca, Francesco** – University of Florence (*Italy*)
28. **Seress, Dániel** – Eötvös Loránd University, Budapest (*Hungary*)
29. **Sokvári, Olivér** – Eötvös Loránd University, Budapest (*Hungary*)
30. **Treaviño, Enrique** – Lake Forest College, IL (*USA*)
31. **Wurzinger, Lena** – TU Graz (*Austria*)
32. **Zheng, Danlei** – University of Amsterdam (*Netherlands*)
33. **Zhong, Yuchen** – Chinese University of Hong Kong (*China*)

PREFACE

In 2013 the Institute of Mathematics at Eötvös Loránd Universty in Budapest, Hungary, launched a series of international summer schools, aimed at senior undergraduate and at graduate (master's and PhD) students in mathematics. The format of the school starting from the second year was a one week long meeting with several series of lectures and some practice classes, usually concentrating on one featured topic (general discrete mathematics, algorithms, graph limits, algebraic geometry and topology etc.) One of the schools was built around the work of Paul Erdős, while another event was meant to introduce various topics through problem solving. A large portion of related materials of these schools can be found at the archives of the website of the series:

`http://www.math.elte.hu/summerschool/?page=download`

The COVID pandemic made it impossible to organize the school in 2020 and 2021, however the introduction of vaccines and the more relaxed travelling environment opened the possibility to organize the 8th such summer school in 2022 between June 27 and July 1. In view of the uncertainties caused by the still ongoing pandemic and the new source of danger coming from the war in the neighborhood, the organizers were quite happy with the response of the student community: there were 33 registered participants coming from 19 institutions in 13 countries. If we look at the home countries of participants, this latter number climbs even higher.

The title of the school was *Topics in number theory: ancient problems, recent results.* Thus the central topic of the school was one of the oldest and most beautiful areas of mathematics (as the famous saying of Gauss claims, "the queen of mathematics") yet it presented recent techniques and also very new developements in the subject. Originally five minicourses were planned, and the lecturers were professors of Eötvös Loránd Universty and the Rényi Mathematical Institute: Gyula Károlyi, Péter Maga, János Pintz, Árpád Tóth and Gergely Zábrádi. Unfortunately Prof. Károlyi had to cancel his lectures so in the last minute Prof. Róbert Freud of Eötvös Loránd University was asked to give a talk on a topic in additive number theory. (The talk was finally presented online, due to the sudden COVID infection of Prof. Freud. Special thanks go to him for giving his talk despite these circumstances!) The series of lectures consisted of three 90 minutes talks with an additional practice class for the lecture series of Prof. Tóth.

Written course notes were distributed to the participants for most lectures, either before or after the lectures. The present booklet is a somewhat brushed up version of these notes, put together into one volume. (Please, note that Prof. Károlyi – whose series of talks had to be cancelled – made the notes of his planned minicourse available for this collection.) These notes can be downloaded from the same website as the notes of the previous schools.

We wish to thank Eötvös Loránd University and the Alfréd Rényi Mathematical Institute for financial support.

We would also like to express our gratitude to all lecturers and contributors of this volume but also to the audience without whose active participation the summer school would have been far less successful.

Budapest, July 20, 2022

István Ágoston
on behalf of the organizers

1/12

A FAVORITE PROBLEM OF ERDŐS: ALL SUMS ARE DISTINCT

Róbert Freud

(SLIDES OF PRESENTATION)

2/12

We assume that the 2^k sums formed of the k positive integers $a_1 < a_2 < \ldots < a_k \leq n$ are distinct. What is the maximum of k (as a function of n)?

The powers of two work, so $\max k \geq 1 + \lfloor \log_2 n \rfloor$.

Upper bound: Each of the 2^k distinct sums are in the interval $[0, nk-1]$, so $2^k \leq nk$.

Taking the logarithm: $k \leq \log_2 n + \log_2 k$ (*).

$k \leq n$ yields $\log_2 k \leq \log_2 n$, so (*) implies $k \leq 2 \log_2 n$ (**).

Taking the logarithm of (**) gives $\log_2 k \leq 1 + \log_2 \log_2 n$, so plugging back into (*) we get $k \leq \log_2 n + \log_2 \log_2 n + 1$.

The current best results are:

$$2 + \lfloor \log_2 n \rfloor \leq \max k \leq \log_2 n + (\log_2 \log_2 n)/2 + 2.$$

Erdős, \$500: Is $\max k - \log_2 n$ bounded?

3/12

To get the improved upper bound, we use that the sums are not uniformly distributed in the interval $[0, nk-1]$ but occur denser around their average.

We shall apply Chebyshev's inequality stating that a random variable assumes values close to its expectation with high probability where closeness is measured by the standard deviation.

Precisely: If the random variable ξ has expectation E and standard deviation D, then $P(|\xi - E| > cD) < 1/c^2$ for any $c > 0$.

Let ξ be the random variable assuming each of the 2^k sums with equal probability $1/2^k$.

4/12

Thus ξ puts each number a_j into the sum independently with probability 1/2–1/2. So, $\xi = \sum_{j=1}^{k} \eta_j$ with independent random variables $\eta_1, \ldots, \eta_k$ where η_j assumes 0 and a_j with probability 1/2–1/2.

Clearly $E(\eta_j) = \dfrac{a_j}{2}$ and $D^2(\eta_j) = \left(\dfrac{a_j}{2}\right)^2$.

Thus $E(\xi) = \displaystyle\sum_{j=1}^{k} E(\eta_j) = \sum_{j=1}^{k} \frac{a_j}{2}$.

And $D^2(\xi) = \displaystyle\sum_{j=1}^{k} D^2(\eta_j) = \sum_{j=1}^{k} \left(\frac{a_j}{2}\right)^2 < \frac{kn^2}{4}$.

So $D(\xi) < n\sqrt{k}/2$.

5/12

We apply Chebyshev's inequality with (say) $c = 2$: The number of sums more remote from the average than the double of the standard deviation is less than one forth of the number of all sums.

So, more than $2^k \cdot \dfrac{3}{4}$ sums fall into an interval of length $4D(\xi) = 2n\sqrt{k}$ with center $E(\xi)$.

All these sums are distinct, so

$$2^k \cdot \frac{3}{4} < 2n\sqrt{k}, \quad \text{i.e.} \quad 2^k < \frac{8n\sqrt{k}}{3}.$$

Taking the logarithms twice as before, we obtain

$$k < \log_2 n + \frac{\log_2 \log_2 n}{2} + 2.$$

6/12

How big can be the sum of reciprocals of such numbers?

For powers of two, it can be arbitrarily close to 2. (We disregard now the condition $a_k \leq n$.)

Erdős conjectured that the sum of reciprocals is always less than 2. (If we allow infinitely many a_i, then the maximum is 2 but only for taking all powers of two.

This conjecture was solved by Ryavec using a nice trick.

Much later, two simple, natural proofs were found from “The Book” showing that, for a given k, the powers of two give the maximal value for the sum of reciprocals.

7/12

Ryavec's proof: Performing the multiplications in

$P = (1 + x^{a_1}) \dots (1 + x^{a_k})$, we get distinct terms x^m.

So $P < 1 + x + x^2 + \dots = 1/(1 - x)$ for $0 < x < 1$.

Magic: Take natural log, divide by x, and integrate from 0 to 1:

$$\sum_{i=1}^{k} \int_0^1 \frac{\log(1 + x^{a_i})}{x} dx < - \int_0^1 \frac{\log(1 - x)}{x} dx. \qquad \triangle$$

Integrating by substitution:

$$x^{a_i} = y; \quad dy = a_i x^{a_i - 1} dx; \quad dx = \frac{dy}{a_i x^{a_i - 1}}.$$

$$\int_0^1 \frac{\log(1 + x^{a_i})}{x} dx = \int_0^1 \frac{\log(1 + y)}{x a_i x^{a_i - 1}} dy = \frac{1}{a_i} \int_0^1 \frac{\log(1 + y)}{y} dy.$$

8/12

So $\left(\sum_{i=1}^{k} \frac{1}{a_i} \right) \int_0^1 \frac{\log(1 + y)}{y} dy < - \int_0^1 \frac{\log(1 - x)}{x} dx.$

We have to show that the integral A on the LHS is the half of the expression B on the RHS.

$$A - B = \left(\int_0^1 \frac{\log(1 + x)}{x} + \frac{\log(1 - x)}{x} \right) dx = \int_0^1 \frac{\log(1 - x^2)}{x} dx.$$

Substituting $t = x^2; dt = 2x dx$, we get

$$A - B = \int_0^1 \frac{\log(1 - t)}{x \cdot 2x} dt = \frac{1}{2} \int_0^1 \frac{\log(1 - t)}{t} dt = -\frac{1}{2} B, \text{ so } A = \frac{B}{2}.$$

9/12

Péter Frenkel's proof when he was still a highschool student(!)

For every i, the 2^i-1 non-empty sums formed from $a_1, a_2, \ldots, a_i$ are distinct positive integers, so the maximal sum satisfies $a_1 + \ldots + a_i \geq 2^i - 1$. (†)

If equality holds for every i, then $a_i = 2^{i-1}$, and we are done.

If not, then changing one or two values a_j, the sum of reciprocals increases while (†) remains valid and we reach equality everywhere in finitely many steps.

Let r be the smallest number with strict inequality in (†), i.e.

$$\begin{aligned} &a_1 + a_2 + \ldots + a_i = 2^i - 1, \quad i = 1, \ldots, r-1, \quad \text{and} \\ &a_1 + a_2 + \ldots + a_r > 2^r - 1. \end{aligned}$$

If we have strict inequality for every $i > r$, then take $a'_r = a_r - 1$ and keep all other a_i unchanged. This clearly works.

10/12

If $s > r$ is the smallest number when (†) holds again with equality, i.e.

$$\begin{aligned} &a_1 + a_2 + \ldots + a_i = 2^i - 1, \quad i = 1, \ldots, r-1 \\ &a_1 + a_2 + \ldots + a_i > 2^i - 1, \quad i = r, \ldots, s-1, \quad \text{and} \\ &a_1 + a_2 + \ldots + a_s = 2^s - 1, \end{aligned}$$

then take $a'_r = a_r - 1$ and $a'_s = a_s + 1$, the other a_i are unchanged.

The sum of reciprocals increases: $\dfrac{1}{a_r} + \dfrac{1}{a_s} < \dfrac{1}{a'_r} + \dfrac{1}{a'_s} \iff \dfrac{a_r + a_s}{a_r a_s} < \dfrac{(a_r-1)+(a_s+1)}{(a_r-1)(a_s+1)} \iff a_r a_s > (a_r - 1)(a_s + 1) \iff a_r - 1 < a_s$, which clearly holds.

It is easy to see that also the new elements are increasing order, satisfy (†), and the procedure leads in finitely many steps to overall equality, i.e. to the powers of two.

11/12

Also the book-proof by Bruen–Borwein is based on $a_1 + \ldots + a_i \geq 2^i - 1$, $i = 1, 2, \ldots, k$ (†).

Let $b_i = 2^{i-1}$, then (†) can be reformulated as

$$a_1 + \ldots + a_i \geq b_1 + \ldots + b_i, \quad i = 1, 2, \ldots, k. \qquad \oplus$$

We show that $\oplus$ implies

$$\frac{1}{a_1} + \ldots + \frac{1}{a_k} \leq \frac{1}{b_1} + \ldots + \frac{1}{b_k}, \qquad \odot$$

for any *real* numbers $0 < a_1 < \ldots < a_k$ and $0 < b_1 < \ldots < b_k$ and equality holds only if $a_i = b_i$ for every i.

12/12

We rewrite $\oplus$ as $c_i = a_1 - b_1 + \ldots + a_i - b_i \geq 0$ for every i.

We have to show $\odot$: $S = \dfrac{1}{b_1} - \dfrac{1}{a_1} + \ldots + \dfrac{1}{b_k} - \dfrac{1}{a_k} \geq 0$.

$$S = \frac{a_1 - b_1}{a_1 b_1} + \frac{a_2 - b_2}{a_2 b_2} + \ldots + \frac{a_k - b_k}{a_k b_k} =$$

$$= \frac{c_1}{a_1 b_1} + \frac{c_2 - c_1}{a_2 b_2} + \ldots + \frac{c_k - c_{k-1}}{a_k b_k} =$$

$$= c_1 \left(\frac{1}{a_1 b_1} - \frac{1}{a_2 b_2} \right) + c_2 \left(\frac{1}{a_2 b_2} - \frac{1}{a_3 b_3} \right) + \ldots + \frac{c_k}{a_k b_k}.$$

Every parenthesis is positive, $c_i \geq 0$, so $S \geq 0$, and

$S = 0 \iff c_i = 0 \iff a_i = b_i$ for every i.

A PROBLEM OF ERDŐS AND TWO PROOFS FROM "THE BOOK"

Róbert Freud

These are the notes for the second part of the talk, given at the Summer school at ELTE in 2022.

Let A be a finite set of positive integers so that adding up any number of distinct elements of A we never get equal sums. How large can be the sum of reciprocals of the elements of A?

Taking suitably many powers of two this sum can be arbitrarily close to 2. Erdős conjectured that the sum is less than 2 for any A. Ryavec verified this by a very tricky proof, where it is not clear why it works. Much later Bruen and Borwein, and independently Frenkel (being a highschool student at that time) found two different simple and natural arguments, so these nice proofs definitely form part of "The Book".

Ryavec's proof: If $A = \{a_1 < a_2 < \ldots < a_k\}$, then performing the multiplication in $P = (1 + x^{a_1}) \ldots (1 + x^{a_k})$ we obtain terms x^m, where m is the sum of some distinct exponents a_i (her $1 = x^0$ represents the empty sum). By assumption all these values of m are distinct, hence $P < 1 + x + x^2 + \ldots = 1/(1 - x)$ if $0 < x < 1$. Now take the (natural) logarithm of both sides, divide by x, and integrate from 0 to 1:

$$\sum_{i=1}^{k} \int_0^1 \frac{\log(1 + x^{a_i})}{x} dx < -\int_0^1 \frac{\log(1 - x)}{x} dx. \tag{1}$$

Substituting on the LHS: $x^{a_i} = y$; $dy = a_i x^{a_i - 1} dx$; $dx = dy/(a_i x^{a_i - 1})$, we obtain

$$\int_0^1 \frac{\log(1 + x^{a_i})}{x} dx = \int_0^1 \frac{\log(1 + y)}{x a_i x^{a_i - 1}} dy = \frac{1}{a_i} \int_0^1 \frac{\log(1 + y)}{y} dy.$$

Thus (1) turns into

$$\left(\sum_{i=1}^{k} \frac{1}{a_i} \right) \int_0^1 \frac{\log(1 + y)}{y} dy < -\int_0^1 \frac{\log(1 - x)}{x} dx.$$

To complete the proof, we have to show that the integral $A = \int_0^1 \frac{\log(1+x)}{x} dx$ on the LHS is the half of $B = -\int_0^1 \frac{\log(1-x)}{x} dx$ on the RHS. Taking

$$A - B = \int_0^1 \left(\frac{\log(1 + x)}{x} + \frac{\log(1 - x)}{x} \right) dx = \int_0^1 \frac{\log(1 - x^2)}{x} dx,$$

and substituting $t = x^2, dt = 2x dx$, we obtain

$$A - B = \int_0^1 \frac{\log(1 - t)}{x \cdot 2x} dt = \frac{1}{2} \int_0^1 \frac{\log(1 - t)}{t} dt = -\frac{1}{2} B, \text{ i.e. } A = \frac{B}{2}.$$

Remark: We can also compute these numerical integrals by using power series:

$$\frac{-\log(1 - x)}{x} = 1 + \frac{x}{2} + \ldots + \frac{x^{j-1}}{j} + \ldots,$$

hence

$$\int_0^1 \frac{-\log(1-x)}{x}dx = \left[x + \frac{x^2}{4} + \ldots + \frac{x^j}{j^2} + \ldots\right]_0^1 = \sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6}.$$

Similarly, we obtain

$$\int_0^1 \frac{\log(1+y)}{y}dy = \left[y - \frac{y^2}{4} + \frac{y^3}{9} - \ldots\right]_0^1 = \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j^2} = \sum_{j=1}^{\infty} \frac{1}{j^2} - 2\sum_{t=1}^{\infty} \frac{1}{(2t)^2} = \frac{\pi^2}{12}.$$

These imply $\left(\sum_{i=1}^{k} \frac{1}{a_i}\right) \frac{\pi^2}{12} < \frac{\pi^2}{6}$, i.e. $\sum_{i=1}^{k}(1/a_i) < 2$.

Frenkel's proof: For any $1 \leq i \leq k$ the $2^i - 1$ sums formed from $a_1, \ldots, a_i$ are distinct, hence the largest sum (*) $a_1 + a_2 + \ldots + a_i \geq 2^i - 1$. We show that (*) implies $\sum_{j=1}^{k}(1/a_i) < 2$.

If (*) holds with equality for all i, then clearly $a_i = 2^{i-1}$. Otherwise we change the value of one or two a_i-s so that (*) remains valid, and the sum of reciprocals increases. The procedure terminates when everywhere we have equality.

Let r be the smallest value when equality does not hold in (*), i.e.

$$\begin{aligned} &a_1 + a_2 + \ldots + a_i = 2^i - 1, \quad i = 1, \ldots, r-1, \quad \text{and} \\ &a_1 + a_2 + \ldots + a_r > 2^r - 1. \end{aligned}$$

If we have $>$ for all $i > r$, then take $a'_r = a_r - 1$, this clearly works. If

$$\begin{aligned} &a_1 + a_2 + \ldots + a_i = 2^i - 1, \quad i = 1, \ldots, r-1 \\ &a_1 + a_2 + \ldots + a_i > 2^i - 1, \quad i = r, \ldots, s-1, \quad \text{and} \\ &a_1 + a_2 + \ldots + a_s = 2^s - 1, \end{aligned}$$

then take $a'_r = a_r - 1$, $a'_s = a_s + 1$. The sum of reciprocals increases: $\frac{1}{a_r} + \frac{1}{a_s} < \frac{1}{a'_r} + \frac{1}{a'_s} \iff \frac{a_r + a_s}{a_r a_s} < \frac{(a_r - 1) + (a_s + 1)}{(a_r - 1)(a_s + 1)} \iff a_r a_s > (a_r - 1)(a_s + 1) \iff a_r - 1 < a_s$, which is true.

The proof by Bruen and Borwein: Taking $b_i = 2^{i-1}$, we can write (*) as $a_1 + \ldots + a_i \geq b_1 + \ldots + b_i$. We show that this implies (**) $(1/a_1) + \ldots + (1/a_k) \leq (1/b_1) + \ldots + (1/b_k)$ for any *real* numbers $0 < a_1 < \ldots < a_k$, $0 < b_1 < \ldots < b_k$.

By (*) we have $c_i = a_1 - b_1 + \ldots + a_i - b_i \geq 0$. Now

$$\frac{1}{b_1} - \frac{1}{a_1} + \ldots + \frac{1}{b_k} - \frac{1}{a_k} = \frac{a_1 - b_1}{a_1 b_1} + \frac{a_2 - b_2}{a_2 b_2} + \ldots + \frac{a_k - b_k}{a_k b_k} =$$

$$\frac{c_1}{a_1 b_1} + \frac{c_2 - c_1}{a_2 b_2} + \ldots + \frac{c_k - c_{k-1}}{a_k b_k} = c_1\left(\frac{1}{a_1 b_1} - \frac{1}{a_2 b_2}\right) + c_2\left(\frac{1}{a_2 b_2} - \frac{1}{a_3 b_3}\right) + \ldots + \frac{c_k}{a_k b_k}$$

which is non-negative, thus proving (**).

SOME APPLICATIONS OF THE COMBINATORIAL NULLSTELLENSATZ

Gyula Károlyi

Throughout these notes $\mathbb{F}$ denotes an arbitrary field, which we later specify, according to the nature of the application, as the real number field $\mathbb{R}$, the complex number field $\mathbb{C}$ or a finite field $\mathbb{F}_p$ for some prime number p, obtained from the ring of integers by modulo p arithmetic. According to Fermat's little theorem, every $0 \neq a \in \mathbb{F}_p$ satisfies $a^{p-1} = 1$. In a more abstract way, it follows from Lagrange's theorem, applied to the multiplicative group of $\mathbb{F}_p$.

1. The Combinatorial Nullstellensatz

The *Combinatorial Nullstellensatz*, formulated by Noga Alon [1] in the late nineties, describes, in an efficient way, the structure of multivariate polynomials whose zero-set includes a Cartesian product over $\mathbb{F}$.

Theorem 1.1. *Let $f = f(x_1, \dots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \dots, x_n]$. Let $S_1, \dots, S_n$ be nonempty subsets of $\mathbb{F}$ and define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If $f(s_1, \dots, s_n) = 0$ for all $s_i \in S_i$, then there exist polynomials $h_1, \dots, h_n \in \mathbb{F}[x_1, \dots, x_n]$ satisfying $\deg(h_i) \leq \deg(f) - \deg(g_i)$ such that $f = \sum_{i=1}^{n} h_i g_i$.*

Example. Here $n = 2$ and for simplicity we denote the variables x_1, x_2 by x and y. Take $\mathbb{F} = \mathbb{R}$ and consider the points $(0,0), (0,1), (1,0), (1,1)$ in the euclidean plane; they form the vertex set of a square. More formally, they are the points of the Cartesian product $S_1 \times S_2$, where $S_1 = S_2 = \{0,1\}$. The polynomial $f(x,y) = (y-x)(y+x-1)$ attains the value 0 at each point $(x,y) \in S_1 \times S_2$. Thus, we define $g_1(x) = x(x-1)$ and $g_2(y) = y(y-1)$. Here each polynomial is of degree 2, and $f = h_1 g_1 + h_2 g_2$ indeed holds with the constant polynomials $h_1 = 1$, $h_2 = -1$.

Theorem 1.1 immediately implies the following non-vanishing criterion that we will refer to as the *Polynomial Lemma.* Informally, it is a strong multivariate analogue of the well-known fact that a univariate polynomial of degree d over a field cannot have more than d roots.

Theorem 1.2. *Let $f = f(x_1, \dots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \dots, x_n]$. Suppose that there is a monomial $\prod_{i=1}^{n} x_i^{d_i}$ such that $\sum_{i=1}^{n} d_i$ equals the degree of f and whose coefficient in f is nonzero. If $S_1, \dots, S_n$ are subsets of F with $|S_i| > d_i$, then there are $s_1 \in S_1, \dots, s_n \in S_n$ such that $f(s_1, \dots, s_n) \neq 0$.*

A standard application of the polynomial method to prove a combinatorial hypothesis works as follows. Assuming the falsity of the hypothesis, build a polynomial whose values are all zero over a large Cartesian product, then compute the coefficient of the appropriate leading term. If that coefficient is not zero, the criterion leads to the desired contradiction.

The difficulty often lies in the computation of that coefficient. This is where the power of the following *Coefficient Lemma*, formulated independently by Lasoń [17] and by Karasev and Petrov [12], comes into play.

Theorem 1.3. *Let $f \in \mathbb{F}[x_1, \dots, x_n]$ be a polynomial of degree $\deg(f) \le d_1 + \dots + d_n$. For arbitrary subsets $S_1, \dots, S_n$ of $\mathbb{F}$ with $|S_i| = d_i + 1$, the coefficient of $\prod x_i^{d_i}$ in f can be written as*

$$\sum_{s_1 \in S_1} \sum_{s_2 \in S_2} \cdots \sum_{s_n \in S_n} \frac{f(s_1, s_2, \dots, s_n)}{g_1'(s_1) g_2'(s_2) \dots g_n'(s_n)},$$

where $g_i(x) = \prod_{s \in S_i} (x - s)$.

A close relative of the Combinatorial Nullstellensatz, this result also implies the Polynomial Lemma: If this coefficient is nonzero, then one of the summands must be nonzero, hence the existence of $s_i \in S_i$ with $f(s_1, \dots, s_n) \neq 0$. Thus we have

$$CN \Rightarrow PL \Leftarrow CL.$$

Both the CN and the CL are relatively easy consequences of the multivariate extension of the Lagrange interpolation formula. Simple as stated, they provide a powerful algebraic tool to attack various problems in discrete mathematics. They lead to proofs of sheer beauty and elegance which we intend to demonstrate through a set of diverse examples.

2. Additive Combinatorics I

Given two nonempty sets of integers $A = \{a_1, \dots, a_k\}$ and $B = \{b_1, \dots, b_l\}$, their sumset is defined as

$$A + B = \{a_i + b_j \mid 1 \le i \le k, 1 \le j \le l\}.$$

Assuming $a_1 < \dots < a_k$ and $b_1 < \dots < b_l$ one can argue that

$$a_1 + b_1 < a_2 + b_1 < \ldots < a_k + b_1 < a_k + b_2 < \ldots < a_k + b_l,$$

thus $A + B$ has at least $k + l - 1$ different elements. In the particular case when

$$A = \{1, 2, \dots, k\}, \quad B = \{1, 2, \dots, l\},$$

the sumset $A + B = \{2, 3, \dots, k + l\}$ has exactly $k + l - 1$ elements.

What happens, if instead of integers we consider the integers modulo a prime p? Thus, we are working in the cyclic group $\mathbb{Z}/p\mathbb{Z}$. Such groups, having no proper nontrivial subgroups have the simplest possible structure among all nontrivial groups. They are exactly the additive structures underlying the finite fields $\mathbb{F}_p$. The problem is that working modulo p we lose the natural ordering of the integers, so the above simple argument does not work. There is of course no way to establish the same result, as the simple example $A = B = A + B = \mathbb{Z}/p\mathbb{Z}$ indicates.

Nevertheless the lower bound remains valid if k, l are not too large, namely when $k+l-1 \le p$. This was first established by Cauchy [5] in 1813 in relation to Lagrange's four-square theorem (every nonnegative integer can be represented as the sum of 4 perfect squares) and rediscovered by Davenport [7] more than 100 years later. Note that $A' \supseteq A$, $B' \supseteq B$ implies $A' + B' \supseteq A + B$, therefore it follows that $A + B = \mathbb{Z}/p\mathbb{Z}$ holds whenever $k + l - 1 \geq p$. The fact that $\mathbb{Z}/p\mathbb{Z}$ is the additive group of the field $\mathbb{F}_p$ opens up the possibility to apply Theorem 1.2 with $\mathbb{F} = \mathbb{F}_p$, which we indicate below; it is probably one of the most straightforward applications of the Polynomial Lemma.

Theorem 2.1. *Let A and B be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$, with $|A| = k$ and $|B| = l$. If $p \geq k + l - 1$, then $|A + B| \geq k + l - 1$.*

Proof. Assume for a contradiction that $|A + B| < k + l - 1$. Then $A + B$ is contained in a set $C \subseteq \mathbb{Z}/p\mathbb{Z}$ of cardinality $|C| = k + l - 2 = (k - 1) + (l - 1)$. We will apply the Polynomial Lemma with $\mathbb{F} = \mathbb{F}_p$, $S_1 = A$, $S_2 = B$. As in the example in Section 1, we denote the variables x_1, x_2 by x and y, respectively. Consider the polynomial

$$f(x, y) = \prod_{c \in C} (x + y - c) \in \mathbb{F}_p[x, y];$$

then $f(a, b) = 0$ for every pair $a \in A$, $b \in B$. The degree of this polynomial is $(k-1)+(l-1)$ and it vanishes on $A \times B$, which is a $k \times l$ Cartesian product. But the coefficient of the leading term $x^{k-1}y^{l-1}$ is $\binom{k+l-2}{k-1}$, which is different from 0 in $\mathbb{F}_p$, given that $k + l - 2 < p$. This contradicts the Polynomial Lemma. □

Of course the arguments of Cauchy and Davenport were entirely different, rather combinatorial in nature. You may try to reconstruct their way of thinking, but be aware, it is not that easy!

3. Geometry I

Let $C_n = \{0, 1\}^n$ be the vertex set of the unit cube in euclidean n-space. It is obvious that one can cover all the vertices by two hyperplanes: take for example those two whose equations are $x_1 = 0$ and $x_1 = 1$, respectively. Suppose next that we want to cover all vertices except the origin by a set of m hyperplanes $H_1, \ldots, H_m$. We have the conditions

$$C_n \setminus \{\mathbf{0}\} \subset \bigcup_{i=1}^{m} H_i, \quad \mathbf{0} \notin H_i \text{ for } i = 1, \ldots, m.$$

This is how to do it with $m = n$ hyperplanes: let H_i be the hyperplane whose equation is $x_i = 1$. An entirely different way to do it is letting H_i be the hyperplane of all points satisfying

$$x_1 + x_2 + \cdots + x_n = i.$$

It was conjectured by Komjáth that less than n hyperplanes will never suffice.

Theorem 3.1. *If the hyperplanes $H_1, \ldots, H_m$ satisfy the above conditions, then $m \geq n$.*

Proof. Here we follow a simplified version of Alon and Füredi [3], based on an application of Theorem 1.2 with $\mathbb{F} = \mathbb{R}$. Note that $C_n = S_1 \times S_2 \times \cdots \times S_n$ with $S_i = \{0, 1\}$ for $1 \leq i \leq n$. Suppose that on the contrary, $m < n$. Since none of the hyperplanes passes through the origin, they are affine but not linear subspaces, hence are determined by linear equations in the normalized form

$$H_i : \quad \sum_{j=1}^{n} a_{ij} x_j = 1.$$

Consider the polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$ defined as

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} x_j - 1 \right) - (-1)^{m-n} \prod_{j=1}^{n} (x_j - 1)\,.$$

The first term in the right-hand side vanishes at every point of $C_n \setminus \{\mathbf{0}\}$ because each such point satisfies the equation of at least one of the hyperplanes H_i. Its value at $\mathbf{0}$ is $(-1)^m$. The second term is also 0 at every point of $C_n \setminus \{\mathbf{0}\}$ for all of them have at least one coordinate equal to 1. Its value at 0 is also $(-1)^m$; the coefficient $(-1)^{m-n}$ was designed so as to achieve this. Therefore f, which is the difference of these two terms, vanishes at every point of C_n.

By the assumption $m < n$, the degree of f is n and the coefficient of the leading term $x_1 x_2 \ldots x_n$ is $-(-1)^{m-n}$, which is different from 0. According to the Polynomial Lemma, f cannot vanish on the whole Cartesian product $C_n = S_1 \times \cdots \times S_n$. This contradiction proves that indeed it must be $m \geq n$. □

Suppose that $m = n$ and the hyperplanes $H_1, \ldots, H_n$ do the job. Consider the $n \times n$ matrix $A = (a_{ij})$. A closer inspection of the above proof reveals that the permanent of the matrix A must be equal to 1. This is a necessary, but alas!, not a sufficient condition; we do not have a complete description of these extremal structures.

4. Graph Theory

Let $G = G(V, E)$ be a simple graph, where V and E stands for the set of vertices and edges, respectively. It is k-regular, if each vertex has the same degree k:

$$|\{u \in V \mid uv \in E\}| = k$$

for every $v \in V$. A subgraph of G is a graph $G' = G'(V', E')$ with $V' \subseteq V$, $E' \subseteq E$. Note that we are not talking about induced subgraphs here. For example, the 4-regular complete graph K_5 on 5 vertices has a 3-regular subgraph isomorphic to K_4. In fact, every 4-regular simple graph has a 3-regular subgraph (see Tashkinov [19]). With the help of the Polynomial Lemma it is easy to prove a slightly weaker result: If G is obtained from a 4-regular graph by adding an extra edge to the set of edges, then it contains a 3-regular subgraph. It is an immediate consequence of a special case ($p = 3$) of the following more general theorem of Alon, Friedland and Kalai [2].

Theorem 4.1. *If p is a prime and G a simple graph of average degree $> 2p-2$ and maximum degree $\leq 2p-1$, then G contains a p-regular subgraph.*

Proof. The goal is to assign to each edge of G 0 or 1 such a way, that there is at least one edge assigned with 1 (to exclude the empty graph), and for every vertex, the number of edges starting at that vertex and having the value 1 is either 0 or p. In view of the assumption on the maximum degree we can rephrase the second condition: the number of such edges must be divisible by p for every vertex. In such an assignment, the edges assigned with 1 form a p-regular subgraph.

If $G = G(V,E)$, the incidence matrix of G is the 0–1 matrix $(a_{ve})_{v\in V, e\in E}$, where $a_{ve} = 1$ if and only if the vertex v is incident to the edge e. Thus, if we introduce a 0–1 variable x_e for every edge $e \in E$, the second condition can be formulated as

$$\sum_{e\in E} a_{ve}x_e = 0 \text{ in } \mathbb{F}_p. \tag{4.1}$$

Accordingly, we consider the following polynomial $f \in \mathbb{F}_p[x_e \mid e \in E]$:

$$f(x_e \mid e\in E) = \prod_{v\in V}\left(1-\left(\sum_{e\in E} a_{ve}x_e\right)^{p-1}\right) - \prod_{e\in E}(1-x_e).$$

Since the average degree of G is $> 2p-2$, that is, $(2p-2)|V| < 2|E|$, we have $(p-1)|V| < |E|$, thus $\deg f = |E|$. Then $\prod_{e\in E} x_e$ is a leading monomial with coefficient $-(-1)^{|E|} \neq 0$. By the Polynomial Lemma, f cannot vanish on $\{0,1\}^{|E|}$. This means that we have a choice $s_e \in \{0,1\}$ for each x_e such that $f(s_e \mid e \in E) \neq 0$. Were $s_e = 0$ for every $e \in E$, the value of the polynomial would also be 0. So this cannot be the case; at least one edge is assigned with 1. It also follows that $\prod_{e\in E}(1-s_e) = 0$, hence $\prod_{v\in V}\left(1-\left(\sum_{e\in E} a_{ve}s_e\right)^{p-1}\right)$ must be different from 0. In view of Fermat's little theorem this means that condition (4.1) is satisfied for every vertex v. □

5. Algebraic Combinatorics

A Laurent polynomial is like a polynomial except that the exponents of the indeterminates may also be negative integers. For example,

$$x^2y^3z^4 - 2x^{-1}y^6z^{-4} + 13y^{-5}z - 21$$

is a Laurent polynomial in the variables x, y, z; its constant term, that is, the coefficient of $x^0y^0z^0$ being -21.

For Laurent polynomials given in a product form, the constant terms often have combinatorial interpretation. More surprisingly, their systematic study originates in statistical mechanics. Perhaps the most famous constant term identity is the one associated with the name of Freeman Dyson. In his seminal paper [8] dated back to 1962, Dyson proposed to replace Wigner's classical Gaussian-based random matrix models by what now is known as the circular ensembles. The study of their joint eigenvalue probability density functions led Dyson to the following conjecture. Consider the family of Laurent polynomials

$$\mathscr{D}(\boldsymbol{x};\boldsymbol{a}) := \prod_{1\le i\ne j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i}$$

parameterized by a sequence $\boldsymbol{a}=(a_1,\dots,a_n)$ of nonnegative integers, where $\boldsymbol{x}=(x_1,\dots,x_n)$ is the sequence of indeterminates. Denoting by $\mathrm{CT}[\mathscr{L}(\boldsymbol{x})]$ the constant term of the Laurent polynomial $\mathscr{L}=\mathscr{L}(\boldsymbol{x})$, Dyson's hypothesis can be formulated as the identity

$$\mathrm{CT}[\mathscr{D}(\boldsymbol{x};\boldsymbol{a})] = \frac{(a_1+a_2+\cdots+a_n)!}{a_1!a_2!\dots a_n!}.$$

Using the shorthand notation $\mathscr{D}(\boldsymbol{x};k)$ for the equal parameter case $\boldsymbol{a}=(k,\dots,k)$, the constant term of $\mathscr{D}(\boldsymbol{x};k)$ for $k=1,2,4$ corresponds to the normalization factor of the partition function for the circular orthogonal, unitary and symplectic ensemble, respectively.

Dyson's conjecture was confirmed independently by Gunson and Wilson (who 20 years later won the Nobel Prize for his work on the renormalization group) in the same year. The most elegant proof, based on Lagrange interpolation, is due to Good [10]. His proof exploits the recursive nature of the multinomial coefficients.

Theorem 1.3 leads to a short direct proof of the equal parameter case. Note that the $k=0$ case is trivial.

Theorem 5.1. *For arbitrary integers $n\ge 2$ and $k\ge 1$,*

$$\mathrm{CT}[\mathscr{D}(x_1,\dots,x_n;k)] = \frac{(nk)!}{(k!)^n}.$$

Proof. Multiplying $\mathscr{D}(\boldsymbol{x};k)$ by $M=\prod x_i^{(n-1)k}$ one finds that the the constant term equals the coefficient of the monomial M in the homogeneous polynomial

$$\prod_{1\le i\ne j\le n}(x_j-x_i)^k,$$

which is the same as the coefficient of M in

$$f(\boldsymbol{x}) = \prod_{1\le i<j\le n}\left(\prod_{u=0}^{k-1}(x_j-x_i-u)\prod_{v=1}^{k}(x_i-x_j-v)\right).$$

We may apply the Coefficient Lemma with $d_i=(n-1)k$ and the choice

$$S_i=\{0,1,\dots,(n-1)k\}$$

for $i=1,\dots,n$. Suppose that $f(s_1,\dots,s_n)\ne 0$ for some $s_i\in S_i$, then $|s_j-s_i|\ge k$ for every $i\ne j$, thus the numbers $s_1,s_2,\dots,s_n$, in some order, must coincide with the numbers $0,k,2k,\dots,(n-1)k$. Moreover, it must be the natural order, for if $s_i>s_j$ for some $i<j$,

then $s_i - s_j \geq k+1$, otherwise $f(s_1, \dots, s_n)$ would be zero. Accordingly, the complicated summation formula in Theorem 1.3 in this case reduces to one nonzero summand,

$$\frac{f(0, k, \dots, (n-1)k)}{g'(0)g'(k)\dots g'((n-1)k)},$$

where $g(x) = x(x-1)\dots(x-(n-1)k)$. The actual substitution can be left to the reader. □

The above idea is from Karasev and Petrov [12]. Can you reconstruct their proof of the full Dyson conjecture?

6. Additive Combinatorics II

According to a recent result of Preissmann and Mischler [18], seating n couples around the King's round table according to a certain royal protocol is always possible if $p = 2n+1$ is a prime number. The precise mathematical formulation is as follows.

Theorem 6.1. *Let $p = 2n+1$ be an odd prime and let $t_1, \dots, t_n$ be arbitrary nonzero elements of $\mathbb{F}_p$. Then the nonzero elements of $\mathbb{F}_p$ can be enumerated as $a_1, \dots, a_n, b_1, \dots, b_n$ such that $b_i - a_i = t_i$ holds for every $i = 1, \dots, n$.*

For example, if $t_1 = \dots = t_n = 1$, then $a_i = 2i-1$, $b_i = 2i$ will do. The below argument, based on the Polynomial Lemma, is again due to Karasev and Petrov [12].

Proof. Consider the polynomial

$$f(\boldsymbol{x}) = \prod_{1 \leq i < j \leq n} (x_j - x_i)(x_j + t_j - x_i)(x_i + t_i - x_j)(x_i + t_i - x_j - t_j) \in \mathbb{F}_p(\boldsymbol{x});$$

it is homogeneous of degree $n(2n-2) = n(p-3)$. The coefficient of the monomial $M = \prod x_i^{p-3}$ is the same as in the polynomial

$$\prod_{1 \leq i \neq j \leq n} (x_j - x_i)^2,$$

which, according to Theorem 5.1, is

$$\mathrm{CT}[\mathscr{D}(x_1, \dots, x_n; 2)] = \frac{(2n)!}{(2!)^n} = \frac{(p-1)!}{2^n} \neq 0.$$

Consider the sets $S_i = \{1, 2, \dots, p-1\} \setminus \{-t_i\}$, then $|S_i| > p-3$. According to the Polynomial Lemma, there are elements $s_i \in S_i$ such that $f(s_1, \dots, s_n) \neq 0$. Put $a_i = s_i$, $b_i = s_i + t_i$; then $b_i - a_i = t_i$ as required. By the choice of s_i, neither a_i nor b_i is zero. Since $f(s_1, \dots, s_n) \neq 0$, the elements $a_1, \dots, a_n, b_1 \dots, b_n$ are pairwise different. □

7. Geometry II

As we have seen in Section 3, covering the vertex set C_n of the hypercube with hyperplanes is simple: two hyperplanes suffice in every dimension, whereas it is never possible using only one hyperplane. In general we address the following problem. Recall that C_n is a $2 \times 2 \times \cdots \times 2$ Cartesian product. Now let $S_i = \{a_{i1}, \ldots, a_{ik}\}$ be k-element subsets of $\mathbb{R}$ for $i = 1, 2, \ldots, n$, and consider their Cartesian product $C = S_1 \times \cdots \times S_n$ in euclidean n-space. It is easy to cover C with a set of k hyperplanes, all parallel to the same coordinate hyperplane. Indeed, for any $1 \leq i \leq n$ one can take the system of hyperplanes

$$\mathscr{H}_i = \{H_{ij} : \ x_i = a_{ij} \quad (j = 1, 2, \ldots, k)\}.$$

Less than k hyperplanes will never do, for $|C| = k^n$, and $|H \cap C| \leq k^{n-1}$ for any hyperplane H, as one can prove it by induction on the dimension n. (How?)

Now consider a system $\mathscr{H}$ of k hyperplanes which cover C. What can we say about its structure? Is it true that $\mathscr{H}$ necessarily coincides with one of the n axis-parallel systems described above? Well, not exactly: the example in Section 1, which is easy to generalize to arbitrary dimensions, demonstrates that it is not true when $k = 2$, and the situation is even worse for $k = 1$. The Combinatorial Nullstellensatz reveals that there are no counterexamples for larger values of k.

Theorem 7.1. *Let $k \geq 3$ and let $\mathscr{H} = \{H_1, \ldots, H_k\}$ be a system of hyperplanes in $\mathbb{R}^n$. If $C \subset H_1 \cup \cdots \cup H_k$, then $\mathscr{H} = \mathscr{H}_i$ for some $i \in \{1, 2, \ldots, n\}$.*

Proof. For simplicity, we prove the result for $n = 2$ and write

$$S_1 = \{a_1, a_2, \ldots, a_k\}, \quad S_2 = \{b_1, b_2, \ldots, b_k\}.$$

As before, we denote the coordinates by x and y. If H_i is the line of equation $A_i x + B_i y + C_i = 0$, then the polynomial

$$f(x, y) = \prod_{i=1}^{k} (A_i x + B_i y + C_i)$$

vanishes on the $k \times k$ Cartesian product $C = S_1 \times S_2$. Applying Theorem 1.1 for this situation, the degree condition implies that the polynomials h_1, h_2 have degree 0. Accordingly, there exist real numbers α, β such that

$$f(x, y) = \alpha \prod_{i=1}^{k} (x - a_i) + \beta \prod_{i=1}^{k} (y - b_i).$$

Comparing the degree k homogeneous parts of the two representations of f we find that

$$\prod_{i=1}^{k} (A_i x + B_i y) = \alpha x^k + \beta y^k.$$

By symmetry, we may assume that $\alpha \neq 0$. As $\alpha = \prod A_i$, it follows that $A_i \neq 0$. Thus, putting $y = 1$ we obtain

$$\prod_{i=1}^{k} \left(x + \frac{B_i}{A_i} \right) = x^k + \frac{\beta}{\alpha}.$$

The polynomial on the left-hand side splits into linear factors over $\mathbb{R}$. On the other hand, if $\beta \neq 0$, then the roots of the polynomial on the right-hand side form the vertex set of a regular k-gon on the plane of the complex numbers, of which at most 2 can lie on the real line. Since $k \geq 3$, the polynomial on the right-hand side splits into linear factors if and only if $\beta = 0$. It follows that $B_1 = \cdots = B_k = 0$, reducing the equation of H_i to $A_i x + C_i = 0$. That is, the lines H_i are all parallel to the y-axis and then it must be $\mathscr{H} = \mathscr{H}_1$. Similarly, the assumption $\beta \neq 0$ leads to $\mathscr{H} = \mathscr{H}_2$. □

From this proof we can extract the hidden algebraic reason: If $\alpha \neq 0$, then the polynomial $x^k + \alpha$ has at most two roots in $\mathbb{R}$. The following example shows that Theorem 7.1 fails if one replaces the real number field by the complex number field.

Example. Let $\varepsilon = e^{2\pi i/3} = \cos 120° + i \sin 120°$. Consider the Cartesian product

$$C = \{0, 1, -\varepsilon\} \times \{0, -1, \varepsilon\} \subset \mathbb{C}^2.$$

One readily checks that it is contained in the union of the following three lines:

$$H_1 : \; x + y = 0, \quad H_2 : \; x + \varepsilon y = -\varepsilon, \quad H_3 : \; x + \varepsilon^2 y = 1.$$

Getting back to $\mathbb{R}^n$ and analyzing the previous proof one finds that the 'hidden algebraic reason' can be generalized to a great extent.

Lemma 7.2. *Consider a polynomial $f(x) = c_0 x^d + c_1 x^{d-1} + \cdots + c_{d-1} x + c_d \in \mathbb{R}[x]$ with $c_0 \neq 0$. If $c_{e-2} = c_{e-1} = 0$ and $c_e \neq 0$ for some e, then the polynomial does not split into linear factors over $\mathbb{R}$.*

Proof. Assume that on the contrary, f has d real roots (counted with the appropriate multiplicities). If α is a root of multiplicity $m > 1$, then α is also a root of f' with multiplicity $m - 1$. Thus, it follows from Rolle's mean value theorem that f' has $d - 1$ real roots. Iterating this $d - e$ times, after normalization we obtain a polynomial

$$g(x) = c_0^* x^e + c_1^* x^{e-1} + \cdots + c_{e-1}^* x + c_e^*$$

with $c_{e-2}^* = c_{e-1}^* = 0$ and $c_0^*, c_e^* \neq 0$, which has e nonzero real roots. The reciprocal polynomial

$$c_e^* x^e + c_{e-1}^* x^{e-1} + \cdots + c_1^* x + c_0^*$$

also has e nonzero roots $\alpha_1, \ldots \alpha_e \in \mathbb{R}$. According to Viète's formulas,

$$\sigma_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_e = -\frac{c_{e-1}^*}{c_e^*} = 0$$

and

$$\sigma_2 = \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \cdots + \alpha_{e-1} \alpha_e = \frac{c_{e-2}^*}{c_e^*} = 0.$$

Consequently,

$$\alpha_1^2+\alpha_2^2+\cdots+\alpha_e^2=\sigma_1^2-2\sigma_2=0,$$

implying $\alpha_1=\alpha_2=\cdots=\alpha_e=0$, a contradiction. □

Alternatively, one may apply Descartes' rule of signs to prove the above lemma. This tool makes it possible to prove the following stability result, a very strong version of Theorem 7.1. Note that the condition on m cannot be improved upon.

Theorem 7.3. *Let $m\le 2k-3$ and let $\mathscr{H}=\{H_1,\dots,H_m\}$ be a system of hyperplanes in $\mathbb{R}^n$. If $C\subset H_1\cup\cdots\cup H_m$, then $\mathscr{H}$ contains a system of k hyperplanes that already covers C. That is, $\mathscr{H}\supseteq\mathscr{H}_i$ for some $i\in\{1,2,\dots,n\}$.*

Proof. We may assume that the system $\mathscr{H}$ is irredundant, that is, no hyperplane H_u occurs twice, and each of them intersects C. Writing the equation of H_u in the form $\sum_{j=1}^n A_{uj}x_j+B_u=0$, the polynomial

$$f(\boldsymbol{x})=\prod_{u=1}^m\left(\sum_{j=1}^n A_{uj}x_j+B_u\right)$$

vanishes on $C=S_1\times\cdots\times S_n$. According to Theorem 1.1 there exist polynomials $h_i\in\mathbb{R}[\boldsymbol{x}]$ with $\deg h_i\le m-k\le k-3$ such that

$$f(\boldsymbol{x})=\sum_{i=1}^n h_i(\boldsymbol{x})\prod_{j=1}^k(x_i-a_{ij}).$$

From each h_i, collect the monomial terms of degree $m-k$ and denote the resulting polynomials by $\widetilde{h}_i$; each of them is either homogeneous of degree $m-k$ or identically zero. Thus we have

$$\prod_{u=1}^m\left(\sum_{j=1}^n A_{uj}x_j\right)=\sum_{i=1}^n x_i^k\widetilde{h}_i(\boldsymbol{x}).$$

Without any loss of generality we may assume that $\widetilde{h}_1\ne 0$. Rewrite the above equation in the form

$$\prod_{u=1}^m\left(\sum_{j=1}^n A_{uj}x_j\right)=\widetilde{h}(\boldsymbol{x})+\widetilde{g}(\boldsymbol{x}),\tag{7.1}$$

where

$$\widetilde{h}(\boldsymbol{x})=x_1^k\widetilde{h}_1(\boldsymbol{x})=\sum_{i=k}^m\widetilde{g}_i(x_2\dots,x_n)x_1^i$$

and

$$\widetilde{g}(\boldsymbol{x})=\sum_{i=2}^n x_i^k\widetilde{h}_i(\boldsymbol{x})=\sum_{i=0}^{k-3}\widetilde{g}_i(x_2\dots,x_n)x_1^i$$

with some polynomials $\widetilde{g}_i\in\mathbb{R}[x_2,\dots,x_n]$. By the assumption $\widetilde{h}_1\ne 0$, there is a largest d with $k\le d\le m$ such that $\widetilde{g}_d\ne 0$. We will argue that $\widetilde{g}=0$.

Suppose that, on the contrary, there is a smallest e with $d \geq e \geq d-k+3$ such that $\widetilde{g}_{d-e} \neq 0$. Then there exist $s_2, \ldots, s_n \in \mathbb{R}$ such that

$$\widetilde{g}_d(s_2, \ldots, s_n) \neq 0 \quad \text{and} \quad \widetilde{g}_{d-e}(s_2, \ldots, s_n) \neq 0.$$

Writing $g_i(s_2, \ldots, s_n) = c_{d-i}$, specializing at $x_j = s_j$ for $2 \leq j \leq n$, equation (7.1) reads as

$$\prod_{u=1}^{m} \left(A_{u1}x_1 + \sum_{j=2}^{n} A_{uj}s_j \right) = c_0 x_1^d + \cdots + c_{d-k}x_1^k + c_e x_1^{d-e} + \cdots + c_d.$$

In particular, exactly d of the coefficients A_{u1} are different from zero. According to Lemma 7.2, the polynomial on the right-hand side does not split into linear factors over $\mathbb{R}$, whereas the polynomial on the left-hand side obviously does. This contradiction proves that indeed $\widetilde{g} = 0$, as claimed.

All in all, we see from (7.1) that the nonzero polynomial

$$\prod_{u=1}^{m} \left(\sum_{j=1}^{n} A_{uj}x_j \right)$$

is divisible by x_1^k. By unique factorization in $\mathbb{R}[\boldsymbol{x}]$ it follows that (at least) k of the above factors are in the form $A_{u1}x_1$ with $A_{u1} \neq 0$. The corresponding hyperplanes H_u, having equation in the form $A_{u1}x_1 + B_u = 0$ are all orthogonal to the x_1-axis. By the irredundancy hypothesis, they must form the system $\mathscr{H}_1$. □

The results of this last section are from [4]. Note that it is possible to prove the above theorems by purely elementary arguments. The point is: The application of the Combinatorial Nullstellensatz made it possible to discover these results in the first place.

8. Further Reading

For a proof of the Combinatorial Nullstellensatz as well as for a wealth of applications, see Alon's original paper [1]. To read more about constant term identities, their relevance in statistical physics and their connection to the Selberg integral, see [16] and the references therein; it contains many applications of the Coefficient Lemma, including additive combinatorics. For the latter subject, we also refer to the expository paper [13] and the recent monograph [11]. See [9, 14, 15] for more delicate applications of Theorem 1.1. The manuscript [6] is probably the most recent advance on the topic of these notes.

References

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

[2] N. Alon, S. Friedland, G. Kalai, Every 4-regular graph plus an edge contains a 3-regular subgraph, *J. Combin. Th. B* **37** (1984) 92–93

[3] N. Alon, Z. Füredi, Covering the cube by affine hyperplanes, *European J. Combin.* **14** (1993) 79–83

[4] J. Borbély, Gy. Károlyi, Covering Cartesian products by hyperplanes, *manuscript*

[5] A.L. Cauchy, Recherches sur les nombres, *J. École Polytech.* **9** (1813) 99–116

[6] P.L. Clark, A. Forrow, J.R. Schmitt, Warning's second theorem with restricted variables, *arXiv:1404.7793*

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

[8] F.J. Dyson, Statistical theory of energy levels of complex systems. I, *J. Math. Phys.* **3** (1962) 140–156

[9] A. Gács, T. Héger, Z.L. Nagy, D. Pálvölgyi, Permutations, hyperplanes and polynomials over finite fields, *Finite Fields Appl.* **16** (2010) 301–314

[10] I.J. Good, Short proof of a conjecture by Dyson, *J. Math. Phys.* **11** (1970) 1884

[11] D.J. Grynkiewicz, Structural Additive Theory, Springer, 2013

[12] R.N. Karasev, F.V. Petrov, Partitions of nonzero elements of a finite field into pairs, *Israel J. Math.* **192** (2012) 143–156

[13] Gy. Károlyi, A compactness argument in the additive theory and the polynomial method, *Discrete Math.* **302** (2005) 124–144

[14] Gy. Károlyi, An inverse theorem for the restricted set addition in Abelian groups, *J. Algebra* **290** (2005) 557–593

[15] Gy. Károlyi, Restricted set addition: The exceptional case of the Erdős–Heilbronn conjecture, *J. Combin. Th. A* **116** (2009) 741–746

[16] Gy. Károlyi, Z.L. Nagy, F.V. Petrov, V. Volkov, A new approach to constant term identities and Selberg-type integrals, *arXiv:1312.6369*

[17] M. Lasoń, A generalization of Combinatorial Nullstellensatz, *Electron. J. Combin.* **17** (2010) #N32, 6 pages

[18] E. Preissmann, M. Mischler, Seating couples around the King's table and a new characterization of prime numbers, *Amer. Math. Monthly* **116** (2009) 268–272

[19] V.A. Tashkinov, 3-regular subgraphs of 4-regular graphs, *Math. Notes* **36** (1984) 612–623

DISTRIBUTION OF PRIMES IN ARITHMETIC PROGRESSIONS

PÉTER MAGA

1. A LITTLE BIT ON COMPLEX FUNCTIONS

Given a domain (open, connected set) $\Omega \subseteq \mathbf{C}$, we say that a function $f : \Omega \to \mathbf{C}$ is holomorphic, if f is differentiable at every point of Ω. Then for any $z_0 \in \Omega$, f is expandable into Taylor series about z_0, i.e. there exist complex numbers $c_0, c_1, \dots$ such that

$$f(z) = \sum_{k=0}^{\infty} c_k (z - z_0)^k$$

is valid on any disc centered at z_0 which is a subset of Ω. Further, insisde such a disc, the series converges absolutely and locally uniformly, and the coefficients are directly matched with the derivatives of f at z_0 by just formally differentiating the Taylor series:

$$c_k = \frac{f^{(k)}(z_0)}{k!}.$$

Now assume that $\Omega \subseteq \mathbf{C}$ is a domain, $z_0 \in \Omega$, and that f is holomorphic function in a small punctured neighborhood of z_0, i.e. f has an isolated singularity at z_0. Assume further that $f(z)(z - z_0)^n$ is bounded in a neighborhood of z_0 for some nonnegative integer n. Taking the smallest such n, we can write the Laurent expansion, with some $c_1, c_2, \dots \in \mathbf{C}$,

$$f(z) = \sum_{k=-n}^{\infty} c_k (z - z_0)^k,$$

which is valid on a punctured neighborhood of z_0. If $n = 0$, then we can in fact remove the singularity and continue f holomorphically to z_0, identifying the new and the old f. If $n > 0$, then we say that f has a pole of order n at z_0. We say that f is meromorphic on Ω, if it is holomorphic on Ω except for some discretely spaced points where it has poles (with removable singularities removed). Using all these, one can easily verify that the meromorphic functions form a field under pointwise addition and multiplication. It is important to keep in mind that under multiplication, there is a cancellation between zeros and poles (e.g. $z \cdot 1/z = 1$), and also under addition, poles might cancel out each other (e.g $1/z + (-1/z) = 0$).

If there is a pole, then the coefficient c_{-1} is called the residue of f at z_0, its significance and also the name will be explained later.

2. DIRICHLET SERIES AND A LITTLE MORE ON COMPLEX FUNCTIONS

Given a sequence $(a_n)_{n \in \mathbf{N}}$ of complex numbers satisfying, we may consider the Dirichlet series

$$D(s) := \sum_{n=1}^{\infty} a_n n^{-s}, \qquad s \in \mathbf{C}.$$

A priori, this is just a formal expression, but one can prove that its convergence domain is a half-plane, by which we mean that if the series is convergent for a certain s_0, then it is also convergent for any s in the half-plane $\Re s > \Re s_0$. Further, in this open half-plane, the convergence is locally uniform, the sum $D(s)$ is a holomorphic (complex analytic) function, and one can calculate the derivatives termwise.

In some cases, one can continue analytically $D(s)$ to some larger domain, as an analogue, think of the power series $1+z+z^2+\dots$, which is convergent only for $|z|<1$, but can be analytically continued to the much larger $\mathbf{C}\setminus\{1\}$ by writing it as $1/(1-z)$: inside $|z|<1$, this is truly the sum of the geometric series, but the form $1/(1-z)$ defines a holomorphic function on the whole $\mathbf{C}\setminus\{1\}$. This is what we mean by analytic continuation to a larger domain, and in the case of Dirichlet series, it is also an important question, if this can be done beyond the convergence domain.

Theorem 1 (Landau's lemma)**.** *If $a_n \geqslant 0$ for every $n \in \mathbf{N}$, then $D(s)$ cannot be continued analytically to any neighborhood of the real boundary point of the convergence domain.*

Proof – not relevant for the class, only a trophy of the complex functions machinery. Renormalizing the coefficients as $a'_n := a_n n^{-\sigma_0}$ (where σ_0 is the real boundary point), we may assume that the real boundary point is 0. By contradiction, assume that there is a small neighborhood of 0 to which $D(s)$ continues analytically as a holomorphic function $\alpha(s)$. Then $\alpha(s)$ is holomorphic on a disc centered at 1 of radius slightly bigger than 1. In the Taylor series

$$\alpha(s) = \sum_{k=0}^{\infty} c_k (s-1)^k,$$

we can calculate the coefficients c_k from the original $D(s)$:

$$c_k = \frac{D^{(k)}(1)}{k!} = \frac{1}{k!}\sum_{k=1}^{\infty} a_n(-\log n)^k n^{-1}.$$

Writing this back to $\alpha(s)$ evaluated at some $-\delta$, for some very small $\delta>0$, where the Taylor series of α is assumed to be convergent, we see

$$\alpha(-\delta) = \sum_{k=0}^{\infty} \frac{(1+\delta)^k}{k!} \sum_{n=1}^{\infty} a_n (\log n)^k n^{-1}.$$

This is a series with nonnegative terms, so we can rearrange it to

$$\alpha(-\delta) = \sum_{n=1}^{\infty} a_n n^{-1} \sum_{k=0}^{\infty} \frac{(1+\delta)^k (\log n)^k}{k!} = \sum_{n=1}^{\infty} a_n n^{-1} e^{(1+\delta)\log n} = \sum_{n=1}^{\infty} a_n n^{\delta},$$

which contradicts that $D(s)$ is not convergent at $-\delta$. □

3. DIRICHLET CHARACTERS

For a fixed $q \in \mathbf{N}$, by a Dirichlet character, we mean a homomorphism of the group $(\mathbf{Z}/q\mathbf{Z})^\times \to \mathbf{C}^\times$, or by a small abuse of terminology, its extension to $\mathbf{N}$ (or even $\mathbf{Z}$) by making it 0 on residue classes which are not coprime to q (and for coprime residue classes, plausibly). The modulo q characters form a group Ξ under pointwise multiplication, and from the fundamental theorem of finite abelian groups (or more elementarily, via the Chinese remainder theorem and the description of primitive roots), one can show that the group of characters modulo q is isomorphic to $(\mathbf{Z}/q\mathbf{Z})^\times$ (even though not canonically). Indeed, let $a_1,\dots,a_r$ be elements of $(\mathbf{Z}/q\mathbf{Z})^\times$ such that every element of $(\mathbf{Z}/q\mathbf{Z})^\times$ can be written in a unique way as $a_1^{k_1}\cdot\ldots\cdot a_r^{k_r}$ under the condition $0 \leqslant k_j \leqslant m_j - 1$, where m_j is the order of a_j. Then by assigning an m_j's root of unity to any a_j, we get χ, and every χ is obtained this way. Let us introduce the notation χ_0 for the trivial character, which is 1 on all coprime residue class.

One can also easily verify the orthogonality relation, for any fixed $a \in \mathbf{Z}$ coprime to q and any $n \in \mathbf{Z}$,

$$\sum_{\chi \in \Xi} \chi(n)\overline{\chi(a)} = \begin{cases} \varphi(q), & \text{if } n \equiv a \bmod q, \\ 0, & \text{otherwise,} \end{cases}$$

where φ is the totient function, the cardinality of $(\mathbf{Z}/q\mathbf{Z})^\times$ (and of Ξ). (Note that there is a dual relation, when we fix two characters and sum over the coprime residue classes, this identifies whether the two characters coincide or not.)

We introduce one more notion about characters. Given a character χ modulo q, it might happen that for some character χ' modulo $q' \mid q$, χ and χ' coincide on residue classes which are coprime to q. For example, the nontrivial character modulo 6 is the same as the nontrivial character modulo 3 apart from even numbers (and on even numbers, a character modulo 6 must vanish by definition). When this happens, we say that χ' induces χ. For every character χ, there is a unique character χ' (with a unique divisor q' of q) such that χ' induces χ. If $q' = q$ (i.e. χ cannot be induced from a lower modulus), then we say that χ is primitive, otherwise, it is imprimitive.

4. THE RIEMANN ZETA FUNCTION AND THE DIRICHLET L-FUNCTIONS

Returning to Dirichlet series, let us consider the most plausible one, namely, when the sequence $(a_n)_{n\in\mathbf{N}}$ is just the constant 1. The resulting Dirichlet series is the famous Riemann zeta function

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s}, \qquad \Re s > 1,$$

the $\Re s > 1$ is imposed, because that it is the convergence half-plane, with absolute and locally uniform convergence there. Also, from the fundamental theorem of arithmetic, we obtain the Euler product form

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}, \qquad \Re s > 1.$$

The product here is taken over the primes, and it means, analogously to infinite sums, $\lim_{N\to\infty} \prod_{p<N} (1 - p^{-s})^{-1}$. (With some analysis, one can prove that the infinite product is also absolutely and locally uniformly convergent in the indicated domain.) With this, one can calculate the logarithmic derivative of zeta:

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \Lambda(n) n^{-s}, \qquad \Re s > 1,$$

where Λ is the von Mangoldt function: $\log p$ on powers of the prime p and 0 otherwise.

In fact $\zeta(s)$ continues meromorphically to $s \in \mathbf{C}$ with a unique simple pole at 1 of residue 1, i.e.

$$\zeta(s) = \frac{1}{s-1} + \text{holomorphic on } \mathbf{C}.$$

The continuation to $\Re s > 0$ can be proven elementarily, much easier than the functional equation.

Similarly, if the coefficient sequence is given by $(\chi(n))_{n\in\mathbf{N}}$ with some Dirichlet character χ modulo q, we obtain the Dirichlet L-function

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_p (1 - \chi(p) p^{-s})^{-1}, \qquad \Re s > 1.$$

This function also admits analytic continuation. When $\chi = \chi_0$, then

$$L(s,\chi_0) = \zeta(s)\prod_{p|q}(1-p^{-s}),$$

so $L(s,\chi_0)$ has a unique simple pole at 1 with residue $\varphi(q)/q$. However, when $\chi \neq \chi_0$, then the Dirichlet series is convergent on the larger domain $\Re s > 0$. This time, there is a holomorphic continuation to the whole $\mathbf{C}$. We again record the logarithmic derivative

$$\frac{L'(s,\chi)}{L(s,\chi)} == -\sum_{n=1}^{\infty}\Lambda(n)\chi(n)n^{-s}, \qquad \Re s > 1,$$

Theorem 2. *For any $\chi \neq \chi_0$, $L(1,\chi) \neq 0$.*

Proof. Consider the function, denoting by Ξ again the group of all modulo q characters.

$$F(s) := \prod_{\chi\in\Xi} L(s,\chi).$$

This product is meromorphic on the whole $\mathbf{C}$ (or on $\Re s > 0$, which is enough for us, and easier as said before), the only potential pole is at 1, simple, and is given by $L(s,\chi_0)$. On $\Re s > 1$, we can take the product of Euler factors:

$$F(s) = \prod_{p\nmid q}\prod_{\chi\in\Xi}(1-\chi(p)p^{-s})^{-1}, \qquad \Re s > 1.$$

Fix some $p \nmid q$, and choose χ' in such a way that $\chi'(p)$ is of maximal order q' among all the $\chi(p)$'s, then all the other orders are divisors of q'. Now group the χ's into collections of size q' as $\chi'\chi, \chi'^2\chi, \dots, \chi'^{q'}\chi$, and consider the product over any such collection:

$$\prod_{j=1}^{q'}(1-\chi'(p)^j\chi(p)p^{-s})^{-1} = (1-p^{-q's})^{-1} = 1 + p^{-q's} + p^{-2q's} + \dots,$$

since $1 - x^{q'} = \prod_{j=1}^{q'}(1-\chi'(p)^j x)$. This means that when we take the product over all $p \nmid q$, we get nonnegative terms, and further, recalling that $q' \mid \varphi(q)$, the coefficient of every pure $\varphi(q)$th power is at least 1.

Now by contradiction, if any $L(1,\chi)$ vanished, then it would cancel the simple pole coming from $L(s,\chi_0)$. Then $F(s)$ would be holomorphic on $\Re s > 0$. But by Landau's lemma, since the coefficients are nonnegative, the convergence half-plane would contain $\Re s > 0$. But this cannot be, since writing $s = 1/\varphi(q)$, we get the reciprocal sum of primes not dividing q, and we know that the reciprocal sum of primes is divergent. □

We remark that the Dirichlet series given as a product has nonnegative coefficients not by chance but for a more profound reason: the Dirichlet series is in fact the zeta function of a (cyclotomic) number field, the coefficienty are counting ideals, and that is why they are nonnegative.

Now Dirichlet's famous theorem on primes in arithmetic progressions is proven by considering, for a coprime to q,

$$\sum_{n\equiv a \bmod q}\Lambda(n)n^{-s} = \frac{1}{\varphi(q)}\sum_{\chi\in\Xi}\overline{\chi(a)}\sum_{n=1}^{\infty}\Lambda(n)\chi(n)n^{-s} = -\frac{1}{\varphi(q)}\sum_{\chi\in\Xi}\overline{\chi(a)}\frac{L'(s,\chi)}{L(s,\chi)}, \qquad \Re s > 1.$$

Since the rightmost expression has a pole at 1 coming from $L(s,\chi_0)$, as $s \to 1$ from above, it tends to ∞. So does then the leftmost expression, and one can easily see that higher prime powers contribute only a finite amount.

5. EVEN MORE ON COMPLEX FUNCTIONS

Let $f : D \to \mathbf{C}$ be a meromorphic function, and assume that $\gamma \subset D$ is a closed, rectifiable curve (in our cases, it will consist of arcs of circles and sides of polygons) that goes about a point z_0 once counterclockwise. Assume that f has no pole on γ and no other than z_0 in the domain bounded by γ. Assume that about z_0, we have the Laurent expansion

$$f(z) = \sum_{k=-n}^{\infty} c_k (z-z_0)^k,$$

Then

$$c_{-1} = \frac{1}{2\pi i}\int_\gamma f(z)\,dz.$$

Intuitively, the reason behind is that for each $n \neq -1$, the term $c_n(z-z_0)^n$ has the primitive function $c_n(z-z_0)^{n+1}/(n+1)$ and Newton–Leibniz applies to give a vanishing integral. The exceptional case $n=-1$, up to scaling, taking $z_0=0$, and deforming the path of integration to a circle is

$$\int_{S^1} z^{-1}\,dz = \int_0^{2\pi} ie^{-i\theta}e^{i\theta}\,d\theta = \int_0^{2\pi} i\,d\theta = 2\pi i,$$

where the applied change of variable is $z=e^{i\theta}$, $dz = ie^{i\theta}\,d\theta$. (Those who have not learned complex functions before, of course, must believe that everything here was correct.) This is why c_{-1} is special, and this is why we call it the residue.

6. PERRON'S FORMULA

We will apply the above considerations in the following setup. Fix some $0<y<\infty$, $y\neq 1$. Fix also some $\sigma>0$. We are interested in integrals of the form

$$\int_{\sigma-iT}^{\sigma+iT} y^s\,\frac{ds}{s}$$

for some large parameter T, i.e. integrals of y^s/s over long vertical lines. It turns out that

$$\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} y^s\,\frac{ds}{s} = \begin{cases} 1+O(y^\sigma \min(1,T^{-1}|\log y|^{-1})) & \text{if } y>1,\\ O(y^\sigma \min(1,T^{-1}|\log y|^{-1})), & \text{if } y<1.\end{cases}$$

Let us first understand the bottom line. Close first the contour as a rectangle in such a way that from $\sigma+iT$ go to $S+iT$ with some superlarge S, then down to $S-iT$, then back to $\sigma-iT$. On the two horizontal lines, the integral in absolute value is at most

$$\int_\sigma^S \frac{y^u}{T}\,du = \left[\frac{y^u}{T|\log y|}\right]_{y=\sigma}^{y=S} \leqslant \frac{y^\sigma}{T|\log y|}.$$

On the far-right vertical segment, the integral in absolute value is at most $y^S T/S$, which is smaller than the previous one, if S is chosen sufficiently large. Since there is no pole inside, the vertical segment on the left must cancel the sum of these. Another way to close the contour is a large circular arc about the origin from $\sigma+iT$ to $\sigma-iT$ (again, on the right). The integration path is of length $O(|\sigma+iT|)$, this is cancelled out by the $|s|=|\sigma+iT|$ in the denominator, and we are left with $O(y^\sigma)$. We choose that contour, which gives the stronger bound. All on all, the statement is proven for $y < 1$.

When $y > 1$, we do the very same, but this time, we have to close the contour on the left. Everything is almost the same, except that this time, we have a pole of y^s/s at 0, and we are interested in the residue there. This is counted from the Taylor expansion of the exponential function as

$$\frac{y^s}{s} = \frac{\exp(s\log y)}{s} = \frac{1}{s} + \text{holomorphic in } s \in \mathbf{C}.$$

Now let x be a large non-integral number, and write $y = x/n$, sum up over $1 \leqslant n < \infty$ with weights $\Lambda(n)$:

$$\sum_{n=1}^{\infty} \Lambda_n \delta_{n<x} = \frac{1}{2\pi i}\sum_{n=1}^{\infty}\int_{\sigma-iT}^{\sigma+iT} \frac{\Lambda(n)}{n^s}\frac{x^s}{s}\,ds + \text{error}.$$

For $\Re s > 1$, we can interchange the summation and the integral and discover the logarithmic derivative of zeta. Writing the optimal $\sigma = 1 + 1/\log x$, and inspecting the error carefully, we arrive at the following.

Theorem 3 (Perron's formula – simplified form). *For any $x \geqslant 2$ and any $2 \leqslant T \leqslant x$, we have*

$$\sum_{n<x} \Lambda(n) = -\frac{1}{2\pi i}\int_{1+1/\log x-iT}^{1+1/\log x+iT} \frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,ds + O\left(\frac{x\log^2 x}{T}\right).$$

7. SOME PROPERTIES OF THE ZETA FUNCTION IN THE CRITICAL STRIP

Since the term x^s/s is too large for $\Re s > 1$, we would like to move the contour to $0 < \Re s = c < 1$. The obvious way is to close it as a rectangle at a real part $0 < c < 1$. The poles of logarithmic derivative ζ'/ζ come from the zeros and poles of zeta. When zeta has a pole (this happens only for $s = 1$), then it contributes residue -1 to the integral of ζ'/ζ, which altogether (with the -1 and the $x^s/s|_{s=1} = x$) gives x. When zeta has a zero, say at ρ, then it contributes similarly $-x^\rho/\rho$ (multiple zeros are to be counted with multiplicity).

(Indeed, all these follow from the Laurent expansion: the logarithmic derivative of a meromorphic function always has simple poles with residues weighted by zeros and poles of the original function:

$$f(z) = a_m z^m + \ldots \rightsquigarrow \frac{f'(z)}{f(z)} = \frac{m}{z} + \ldots, \qquad f(z) = a_m z^{-m} + \ldots \rightsquigarrow \frac{f'(z)}{f(z)} = -\frac{m}{z} + \ldots, \qquad m \in \mathbf{N},$$

while if $f(z) = a_0 + a_1 z\ldots$ with $a_0 \neq 0$, then the logarithmic derivative is holomorphic in a small neighborhood of f with constant term $a_1/a_0 \in \mathbf{C}$.)

Of course, we want to choose the rectangle in such a way that there is no pole on that, and also to satisfy that the connecting vertical lines contribute a small value. The first is obvious to satisfy, since there are only countably many zeros for any meromorphic function, the second one requires some analysis of zeta in the critical line. Without going into details (which would require even more on complex functions), we just state that T can be modified by at most 1 such that the connecting vertical lines contribute $O(\log T)$. Also, the integral on the left side is $O(x^c \log^2 T)$.

$$\sum_{n<x} \Lambda(n) = x - \sum_{\substack{\rho:\zeta(\rho=0)\\ \Re\rho>c, |\Im\rho|<T}} \frac{x^\rho}{\rho} + O\left(\frac{x\log^2 x}{T}\right) + O(x^c \log^2 T).$$

8. PRIME NUMBER THEOREMS

We have two degrees of freedom, namely, in the choice of c and in the choice of T. To get a prime number theorem, T has to be as large as possible (up to x) and c as small as possible to keep the first and the second error terms at minimum. However, zeta has many zeros in the critical strip, and we can even prove that they are spaced symmetrically to the critical line $\Re s = 1/2$ (and also to the real line, obviously). Given this, without analysing how the zeros are spaced, we have to combine c and T in such a way that there is no zero counted in the second term. This is why *zero-free regions* are so important.

The Riemann Hypothesis predicts that all the nontrivial zeros lie on the critical line, hence we can take $c = 1/2 + \varepsilon$ and $T \in (x-1, x)$.

Theorem 4 (prime number theorem conditional to the Riemann Hypothesis)**.** *We have, for $x \geqslant 2$,*

$$\sum_{n<x} \Lambda(n) = x + O_\varepsilon(x^{1/2+\varepsilon}).$$

If we assume a weak version of the Riemann Hypothesis that there are no zeros of real part above some $1/2 < \delta < 1$, we receive something weaker.

Theorem 5 (prime number theorem conditional to a δ-quasi Riemann Hypothesis)**.** *We have, for $x \geqslant 2$,*

$$\sum_{n<x} \Lambda(n) = x + O_\varepsilon(x^{\delta+\varepsilon}).$$

In fact, in both cases, the x^ε is known to be $\log^2 x$.

There are however zero-free regions which are known unconditionally. The classical de la Vallée Poussin type zero-free region is $\sigma > 1 - C/(2 + \log T)$ with some absolute constant $C > 0$, i.e. if we wanted to go up to height T, we can go below 1 essentially by $1/\log T$ with the real part. This gives rise to the following.

Theorem 6 (prime number theorem of de la Vallée Poussin, 1899)**.** *There exists some $C > 0$ such that, for $x \geqslant 2$,*

$$\sum_{n<x} \Lambda(n) = x + O(xe^{-C\sqrt{\log x}}).$$

The Vinogradov–Korobov zero-free region is $\sigma > 1 - C/((\log T)^{2/3}(\log\log T)^{1/3})$ for some $C > 0$ and for any large enough T, and it leads to the following.

Theorem 7 (prime number theorem of Vinogradov–Korobov, 1958)**.** *There exists some $C > 0$ such that, for x large enough,*

$$\sum_{n<x} \Lambda(n) = x + O(xe^{-C(\log x)^{3/5}/(\log\log x)^{1/5}}).$$

9. PRIME NUMBER THEOREMS FOR ARITHMETIC PROGRESSIONS

If we want to prove a prime number theorem for a fixed modulus q as $x \to \infty$, then essentially the whole procedure can be repeated with simple modifications. Namely, the role of zeta is taken by $L(s,\chi)$ where χ runs through all the characters modulo q, recalling the averaging procedure and that the logarithmic derivative of $L(s,\chi)$ reproduces the character-weighted von Mangoldt:

$$\sum_{n \equiv a \bmod q} \Lambda(n) n^{-s} = \frac{1}{\varphi(q)} \sum_{\chi \in \Xi} \overline{\chi(a)} \sum_{n=1}^{\infty} \Lambda(n)\chi(n) n^{-s} = -\frac{1}{\varphi(q)} \sum_{\chi \in \Xi} \overline{\chi(a)} \frac{L'(s,\chi)}{L(s,\chi)}, \qquad \Re s > 1.$$

For a single χ, Perron's formula takes the shape, for $2 \leqslant T \leqslant x$,

$$\sum_{n<x} \Lambda(n)\chi(n) = -\frac{1}{2\pi i}\int_{1+1/\log x - iT}^{1+1/\log x + iT} \frac{L'(s,\chi)}{L(s,\chi)}\frac{x^s}{s}\,ds + O_q\left(\frac{x\log^2 x}{T}\right).$$

Now we shift the contour to the left of the line $\Re s = 1$, for $\chi = \chi_0$, we pick the pole of zeta, and no other L-functions admit a zero or pole on $\Re s = 1$. If the contour shift does not take a zero of $L(s,\chi)$, then we can formulate prime number theorems in arithmetic progressions. If the modulus q is fixed, then the very same zero-free regions are known with the implied constants depending on q. Therefore, for a fixed modulus q and any a coprime to q, one can simply have the following generalization, say, of de la Vallée Poussin's prime number theorem.

Theorem 8. *For any $q \in \mathbf{N}$ and a coprime to q, there exists some $C_q > 0$ such that for $x \geqslant 2$,*

$$\sum_{\substack{n<x \\ n\equiv a \bmod q}} \Lambda(n) = \frac{x}{\varphi(q)} + O_q(xe^{-C_q\sqrt{\log x}}).$$

However, for applications, one usually has to choose q as large as possible in terms of x, i.e. we would like to make the O_q explicit in terms of q. Unfortunately, we can do somewhat little for a single character χ and the corresponding L-function $L(s,\chi)$, but it turns out that they behave well in a family: if a certain $L(s,\chi)$ admitted a zero too close to 1 (believing the Generalized Riemann Hypothesis, we conjecture that such zeros do not exist at all), then many others do not.

10. AN ILLUSTRATION OF THE ZERO-REPULSION

The most complicated characters are the quadratic one, i.e. when $\chi \neq \chi^2 = \chi_0$. Namely, for χ_0 and for $\chi^2 \neq \chi_0$, we can repeat (for example) the de la Vallée Poussin type zero-free region to get that for $L(s,\chi)$, $\Re s > 1 - c/\log(q(2+T))$ is a zero-free region, where q is the conductor of χ, i.e. the modulus corresponding to the primitive character inducing q. For simplicity, assume from now on that χ itself is primitive, i.e. q is itself the modulus of χ.

Unfortunately, we are unable at the moment, however, to rule out the possibility that if χ is a quadratic character, then there is a (necessarily real) zero of $L(s,\chi)$ in a small, namely it can happen that

$$L(\beta,\chi) = 0,$$

where $1-\beta < c/\log q$, i.e. up to our current knowledge, this can happen, no matter how small $c > 0$ is, for some quadratic character χ. Instead of $(\log q)^{-1}$, however, we can write $q^{-\varepsilon}$ for any $\varepsilon > 0$.

Theorem 9 (Siegel)**.** *For any $\varepsilon > 0$, there exists some $c(\varepsilon) > 0$ such that for any primitive quadratic character χ of modulus q, $L(s,\chi)$ does not admit a zero on the segment $[1-c(\varepsilon)q^{-\varepsilon}, 1]$.*

Sketchy proof of an equivalent statement along the lines of Goldfeld. One can translate the statement to that $L(1,\chi) \geqslant c(\varepsilon)q^{-\varepsilon}$ with some potentially different $c(\varepsilon)$ (the transition is not trivial, but neither particularly deep nor complicated). Let $0 < \varepsilon < 1/2$ be given (the statement $\varepsilon \geqslant 1/2$ follows from this, and anyways follows from Dirichlet's class number formula).

Consider the – at the moment, not fully specified, since χ_1, χ_2 will be varying – function $f(s) = \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2)$. This is a nonnegative term Dirichlet series with coefficient 1 for 1^{-s}, and again, not by chance but because this is the zeta function of a (biquadratic) number field.

We claim first that there exists some primitive quadratic character χ_1 modulo q_1 and some $1-\varepsilon<\beta<1$ such that no matter what χ_2 and q_2 are, $f(\beta)\leqslant 0$. Indeed, if there is no $L(s,\chi)$ which would vanish on $(1-\varepsilon,1)$, then the statement is an immediate consequence of that ζ is negative on $(0,1)$ and all the other factors are positive on $(1-\varepsilon,1)$. If there is some χ_1 modulo q_1 and $1-\varepsilon<\beta<1$ such that $L(\beta,\chi_1)=0$, then the claim is also true – no matter what χ_2 and q_2 are.

With this in our toolbox, consider the integral, for any $x>0$ nonintegral,

$$\int_{2-i\infty}^{2+i\infty} f(s+\beta)\frac{x^s}{s(s+1)(s+2)(s+3)(s+4)}\,ds.$$

First note that this can be shown to be $\gg 1$. The reason behind is that for $x>1$,

$$\int_{-2+i\infty}^{2+i\infty}\frac{x^s}{s(s+1)(s+2)(s+3)(s+4)}\,ds=\begin{cases}\frac{(1-x)^4}{4!}, & \text{if } 0<x<1,\\ 0, & \text{if } x>1.\end{cases}$$

This can be shown similarly to our earlier residue calculation before Perron's formula. Now the nonnegativity of the coefficients in the Dirichlet series of $f(s)$ together with that the first coefficient is 1 gives the statement. (One can derive a relative of Perron's formula, this time even without error terms, since the artificially built-in denominator makes the integral absolutely convergent.)

On the other hand, shifting the contour to $s=-\beta$, and using the functional equation, one can see that the integral is (using also the functional equation of L-functions)

$$L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2)\frac{x^{1-\beta}}{(1-\beta)(2-\beta)(3-\beta)(4-\beta)(5-\beta)}+\frac{f(\beta)}{4!}+O\left(\frac{(q_1q_2)^{1+\varepsilon}x^{-\beta}}{1-\beta}\right).$$

Now the second term is nonpositive by assumption, so the first term has to be in magnitude at least as much as the error term. Consequently, if x is carefully chosen such that the error term is about a small constant, and to this aim, x has to be a small ($\varepsilon\cdot\ldots$) power of q_2, then we obtain

$$1\ll L(1,\chi_1)L(1,\chi_2)L(\chi_1\chi_2)q_2^{\varepsilon\cdot\ldots},$$

and using the simple upper bounds $L(1,\chi_1)\ll\log q_1$, $L(1,\chi_1\chi_2)\ll\log(q_1q_2)$, we obtain the statement. □

Getting back to prime numbers (from this, of course, a long path is needed), we get the following.

Theorem 10 (Siegel–Walfisz)**.** *For any $A>0$, there exists a constant $c_A>0$ such that for any $x>2$, $q\leqslant(\log x)^A$ and any a coprime to q,*

$$\sum_{\substack{n\leqslant x\\ n\equiv a \bmod q}}\Lambda(n)=\frac{x}{\varphi(q)}+O(xe^{-c_A\sqrt{\log x}}).$$

11. THE BOMBIERI–VINOGRADOV THEOREM

The Siegel–Wafisz theorem allows that

$$\sum_{\substack{n\leqslant x\\ n\equiv a \bmod q}}\Lambda(n)-\frac{1}{\varphi(q)}\sum_{n\leqslant x}\Lambda(n)$$

is considerably large for a single q, even if q is only a power of x. However, if we average in q even up to almost $\sqrt{x}$, then we have a significant saving.

Theorem 11 (Bombieri–Vinogradov). *For any $A > 0$, there exists some $B > 0$ such that, for $x \geqslant 2$,*

$$\sum_{q \leqslant Q} \sup_{\substack{a \bmod q \\ (a,q)=1}} \left| \sum_{\substack{n \leqslant x \\ n \equiv a \bmod q}} \Lambda(n) - \frac{1}{\varphi(q)} \sum_{n \leqslant x} \Lambda(n) \right| = O_A\left(\frac{x}{(\log x)^A}\right),$$

for any $Q \leqslant x^{1/2}/(\log x)^B$.

Apart from log's, the number of q's is about $\sqrt{x}$, and Generalized Riemann Hypothesis predicts an error $\sqrt{x}$, hence this can be viewed as an "on average" form of the Generalized Riemann Hypothesis.

12. A GLANCE AT SELBERG'S SIEVE

Let $\mathscr{A}$ be a finite set of positive integers, $\mathscr{P}$ a set of primes, and for each $p \in \mathscr{P}$, let $\mathscr{A}_p \subseteq \mathscr{A}$ (in applications, this is usually the elements of $\mathscr{A}$ which fall into the union of some prescribed residue classes). For some $z > 0$, let

$$P(z) := \prod_{\substack{p \in \mathscr{P} \\ p \leqslant z}} p.$$

We are interested in the size of the set $\mathscr{A} \setminus \cup_{p|P(z)} \mathscr{A}_p$, and we express it in terms of the sizes of the sets $\mathscr{A}_d := \cap_{p|d} \mathscr{A}_p$, where d runs through the square-free numbers composed as products of primes in $\mathscr{P}$ (in the application, these sizes are close to their expectations, e.g. $\#\mathscr{A}_{pq}/\#\mathscr{A} \approx (\#\mathscr{A}_p/\#\mathscr{A})(\#\mathscr{A}_q/\#\mathscr{A})$ for $p \neq q$ primes in $\mathscr{P}$).

Theorem 12 (Selberg). *Assume that for some multiplicative function g satisfying $g(p) < 1$ for any $p \in \mathscr{P}$, we have*

$$\#\mathscr{A}_d = g(d)X + R_d$$

with some real number g. Then setting $h(n) := \sum_{d|n} \mu(d)/g(n/d)$ and $V(z) = \sum_{d \leqslant z, d|P(z)} \mu^2(d)/h(d)$, we have

$$\#\left(\mathscr{A} \setminus \bigcup_{p|P(z)} \mathscr{A}_p\right) = \frac{X}{V(z)} + O\left(\sum_{\substack{d_1, d_2 \leqslant z \\ d_1, d_2 | P(z)}} |R_{[d_1,d_2]}|\right).$$

The idea of the proof, very briefly. Let $(\lambda_d)_{d|P(z)}$ be a collection of weights satisfying $\lambda_1 = 1$ and $\lambda_d = 0$ for $d \geqslant z$. For any fixed $a \in \mathscr{A}$, let $D(a)$ be the product of primes for which $a \in \mathscr{A}_p$. Then

$$\sum_{\substack{d|P(z) \\ \mathscr{A}_d \ni a}} \mu(d) = \sum_{d|(P(z),D(a))} \mu(d) \leqslant \left(\sum_{d|(P(z),D(a))} \lambda_d\right)^2 = \left(\sum_{\substack{d|P(z) \\ \mathscr{A}_d \ni a}} \lambda_d\right)^2.$$

With this, the set in question has size

$$\sum_{d|P(z)} \mu(d) \sum_{a\in\mathscr{A}_d} 1 = \sum_{a\in\mathscr{A}_d} \sum_{\substack{d|P(z)\\ \mathscr{A}_d\ni a}} \mu(d) \leqslant \sum_{a\in\mathscr{A}_d} \left(\sum_{\substack{d|P(z)\\ \mathscr{A}_d\ni a}} \lambda_d \right)^2 = \sum_{d_1,d_2\leqslant z} \lambda_{d_1}\lambda_{d_2}\#\mathscr{A}_{[d_1,d_2]}.$$

The rest (and the real matter) of the proof is understanding and optimizing the bilinear form (in $(\lambda_d)_{d|P(z)}$). □

LITERATURE RECOMMENDATION (INCLUDING SELF-ADVERTISING)

For some parts, more details can be found in my online notes, but be careful, there are many typos. I also suggest Terry Tao's notes on his blog. The book of Montgomery and Vaughan titled Multiplicative Number Theory I.: Classical Theory is also a good source. As for Selberg's sieve, one can consult the relevant chapters of Friedlander–Iwaniec's Opera de Cribro and/or Cojocaru–Murty's An Introduction to Sieve Methods and their Applications. Of course, there are many excellent other texts on anything covered or mentioned in the class.

GAPS BETWEEN CONSECUTIVE PRIMES

János Pintz

1. History

Gauss (conjecture 1792–1793):

$$\pi(x) := \sum_{p\in\mathcal{P}, p\le x} 1 \sim \text{li } x = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x},$$

i.e. density of primes around t is $\sim \dfrac{1}{\log t}$.

Riemann's lecture and paper (1859):

Introduction of $\zeta(s) = \sum\limits_{n=1}^{\infty} \dfrac{1}{n^s}$ as a function of $s = \mathbb{C}$.

(Euler 1737 the same function $\zeta(s) = \prod\limits_p \left(1 - \dfrac{1}{p^s}\right)^{-1}$ for real $s \to 1^+$).

($p, p_1, \dots, p_i$ are always primes, $\mathcal{P}$ = set of all primes)

Riemann's lecture: 7 unproved assertions

5 proved around 1900, 1 $(\pi(x) < \text{li } x)$ disproved in 1914.

Open: Riemann Hypothesis (RH)

$\zeta(s) = 0, \quad s = \sigma + it, \quad 0 \le \sigma \le 1 \Longrightarrow \sigma = 1/2$

(true for the first $4 \cdot 10^{13}$ zeros)

Generalized Riemann Hypothesis (GRH): same for Dirichlet's L-functions

How was Riemann led to this conjecture?

$$\text{RH} \Longleftrightarrow \pi(x) := \text{li } x + O\big(\sqrt{x}\log x\big)$$

Remark.

$$\text{li } x = \sum_{n=1}^{R} \frac{(n-1)!x}{(\log x)^n} + O\left(\frac{x}{(\log x)^{R+1}}\right)$$

Prime Number Theorem (PNT) (Hadamard, 1896, de la Vallée Poussin 1896).

$$\pi(x) \sim \text{li } x \sim \frac{x}{\log x}.$$

Average distance between primes

$$d_n : \; p_{n+1} - p_n \approx \log p_n \sim \log n \qquad \text{(on \textit{average})}$$

Twin prime conjecture

$$d_n = 2 \text{ infinitely often (i. o.)}$$

How close can get consecutive primes to each other infinitely often?

$$\Delta_1 := \liminf_{n\to\infty} \frac{d_n}{\log n}$$

$\Delta_1 \leq 1$ follows trivially from PNT (in fact, already from a work of Chebyshev in 1848)

Hardy–Littlewood (1926) GRH $\Longrightarrow \Delta_1 \leq 2/3$
Rankin (1940) GRH $\Longrightarrow \Delta_1 \leq 3/5$

Erdős (1940, unconditionally) $\Delta_1 < 1$

Ricci (1954) $\Delta_1 \leq 15/16$

Bombieri–Davenport (1966) $\Delta_1 < 1/2$ $(\Delta_1 \leq 0.4665\ldots)$

using the Bombieri–Vinogradov theorem (BV)

$\vdots$

H. Maier (1988) $\Delta_1 < 0.2484\ldots$

Theorem 1 (Goldston–Pintz–Yildirim 2006) $\Delta_1 = 0$

Theorem 2 (GPY, conditional) *If BV is true with an exponent $b > 1/2$, i.e. if for any $A > 0$*

$$\max_{x\leq X} \max_{q\leq x^b} \max_{(\ell,q)=1} \left| \pi(x,q,\ell) - \frac{\text{li}\, x}{\varphi(q)} \right| \ll \frac{X}{(\log X)}, \tag{1.1}$$

then $d_n \leq C(b)$ i. o.

Corollary. *If the Elliott–Halberstam conjecture is true, i.e.* (1.1) *is true for any $b < 1$ then $d_n \leq 16$ i. o.*

Theorem 3 (Y. Motohashi–Pintz). *If the above BV theorem is true with a $b > 1/2$ under the restriction ($\forall\varepsilon$ fixed)*

$$p \mid q \Longrightarrow p \leq X^\varepsilon \qquad (q \leq X^b) \tag{1.2}$$

i.e. for smooth values of q then

$$d_n \leq C(b) \quad \textit{i.o.}$$

Theorem 4 (GPY, 2010). $d_n \ll_\varepsilon (\log n)^{1/2+\varepsilon}$ *i. o.*

Theorem 5 (J. P., 2014). $d_n \ll_\varepsilon (\log n)^{3/7+\varepsilon}$ *i. o.*

Theorem 6 (Zhang, 2014) $d_n \le 7 \cdot 10^7$ *i. o.*

Theorem 7 (Maynard + Polymath, 2015) $d_n \le 246$ *i. o.*

Remark. Maynard's method works also with a BV type theorem with an arbitrary fixed small $b > 0$ just the consequence is $d_n \le C^*(b)$ i. o. with a large value of $C^*(b)$ if b is small.

2. Basic idea of the proof of $\Delta_1 = 0$

Let

$$\mathcal{H} = \{h_1, h_2, \ldots, h_k\} \subseteq [1, H] \cap \mathbb{Z}.$$

Our aim is to find at least two primes among $n+h_1, n+h_2, \ldots, n+h_k$, where $n \in (N, 2N)$. We get then

$$p' = n + h_j, \quad p = n + h_i, \quad |h_j - h_i| \le H, \quad p, p' \le 2N + H.$$

We try to choose n within $N+1, \ldots, 2N$ with probability w_n, $\sum\limits_{n=N+1}^{2N} w_n = 1$.

(i) If $w_n = \dfrac{1}{N}$ (equal probability) $\Longrightarrow$ expected number of primes among $n+h_i$ $(i = 1, \ldots, k)$ is

$$E_1 \sim \sum_{i=1}^{k} w_{n+h_i} = k \cdot \frac{1}{\log N} > 1 \Longleftrightarrow k > \log N.$$

(ii) Generalized von Mangoldt function

$$\Lambda_k(n) = \sum_{d \mid n} \mu(d) \log^k \frac{n}{d} = 0 \text{ if } \nu(n) = \sum_{p \mid n} 1 > k$$

indicates the function

$$w_n = \sum_{d \mid P(n,\mathcal{H})} \mu(d) \log^k \frac{P(n,\mathcal{H})}{d}, \quad P(n,\mathcal{H}) = \prod_{i=1}^{k} (n + h_i) \tag{2.1}$$

might be suitable.

Problem 1: We can't evaluate $\sum\limits_{i=n+1}^{n+k} w_i$.

Problem 2: We need $w_n \ge 0$.

(iii) Selberg's idea: Truncate the above w_n at $d \le R$ with an $R = N^c$, $c < 1$ (helps to evaluate $\sum w_i$).

This method works and gives $\Delta_1 \le 1 - b$ if we know the BV theorem with the exponent b.

In particular this gives the Bombieri–Davenport theorem $\Delta_1 \le 1/2$ for $b = 1/2$.

(iv) GPY. Let us be more modest. Try to *approximate* the situation when

$$\exists\, n \in (N, 2N],\ \ \nu(P(n,\mathcal{H})) \le k + \ell \qquad 1 \le \ell \le k-2 \Longrightarrow$$

at least two numbers among $n + h_i$ are primes.

Proof of Theorems 1 and 2. Introduction

The idea (iv) is suitable to reach $\Delta_1 = 0$ and (surprisingly) to prove the Bounded Gap theorem, i.e. $d_n \le C(b)$ i. o. if $b > 1/2$ (Theorem 2).

Proof (version simplified by Y. Motohashi, 2006 GMPY Proc. Japan Acad. Ser. Math.)

Notation number of $n + h_i$, $i = 1, 2, \dots, k$ where we search for two primes.

R truncation for the divisors d of $P(n,\mathcal{H}) = \prod\limits_{i=1}^{k}(n+h_i)$, $\mathcal{H} = (h_1, \dots, h_k) \subseteq [1, H]$

N range for n: $n \in (N, 2N]$. Suppose

$$H \ll \log N \ll \log R \le \log N$$

$\ll$ is Vinogradov's symbol $f \ll g$ means $|f| \ll C|g|$ with some constant $C > 0$.

$k, \ell > 0$ are arbitrary but bounded

c generic constant, $c > 0$ (may be different at different occurrences, may depend on k, ℓ but not on N).

Sieve notation:

$$\Omega(p) := \#\ \text{ of different residue classes among } h_i (\text{mod } p)\ \ (\le k)$$

$$P(n,\mathcal{H}) := \prod_{i=1}^{k}(n+h_i);\ \Omega(d) := \prod_{p|d}\Omega(p)$$

$$\Omega(d) \le k^{\nu(d)} := \tau_k(d) = \sum_{d=d_1 d_2 \dots d_k} 1 \ \text{ if } d \text{ is square-free}$$

Condition: $\Omega(p) < p$ for all $p \Leftrightarrow \mathcal{H}$ is *admissible*

(this gives the chance for all $n + h_i$ to be primes *simultaneously*).

Remark. Dickson's conjecture (1905). If $\mathcal{H}$ is admissible, then all $n + h_i$ are simultaneously primes infinitely often.

Definition.

$$\mu(n) = (-1)^r \ \text{ if } \ n = p_1 \dots p_r,\ n \text{ squarefree},$$

$$\mu(n) = 0 \ \text{ if } \ \exists\, m > 1\ m^2 \mid n.$$

$\mu(n)$ is the well-known Möbius-function

$$\lambda_R(d,a) = \begin{cases} 0 & \text{if } d > R, \\ \frac{1}{a!}\mu(d)\left(\log \frac{R}{d}\right)^a & \end{cases} \qquad \text{(if d is not squarefree then $\lambda_R(d,a)=0$)}$$

$$\Lambda_R(n,\mathcal{H},a) = \sum_{d \mid P(n,\mathcal{H})} \lambda_R(d,a) = \frac{1}{a!} \sum_{\substack{d \mid P(n,\mathcal{H}) \\ d \le R}} \mu(d) \left(\log \frac{R}{d}\right)^a .$$

Choice of $a := k + \ell \quad 1 \le \ell < k$

Choice of weights w_n: $w_n = \Lambda_R^2(n,\mathcal{H},k+\ell) \ge 0$

$$S = \sum_{N<n\le 2N} \Lambda_R^2(n;\mathcal{H},k+\ell) = \sum_{d_1,d_2} \lambda_R(d_1;k+\ell)\lambda_R(d_2;k+\ell) \sum_{\substack{N<n\le 2N \\ [d_1,d_2] \mid P(n,\mathcal{H})}} 1 \tag{3.1}$$

$$d_1, d_2 \big| P(n,\mathcal{H}) \Leftrightarrow [d_1,d_2] \big| P(n,\mathcal{H}) \qquad ([a,b] = lcm(a,b))$$

$$S = N\mathcal{T} + O\biggl(\sum_d |\nu(d)||\lambda_R(d;k+\ell)|\biggr)^2 \tag{3.2}$$

Main term is $N\mathcal{T}$ with

$$\mathcal{T} = \sum_{d_1,d_2} \frac{\Omega([d_1,d_2])}{[d_1,d_2]} \lambda_R(d_1;k+\ell)\lambda_R(d_2;k+\ell). \tag{3.3}$$

Since $\Omega(d) \le \tau_k(d) = \sum_{d=d_1d_2\ldots d_k} 1$ (generalized divisor function)

$$S = N\mathcal{T} + O\bigl(R^2(\log R)^c\bigr). \tag{3.4}$$

Lemma. $\lambda_R(d,a) = \mu(d)\cdot \frac{1}{2\pi i}\int\limits_{(1)} \left(\frac{R}{d}\right)^s \frac{ds}{s^{a+1}} \qquad \Biggl(\int\limits_{(A)} = \int\limits_{A-i\infty}^{A+i\infty}\Biggr)$

(Proof: if $d > R \Leftrightarrow \frac{R}{d} < 1$ we move the line to a large $A > 0$;
if $d < R$ we move to a line $A < 0$ $|A|$ large and we get a residue at $s = 0$.)

$$\mathcal{T} = \frac{1}{(2\pi i)^2} \int\limits_{(1)}\int\limits_{(1)} F(s_1,s_2,\Omega) \frac{R^{s_1+s_2}}{(s_1s_2)^{k+\ell+1}} ds_1 ds_2 \tag{3.5}$$

$$\begin{aligned} F(s_1,s_2,\Omega) &= \sum_{d_1,d_2} \mu(d_1)\mu(d_2) \frac{\Omega(d_1,d_2)}{[d_1,d_2]d_1^{s_1}d_2^{s_2}} \\ &= \prod_p \left(1 - \frac{\Omega(p)}{p}\left(\frac{1}{p^{s_1}} + \frac{1}{p^{s_2}} - \frac{1}{p^{s_1+s_2}}\right)\right) \end{aligned} \tag{3.6}$$

$\Omega(p) = k$ for $p > H$ so

$$G(s_1, s_2, \Omega) = F(s_1, s_2, \Omega) \left(\frac{\zeta(s_1+1)\zeta(s_2+1)}{\zeta(s_1+s_2+1)} \right)^k \tag{3.6}$$

because

$$\prod_p \left(1 - \frac{k}{p^{s_1+1}}\right) \approx \prod_p \left(1 - \frac{1}{p^{s+1}}\right)^k = \frac{1}{\zeta(s_1+1)^k}.$$

Thus $G(s_1, s_2, \Omega)$ is regular and bounded for $\mathrm{Re}\ s_1, \mathrm{Re}\ s_2 > -c$

$$\mathfrak{S}(\mathcal{H}) = G(0, 0, \Omega) = \prod_p \left(1 - \frac{\Omega(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} > 0$$

since $\Omega(p) < p$ and $\Omega(p) = k$ for $p > H$

$$\left(\prod_p \left(1 - \frac{k}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} > 0. \right)$$

The product representation of F and so G implies that G is uniformly bounded for $p > H$.

For $k^2 < p \leq H$ the logarithm of each p-factor is for $\mathrm{Re}\ s_i \geq \sigma \geq -c$

$$\ll H^{-2c} \frac{1}{p} \Rightarrow \sum_{p \leq H} H^{-2\sigma} \frac{1}{p} \ll \exp\left(c(\log N)^{-2\sigma} \log\log N\right)$$

$$\mathcal{T} = \frac{1}{(2\pi i)^2} \int_{(1)} \int_{(1)} G(s_1, s_2, \Omega) \left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)} \right)^k \frac{R^{s_1+s_2}}{(s_1 s_2)^{k+\ell+1}} ds_1 ds_2 \tag{3.7}$$

$$U := \exp\left(\sqrt{\log N}\right). \tag{3.8}$$

Let us move the integration line for s_1 and s_2 to $1/\log U + it$, and $1/(2\log U) + it$, resp. and truncate them at $|t| \leq U$ and $|t| \leq U/2$, resp. $\Rightarrow L_1, L_2$

$$\mathcal{T} = \int_{L_1} \int_{L_2} + O\left(\exp\left(-c\sqrt{\log N}\right)\right) \tag{3.9}$$

since $\zeta(1+s), 1/\zeta(1+s) \ll \log|t|$ if $|t| \geq 2$, $\sigma \geq 0$.

Next step: shift $L_1 \to L_3 = -c/\log U + it$, $|t| \leq 0$

Singularities at $s_1 = 0$ (pole of order $\ell + 1$) and

$s_1 = -s_2$ (pole of order k)

ζ behaves sufficiently nicely, so

$$\mathcal{T} = \frac{1}{2\pi i} \int\limits_{L_2} \left\{ \operatorname*{Res}_{s_1=0} + \operatorname*{Res}_{s_1=-s_2} \right\} ds_2 + O\left(\exp\left(-c\sqrt{\log N}\right)\right) \tag{3.10}$$

$$\operatorname*{Res}_{s_1=-s_2} = \frac{1}{2\pi i} \int\limits_{C(s_2)} G(s_1, s_2, \Omega) \left(\frac{\zeta(s_1+s_2+1)}{\zeta(s_1+1)\zeta(s_2+1)} \right)^k \frac{R^{s_1+s_2} ds_1}{(s_1 s_2)^{k+\ell+1}} \tag{3.11}$$

$C(s_2) : |s_1 + s_2| = 1/\log N$

$G(s_1, s_2, \Omega) \ll (\log\log N)^c, \quad \zeta(s_1+s_2+1) \ll \log N, \ \ R^{s_1+s_2} \ll 1$

$$\left(s_1\zeta(s_1+1)\right)^{-1} \ll (s_2+1)^{-1} \log(|s_2|+2)$$

$$\operatorname*{Res}_{s_1=-s_2} \ll (\log N)^{k-1} (\log\log N)^c \left(\frac{\log(|s_2|+2)}{|s_2|+1} \right)^{2k} |s_2|^{-2\ell-2}$$

$$\mathcal{T} = \frac{1}{2\pi i} \int\limits_{L_2} \left\{ \operatorname*{Res}_{s_1=0} \right\} ds_2 + O\left((\log N)^{k+\ell-1/2} (\log\log N)^c\right) \tag{3.12}$$

To evaluate the integral, let

$$Z(s_1, s_2) = G(s_1, s_2, \Omega) \underset{\downarrow}{\left(\frac{(s_1+s_2)\zeta(s_1+s_2+1)}{s_1\zeta(s_1+1)s_2\zeta(s_2+1)} \right)^k} \tag{3.13}$$

regular at $s_1 = 0$, $s_2 = 0$, $s_1 = -s_2$
(in particular, regular at $(0,0)$
and its neighborhood)

$$\operatorname*{Res}_{s_1=0} = \frac{R^{s_2}}{\ell! s_2^{\ell+1}} \left(\frac{\partial}{\partial s_1} \right)^\ell_{s_1=0} \left\{ \frac{Z(s_1,s_2)}{(s_1+s_2)^k} R^{s_1} \right\}.$$

We write this into (3.12) and shift the contour L_2 to

$$L_4 = -\frac{c}{\log U} + it, \quad |t| \le U/2.$$

Similarly as before, the new integral is $O\left(\exp\left(-c\sqrt{\log N}\right)\right)$

$$\mathcal{T} = \operatorname*{Res}_{s_2=0} \operatorname*{Res}_{s_1=0} + O(\log N)^{k+\ell} = \frac{1}{(2\pi)^2} \int\limits_{C_2} \int\limits_{C_1} \frac{Z(s_1,s_2) R^{s_1+s_2}}{(s_1+s_2)^k (s_1 s_2)^{\ell+1}} ds_1 ds_2 + O(\log N)^{k+\ell}$$

with $C_1 := \left\{s_1; |s_1| = \varrho\right\}, \ C_2 = \left\{s_2; |s_2| = 2\varrho\right\}$ with a small $\varrho > 0$.

Let us write $s_1 = s$, $s_2 = s\xi$; $C_3 = \{\xi; |\xi| = 2\}$

$$\begin{aligned}\frac{1}{(2\pi i)^2} \int\limits_{C_3} \int\limits_{C_1} \frac{Z(s, s\xi) R^{s(\xi+1)}}{(\xi+1)^k \xi^{\ell+1} s^{k+2\ell+1}} ds d\xi &= \\ = \frac{Z(0,0)}{2\pi i (k+2\ell)!} (\log R)^{k+2\ell} \int\limits_{C_3} \frac{(\xi+1)^{2\ell}}{\xi^{\ell+1}} d\xi \\ + O\left((\log N)^{k+2\ell-1} (\log\log N)^c\right)\end{aligned}$$

We obtained now the sum of weights

$$w_n = \Lambda_R(n, \mathcal{H}, k+\ell)^2.$$

Lemma 1. *If $H \ll \log N \ll \log R \le \log N$, $R \ll \sqrt{N}/(\log N)^C$ with a large C, k, ℓ bounded then*

$$\sum_{N<n\le 2N} \Lambda_R(n, \mathcal{H}, k+\ell)^2 = \frac{\mathfrak{S}(\mathcal{H})}{(k+2\ell)!} \binom{2\ell}{\ell} N (\log R)^{k+2\ell} + O\big(N (\log N)^{k+2\ell-1} (\log\log N)^c\big).$$

4. Twist with primes

Let $\theta(n) = \begin{cases} \log n & \text{if } n = p \in \mathcal{P}, \\ 0 & \text{otherwise.} \end{cases}$

$$\sum_{N<n\le 2N} \Lambda_R^2(n, \mathcal{H}, k+\ell)^2 \theta(n+h) \qquad \Bigg(\approx \sum_{\substack{n+h\in\mathcal{P} \\ N<n\le 2N}} w_{n+h} \log N\Bigg) \tag{4.1}$$

Observation: if $h \in H$, $n+h \in \mathcal{P}$, $R < N$, then $d \Big| \prod\limits_{h_i\in\mathcal{H}} (n+h_i) \Leftrightarrow d \Big| \prod\limits_{\substack{h_i\in\mathcal{H} \\ h_i\ne h}} (n+h_i)$, that is

$$\Lambda_R(n, \mathcal{H}, j) = \Lambda_R(n, \mathcal{H} \setminus \{h\}, j) \ \text{ for any } j$$

provided $R < N$ since $d \le R < N < n + h_i$.

This means that we can assume $h \notin \mathcal{H}$.

Crucial information: "on average" $\theta(n) = 1$. This is true for arithmetic progressions as well by the BV theorem with exponent b, i.e. if instead of $\pi(x, q, a)$ we work with $\big((a,q) = \gcd(a,q) = 1$, $\varphi =$ Euler's $\varphi\big)$

$$\vartheta(x, q, a) = \sum_{\substack{n\le x \\ n\equiv a(q)}} \theta(n) \tag{4.2}$$

then $\forall A > 0$

$$\sum_{q\le x^b} \max_{y<x} \max_{(a,q)=1} \left| \vartheta(y, q, a) - \frac{y}{\varphi(q)} \right| \ll_A \frac{x}{(\log x)^A}. \tag{4.3}$$

Suppose $R \le N^{b/2} \big/ \log^A N$ (and $h \notin \mathcal{H}$).

$$\text{(4.4)} \qquad \sum_{d_1,d_2} \lambda_R(d_1,k+\ell)\lambda_R(d_2,k+\ell) \sum_{\substack{n+h\in\mathcal{P}\\ d_1,d_2\mid P(n,\mathcal{H})}} \log(n+h)$$

$$= \sum_{d_1,d_2} \lambda_R(d_1,k+\ell)\lambda_R(d_2,k+\ell) \sum_{\substack{a \bmod [d_1,d_2]\\ [d_1,d_2]\mid P(a)\\ (a+h,[d_1,d_2])=1}} \vartheta\big(N,[d_1,d_2],a+h\big) + O\big(R^2(\log N)^c\big)$$

$$= N\mathcal{T}^* + O\big(N/(\log N)^{A/3}\big)$$

where

$$\text{(4.5)} \qquad \mathcal{T}^* = \sum_{d_1,d_2} \frac{\lambda_R(d_1,k+\ell)\lambda_R(d_2,k+\ell)}{\varphi([d_1,d_2])} \sum_{\substack{a \bmod [d_1,d_2]\\ [d_1,d_2]\mid P(a)\\ (a+h,[d_1,d_2])=1}} 1.$$

How do we get the error term $O\big(N/(\log N)^{A/3}\big)$?

First case if $\Omega([d_1,d_2]) = \tau_k([d_1,d_2]) \le (\log N)^{A/2}$.

In this case we apply the BV theorem (4.3) directly in $\forall AP$.

The 2nd case when $\Omega([d_1,d_2]) > (\log n)^{A/2}$ then

$$\ll N(\log R)^{2(k+\ell)}\log N \sum_{d_1,d_2\le R} \frac{\tau_k([d_1,d_2])}{(\log N)^{A/2}} \frac{\tau_k([d_1,d_2])}{[d_1,d_2]}$$
$$\ll N\frac{(\log N)^c}{(\log N)^{A/2}} < \frac{N}{(\log N)^{A/3}}$$

since

$$\sum_{n\le Y} \frac{\tau_k^2(n)\cdot\tau(n)}{n} \le \log^c Y \quad (c \text{ may always depend on } k).$$

Evaluation of $\mathcal{T}^*$ is similar to that of $\mathcal{T}$

# of residue classes a mod $[d_1,d_2]$ with

$$[d_1,d_2] \mid P(a,\mathcal{H}) \ \text{ and } \ (a+h,[d_1,d_2]) = 1$$

is by multiplicity the same as the product of

$$\#\ a \quad \bmod p \ \text{ with } \ p \,\Big|\, \prod_{i=1}^{k}(a+h_i), \quad p \nmid a+h.$$

If $h \in \mathcal{H}$ this is $\Omega_{\mathcal{H}}(p) - 1$ with $\mathcal{H}^+ = \mathcal{H}\cup\{h\}$.

If $h \notin \mathcal{H}$ this is the same as $\Omega_{\mathcal{H}^+}(p) - 1$ with $\mathcal{H}^+ = \mathcal{H} \cup \{h\}$.

We denote $\Omega_{\mathcal{H}^+}(p) = \Omega^+(p)$.

In the evaluation of $\mathcal{T}^*$ everything is analogous as in the evaluation of $\mathcal{T}$ just the role of $1 - \dfrac{\Omega(p)}{p}$ will be played by $1 - \dfrac{\Omega^+(p) - 1}{p-1}$ in the Euler product.

For $p > H$ we have by $h \notin \mathcal{H}$

$$\Omega^+(p) = k+1, \qquad \Omega^+(p) - 1 = k.$$

If $\mathcal{H}^+$ is admissible then analogously to $\mathcal{T}$ we get for $h \notin \mathcal{H}$

$$\mathcal{T}^* = \frac{\mathfrak{S}(\mathcal{H}^+)}{(k+2\ell)!}\binom{2\ell}{\ell}(\log R)^{k+2\ell} + O\left((\log N)^{k+2\ell-1}(\log\log N)^c\right). \tag{4.6}$$

If $\mathcal{H}^+$ is not admissible, i.e. $\mathfrak{S}(\mathcal{H}^+) = 0$ then the Euler product vanishes. Argument is similar with the main term equal 0.

If $h \in \mathcal{H}$ then $\left|\mathcal{H} \setminus \{h\}\right| = k-1$, therefore $k + \ell = k - 1 + \ell + 1$, so Section 3 is valid with the change $k \to k-1$, $\ell \to \ell + 1$.

Summarizing, the results of Section 4 yield

Lemma 2.

$$\sum_{N<n\le 2N} \Lambda_R^2(n, \mathcal{H}, k+\ell)\theta(n+h) =$$
$$= \begin{cases} \dfrac{\mathfrak{S}(\mathcal{H}\cup\{h\})}{(k+2\ell)!}\binom{2\ell}{\ell} N(\log R)^{k+2\ell} + O(B_1) & \text{if } h \notin \mathcal{H}, \\ \dfrac{\mathfrak{S}(\mathcal{H})}{(k+2\ell+1)!}\binom{2(\ell+1)}{\ell+1} N(\log R)^{k+2\ell+1} + O(B_2) & \text{if } h \in \mathcal{H} \end{cases}$$

where $B_1 = N(\log N)^{k+2\ell-1}(\log_2 N)^c$, $B + N(\log N)^{k+2\ell}(\log_2 N)^c$, $\log_2 N = \log\log N$.

5. Proofs of Theorems 1–2

We shall consider the average of the number of primes in all k-tuples $\mathcal{H} \subseteq [1, 2, \dots H]$ averaged over $(N, 2N]$ with the weights $w_n = \Lambda_R^2(n; \mathcal{H}; (k+\ell))$ with a free parameter $\ell \in [1, k-1]$

$$I = \sum_{\substack{\mathcal{H}\subseteq[1,H] \\ |\mathcal{H}|=k}} \sum_{N<n\le 2N} \left(\sum_{h\le H} \theta(n+h) - \log 3N\right) \Lambda_R^2(n; \mathcal{H}; k+\ell). \tag{5.1}$$

If $I > 0$ then $\exists n \in (N, 2N]$ such that

$$\sum_{h\le H} \theta(n+h) - \log 3N > 0 \tag{5.2}$$

so there is an interval of length H, between N and $2N + H < 3N$ containing at least two primes:

$$\min_{N<p_r\le 2N+H}(p_{r+1}-p_r) \le H. \tag{5.3}$$

Since in the evaluations of Lemma 1 and Lemma 2 we have

$$\mathfrak{S}(\mathcal{H}) = \prod_p \left(1-\frac{\Omega_{\mathcal{H}}(p)}{p}\right)\left(1-\frac{1}{p}\right)^{-k}$$

we need

Lemma 3 (Theorem of Gallagher (1976)).

$$\sum_{\substack{\mathcal{H}\subseteq[1,H]\\ |\mathcal{H}|=k}} \mathfrak{S}(\mathcal{H}) = (1+o(1))H^k \qquad \text{if } k \text{ fixed},\ \ H\to\infty. \tag{5.4}$$

Lemmas 1 and 3 yield for I in (5.1)

$$I = \sum_{\substack{\mathcal{H}\subseteq[1,H]\\ |\mathcal{H}|=k}} \sum_{N<n\le 2N} \Bigg\{\sum_{\substack{h\le H\\ h\notin\mathcal{H}}} + \sum_{\substack{h\le H\\ h\in\mathcal{H}}}\Bigg\}\theta(n+h)\Lambda_R^2(n,\mathcal{H},k+\ell) \tag{5.5}$$
$$- \frac{NH^k}{(k+2\ell)!}\binom{2\ell}{\ell}\log N(\log R)^{k+2\ell} + o\big(NH^k(\log N)^{k+2\ell+1}\big).$$

We can evaluate the first term by Lemma 2:

$$I = \frac{NH^{k+1}}{(k+2\ell)!}\binom{2\ell}{\ell}(\log R)^{k+2\ell} + \frac{kNH^k}{(k+2\ell+1)!}\binom{2(\ell+1)}{\ell+1}(\log R)^{k+2(\ell+1)} \tag{5.6}$$
$$-\frac{NH^k}{(k+2\ell)!}\binom{2\ell}{\ell}\log N(\log R)^{k+2\ell}(1+o(1)) =$$
$$= \left(H + \frac{k}{k+2\ell+1}\cdot\frac{2(2\ell+1)}{\ell+1}\log R - \log N(1+o(1))\right)\binom{2\ell}{\ell}\frac{NH^k(\log R)^{k+2\ell}}{(k+2\ell)!}$$

if $R \ge N^c$, by $\binom{2(\ell+1)}{\ell+1} = \dfrac{(2\ell+2)(2\ell+1)}{(\ell+1)^2} = \dfrac{2(2\ell+1)}{\ell+1}$.

We have $I > 0$ if $R = N^{b/2}\big/\log^A N$ and

$$H > \left(1+\varepsilon - \frac{k}{k+2\ell+1}\cdot\frac{2(2\ell+1)}{\ell+1}\cdot\frac{b}{2}\right)\log N. \tag{5.7}$$

Choosing $\ell = \left[\sqrt{k}\right]$, say, we need just

$$H > \big(1-2b(1+o_k(1)\big)\log N \qquad o_k(1)\to 0 \ \text{ as } \ k\to\infty. \tag{5.8}$$

Therefore

$$\Delta_1 = \liminf_{n\to\infty} \frac{d_n}{\log n} \le \max(0, 1-2b).$$

This gives $\Delta_1 = 0$ if $b = 1/2$.

Remark. If $\Lambda_R = \Lambda_R(n; \mathcal{H}; k)$ that is, $\ell = 0$ then we need $H \ge (1 - b + o(1)) \log N$ which implies only $\Delta_1 \le 1/2$ for the optimal choice $b = 1/2$.

Let us assume $b > 1/2$. Then for $k > k_0(b)$ (5.7) will hold, that is, we obtain

$$d_n \le H \quad \text{if} \quad H \ge C'(k) = C_0(b) \Longrightarrow$$

$$d_n \le C_0(b) \quad \text{i. o.} \tag{5.8}$$

6. Further developments, new problems on gaps between primes

Polignac's conjecture (1849): for every $k > 0$ we have $d_n = 2k$ i. o.

BOUNDED GAPS BETWEEN CONSECUTIVE PRIMES

Theorem A (Maynard 2015). *We have for any m*

$$\liminf_n (p_{n+m} - p_n) \ll e^{4m}. \tag{6.1}$$

Method: a k dimensional sieve, the weights depend on $d_1, \dots, d_k$ if $d = d_1 \dots d_k \mid P(n, \mathcal{H}) = \prod_{c=1}^{k} (n + h_i)$, $d_i \mid n + h_i$

Theorem B (Maynard 2015). *A positive proportion of all admissible k-tuples $\mathcal{H} = \{h_i\}_{i=1}^k$ satisfies Dickson's k-tuple conjecture, i.e.,*

$$\{n + h_i\}_{i=1}^k \in \mathcal{P}^k \quad \textit{for infinitely many } n. \tag{6.2}$$

Theorem C (Maynard 2015). $\liminf_{n\to\infty} (p_{n+1} - p_n) \le 600$.

Theorem D (Tao + Polymath 8): $\liminf_{n\to\infty} (p_{n+1} - p_n) \le 246$.

Theorem E (Maynard, 2013): *EH* $\Longrightarrow \liminf_{n\to\infty} (p_{n+1} - p_n) \le 12$.

LARGE GAPS BETWEEN CONSECUTIVE PRIMES

$$\lambda := \limsup_{n\to\infty} \frac{d_n}{\log n} \qquad (\ge 1)$$

Backlund (1929): $\lambda \ge 2$

Brauer–Zeitz (1930): $\lambda \geq 4$

Westzynthius (1931): $\lambda = \infty$

Erdős 1935: $\limsup\limits_{n\to\infty} \dfrac{d_n/\log n}{\log_2 n/(\log_3 n)^2} \geq 2e^\gamma \qquad \log_\nu n = \underbrace{\log\ldots\log}_{\nu} n$

Rankin 1938: $\limsup\limits_{n\to\infty} \dfrac{d_n}{g(n)\log n} \geq C \quad g(n) = \dfrac{\log_2 n \log_4 n}{(\log_3 n)^2}$

Erdős (1979) offered USD 10,000: C can be arbitrary

Results reached after 1979:

H. Maier – C. Pomerance (1990):	$C = 1.31\ldots e^\gamma$
J. Pintz (1997):	$C = 2e^\gamma$

Theorem F (Ford–Green–Konjagin–Tao; Maynard, arXiv, Aug. 2014): *Erdős's conjecture is true.*

Theorem G (Ford–Green–Konjagin–Maynard–Tao, arXiv, Dec. 2014):

$$\limsup_{n\to\infty} \frac{d_n}{h(n)\log n} \geqslant C, \qquad h(n) = \frac{\log_2 n \log_4 n}{\log_3 n}.$$

CHAINS OF LARGE GAPS BETWEEN CONSECUTIVE PRIMES

Problem of Erdős (1949): $\limsup\limits_{n\to\infty} \dfrac{\min(d_{n+1},\ldots,d_{n+k})}{\log n} \overset{?}{=} \infty$

Erdős (1949): the above is true for $k = 2$

Helmut Maier 1985: $\limsup\limits_{n\to\infty} \dfrac{\min(d_{n+1},\ldots,d_{n+k})}{g(n)\log n} > 0$

ARITHMETIC PROGRESSIONS OF GENERALIZED TWIN PRIMES

Theorem H (Green–Tao, 2004): *The primes contain arbitrarily long (finite) arithmetic progressions.*

(Previously this was known only for 3-term AP's by results of Čudakov, Estermann and van der Corput in 1937–38.)

Theorem 1 (J. P., arXiv 2013): *There exists an absolute constant C_0 and an even $d \leq C_0$ with the following property. For every k there is a k-term AP of primes such that for each element p of the progression $p + d$ is also a prime, more exactly, the prime following p.*

Remark. One can prove Theorem 1 with $C_0 = 246$.

POLIGNAC NUMBERS

Def: $2k$ is a Polignac number if $d_n = 2k$ i.o.

Polignac's Conjecture: *Every positive even number is a Polignac number.*

Proposition. *Bounded Gaps Conj.* $\Leftrightarrow$ $\exists$ *at least one Pol. number.*

Theorem 2 (J. P., arXiv 2013): *There are infinitely many Polignac numbers, and their lower asymptotic density is positive.*

Corollary: *For* $\forall k$ $\exists$ k*-term AP of Polignac numbers.*

Theorem 3 (J. P., arXiv 2013): *If* r_n *is the* n^{th} *Polignac number, then* $r_{n+1} - r_n \le C$ (C *ineffective*).

THE NORMALIZED VALUE DISTRIBUTION OF d_n

$$\text{Prime Number Theorem: } \Rightarrow \frac{1}{N}\sum_{n=1}^{N} \frac{d_n}{\log n} = 1. \tag{6.3}$$

Conjecture (Erdős): $d_n/\log n$ *is everywhere dense in* $[0,\infty]$, *i.e.*

$$J = \left\{\frac{d_n}{\log n}\right\}' = [0,\infty]. \tag{6.4}$$

Theorem (Ricci 1954, Erdős 1955): J *has a positive (Lebesgue) measure.*

However, no finite limit point was known till 2005.

Theorem (Goldston–Pintz–Yıldırım, 2005–9): $0 \in J$.

Theorem 4 (J. P., arXiv 2013): $\exists c$ *(ineffective) such that* $[0,c] \subset J$.

Theorem I (D. Banks, T. Freiberg, J. Maynard, arXiv 2014): *For every* $T > 0$ *we have*

$$\lambda(J \cap [0,T]) > (1+o(1))T/8.$$

Theorem 5 (J. P., arXiv 2015): *For every* $T > 0$ *we have*

$$\lambda(J \cap [0,T]) > (1+o(1))T/4.$$

Theorem I (J. Merikoski, 2020). *For every $T > 0$ we have*

$$\lambda(J \cap [0,T]) > (1+o(1))T/3.$$

Def: Let $\mathcal{F}$ be the class of functions satisfying with an arbitrarily large c_0 and for every $\varepsilon > 0$ with an $N_0(\varepsilon)$ for $N > N_0(\varepsilon)$.

(i) $f(x) \nearrow \infty,\ \ f(x) \le c_0 g(x) \log x,$

(ii) $(1-\varepsilon)f(N) \le f(n) \le (1+\varepsilon)f(N)$ if $n \in [N, 2N]$.

Theorem 6 (J. P., arXiv 2014): *If $f \in \mathcal{F}$, $J_f = \{d_n/f(n)\}'$ then $\exists c_f$ (ineffective) such that $[0, c_f] \subset J_f$.*

Theorem 7 (J. P., arXiv 2014): *Let $\{f_i\}_{i=1}^{\infty} \subset \mathcal{F}$, $\displaystyle\lim_{x\to\infty} \frac{f_{i+1}(x)}{f_i(x)} = \infty$. Then apart from at most 98 functions $f_i(x)$*

$$J_f = \left\{ \frac{d_n}{f(n)} \right\}' = [0, \infty).$$

Corollary: *Let $\eta(x) \to 0$ arbitrary, $F(x), \eta(x)F(x) \in \mathcal{F}$. Then we have an $f \in \mathcal{F}$ with*

$$\eta(x)F(x) \le f(x) \le F(x), \quad J_f = \left\{ \frac{d_n}{f(n)} \right\} = [0, \infty).$$

COMPARISON OF CONSECUTIVE VALUES OF d_n

Erdős (1948) $\displaystyle\liminf_{n\to\infty} \frac{d_{n+1}}{d_n} < 1 < \limsup \frac{d_{n+1}}{d_n}$

Erdős (1956) "One would of course conjecture that

$$\liminf_{n\to\infty} \frac{d_{n+1}}{d_n} = 0 \text{ and } \limsup_{n\to\infty} \frac{d_{n+1}}{d_n} = \infty \ \left(\Leftrightarrow \liminf_{n\to\infty} \frac{d_n}{d_{n+1}} = 0 \right) \tag{6.5}$$

but these conjectures seem very difficult to prove."

Theorem 8 (J. P., arXiv 2013): *Erdős's conjecture* (6.5) *is true, we have even*

$$\liminf_{n\to\infty} \frac{d_{n+1} g(n) \log n}{d_n} < \infty, \quad \limsup_{n\to\infty} \frac{d_{n+1}}{d_n g(n) \log n} > 0 \tag{6.6}$$

CHAINS OF CONSECUTIVE VALUES OF d_n

Theorem 9 (J. P., arXiv 2014): *If $f(x) \in \mathcal{F}$, k arbitrary then we have an infinite sequence of integers n with*

$$c_1(k)f(n) \le d_{n+i} \le c_2(k)f(n) \quad \text{for} \quad i = 1, 2, \dots, k.$$

($c_1(k), c_2(k)$ explicitly calculable constants).

Remark 1. Since $f(x)$ can tend arbitrarily slowly to ∞ this is a common generalization of the results of Maynard and Theorem F of Ford–Green–Konjagin–Tao/Maynard.

Another combination of these methods yield

Theorem 10 (J. P., arXiv 2014): *For every k_0 there is a $k \in \left[k_0, Ce^{4k_0}\right]$ with*

$$\limsup_{n\to\infty} \frac{\min(d_n, d_{n+k+1})}{\max(d_{n+1}, \dots, d_{n+k})g(n)\log n} > c'(k).$$

Remark 2. This was proved little later by Ford–Maynard–Tao with $h(n)$ instead of $g(n)$.

COMPARISON OF ℓ CONSECUTIVE VALUES OF d_n

Erdős and Turán (1948). Give a necessary and sufficient condition that (k is fixed)

$$\sum_{i=1}^{k} a_i p_{n+i}$$

should have infinitely many sign changes as $n \to \infty$.

Remark. $\sum_{i=1}^{k} a_i = 0$ is clearly necessary by $p_n \sim p_{n+k}$. If this is true then the original problem can be reformulated.

Problem (Erdős–Turán (1948)): Give a necessary and sufficient condition that (ℓ is fixed)

$$\sum_{i=1}^{\ell} \alpha_i d_{n+i}$$

should have infinitely many sign changes as $n \to \infty$.

Conjecture (Erdős, 1972): *The condition is that the non-zero elements of $\{\alpha_i\}_{i=1}^{\ell}$ cannot all have the same sign.*

Theorem 11 (J. Pintz, 2015): *The above conjecture of Erdős is true.*

Theorem 12 (J. Pintz, arXiv 2015): *There exists a $c(\ell) = C_1 e^{-C_2 \ell}$ for every ℓ such that*

$$\limsup_{n\to\infty} \frac{d_n}{\max(d_{n-e}, \dots, d_{n-1}, d_{n+1}, \dots, d_{n+\ell})(\log n)^{c(\ell)}} > 0.$$

Remark. A little later this was improved by S. Konjagin to $c(\ell) = 1/8$ (for every ℓ).

Note: combined with Theorem 5 his method yields this even with $c(\ell) = 1/4$.

ELLIPTIC CURVES (MINICOURSE)

Árpád Tóth

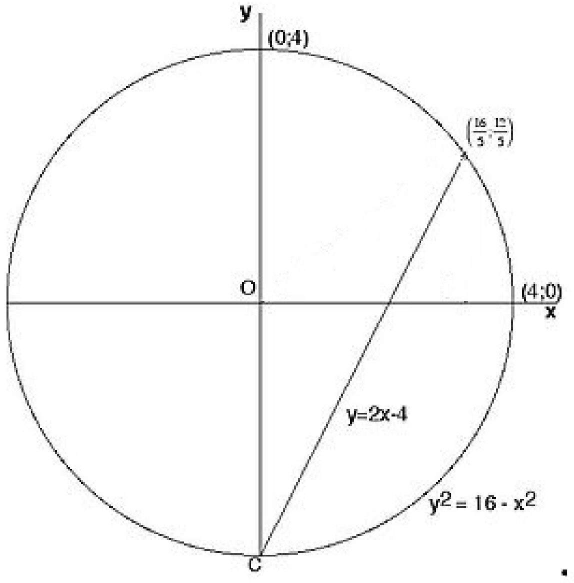
Contents

1. Introduction

1.1. **The genesis of elliptic curves.** Elliptic curves first appeared in Diophantus' Arithmetica cca 3rd century C.E. In its subject, its tools and organization this book is very different from other mathematical treatises of antiquity. The Arithmetica consists of problems, numerous examples of Diophantine equations, some challenging even today. Because it does not give a theoretical discussion some people view the book unfavourably, but it contains more than just individual tricks. The main invention is a symbolic notation for a variable, for powers, for equality, the negative sign among others. Diophantus used this machinery for a well defined algebraic method that we now discuss.

Example 1.1. Express 16 as the sum of 2 squares. Let x^2 be one of the squares. Let the other side be $mx - 4$. Diophantus has no notation for a second variable, and choses $m = 2$. The equation $x^2 + (2x - 4)^2 = 16$ then easily leads to $x = 16/5$ when $y = 12/5$.

This has a simple geometric illustration.



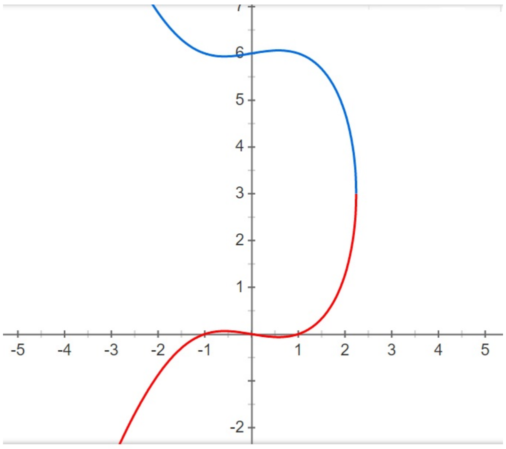
The point of this "chord" method is, that a line through a point on the circle, in this case $(-4, 0)$ will intersect the circle in on other point. If the line has rational slope, the coordinates of the other intersection will also be rational.

Example 1.2. Divide a number so that its product is a cube minus its side. This is the equation

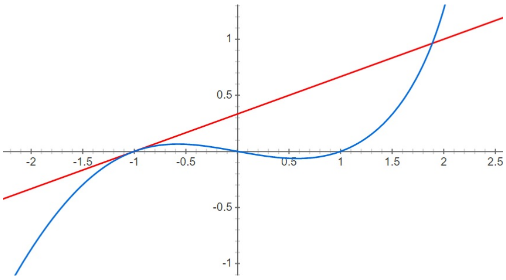
$$y(6 - y) = x^3 - x$$

with an obvious point $P(-1, 0)$. Again choose a linear function, $x = ay - 1$ through P, Diophantus finds a so that $y = 0$ is a double root of $y(6 - y) - (ay - 1)^3 + (ay - 1)$. This happens when $a = 3$, when the equation becomes $-y^2 = 27y^3 - 27y^2$. Therefore $y = 26/27$ and $x = 17/9$ is another solution.

It is again illustrative to view this method on a graph, Dipohantus constructs the tangent line at the point $(-1, 0)$.



The graph of $y(6-y) = x^3 - x$



The tangent line at $(-1, 0)$

Further examples of the method came much later after Diophantus' work reappeared during the Renaissance. Here are two due to Fermat.

Example 1.3. An integer n is called a congruent number if it is the area of a right triangle with rational sides. This leads to the equation

$$y^2 = x^3 - n^2 x.$$

Fermat proved that 1 is not a congruent number. This also establishes the case $n = 4$ of Fermat's last theorem.

Example 1.4. Consider the equation $x^3 + y^3 + z^3 = 0$. This is a homogeneuos cubic, and so the tangent and chord method of Diophantus can be used to analyze it. While there are simpler methods, this again can be used to handle FLT, this time for $n = 3$.

We should mention that the method stops here at degree 3. We can deal with the $n = 4$ case of Fermat's last theorem because the equation $y^2 = f(x)$, for f of degree 4 can be transformed into the form $y^2 = g(x)$ with g of degree 3. The situation for higher degree equations is interesting. It was conjectured by Mordell and proved by Faltings that (under mild conditions) they have only finitely many rational solutions. However the proof is ineffective, it gives an upper bound for the number of solutions but not for their size.

The geometric method explains why quadratic equations have parametric solutions, such as for Pythagorean triples. It also explains why cubic (and higher degree) curves do not. We will concentrate on cubic curves, that have a tangent line at every point, they are the elliptic curve of the title. As a warm up we first state the main theorem on quadratic equations, called conics.

Theorem 1.5 (Legendre's theorem on conics)**.** *Consider the equation*

$$ax^2 + by^2 + cz^2 = 0,$$

with $a, b, c \in \mathbb{Z}$ pairwise co-prime and square-free. If they have all the same sign, the equation has no non-trivial rational solutions. If they are not all of the same sign, then *the equation has a non-trivial rational solution if and only if all of the following three congruences have solutions:*

(1) $$u^2 \equiv -bc\ (|a|),$$

(2) $$v^2 \equiv -ca\ (|b|),$$

(3) $$w^2 \equiv -ab\ (|c|).$$

Remark. When there is a rational solution, all rational solutions can be parameterized using the chord method of Diophantus.

1.2. **Outline of the course.** The main goal is to prove that the tangent-chord method leads to an operation that makes the solution set of the cubic a group. This relies on understanding the notion of degree geometrically. It also requires to enlarge our point of view, we need both an algebraic and a geometric closure of sort. The latter is provided by the so-called projective plane, and we will start with that. The algebraic closure arises from the use of complex numbers. We briefly review the complex analysis that we need. Elliptic curves over $\mathbb{C}$ will follow, and we will show how to define the group structure on the solution set. It will be obvious from the description that the rational solutions form a subgroup and we will investigate its properties. The most important is the Mordell-Weil theorem, which says that this group is isomorphic to $\mathbb{Z}^r \times A$ for some finite abelian group A. We will show how to determine A for any curve, and also r for certain special cases. (The general case requires machinery outside of the scope of this mini-course.)

1.3. **Exercises.**

Exercise 1.1. We call a line in the plane rational if it has an equation of the form $ax+by=c=0$, with all of a, b and c rational numbers. Show the following:

a) If L_1 and L_2 are rational lines, then their intersection has rational coordinates.
b) If P_1 and P_2 are points with rational coordinates then the line through P_1 and P_2 is rational.
c) Let Q be of degree 2, and C the conic given by $Q(x, y) = c$. Assume that $(x_1, y_1) \in C$ is a rational point. Show that every line that is not tangent to C at x_1, y_1 intersects C at another rational point (x_2, y_2).

Exercise 1.2. Show that if (a, b, c) is a primitive (i.e. $\gcd(a, b, c) = 1$) Pythagorean triple, $a^2 + b^2 = c^2$ then there are integers m, n, $(m, n) = 1$, such that (with a possible reordering) $a = m^2 - n^2, b = 2mn$ and $c = m^2 + n^2$.

Exercise 1.3. Parameterize all rational solutions of the equation $x^2 + y^2 = 2$. (Hint: project from a rational point on the curve to a rational line. What line gives the simplest formula?)

Exercise 1.4. Consider the curve $C : y(6-y) = x^3 - x$ and the points $P(0, 0)$ and $Q(1, 6)$, both of which lie on C. Find the intersection of the curve C and the line through P and Q.

Show in general that if P, Q are points on C with rational coordinates, then the line through P and Q intersects the curve in a third point which also has rational coordinates. Discuss the degenerate cases, when this statement needs to be corrected (by adding the point at infinity).

Exercise 1.5. For each of the following equations find a rational solution or prove that there are none.

a) $x^2 + y^2 = 6$ b) $3x^2 + 5y^2 = 4$ c) $3x^2 + 6y^2 = 4$

Exercise 1.6. Prove that for every exponent $k \geq 1$, the congruence

$$x^2 + 1 \equiv 0 \pmod{5^k}$$

has a solution $x_k \in \mathbb{Z}/5^k\mathbb{Z}$. (b) Prove that the solutions in (a) can be chosen to satisfy

$$x_{k+1} \equiv x_k \pmod{5^k} \quad \text{for every } k \geq 1$$

(c) Prove that if we require the list of solutions $x_1, x_2, x_3, \ldots$ to satisfy (b), then there are exactly two lists of solutions, the first being characterized by $x_1 \equiv 2 \pmod 5$ and the second by $x_1 \equiv 3 (\bmod 5)$.

Exercise 1.7. Show that the conditions (1), (2) and (3) are necessary.

Exercise 1.8. *This exercise shows that Legendre's theorem completely solves the existence of rational points on any conics.*

a) Let $q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$ with $b^2 - 4ac \neq 0$. Show that with suitable x_0, y_0 the change of variables $x = x_0 + u$, $y = y_0 + b$ transforms $q(x, y)$ into $au^2 + buv + cv^2 + F$. Also show that if $a, b, c, d, e, f \in \mathbb{Q}$ then $F \in \mathbb{Q}$ as well.
b) Show that a suitable linear change of variables $u = \alpha x + \beta y,\ v = \gamma x + \delta y$, with $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ transforms the equation $ax^2 + bxy + cy^2 + f = 0$ into one of the form $Au^2 + Bv^2 + C = 0$.
c) Show that by chosing suitable multiples $u = \alpha x$, $y = \beta y$ and clearing denominators we can transform into the equation $Ax^2 + By^2 + C$ anto one of the form $au^2 + bv^2 + c$, where $a, b, c \in \mathbb{Z}$ are each squarefree and *pairwise* relatively prime .

Exercise 1.9. *This exercise shows how to test the conditions in Legendre's theorem.* We are interested in establishing whether $u^2 \equiv d\ (n)$ is solvable or not.

a) Let $n = n_1 n_2$ where $(n_1, n_2) = 1$. Show that

$u^2 \equiv d \pmod{n}$ is solvable $\iff$ both $u_1^2 \equiv d \pmod{n_1}$ and $u_2^2 \equiv d \pmod{n_2}$ are solvable.

b) By the above the solvability question reduces to understanding whether $u^2 \equiv d \pmod{p^k}$ is solvable, for p prime. Show that if $(p, d) = 1$ then

$$u^2 \equiv d \pmod p \text{ is solvable } \implies u^2 \equiv d \pmod{p^k} \text{ is solvable for any } k.$$

(Hint: try to "lift" any solution $\bmod p^k$ to a solution $\bmod p^{k+1}$.)

c) Show that if p is odd then $u^2 \equiv d \pmod p$ is solvable if and only if $u^{(p-1)/2} \equiv 1 \pmod p$. (Alternatively this can be determined using quadratic reciprocity.)

d) What happens for $p = 2$?

Exercise 1.10. *A number is congruent if it the area of a right triangle with rational sides. In this exercise we will see how this old Arabic problem leads to the curve $y^2 = x^3 - x$.*

a) Assume that 1 is congruent. Show that this is equivalent to the existence of a primitive Pythagorean triple (a, b, c) such that
$$ab = 2r^2.$$
b) Let $a = m^2 - n^2$, $b = 2mn$ as in exercise 1.2. This leads to the equation
$$mn(m + n)(m - n) = r^2.$$
Show that there exist $m, n \in \mathbb{Z}$ $(m, n) = 1$, satisfying this equation if and only if there exist rational numbers x, y such that $y^2 = x(x^2 - 1)$. (Hint: divide by an appropriate power of n.)
c) Continuing the above show that the numbers $m, n, (m+n), (m-n)$ are pairwise relatively prime, and therefore they are all squares
$$m = x^2, \quad n = y^2, \quad m + n = z^2, \quad m - n = w^2,$$
for some integers x, y, z, w.
d) Show that the triple $(z - w, z + w, 2x)$ is a Pythagorean triple with smaller square area than the original. Conclude that no such triples exist.

2. Background

2.1. The projective plane.

Definition 2.1. Let K be a field. By $\mathbb{P}^2(K)$ we mean the set of lines of K^3 through $0, 0, 0$, (the set of 1-dimensional linear subspaces). This can be alternatively defined as the set of equivalence classes of $K^3 \setminus (0, 0, 0)$, where we have
$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \iff \exists \lambda \in K^*(x_2, y_2, z_2) = \lambda(x_1, y_1, z_1)$$

We will denote the equivalence class of (x, y, z) by $(x : y : z)$. Note that $\mathbb{P}^2(K)$ is covered by three ordinary planes: $x \neq 0$, $y \neq 0$ and $z \neq 0$. This means the following the set $\{(x : y : z) : z \neq 0\}$ is well defined since if $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ and $z_1 \neq 0$ then also $z_2 \neq 0$. Moreover each point in this set has a *unique* representative of the form $(x, y, 1)$. Clearly such points form an ordinary plane, that we denote $\mathcal{P}_z$. The the complement of this ordinary plane, the points $\{(x : y : 0\}$ form a line, that we will call the line at infinity of $\mathcal{P}_z$. Similarly we can define the planes $\mathcal{P}_x$, $\mathcal{P}_y$. A moments thought reveals that $\mathbb{P}^2(K) = \mathcal{P}_x \cup \mathcal{P}_y \cup \mathcal{P}_z$. If F is a homogeneous polynomial of some degree, then the set $V_F = \{(x : y : z) : F(x, y, z) = 0\}$ is well defined. In the special case that $F(x, y, z) = Ax+By+Cz$ is a non-zero linear function, we will call V_F a line, its intersection of any of the 3 coordinate planes is an ordinary line, or empty.

If $F(x, y, z)$ is homogeneous of degree d then its restrictions to $\mathcal{P}_z$ leads to the polynomial $f(x, y) = F(x, y, 1)$ of degree d. Conversely given a polynomial $f(x, y)$ of degree d the expression $z^d f(x/z, y/z)$ defines a homogeneous polynomial of degree d. This process is called homogenization.

2.2. **Tangent lines.** Let $C : F(x,y) = 0$ be a curve, and $P(a,b) \in C$ such that $(\frac{\partial F}{\partial x}(a,b), \frac{\partial F}{\partial y}(a,b)) \neq (0.0)$. Then the line $\frac{\partial F}{\partial x}(a,b)(x-a) + \frac{\partial F}{\partial y}(a,b))(y-b)$ is tangent to C.

This is based on a multivariable Taylor's expansion. If $F(x_1, x_2)$ is a polynomial and we define a new polynomial $p(v_1, v_2) = F(a + v_1, b + v)$, then

$$\begin{aligned} p(v_1, v_2) =& F(a,b) \\ &+ \frac{\partial F}{\partial x_1}(a,b)v_1 + \frac{\partial F}{\partial x_2}(a,b)v_2 \\ &+ \frac{\partial^2 F}{\partial x_1^2}(a,b)\frac{v_1^2}{2!} + \frac{\partial^2 F}{\partial x_1 \partial x_2}(a,b)v_1 v_2 + \frac{\partial^2 F}{\partial x_2^2}(a,b)\frac{v_2^2}{2!} \\ &+ \frac{\partial^3 F}{\partial x_1^3}(a,b)\frac{v_1^3}{3!} + \frac{\partial^3 F}{\partial x_1^2 \partial x_2}(a,b)\frac{v_1^2 v_2}{2!} + \frac{\partial^3 F}{\partial x_1 \partial x_2^2}(a,b)\frac{v_1 v_2^2}{2!} + \frac{\partial^3 F}{\partial x_2^3}(a,b)\frac{v_2^3}{3!} \\ &+ \text{... higher order terms} \end{aligned}$$

The tangent line can be described alternatively as follows. Take a point $P(a,b)$ on the curve C given by equation $F(x,y) = 0$. If $\frac{\partial F}{\partial y}(a,b) \neq 0$ there is a function $g(x)$ defined in a neighborhood of a such that if we consider a small piece of the curve that goes through (a,b) then it is given as a graph $y = g(x)$. Then the usual tangent line is given as the one with slope $g'(a)$. For us, when $F(x,y) = y^2 - f(x))$, with $f(x) = x^3 + Ax + B$, we can simply choose one of $\pm\sqrt{f(x)}$, the sign being determined by the sign of b.

2.3. **Exercises.**

Exercise 2.1. Identify points that are the same on $\mathbb{P}^3(\mathbb{Q})$. Find triplets that lie on the same line.

$$\begin{array}{llrr} (0:0:1), & (1:0:1), & (2:0:4), & (4:4:0), \\ (1:0:2), & (0:0:\pi), & (23:0:23), & (2:-3:4), \\ (-2:-2:0), & (-3:0,6), & (3e:3e:3e), & (-4:6:-8) \end{array}$$

Exercise 2.2. Write down the homogenized form of the following

a) $x^2 + 2xy + y^2 = y$

b) $y^2 = x^3 + 1$

c) $x^2 = y^2$

Exercise 2.3. *The following exercise gives a quick method to find tangents. It is a special case of a method that is usually referred to as implicit differentiation.* Assume that we have the curve $y^2 = f(x)$, and the point x_1, y_1 is on the curve, i.e. it satisfies $y_1^2 = f(x_1)$. Assume also that $y_1 \neq 0$ and that $\lambda = \frac{f'(x_1)}{2y_1}$. Show that the line $y = \lambda(x - x_1) + y_1$ is tangent to the curve $y^2 = f(x)$.

Exercise 2.4. Find the equation of the tangent line for the following curves and points.

a) $C : x^2 + y^2 = 1$, at $(\frac{3}{5}, \frac{4}{5})$	b) $C : y^2 = x^3 + 1$, at $(-1, 0)$	c) $C : y^2 = x^3 + 2x + 1$, at $(1, 2)$

Exercise 2.5. Homogenize and find the points at infinity of $V : x^4 + xy - y^4 = 0$.

Exercise 2.6. Find all singular points (including possibly at infinity) of the following curves

a) $x^2 + y^2 = 1$ b) $x^2 + y^2 = 0$ c) $y^2 = x^3$

Exercise 2.7. Let $E : y^2 = x^3 + Ax + B$ be a cubic curve. Show that E is smooth (have no singular points) if and only if the roots of $x^3 + Ax + B = 0$ are different. Moreover show that this happens if and only if $-4A^3 - 27B^2 \neq 0$.

2.4. **Some analytic tools over the complex field.** Yesterday in the other lecture we discussed briefly complex numbers and complex analysis. We touched upon the following notions:

- Differentiability. Rules work the same way, but the consequences are very diffwerent.
- Examples of holomorphic functions: power series, analytic functions.
- The concept of meromorphic function, for example rational functions. (Quotient of two polynomials.)
- Line integrals, and the residue theorem.
- Finally the concept of the Riemann sphere $\mathbb{C} \cup \{\infty\}$ makes some arguments much simpler.

Definition 2.2. Order at a point for non-constant functions:

$$\operatorname{ord}_a f = n \iff \lim_{z \to a} \frac{f(z)}{(z-a)^n} = c \neq 0, \infty. \tag{4}$$

Lemma 1. *Order is well defined.*

There are two types of representation of meromorphic functions that are very useful:

- $f = g + h$ where g is holomorphic and h is a rational function written using the method partial fractions as a sum of Laurent polynomials.
- $f = g \cdot h$ where g is a non-vanishing holomorphic function and h is a rational function.

The main tool for us is the residue theorem for meromorphic functions and its corollaries, esp. Liouville's theorem, and the argument principle.

Theorem 2.3 (Liouville). *If $f : \mathbb{C} \to \mathbb{C}$ is differentiable everywhere and bounded then f is constant.*

Corollary 1 (Fundamental theorem of algebra). *If $p(z)$ is a polynomial then it has a root in $\mathbb{C}$.*

Theorem 2.4. *Let $f(z)$ be meromorphic in a connected open set U and let γ be a simple closed curve that together with its interior lies entirely in U. (For us these curves will either be circles, or the boundary of some parallelogram, when the interior of γ is easy to define.)*

(1) *(The argument principle.)*

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)} = \sum_{a, \operatorname{ord}_a f \neq 0} \operatorname{ord}_a f,$$

where the sum is over points inside γ. Note that this is a finite sum, the number of zeros minus the number of poles inside γ, (both counted with multiplicities, their order).

(2)

$$\frac{1}{2\pi i}\int_\gamma z\,\frac{f'(z)}{f(z)} = \sum_{a, \operatorname{ord}_a f \neq 0} (\operatorname{ord}_a f)a.$$

(3) *Assume that γ is a simple curve, not necessarily closed, with endpoints a and b, and that $f(z)$ is holomorphic along γ and $f(b) = f(a)$. Then*

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)} \in \mathbb{Z}.$$

2.5. Exercises.

Exercise 2.8. Find all a such that $\operatorname{ord}_a f$ is non-zero, when

$$f(z) = \frac{z^2+z+1}{z^4-2z^2+1}, \qquad g(z) = \frac{1}{z} - \frac{1}{z-1} - \frac{1}{z+1}.$$

Exercise 2.9. Let $p(z) = z^5 - 6z^4 - z + 12$. Evaluate the following limits, where C_R is the circle of radius R centered at the origin (with positive orientation)

a) $\displaystyle\lim_{R\to\infty} \frac{1}{2\pi i}\int_{C_R} \frac{p'(z)}{p(z)} dz$ b) $\displaystyle\lim_{R\to\infty} \frac{1}{2\pi i}\int_{C_R} z\frac{p'(z)}{p(z)} dz$

(Hint: Do not try to this from the definition, use the residue theorem.)

3. Elliptic curves over the complex field

3.1. Complex elliptic functions are doubly periodic: sketch.

Consider the equation

$$E : y^2 = x^3 + Ax + B.$$

If $D = -4A^3 - 27B^2 \neq 0$ then curve is smooth, at each point P on the curve there is a unique tangent line touching the curve at P. We refer to the solution set $E(K)$ with coordinates in a field K with the point at infinity an elliptic curve over K.

In this section we will mainly be interested in parameterizing these curves. Such a parameterization is only possible analytically, there are no algebraic formulas like for the Pythagorean triples. (This is a theorem, the proof requires some tools but is not hard.)

Therefore we will restrict to

$$K = \mathbb{C}$$

because it is nicer both from the algebraic and the analytic point of view. This means, that *the x and y variables in the equation E are now allowed to take on complex values*!

Remark. Note that when $K = \mathbb{R}$ this truly is a curve, but when $K = \mathbb{Q}$ it no longer has the usual geometric meaning. Also note that for $K = \mathbb{C}$ this "curve" is now 2-dimensional, but we will still call it a curve, a complex curve.

Theorem 3.1. *A complex elliptic curve is a torus.*

Sketch of proof. Every instance of x, y now refers to possible *complex* values.

Let $f(x) = (x - e_1)(x - e_2)(x - e_3)$. Cut the Riemann sphere at the segment $[e_1, e_2]$ and $[e_3, \infty]$. Then $\sqrt{f(x)}$ may be defined on this domain as an analytic function, and there are two choices, they differ by ±1. The Riemann surface of the curve is then the two cut spheres glued together, which is a torus.

An alternative and more formal proof relies on 1) the topological classification of surfaces by the Euler characteristic (genus) and 2) calculating the Euler characteristic of E. □

We skip the history, but parameterization via differential equations arose classically: find $x(t), y(t)$ such that they satisfy

$$y^2(t) = x^3(t) + Ax(t) + B, \quad x'(t) = y(t). \tag{5}$$

This leads to the differential equation

$$x'(t) = \sqrt{x^3 + Ax + B}.$$

This a separable differential equation whose solution is $x(t) = F^{-1}(t - a)$ where

$$F'(x) = \frac{1}{\sqrt{x^3 + Ax + B}}.$$

It is a standard fact that such a function F exists in a neighborhood of the origin if A, B are real, and $B > 0$.

However we are interested in the inverse function. It was Abel who first discovered that this inverse when extended to $\mathbb{C}$ is doubly periodic, $\exists \omega_1, \omega_2$ linearly independent over $\mathbb{R}$ such that $x(t + \omega_1) = x(t)$ and $x(t + \omega_2) = x(t)$. From our modern point of view this is justified by Theorem 3.1.

We want to derive this parameterization now, without going through how it was proved historically. This shortcut was achieved by Weierstrass who constructed a doubly periodic meromorphic function that produces a complex function $\wp(z)$ that satisfies

$$(\wp'(t))^2 = 4\wp^3(z) + A\wp(z) + B.$$

The input for this construction is a lattice Λ.

Definition 3.2. A lattice is a set of the form $\{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ for ω_1, ω_2 linearly independent over $\mathbb{R}$.

Theorem 3.3 (Weierstrass)**.** *Let $\Lambda = \{m\omega_1 + n\omega_2\}$ be a lattice.*

(1) The series

$$\sum_{\omega \in \Lambda} \frac{1}{(z - \lambda)^3} \tag{6}$$

converges uniformly on any compact set that is disjoint from Λ*.*

(2) *For* $z \notin \Lambda$ *define* $f(z)$ *by the sum. Then* $f(z)$ *is meromorphic and* $f(z+\omega) = f(z)$ *for any* $\omega \in \Lambda$*. Explicitly,* f *is holomorphic at all points not in* Λ*, and has poles of order 3 at points in* Λ*.*

(3) *The function* $f(z)$ *has a primitive* $F(z)$ *which is also doubly periodic. It is given explicitly as follows. Let*

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda in \Lambda, \lambda \neq 0} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \tag{7}$$

Then $\wp'(z) = -2f(z)$*.*

3.2. **The field of elliptic functions.**

Definition 3.4. Let Λ be a lattice. An elliptic function (with respect to Λ) is a meromorphic function that satisfies $f(z+\lambda) = f(z)$ for all $\lambda \in \Lambda$.

The following are the three main theorems from complex analysis that we will use.

Theorem 3.5 (Liouville)**.** *A holomorphic doubly periodic function is constant.*

We will need some technical observations, for which we select a fundamental parallelogramm for Λ: $\mathcal{F}_a = \{a + s\omega_1 + t\omega_2 : s, t \in [0,1)\}$.

Proposition 1. (1) *Let* γ *be the boundary of* $\mathcal{F}_a$ *paremeterized anti-clockwise. If* f *is an elliptic function that has no pole on* γ *then we have*

$$\int_\gamma f(z)dz = 0$$

(2) *If* $f(z) \neq c, \infty$ *on the boundary then*

$$\frac{1}{2\pi i} \int_\gamma \frac{f'(z)}{f(z) - c} dz = 0$$

(3) *If* $f(z) \neq 0, \infty$ *on the boundary then*

$$\frac{1}{2\pi i} \int_\gamma \frac{zf'(z)}{f(z)} dz \in \Lambda.$$

Proof. The first claim follows since the integrals along the sides cancel. The second is an immediate consequence. Finally in the third integral, the sides do not cancel but give integral multiples of ω_1, ω_2. (This requires some extra care and the last claim of Theorem 2.4.) □

An important corollary is the following:

Theorem 3.6. *If* f *is a non-constant an elliptic function then the set* $\{z \in \mathcal{F} : f(z) = c\}$ *is finite, and when counted by multiplicity is independent of* c*. We denote this by* $\deg f$*. If* f *is not constant then* $\deg f \geq 2$*.*

Proof. The theorem above shows that the number of solutions $f(z) = c$ is the same as the number of poles. (Both with multiplicities.)

If there is only a single pole, then the residue there must be 0, showing that such functions do not exist. □

Another important corollary is

Theorem 3.7. *Let f be a non-constant an elliptic function and let also $Z_0 = \{z \in \mathcal{F} : f(z) = 0\}$, $Z_\infty = \{z \in \mathcal{F} : f(z) = \infty\}$. For any $z_j \in Z_0$ let μ_j be its multiplicity as a zero. Similarly for any $w_k \in Z_\infty$ let ν_j be its multiplicity as a pole. Then we have that*

$$\sum_{z_j \in Z_0} \mu_k z_j - \sum_{w_k \in Z\infty} \nu_k w_k \in \Lambda. \tag{8}$$

Remark. The theorem can be rephrased using the notion of order at a point as in (4). Then it says

$$\sum_{z \in \mathcal{F}} (\operatorname{ord}_z f) z \in \Lambda.$$

Proof. The claim follows from part 3 of Proposition 1. □

Definition 3.8. Let Λ be a lattice. We say that $z_1 \equiv z_2 \bmod \Lambda$ if $z_1 - z_2 \in \Lambda$. This is an equivalance realtion and we denote the set of equivalence classes by $\mathbb{C}/\Lambda$. If $z \in \mathbb{C}$ then its equivalence class is denoted as $[z]$.

Remark. Note that $[z_1] + [z_2] \overset{def}{=} [z_1 + z_2]$ makes $\mathbb{C}/\Lambda$ a group.

Definition 3.9. A divisor is a function $D : \mathbb{C}/\Lambda \to \mathbb{Z}$ such that $\{[z] : D([z]) \neq 0\}$ is finite. We will write divisors as $D = \sum n_j [z_j]$, as a formal sum, listing the points where D is non-zero, together with their values.

We will say that a divisor D is non-negative, $D \geq 0$, if $n_j \geq 0$ for all j.

Example 3.10. Let f be an elliptic function. Then $[z] \mapsto ord_{[z]} f$ is a divisor. We will denote this divisor by (f). Divisors of this sort will be referred to as principal divisors. If D_1 and D_2 are divisors such that $D_1 - D_2 = (f)$ for some elliptic function f, we will call them equivalent which we denote by $D_1 \sim D_2$.

Remark. Note that with our convention $(f) = \sum (\operatorname{ord}_{[z]} f)[z]$. This of course can also be interpreted as a sum in $\mathbb{C}/\Lambda$. This seems confusing but we will see that there is a close connection between the two notions.

Lemma 2. *Assume that f and g are elliptic functions with respect to the lattice Γ. If $(f) = (g)$ then $f = cg$ for some $c \in \mathbb{C}^*$.*

Definition 3.11. Let D be a divisor.

$$\mathcal{L}(D) = \{f \text{ elliptic} : (f) + D \geq 0\}$$

Theorem 3.12 (Special case of the Riemann-Roch theorem). *We have for each $n \in \mathbb{Z}$*

$$\dim \mathcal{L}(n[0]) = \begin{cases} 0 & \textit{if } n < 0 \\ 1 & \textit{if } n = 0 \\ n & \textit{if } n \geq 1. \end{cases} \tag{9}$$

Proof. The top 2 claims follows from Liouville. The $n = 1$ case was proved in Theorem 3.6.

For the case $n \geq 2$ note that $\wp, \wp', ..., \wp^{(n-2)}$ have poles only at $[0]$ and the order of the poles are $2, 3, ..., n$. Therefore these functions are in $\mathcal{L}(n[0])$, and are linearly independent. Moreover if $f \in \mathcal{L}(n[0])$ then there are $c_2, c_3, ..c_n$ such that

$$f - c_2\wp - c_3\wp' - ... - c_n\wp^{(n)} \in \mathcal{L}([0]),$$

and so is some constant c_1. □

Corollary 2 (The Weierstrass equation.). *Let Λ be a lattice and $\wp(z) = \wp_\Lambda(z)$ the associated Weierstrass function. Then we have*

$$(\wp'(z))^2 = 4\wp(z)^3 + A\wp(z) + B \tag{10}$$

for some $A = A_\Lambda, B = B_\Lambda$.

The proof of the corollary is based on $1, \wp, wp'\wp^2, \wp\wp', \wp^3$ and $(\wp')^2$ all being in $\mathcal{L}(6[0])$. The final form of the equation is given in the exercises below.

Theorem 3.13. *The map*

$$\phi : [z] \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1) & z \notin \Lambda \\ (0 : 1 : 0) & z \in \Lambda \end{cases}$$

is a bijection from $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$.

Proof. By Theorem 3.6 for any $x \in \mathbb{C}$ there are either two $z \in \mathcal{F}$ such that $\wp(z) = x$, or there is a single z such that $\wp(z) = x$ and $\wp'(z) = 0$. In the first case the z-s are such that $[z_1] = -[z_2]$, when $\wp'(z_1) = -\wp'(z_2)$. □

3.3. **Transport of the group structure.** We have the following converse for Theorem 3.7. It is a special case of a theorem due to Abel and Jacobi that treats general curves.

Theorem 3.14 (Abel-Jacobi theorem for elliptic curves). *A divisor $D = \sum_j n_j[z_j]$ is a principal divisor if and only if*

$$|D| = \sum_j n_j = 0, \quad \textit{and } \sum_j n_j z_j \in \Lambda, \ \textit{where the sum is taken in } \mathbb{C}.$$

We will not prove the whole theorem. The idea is to use induction based the following

Proposition 2. *For any points P, Q we have that*

$$[P] + [Q] \sim [P + Q] + [\infty].$$

Proof. Let $f(z) = \wp(z) - \wp(P+Q)$. Then $(f) = [P+Q] + [-P-Q] - 2[\infty]$. Therefore it is enough to show that

$$[P] + [Q] + [-P-Q] - 3[\infty] \sim \emptyset \tag{11}$$

We will only do this when P, Q and R are different. Choose a, b, c in a such a way that $f(z) = a\wp(z) + b\wp'(z) + c$ vanishes at P and Q. Note that the degree of f is 3 and the divisor of f is

$$(f) = [P] + [Q] + [R] - 3[\infty]$$

for some R. By Theorem 3.7 R satisfies $P + Q + R \in \Lambda$. Therefore $[R] = [-P-Q]$. □

Since there is a bijection ϕ bewteen $E(\mathbb{C})$ and $\mathbb{C}/\Lambda$ we can transport the group structure on $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$, i.e we can define an operation " $+_E$ " on $E(\mathbb{C})$ such that

$$\phi([z_1] + [z_2]) = \phi(z_1) +_E \phi(z_2). \tag{12}$$

The arguments above basically do this for us, $P + Q + R = \infty$ should hold if and only if P, Q, R lie on a line.

Theorem 3.15 (The group law). *Let $P(x_1, y_1), Q(x_2, y_2)$ be points on $E(\mathbb{C})$. Denote the point $(0 : 1 : 0)$ by ∞ and define the following binary operation $+_E : E(\mathbb{C}) \times E(\mathbb{C}) \to E(\mathbb{C})$*

1. *$P +_E \infty = \infty +_E P = P$ for all P.*
2. *Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2) \in E(\mathbb{C})$.*
   - (a) *If $x_1 = x_2$, but $y_1 \neq y_2$ define $P_1 +_E P_2 = \infty$.*
   - (b) *If $x_1 \neq x_2$ let L be the line though P and Q and define $P +_E Q = (x_3, -y_3)$ where (x_3, y_3) is the third point of intersection of L with E.*
   - (c) *If $x_1 = x_2$ and $y_1 = y_2 \neq 0$, (i.e. $P_1 = P_2$) then let L be the tangent line to E at P and define $P +_E P = (x_3, -y_3)$ where (x_3, y_3) is the third point of intersection of L with E.*
   - (d)
   - (e) *If $x_1 = x_2$ and $y_1 = y_2 = 0$, then define $P_1 +_E P_2 = \infty$.*

Then we have that $+_E : E(\mathbb{C}) \times E(\mathbb{C}) \to E(\mathbb{C})$ makes $E(\mathbb{C})$ an abelian group.

Remark. Note that the last case $x_1 = x_2$ and $y_1 = y_2 = 0$, the tangent line still intersect E at a third point $(0 : 1 : 0)$, but only in the projective plane.

Proof. Note that $\phi([0]) = \infty$ which shows that equation (12) holds for the first two cases. For the third we may use the argument Proposition 2. When the points $P_j = \phi(z_j)$ are different then $z_1 + z_2 + z_3 \in \Lambda$ iff

$$\det \begin{pmatrix} \wp(z_1) & \wp'(z_1) & 1 \\ \wp(z_2) & \wp'(z_2) & 1 \\ \wp(z_3) & \wp'(z_3) & 1 \end{pmatrix} = 0. \tag{13}$$

This is exactly the equation that the points P_1, P_2, P_3 lie on one line. The final case is left as an exercise. □

Remark. From now on we will drop the notation E from $+_E$.

3.4. **Exercises.**

Exercise 3.1. *The convergence of the series defining $\wp$ is based upon the following estimate.* Let $N_\Lambda(R)$ denote the number of points in Λ with length at most R, i.e. $N_\Lambda(R) = |\{\omega \in \Lambda||\omega| \leq R\}|$. Show that $N_\Lambda(R) \leq cR^2$ where c depends on Λ only.

Exercise 3.2. *This exercise derives the Weierstrass equation (10) in explicit form.*

a) Show that
$$\frac{1}{(z-a)^2} = \sum_{n=0}^{\infty} \frac{n+1}{a^{n+2}} z^n.$$

b) Let Λ be a lattice. Show that $G_n(\Lambda) = \sum_{0 \neq \lambda \in \Lambda} \lambda^{-n}$ converges for $n \geq 3$ and vanishes for n odd.

c) Let $r := \min\{|\lambda| : 0 \neq \lambda \in \Lambda\}$. Then for $0 < |z| < r$ the $\wp$-function has the following Laurent expansion
$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2} z^{2n}.$$
(Hint: a theorem of Weierstrass guarantees that we can do this term by term and then add.)

d) Show that the Laurent expansion of $\wp^3$ is
$$\wp^3(z) = \frac{1}{z^6} + \frac{c}{z^2} + ...$$
What is the value of c?

e) Find the Laurent expansion $\wp'$ and show that
$$(\wp'(z))^2 = \frac{4}{z^6} + \frac{c'}{z^2} + ...$$
What is the value of c'?

f) Find an explicit form of Weierstrass differential equation with A, B expressed in terms of $G_4(\Lambda)$ and $G_6(\Lambda)$.

Exercise 3.3. Let $\Lambda_i = \mathbb{Z} + \mathbb{Z}i$. Show that $G_6(\Lambda) = 0$. Let $\Lambda_\omega = \mathbb{Z} = \mathbb{Z}\omega$, where $\omega = \frac{1+\sqrt{3}i}{2}$. Show that $G_4(\Lambda) = 0$.

Exercise 3.4. Fix a lattice Λ. Show that the field of elliptic functions $\mathcal{E}_\Lambda$ has transcendence degree 1 over $\mathbb{C}$.

Exercise 3.5. Modify the proof of Proposition 2 to treat the case when $P = Q$ and show that (12) holds in case 4 in Theorem 3.15.

Exercise 3.6. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice and consider the group $\mathbb{C}/\Lambda$. Show that the set $\{[z] : n[z] = [0]\}$ is finite. What is its cardinality? (Here $n[z]$ means $[z] + ...[z]$, n times, or equivalently $[nz]$.) Given a point $[z] \in \mathbb{C}/\lambda$ how many $[z'] \in \mathbb{C}/\lambda$ exist for which $2[z'] = [z]$. (Hint: think either geometrically or in terms of congruences mod Λ.)

Exercise 3.7. When the group law is transported to the curve $E : y^2 = x^3 + Ax + B$ what is the geometric meaning of the points of order 2, i.e. those for which $2P = \infty$? What is the geometric meaning of the points of order 3, for which $3P = \infty$?

4. Elliptic curves over $\mathbb{Q}$

4.1. **The group law algebraically.**

Theorem 4.1 (The group law-over $\mathbb{Q}$)**.** *Let $P(x_1, y_1), Q(x_2, y_2)$ be points on $E(\mathbb{Q})$. Denote the point $(0 : 1 : 0)$ by ∞ and define the following operation*

(1) $P + \infty = \infty + P = P$ for all P.

(2) If $x_1 \neq x_2$ let let L be the line though P and Q and define $P + Q = (x_3, -y_3)$ where (x_3, y_3) is the third point of intersection of L with E.

(3) If $x_1 = x_2$ and $y_1 = y_2$, (i.e. $P = Q$) then let Let L be the tangent line to E at P and define $P + P = 2P = (x_3, -y_3)$ where (x_3, y_3) is the third point of intersection of L with E.

(4) If $x_1 = x_2$, but $y_1 \neq y_2$ define $P_1 + P_2 = \infty$.

Then we have that $+ : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})$ makes $E(\mathbb{Q})$ an abelian group.

Proof. Since $E(\mathbb{C})$ is a group it is enough to show that if $P_1, P_2 \in E(\mathbb{Q})$ then so is $P_1 + P_2$, an elementary fact. □

Remark. We can calculate the group law on $E : y^2 = f(x)$, $f(x) = x^3 + Ax + B$ explicitly. These lead to purely algebraic formulas for which it is possible to prove the group property without any reference to elliptic functions (or even complex numbers).

The calculations are as follows. Let the line through $P_1(x_1, y_1)$ and $P_2(x_2, y_2$ has slope slope $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. The equation of the line is $y = \lambda x + \nu$, with and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$ still rational.

We want to find x_3, y_3, the x and y coordinates of the third intersection. Now x_1, x_2 and x_3 are the solutions of the (single variable) cubic

$$f(x) - (\lambda x + \nu)^2 = x^3 - \lambda^2 x^2 + (A - 2\lambda\nu)x + \bigl(B - \nu^2\bigr) = 0.$$

By Viete's formulae $x_1 + x_2 + x_3 = \lambda^2$, and so

$$x_3 = \lambda^2 - x_1 - x_2, \text{ and } y_3 = \lambda x_3 + \nu. \tag{14}$$

When $P_1 = P_2 = (x, y)$ we have to use the tangent line with slope $\lambda = \frac{f'(x_1)}{2y_1}$. This leads to

$$x\text{-coordinate of } 2P = \lambda^2 - 2x = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} \tag{15}$$

where we have used that $y^2 = f(x)$.

Example 4.2. Let E be the elliptic curve

$$y^2 = x^3 + 17.$$

To add $P_1 = (-1, 4)$ and $P_2 = (2, 5)$ first find the line $y = \lambda x + \nu$ through P_1 and P_2. Since $\lambda = \frac{1}{3}$, we have

$$x_3 = \lambda^2 - x_1 - x_2 = -\frac{8}{9}.$$

Using either P_1 or P_2 we get $\nu = \frac{13}{3}$ and so

$$y_3 = \lambda x_3 + \nu = \frac{109}{27},$$

which gives

$$P_1 + P_2 = (x_3, -y_3) = \left(-\frac{8}{9}, -\frac{109}{27}\right)$$

To compute $2P_1$ we first get the slope of the tangent line

$$\lambda = \frac{f'(x_1)}{2y_1} = \frac{f'(1)}{8} = \frac{3}{8}.$$

This immediately gives

$$x(2P) = \lambda^2 - 2x(P) = \frac{137}{64}.$$

To get the full equation $y = \frac{3}{8}x + \nu$ for the tangent line, plug $(x, y) = (-1, 4)$ to get $\nu = \frac{35}{8}$. and so $2P_1 = \left(\frac{137}{64}, -\frac{2651}{512}\right)$.

Note that the coordinates of $2P$ are more complicated, they are expressed by significantly more digits than what we started with. This is a typical situation, as we will see below.

4.2. The structure of $E(\mathbb{Q})$.

Theorem 4.3 (The Mordell-Weil theorem)**.** *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Q}$. Then the group $E(\mathbb{Q})$ is finitely generated.*

Corollary 3. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Q}$. There are points $P_1, P_2, ..., P_n$, such that all rational points on E can be found by repeated applications of the tangent and chord method of Diophantus.*

Note that the Mordell-Weil theorem implies that the group $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}^r \oplus A$, for some $r \in \mathbb{N}$ and some finite abelian group A. Both r and A are well defined (see exercise 4.1). Moreover the equation $y^2 = x^3 + Ax + B$ has infinitely many solutions iff $r > 0$. It is interesting problem determine r and A. The former is a very hard question, about which we will only hint at the end of the next section. The latter, the so-called torsion points can be determined effectively using the following theorem.

Theorem 4.4 (Lutz-Nagell theorem)**.** *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Z}$. Let $E_{tors}(\mathbb{Q})$ be the set of points of $E(\mathbb{Q})$ of finite order.*

1. *If $(x, y) \in E_{tor}(\mathbb{Q})$ then $x, y \in \mathbb{Z}$.*
2. *If $(x, y) \in E_{tor}(\mathbb{Q})$ then either $y = 0$ or $y^2 | D$, where $D = -4A^3 - 27B^2$ is the discriminant of E.*

Corollary 4. *Both the Mordell-Weil and Lutz-Nagell theorems show that $E_{tors}(\mathbb{Q})$ is finite. If by pure chance we find a point whose coordinates are not integral we have also shown that there infinitely many solutions to $y^2 = x^3 = Ax + B$*

Remark. The set of integral points in general are different from the points of finite order, i.e. the inclusion is strict. By a *hard* theorem of Siegel there are only finitely many such points, but determining integral points on a curve is not an obvious task since we do not have a priori bounds for them.

4.3. **Proof of Lutz-Nagell assuming integrality.** We will not prove the full theorem, only the conditions for y, assuming that integrality was already proved. The proof that torsion points have integer coordinates can be found [1]. While it is lengthy, it is elementary.

Lemma 3. *Assume that $2P \neq \infty$ and that P and $2P$ have integer coordinates. Then $y_P|D$.*

Proof. $x(2P) + 2x(P) = \lambda^2$, where λ is the slope of the tangent, $\lambda = \frac{f'(x(P))}{2y(P)}$. Since $2P$ is also torsion, $x(2P)$ is an integer and we musy have $y(P)|f'(x(P))$. Moreover we have shown (Exercise 4.5) that there are polynomials $a(x), b(x) \in \mathbb{Z}[x]$ such that

$$a(x)f(x) + b(x)f'(x) = D.$$

By substituting $x = x(P)$ this shows that $y|D$. □

Of course to prove the full theorem, that $y^2|D$, we need to do better. Let $x(2P) = \frac{x^4-2Ax^2-8Bx+A^2}{4(x^3+Ax+B)} = \frac{\psi(x)}{4f(x)}$ as in (15). Then (Exercise 4.6) we still have that there exist $m(x), n(x) \in \mathbb{Z}[x]$ such that

$$m(x)\psi(x) + n(x)f(x) = D. \tag{16}$$

The same argument then shows that $y^2|D$.

4.4. **Exercises.**

Exercise 4.1. a) Let $(G, +)$ be an abelian group. We will say that $g \in G$ has finite order if $ng = \overbrace{g + .. + g}^{n\ times} = 0$. Such points are also referred to as torsion points. Show that the set $G_{tor} = \{g \in G\ :\ g \text{ has finite order}\}$ is a subgroup.

b) Assume further that G is finitely generated. Show that G_{tor} is finite and is the maximal finite subgroup of G.

Exercise 4.2. Let $(G, +)$ be an abelian group. We will say that $g_1, ...g_r$ are linearly independent over $\mathbb{Z}$ if $\sum_{j=1}^{r} m_j g_j = 0$ with $m_j \in \mathbb{Z}$ is only possible if $m_j = 0$ for $j = 1, ...r$.

a) Given $\{g_1, ...g_r\}$, show that if one of $g_j \in G_{tor}$ then the elements are not independent

b) Let $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & -1 \end{pmatrix}$. View elements of $\mathbb{Z}^3$ as column vectors and consider the groups $G_0 = \{g \in \mathbb{Z}^3 : Ag = \mathbf{0}\}$ and $G_1 = \{Ag : g \in \mathbb{Z}^3\}$. Show that these sets are groups without torsion and find independent generators of them.

Exercise 4.3. Calculate the torsion subgroup for the following elliptic curves

a) $y^2 = x^3 - 1$ b) $y^2 = x^3 + 1$ c) $y^2 = x^3 - 4$ d) $y^2 = x^3 - 2$

Exercise 4.4. Let $E : y^2 = x^3 - a^2x + 1$ and $P = (0, 1)$. Calculate $2P$ and show that if a is odd then P has infinite order.

Exercise 4.5. The proof of the Lutz-Nagell theorem relies on certain linear relations among polynomials with integer coefficients. This is a harder question then looking at the greatest common divisor in $\mathbb{Q}[x]$, as we have to stay in $\mathbb{Z}[x]$. Here is an example. Let $f(x) = x^3 + Ax + B$ and $D = -4A^3 - 27B^2$. (It is also called the discriminant of the cubic $f(x)$. If $A, B \in \mathbb{Z}$ then there are polynomials $m(x), n(x) \in \mathbb{Z}[x]$ such that

$$m(x)f(x) + n(x)f'(x) = D. \tag{17}$$

This is easy in $\mathbb{Q}[x]$ the point is that these polynomials have integral coefficients. The following is just one of many approaches highlighting a remark in [1]. (Exercise 2.11, page 62.)

a) Assume that $m_1, n_1 \in \mathbb{Q}[x]$ satisfy the equation (17). Show that if $m_2(x) = m_1(x) + k(x)f'(x)$ then there exists $n_2(x)$ so that $m_2(x)f(x) + n_2(x)f'(x) = D$ still holds.

b) Show that if some $m, n \in \mathbb{Q}[x]$ satisfy (17) then there is a solution for which $\deg m \leq 2$. Why does this imply that $\deg n \leq 3$?

c) Let V be the vector space $V = \{(m(x), n(x)) \in \mathbb{Q}[x] \times \mathbb{Q}[x] : \deg m \leq 2, \deg n \leq 3\}$ and consider the linear transformation

$$T : V \to \{q(x) \in \mathbb{Q}[x] : \deg q \leq 5\}, \qquad (m, n) \mapsto m(x)f(x) + n(x)f'(x)$$

Write down the matrix of T in a suitable basis and show that its determinant is D.

d) Show that $m(x)f(x) + n(x)f'(x) = D$ has a unique solution $(m, n) \in V$ to and that the coefficients of m and n are integers.

Exercise 4.6. Prove the claim in (16). (Hint you may proceed as above, or simply use the Euclidean algorithm in $\mathbb{Q}[x]$ and then clear denominators.)

5. Outline of the Mordell-Weil theorem

In this section we make a roadmap for the proof of this theorem. Most of the details of the proofs are omitted.

5.1. Heights.

Definition 5.1. Height of $x = \frac{m}{n}$ with $(m, n) = 1$ is $H(x) = \max(|m|, |n|)$. We will also use the logarithmic height $h(x) = \log H(x)$.

If $P(x, y)) \in E : y^2 = x^3 + Ax + B$, then we define $H(P) = H(x)$ and $h(P) = h(x)$. By convention we set $h(\infty) = 0$. Note that the height is always non-negative.

Proposition 3. *(1) The set $\{P \in E(\mathbb{Q}) : h(p) \leq M\}$ is finite for any M.*

(2) For any point $Q \in E(\mathbb{Q})$ there is a constant $t_Q \in [0, \infty)$ such that

$$h(P + Q) \leq 2h(P) + t_Q \tag{18}$$

(3) There is a constant t_E such that

$$h(2P) \geq 4h(P) - t_E \tag{19}$$

for all $P \in E(\mathbb{Q})$.

The proofs are omitted. They are elementary, but non-trivial and rather lengthy. See for example Chapter 3 of [1].

5.2. **Infinite descent.** The descent mechanism was invented by Fermat in his proof of the impossibility to solve $x^4 + y^4 = z^2$, also the congruent number problem for $n = 1$. His descent proofs are based on a general induction principle that if there are solutions, then there is one which is minimal, as well as a very concrete construction of a smaller solution starting from any given one, (Exercise 1.10). We will only illustrate the former in this section. However we still need to know something about our elliptic curve to be able to generalize Fermat's approach of getting a smaller solution. His explicit construction is replaced by the the height bounds above as well as the following

Theorem 5.2 (Weak Mordell-Weil Theorem). *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with A, B rational numbers. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Remark. The statement means that that there are finitely many points $Q_1, ..., Q_k$ such that any point $P \in E(\mathbb{Q})$ can be written as $P = 2P' + Q_j$ for some j.

We will postpone the proof of the above theorem and highlight its immediate consequence, the strong Mordell-Weil theorem.

Theorem 5.3. *Let G be an abelian group with a function $h : G \to [0, \infty)$ that satisfies the statements in Proposition 3 and such that $G/2G$ is finite. Then G is finitely generated.*

Proof. Let $Q_1, ...Q_k$ be representatives of $G/2G$ and let $K = \max(t_{Q_j})$, with t_{Q_j} as in (18). Note that when $P = \infty$ the bound (18) shows that $h(Q_j) \leq t_{Q_j}$.

Let also $M = K + t_E$, where t_E as in (19). The set $\{P \in G : h(P) \leq M\}$ is finite. Let H be the subgroup generated by this set. We will show that $H = G$.

Assume on the contrary that there is $P \in G$, $P \notin H$. Since there are only finitely many elements of height less than or equal to $h(P)$ there is one of minimal height that is still not in H. Assume that it is already P.

Now $P = 2P' - Q_j$ for some $P' \in G$. The height bounds give

$$h\left(P + Q_i\right) \leq 2h(P') + t_{Q_i} \leq 2h(P') + K$$

and

$$4h\left(P'\right) \leq h\left(2P'\right) + t.$$

It follows that

$$4h\left(P'\right) \leq h\left(2P'\right) + t \leq h\left(P + Q_i\right) + t \leq 2h(P) + M.$$

Clearly $h(P) > M$ since $P \notin H$. This shows that

$$h(P') \leq \frac{3}{4} h(P)$$

and so the height of P' is strictly less that that of P. But then $P' \in H$ by the assumption that P has minimal height among elements not in H. This in turn leads to a contradiction since $2P' + Q_j \in H$. □

5.3. **The weak Mordell-Weil theorem.** This is about the statement that the group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. We will only show this when

$$E : y^2 = f(x),$$

where

$$f(x) = x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3), \text{ with } e_1, e_2, e_3 \in \mathbb{Z}.$$

Note that the product of the $x - e_j$-s is a square. We will see that P is in $2E(\mathbb{Q})$ if and only if each of these factors are already squares themselves.

Definition 5.4. Assume that $P(x, y) \in E(\mathbb{Q})$. Write each of the rational numbers $x - e_j$ as a product of a square-free integer b_j and u_j^2, the square of a rational number u_j:

$$x - e_j = b_j u_j^2, \quad b_j = b_j(P) \in \mathbb{Z}, u_j = u_j(P) \in \mathbb{Q}. \tag{20}$$

If $P = \infty$ we define $b_j(\infty) = 1$ for $j = 1, 2, 3$. If $P = (e_1, 0)$ we define b_2, b_3 as usual whereas we define b_1 by writing

$$(e_1 - e_2)(e_1 - e_3) = b_1 u_1^2.$$

The extension to the other two roots e_2 and e_3 goes similarly.

Theorem 5.5. *Then we have the following*

1. *Let $D = -4A^3 - 27B^2$. Then $D = d^2$, where $d = (e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$ and for $P \in E(\mathbb{Q})$, $b_j(P)|D$, for each j.*
2. *For any $P, Q \in E(\mathbb{Q})$*

$$b_j(P) b_j(Q) b_j(P + Q) = v_j^2 \tag{21}$$

for some $v_j \in \mathbb{Q}$.

3. *$b_1(P) = b_2(P) = b_3(P) = 1$ if and only if $P \in 2E(\mathbb{Q})$.*
4. *Assume that $b_1, b_2, b_3 \in \mathbb{Z}$ are such that $b_j|D$ for each j. If not all of the b_j-s are 1, then there exist $P \in E(\mathbb{Q})$ such that $b_j(P) = b_j$ if and only if the system of equations*

$$b_1 u_1^2 - b_2 u_2^2 = e_2 - e_1 \tag{22}$$

$$b_1 u_1^2 - b_1 b_2 u_3^2 = e_3 - e_1 \tag{23}$$

has a solution $u_1, u_2, u_3 \in Q^*$. If such a solution exists, one may choose $P = (b_1 u_1^2 + e_1, b_1 b_2 u_1 u_2 u_3)$. If all the b_j-s are 1, we may choose $P = \infty$.

Corollary 5. *For each triple (b_1, b_2, b_3) where $b_j|D$ for each j, select $Q = Q_{b_1,b_2,b_3} \in E(\mathbb{Q})$ for which $b_j(Q) = b_j$, if such a Q exist. Clearly this list is finite say $Q_1, ..., Q_l$. Then we have that any $P \in E(\mathbb{Q})$ can be written as $2P' + Q_k$ for some $k \in \{1, ..., l\}$.*

The proof of the corollary. Assume that $P \in E(\mathbb{Q})$, and that $b_j(P) = b_j$. Let $Q_k = Q_{b_1,b_2,b_3}$ be the selected point for which $b_j(Q) = b_j$. Note that $b_j(-Q_k) = b_j(Q_k)$ since they have the same x-coordinates, and the b_j only depend on those. By (21)

$$b_j(P)b_j(-Q_k)b_j(P - Q_k) = v_j^2,$$

but $b_j(P) = b_j(-Q)$ and so $b_j(P - Q_k)$ is a square-free number which is also a square. This is only possible if $b_j(P - Q_k) = 1$. Since this must hold for each j we have by the description of $2E(\mathbb{Q})$ in 3. that $P - Q_k$ must lie in that subgroup, $P - Q_k = 2P'$ for some $P' \in E(\mathbb{Q})$. □

Remark. The theorem can be rephrased again using group theory. For an integer $b \in \mathbb{Z}$ let $sf(b)$ denote its square-free part, with the same sign. For example $sf(25) = 1, sf(-12) = -3$. Introduce the the equivalence relation on $\mathbb{Q}^*$: $r_1 \sim r_2$ if and only if $r_1/r_2 = t^2$. for some $t \in \mathbb{Q}^*$. This is the same as $sf(r_1) = sf(r_2)$. If we denote the equivalence class of r by $\langle r\rangle$ then the equivalance classes form a group under multiplication defined by $\langle r_1\rangle\langle r_2\rangle = \langle r_1r_2\rangle$. We denote this group by $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. The second claim means that each "b_j" is a group homomorphism from $E(\mathbb{Q})$ to $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. By the first assertion the image is a finite group G_D, generated by $\langle -1\rangle$ and $\langle p\rangle$ for primes $p|D$. Finally the third statement shows that if we combine the three maps into a joint homomophism.

$$E(\mathbb{Q}) \to G_D \times G_D \times G_D \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

then the image is isomorphic to $E(\mathbb{Q})/2E(\mathbb{Q})$.

Remark. The last claim is of a different nature. It is rather easy to see that it holds, and in theory it could be used to find generators of $E(\mathbb{Q})$. This is based on the fact that for a commutative group $G = \mathbb{Z}^r \times A$, with A finite, $|G/2G| = 2^r|A/2A|$. In the elliptic curve case for a general cubic, whose roots are not necessarily rational we have that the finite part $A = E_{tor}(\mathbb{Q})$ satisfies

$$|E_{tor}(\mathbb{Q})/2E_{tor}(\mathbb{Q})| = \begin{cases} 1 & \text{if } f \text{ has no rational roots,} \\ 2 & \text{if } f \text{ has exactly 1 rational root,} \\ 4 & \text{if all roots of } f \text{ are rational.} \end{cases}$$

However it may not be easy to determine if the system (22) has solution. We illustrate this via the congruence number courve as an example.

Example 5.6. Let $E : y^2 = x^3 - x = x(x - 1)(x + 1)$. Then $D = 4 = 2^2$. The possible square-free integers dividing D are ±1 and ±2. We will number the roots as $e_1 = 0, e_2 = 1$ and $e_3 = -1$. We now have to decide for which pairs (b_1, b_2) do we have a solution of the system (22). For example when $b_1 = b_2 = 1$ we may simply choose ∞. Also for the obvious points $(0,0), (1,0)$ and $(-1,0)$ we may calculate the image directly. For example for $(0,0)$ we have to find the square-free parts of $(e_1-e_2)(e_1-e_3)=-1$, $e_1-e_2=-1$ and $e_1-e_3=1$. Clearly this gives $b_1=-1, b_2=-1$. Similarly for $(1,0)$ we have $(b_1,b_2)=(1,2)$, and for $(-1,0)$ we have $(b_1,b_2)=(-1,-2)$.

There are also a number of cases when we can use simple observations to deduce that a non-trivial solution does not exist. For example when $b_1=-1$ and $b_2=1$ the equation $-u_1^2-u_2^2=1$ clearly has no solution even in $\mathbb{R}$. We may summarize this in a table

b_1 \ b_2	1	2	-1	-2
1	∞		None:$\mathbb{R}$	
2	$(1,0)$			
-1			(0.0)	
-2			$(-1,0)$	

By the group theoretical description we know that the number of pairs for which a solution exists is either $4,8$ or 16 depending on whether the "rank" r is $0,1$ or 2. It is clear that 16 is no longer an option. One can find a few more cases that can be excluded, but showing this way, that $r=0$ is not feasible. Fermat's proof (see exercise 1.10) shows this as well as exercise 5.1. While there it may look like an isolated lucky coincidence the book [1] outlines a general method that broadly extends the scope of Fermat's trick.

The following is a useful little observation.

Proposition 4. *Assume that $(x,y)\in E(\mathbb{Q})$. Then we have $x=\frac{u}{t^2}$, $y=\frac{v}{t^3}$ for some integers u,v,t such that $(u,t)=(v,t)=1$.*

Proof. Let $x=\frac{u}{m}$, $y=\frac{v}{n}$ be in lowest form. After clearing the denominators we have

$$v^2m^3=u^3n^2+Aum^2n^2+Bm^3n^2.$$

Clearly $n^2|v^2m^3$ and then $n^2|m^3$. On the other hand $m|u^3n^2$ and so $m|n$, since $(u,m)=1$. This shows that $m^3|Aum^2n^2$ and so $m^3|u^3n^2$ which in turn implies that $m^3|n^2$ and so $m^3=\pm n^2$. By changing the sign u we may assume that $m^3=n^2$. Let $t=\frac{n}{m}$. Then $t^2=m$ and $t^3=n$. □

We define for each prime p a map β_p from $\mathbb{Q}^*$, the multiplicative group of the non-zero rational numbers into the group

$$\mu_2=\{1,-1\}\subset\mathbb{Q}^*.$$

Recall that for $x\in\mathbb{Q}^*$

$$v_p(x)=k \iff x=p^k\left(\frac{m}{n}\right), \text{ with } (p,mn)=1.$$

Then we define

$$\beta_p(x)=(-1)^{v_p(x)}. \tag{24}$$

Note that $\beta_p(x)$ is 1 or -1 depending on whether in the factorization of x the exponent of p is even or odd.

We also introduce $\beta_\infty(x) = \operatorname{sgn}(x)$, for $\operatorname{sgn}(x) = x/|x|$ the sign of x. It is easy to see (Exercise 5.2) that x is a square in $\mathbb{Q}^*$ if and only if $\beta_\infty(x) = 1$ and $\beta_p(x) = 1$ for all primes p.

Lemma 4. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve, with discriminant $D = -4A^3 - 27B^2$. Assume also that $x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$ with $e_1, e_2, e_3 \in \mathbb{Q}$. If $p \nmid D$ and $P = (x, y) \in E(\mathbb{Q})$ then*

$$\beta_p(x - e_j) = 1 \text{ for } j = 1, 2, 3. \tag{25}$$

The proof is an easy corollary of Proposition 4 and of the factorization of $D = d^2$ in terms of the roots. It is left as an exercise. (5.3)

We will now introduce a map from $E(\mathbb{Q})$ to the group $G_{l+1} \times G_{l+1} \times G_{l+1}$, where $G_{l+1} = \overbrace{\mu_2 \times ... \times \mu_2}^{l+1 \ times}$ and where $l = \omega(D)$ is the number of different prime factors of D. The main purpose of this map is to show that it is a homomorphism with kernel $2E(\mathbb{Q})$. Since G_{l+1} is finite this immediately implies the weak Mordell-Weil theorem.

Definition 5.7. (1) For a given discriminant $D = p_1^{e_1}..p_l^{e_l}$ and $x \in \mathbb{Q}^*$ let $\beta_D(x) = (\beta_{p_1}(x), ..., \beta_{p_l}(x), \beta_\infty(x))$.

(2) For $j = 1, 2, 3$ let $\phi_j : E(\mathbb{Q}) \to G$ be the function given for $P = (x, y)$ by

$$\phi_j(P) = \begin{cases} 1, & \text{if } P = \infty, \\ \beta_D(x - a_i)(x - a_k) & \text{if } x = a_j \\ \beta_D(x - a_j) & \text{otherwise.} \end{cases}$$

Theorem 5.8. *Let $\phi = (\phi_1, \phi_2, \phi_3) : E(\mathbb{Q}) \to G_{l+1} \times G_{l+1} \times G_{l+1}$,*

$$P(x, y) \mapsto (\phi_1(x), \phi_2(x), \phi_3(x)).$$

(1) The map ϕ is a homomorphism from $E(\mathbb{Q})$ to $G_{l+1} \times G_{l+1} \times G_{l+1}$.
(2) The kernel of ϕ is $2E(\mathbb{Q})$.
(3) The value of ϕ_3 is determined by ϕ_1, ϕ_2.

We will give the proof of this theorem in the exercises.

5.4. **Exercises.**

Exercise 5.1. Let $E : y^2 = x^3 - x$.

a) Assuming that Theorem5.5 holds show that if $P(x, y) \in E(\mathbb{Q})$, with $y \neq 0$ then $\exists P' \in E(\mathbb{Q})$ such that $2P' = P$. (Hint: use the criterion in 3. of Theorem 5.5 and argue as in Exercise 1.10.)

b) Show by using the explicit duplication formula (15) that if $P' = (x', y') \in E(\mathbb{Q})$, such that $y' \neq 0$, then $h(P') < h(2P')$.

c) Conclude that there are no non-trivial solutions to $y^2 = x^3 - x$ and so $|E(\mathbb{Q})| = 4$.

Exercise 5.2. Show that x is a square in $\mathbb{Q}^*$ if and only if $\beta_\infty(x) = 1$ and $\beta_p(x) = 1$ for all primes p.

Exercise 5.3. Prove Lemma 4, that is if $p \nmid D$ and $P(x, y) \in E(\mathbb{Q})$ then

$$\beta_p(x - e_j) = 1 \text{ for } j = 1, 2, 3.$$

Exercise 5.4. Let $E : y^2 = f(x) = (x-e_1)(x-e_2)(x-e_3)$ and $P_1(x_1, y_1), P_2(x_2, y_2 \in E(\mathbb{Q})$. Let also $y = \lambda x + \nu$ be the line through P_1 and P_2 and $g(x)$ be the cubic polynomial

$$g(x) = f(x) - (\lambda x + \nu)^2.$$

a) Show that $g(x) = (x - x_1)(x - x_2)(x - x_3)$ where x_3 is the x coordinate of $P_1 + P_2$.
b) Assume that $p|D$ and consider the matrix with entries $\beta_p(x_i - e_j)$. Show that the product of each row is 1. Also show that the product of each column is 1.
c) Repeat the above with the matrix with entries $\beta_\infty(x_i - e_j)$.
d) Show that ϕ is a homomorphism, $\phi(P_1 + P_2) = \phi(P_1)\phi(P_2)$. (Hint: it is enough to consider this componentwise for a fixed $p|D$ and one of the roots e_j. Be careful with the special cases!)

Exercise 5.5. Assume again that $E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$. Let $P_1(x_1, y_1)$ be such that $y_1 \neq 0$. Then we know that

$$f(x) - (\lambda(x - x_1) + y_1)^2 = (x - x_1)^2(x - x_2),$$

where $\lambda = \frac{f'(x_1)}{2y_1}$ and $2P = (x_2, y_2)$.

a) Show that $x_2 - e_1 = \left(\frac{\lambda(e_1-x_1)+y_1}{e_1-x_1}\right)^2$
b) Show that $\lambda(e_1 - x_1) + y_1 = \frac{e_1-x_1}{2y_1}(f'(x_1) + 2(x_1 - e_2)(x_1 - e_3))$.
c) Show that $e_2 + e_3 = -A - e_1$ and that $e_2e_3 = \frac{x_1^3+Ax_1-y_1^2}{e_1}$.
d) Finally evaluate $(x_1 - e_2)(x_1 - e_3)$ in terms of x_1, y_1 and e_1 only and conclude that

$$x_2 - e_1 = a_1^2, \text{ where } a_1 = \frac{A - x_1^2}{2y_1} + \frac{x_1}{y_1}e_1 + \frac{1}{y_1}e_1^2 \tag{26}$$

Exercise 5.6. *This exercise is a crucial step in proving that* $\ker\phi = 2E(\mathbb{Q})$. Assume that x is such that $x - e_j = a_j^2$ for some $a_j \in \mathbb{Q}^*$. We want to construct x_1 in formula (26) above such that we have $y_1^2 = f(x_1)$ and that $2P(x_1, y_1) = (x, a_1a_2a_3)$.

a) Show that the system of equations

$$\begin{aligned} u_0 + u_1e_1 + u_2e_1^2 &= a_1 \\ u_0 + u_1e_2 + u_2e_2^2 &= a_2 \\ u_0 + u_1e_3 + u_2e_3^2 &= a_3 \end{aligned}$$

has a unique solution $(u_0, u_1, u_2) \in \mathbb{Q}^3$.

b) Following (26) we want to set $u_2 = \frac{1}{y_1}$ and $u_1 = \frac{x_1}{y_1}$. Show that this choice satisfies $y_1^2 = f(x_1)$ iff

$$u_2 = u_1^3 + Au_1u_2^2 + Bu_2^3.$$

Exercise 5.7. *While it is possible to show directly that above equations are satisfied, the calculations are rather lengthy. We present here an alternative.*

(1) Given $P \in E(\mathbb{C})$, how many $P' \in E(\mathbb{C})$ exist such that $2P' = P$? (Hint: how many z' satisfies $2z' \equiv z \mod \Lambda$? See exercise 3.6.)

(2) How many $P' \in E(\mathbb{C})$ exist for which $x(2P') = x(P)$?

(3) Show that if $x(2P') = x(P)$ and we set $u_0 = \frac{A - x(P')^2}{2y(P')}$, $u_1 == \frac{x(P')}{y(P')}$ and $u_2 = \frac{1}{y(P')}$ then u_0, u_1, u_2 satisfy the linear system in the previous problem with the right hand sides being $\pm a_1, \pm a_2, \pm a_3$ with a unique choice of the signs.

(4) Therefore show that the coordinates constructed in the previous exercise correspond to one of the P' for which $2P' = (x, y)$, which therefore have rational coordinates.

Main reference for the mini-course

[1] Silverman, J.H. and Tate, J.T., 1992. Rational points on elliptic curves (Vol. 9). New York: Springer-Verlag. *The minicourse was mostly based on this book. It is a must read even for people familiar with the subject.*

For further reading

[1] Ash, A., Gross, R. and Gross, R., 2012. Elliptic tales: curves, counting, and number theory. Princeton: Princeton University Press. *Concentrates more on the so-called L-functions of elliptic curves. Do not know what they are? You will after finishing this book. A very readable account.*

[2] Ash, A. and Gross, R., 2008. Fearless symmetry. In Fearless Symmetry. Princeton University Press. *A more general view of L-functions, still very elementary.*

[3] Ireland, K., Rosen, M.I. and Rosen, M., 1990. A classical introduction to modern number theory (Vol. 84). Springer Science & Business Media. *This is a broad introduction to number theory, as the title says. It puts a strong emphasis on direct arithmetic applications. Contains a lot of information about elliptic curves, including the proof of Mordell-Weil in general.*

[4] Washington, L.C., 2008. Elliptic curves: number theory and cryptography. Chapman and Hall/CRC. *Somewhere in between Silverman-Tate and Silverman. Contains a wealth of information from a rather concrete point of view.*

For advanced studies

[1] Cremona, J. E. Algorithms for modular elliptc curves. Available freely online at: https://johncremona.github.io/book/fulltext/index.html *This is very advanced, but as the title shows, very concrete.*

[2] Koblitz, N.I., 2012. Introduction to elliptic curves and modular forms (Vol. 97). Springer Science & Business Media. *Uses the congruent number problem as a motivation. Very readable but much wider in scope, rather high level and assumes a great amount of knowledge of complex analysis.*

[3] McKean, H. and Moll, V., 1999. Elliptic curves: function theory, geometry, arithmetic. Cambridge University Press. *This is again a book which has a fair amount of analysis. It also gives some classical applications outside of number theory.*

[4] Silverman, J.H., 2009. The arithmetic of elliptic curves (Vol. 106, pp. xx+-513). New York: Springer. *The standard reference to turn to. Knowledge about elliptic curves beautifully organized into a coherent theory. As usual it can be better appreciated if the reader is already familiar with some of that knowledge, say from Silverman-Tate.*

p-ADIC METHODS IN ARITHMETIC

Gergely Zábrádi

These are the notes of a minicourse given by the author at ELTE in June 2022. Nothing in these notes are original or new. The text has been influenced by the books of Gouvea and Serre [3, 4]. The goal of the course is to explain the local–global principle in arithmetic through the proof of the Theorem of Hasse and Minkowski.

1. Introduction

Why do diophantine equations have no solutions? We start by the following trivial examples.

Example 1. Consider the equation $x^2 + y^2 = -1$ in $\mathbb{Z}$ (or in $\mathbb{Q}$). It has no solutions *because* it has no solutions over $\mathbb{R}$ either (which contains $\mathbb{Z} \subset \mathbb{Q}$).

Example 2. Consider the equation $x^2 - 3y^2 = -1$ in $\mathbb{Z}$. It has no solutions since there are no solutions modulo 3 either (one could also argue mod 4).

I claim that the above 2 types of obstruction have the same nature! To see this at first investigate whether Example 2 has solutions in $\mathbb{Q}$. Finding a common denominator write $x = \frac{a}{c}$ and $y = \frac{b}{c}$ with $(a, b, c) = 1$ to obtain $a^2 - 3b^2 = -c^2$. We may argue the same way: Since -1 is not a square mod 3, we must have $3 \mid c$ and $3 \mid a$ whence $9 \mid a^2 + c^2 = 3b^2$ deducing $3 \mid b$, as well—contradiction. In fact, we have just shown that this equation has no solutions in the field $\mathbb{Q}_3$ of 3-adic numbers. In order to motivate what those are, let us start with the analogy between arithmetic and $\mathbb{Z}$ and arithmetic in $\mathbb{C}[t]$.

ring	$\mathbb{Z}$	$\mathbb{C}[t]$
UFD	✓	✓
PID	✓	✓
maximal ideals	primes	$\{(t-c) \mid c \in \mathbb{C}\}$
local expansion	$a_0 + a_1 p + \cdots + a_n p^n$ only for nonnegative integers $(a_i \in \{0, 1, \ldots, p-1\})$	$a_0 + a_1(t-c) + \cdots + a_n(t-c)^n$ any polynomial $(a_i \in \mathbb{C})$
fraction field	$\mathbb{Q}$	$\mathbb{C}(t) = \{\frac{f}{g} \mid f, g \in \mathbb{C}[t], g \neq 0\}$
local expansion of fractions	???	$\sum_{n=-N}^{\infty} a_n (t-c)^n$

Note that the local expansion of fractions $\frac{f}{g}$ at c converges in a punctured neighbourhood of c since "t is close to c", ie. "$(t-c)$ is close to 0" $\Rightarrow$ $(t-c)^n \to 0$ as $n \to +\infty$. Replacing $(t-c)$ with the prime $p \in \mathbb{Z}$ makes us want to have $p^n \to 0$ in some metric.

Definition. For a nonzero rational number $\frac{a_1}{b_1} p^k$ with $p \nmid a_1, b_1$, $k \in \mathbb{Z}$ denote by $|\frac{a_1}{b_1} p^k|_p := p^{-k}$ the *p-adic absolute value.* In other words we have $|\alpha|_p = p^{-v_p(\alpha)}$ where v_p denotes the exponent of p in the prime decomposition of a number. Further, put $|0|_p := 0$.

Lemma 1.1. *For all $x, y \in \mathbb{Q}$ we have*

(1) $|x|_p = 0 \Leftrightarrow x = 0$.

(2) $|xy|_p = |x|_p|y|_p$.
(3) $|x+y|_p \leq \max(|x|_p, |y|_p)(\leq |x|_p + |y|_p)$.

Proof. Left to the reader. □

The third inequality above is called the ultrametric inequality. Absolute values are functions $|\cdot|\colon K \to \mathbb{R}^{\geq 0}$ satisfying the above first 2 conditions and the triangle inequality (third condition with just $\leq |x| + |y|$ on the right). An absolute value is called nonarchimedean if the ultrametric inequality is also satisfied, otherwise we call it archimedean. We call two absolute values $|\cdot|$ and $|\cdot|'$ *equivalent* if there exists a real number $s > 0$ such that $|x|^s = |x|'$ for all $x \in K$. Fact: two absolute values on K are equivalent if and only if they induce the same topology on K.

Theorem 1.2 (Ostrowski). *Any absolute value on $\mathbb{Q}$ is equivalent to one of the following (pairwise inequivalent) absolute values:*

(1) The trivial absolute value $|x|_1 = \begin{cases} 1 \text{ if } x \neq 0 \\ 0 \text{ if } x = 0 \end{cases}$.
(2) The usual archimedean absolute value $|\cdot|_\infty$.
(3) The p-adic absolute value $|\cdot|_p$ *for some prime p.*

Definition. The field $\mathbb{Q}_p$ of p-adic numbers is the *completion* of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Here by completion we mean the equivalence classes of Cauchy sequences. Two Cauchy sequences are *equivalent* if their merge is also a Cauchy sequence.

We recall some basic facts about $|\cdot|_p$ and $\mathbb{Q}_p$:

(1) If $(x_n)_{n\geq 1} \subset \mathbb{Q}$ is Cauchy in $|\cdot|_p$ then $|x_n|_p$ stabilizes or $|x_n|_p \to 0$. Indeed, the range of $|\cdot|_p$ on $\mathbb{Q}$ is $p^{\mathbb{Z}} \cup \{0\}$ which has no limit point other than 0. In particular, the range of $|\cdot|_p$ on $\mathbb{Q}_p$ is the same set as $p^{\mathbb{Z}} \cup \{0\}$ is closed in $\mathbb{R}$.
(2) Elements of $\mathbb{Q}_p$ have a *unique* p-adic expansion of the form

$$0 \neq x = \sum_{n=-N}^{\infty} a_n p^n \qquad a_n \in \{0, 1, \ldots, p-1\}, a_{-N} \neq 0 \ .$$

(3) One could in fact work with any other set of representatives of $\mathbb{Z}/(p) = \mathbb{F}_p$ instead of $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}$.
(4) The closed unit disk

$$\mathbb{Z}_p := \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\} = \{a_0 + a_1 p + \cdots + a_n p^n + \cdots\}$$

is a subring! It is closed under addition due to the ultrametric inequality. $\mathbb{Z}_p$ is called the *ring of p-adic integers.*
(5) We have $\mathbb{Z}_p/(p^n) \simeq \mathbb{Z}/(p^n)$. $\mathbb{Z}_p$ is a complete discrete valuation ring , in particular it has unique factorization with single prime p.

Example 3. Let $p = 5$. We compute

$$\frac{35}{31} = \frac{2 \cdot 5 + 5^2}{1 + 5 + 5^2} = \frac{2p + p^2}{1 + p + p^2} = 2p + 4p^2 + 3p^3 + p^4 + 4p^5 + \cdots + 4p^n + \cdots =$$
$$= 2p + 4p^2 + 3p^3 + p^4 + 3p^5 \frac{1}{1-p} \ .$$

Indeed, one has to "carry over" when multiplying or adding. Further, we have

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots \ .$$

In particular, there is a p-adic expansion of any not necessarily positive integer.

2. Solving equations in $\mathbb{Z}_p$ (or in $\mathbb{Q}_p$)

Lemma 2.1. *Let $f_1, \dots, f_k \in \mathbb{Z}_p[x_1, \dots, x_m]$ be polynomials. The following are equivalent:*

(1) *$f_1, \dots, f_k$ have a common root in $\mathbb{Z}_p^m$;*
(2) *$f_1, \dots, f_k$ have a common root in $(\mathbb{Z}/(p^n))^m$ for all $n \geq 1$.*

Sketch of proof. (1) ⇒ (2): We may reduce the common root mod p^n and use the fact $\mathbb{Z}_p/(p^n) \simeq \mathbb{Z}/(p^n)$.

(2) ⇒ (1): One may argue using the fact that $\mathbb{Z}_p$ is a compact topological space therefore so is $\mathbb{Z}_p^m$. Alternatively, one could use König's lemma: put $A_n \subseteq \mathbb{Z}/(p^n)$ the set of mod p^n solutions. These are finite sets and there is a reduction map $A_{n+1} \to A_n$ for all $n \geq 1$. Further, by assumption $A_n \neq \emptyset$ for any $n \geq 1$. Assume all the elements of A_1 can only be lifted to some finite level. Since A_1 is finite, there is a maximum of these levels, say n. However, A_{n+1} is nonempty, and any element in A_{n+1} reduces to an element in A_1 contradicting that n was the maximum level of all the lifts of elements of A_1. Therefore the subset $B_j \subseteq A_j$ consisting of elements of A_j that can be lifted arbitrarily is nonempty for any $j \geq 1$. Any element in B_1 lifts to an element in B_2 which lifts to an element B_3 and so on, so in the limit we obtain a p-adic common root of $f_1, \dots, f_k$ as a sequence of compatible elements in A_n $(n \geq 1)$. □

Proposition 2.2. *Let $f_1, \dots, f_k \in \mathbb{Z}_p[x_1, \dots, x_m]$ be* homogeneous *polynomials. Then the following are equivalent:*

(1) *$f_1, \dots, f_k$ have a nontrivial common root in $\mathbb{Q}_p^m$;*
(2) *$f_1, \dots, f_k$ have a nontrivial common root in $\mathbb{Z}_p^m$;*
(3) *$f_1, \dots, f_k$ have a primitive common root in $(\mathbb{Z}/(p^n))^m$ for all $n \geq 1$.*

Here by trivial root we mean $(0, \dots, 0)$ and by primitive root we mean a tuple $(\alpha_1, \dots, \alpha_m)$ with greatest common divisor $\gcd(\alpha_1, \dots, \alpha_m) = 1$.

Proof. (1) and (2) are equivalent since we may multiply any root in $\mathbb{Q}_p^m$ by the least common multiple of the denominators of the coordinates which is still a solution as $f_1, \dots, f_k$ are homogeneous. In particular, there is a nontrivial solution if and only if there is a primitive one. (2) and (3) are equivalent by Lemma 2.1. □

Lemma 2.3 (Hensel)**.** *Let $f(x) \in \mathbb{Z}_p[x]$, $n, k \in \mathbb{Z}$ with $0 \leq 2k < n$. Assume $f(\alpha) \equiv 0 \pmod{p^n}$ and $v_p(f'(\alpha)) = k$. Then there is a $\beta \in \mathbb{Z}_p$ such that $f(\beta) \equiv 0 \pmod{p^{n+1}}$, $v_p(f'(\beta)) = k$, and $\beta \equiv \alpha \pmod{p^{n-k}}$.*

Proof. We look for β in the form $\beta = \alpha + p^{n-k}z$ and compute

$$f(\beta) = f(\alpha + p^{n-k}z) = f(\alpha) + p^{n-k}zf'(\alpha) + (p^{n-k}z)^2(\cdots) \equiv f(\alpha) + p^{n-k}zf'(\alpha) \pmod{p^{n+1}}$$

since $p^{n+1} \mid p^{2n-2k}$. On the other hand, $v_p(p^{n-k}f'(\alpha)) = n - k + k = n \leq v_p(f(\alpha))$ whence $z := -\frac{f(\alpha)}{p^{n-k}f'(\alpha)}$ lies in $\mathbb{Z}_p$. □

Theorem 2.4. *Let $f \in \mathbb{Z}_p[x_1, \dots, x_m]$, $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{Z}_p^m$, $n, k \in \mathbb{Z}$ with $0 \leq 2k < n$. Assume there exists an index $j \in \{1, \dots, m\}$ such that $f(\alpha) \equiv 0 \pmod{p^n}$ and $v_p\left(\frac{\partial f}{\partial x_j}(\alpha)\right) = k$. Then there exists a $\beta \in \mathbb{Z}_p^m$ such that $f(\beta) = 0$ and $\beta \equiv \alpha \pmod{p^{n-k}}$.*

Proof. We apply Lemma 2.3 repetitively on the 1-variable polynomial $f(\alpha_1, \dots, x_j, \dots, \alpha_m)$ in order to find $\beta = (\beta_1, \dots, \beta_m)$ such that $\beta_i = \alpha_i$ for all $j \neq i \in \{1, \dots, m\}$. □

Corollary 2.5. *The polynomial $x^{p-1} - 1$ splits completely over $\mathbb{Z}_p$. In particular, the group $\mathbb{Z}_p^\times$ splits as a direct product $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ (where μ_{p-1} denotes the group of $p - 1$th roots of unity).*

Proof. The polynomial $x^{p-1} - 1$ has $p - 1$ distinct roots in $\mathbb{F}_p = \mathbb{Z}/(p)$ which all lift to $\mathbb{Z}_p$ by Lemma 2.3 ($n = 1$, $k = 0$: the value of the derivative $(x^{p-1} - 1)' = (p - 1)x^{p-2}$ is not divisible by p at the roots mod p). □

Proposition 2.6. *Assume $p \neq 2$. Then any $u \in 1 + p\mathbb{Z}_p$ has a square root in $\mathbb{Z}_p$.*

Proof. The polynomial $x^2 - u$ has two distinct roots mod p since the derivative $(x^2 - u)' = 2x$ does not vanish mod p at ± 1, so we may apply Lemma 2.3 with $n = 1$, $k = 0$. □

Proposition 2.7. *Assume $p = 2$. Then any $u \in 1 + 8\mathbb{Z}_p$ has a square root in $\mathbb{Z}_2$.*

Proof. The polynomial $x^2 - u$ has the root 1 mod $8 = 2^3$ and the valuation of the derivative $(x^2 - u)' = 2x$ at 1 equals $v_2(2) = 1$, so we may apply Lemma 2.3 with $n = 3$, $k = 1$. □

Corollary 2.8. *We have*

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = \begin{cases} \langle p, u \rangle = \{1, p, u, pu\} \simeq C_2 \times C_2 & \text{if } p \neq 2 \\ \langle 2, 5, -1 \rangle = \{\pm 1, \pm 2, \pm 5, \pm 10\} \cong C_2 \times C_2 \times C_2 & \text{if } p = 2\ . \end{cases}$$

Here u denotes a quadratic nonresidue mod p, ie. $\left(\frac{u}{p}\right) = -1$.

Proof. The multiplicative group decomposes as a direct product $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p \times \simeq p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p)$. The result follows from Propositions 2.6 and 2.7 noting $(\mathbb{Z}/(8))^\times = \langle -1, 5 \rangle$. □

3. Statement and application of Theorem of Hasse and Minkowski

It is nice to have some obstructions to the existence of rational solutions of diophantine equations, but how does one guarantee the existence of such? Hasse's local–global principle is that whenever the polynomials $f_1, \dots, f_k \in \mathbb{Q}[x_1, \dots, x_m]$ have a common (nontrivial) root in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p then there should be a common (nontrvial) root in $\mathbb{Q}$, too (if the polynomials are homogeneous). However, the following famous counterexample due to Ernst Selmer (1951) shows that this is, unfortunately, not always the case:

Example 4. The equation $3x^3 + 4y^3 + 5z^3$ has nontrivial solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p, but no nontrivial solutions in $\mathbb{Q}$.

Hint of proof. The existence of real and p-adic solutions is not that hard, one first finds solutions mod p and lifts them using Hensel's lemma (one has to distinguish the cases of $p = 3, 5$). The proof of nonexistence of rational solutions requires some algebraic number theory (arithmetic in the ring $\mathbb{Z}[\sqrt[3]{6}]$) or elliptic curves. See the notes of Keith Conrad [2] and the book of Cassels [1] for details. □

However, for quadratic forms we have the following result of Hasse and Minkowski from the 1920s:

Theorem 3.1 (Hasse–Minkowski)**.** *Assume $f \in \mathbb{Q}[x_1, \dots, x_m]$ is homogeneous of degree 2. The the following are equivalent:*

(1) *there exists an $\alpha \neq 0$ in $\mathbb{Q}^m$ such that $f(\alpha) = 0$;*
(2) *there exists an $\alpha^{(\infty)} \neq 0$ in $\mathbb{R}^m$ such that $f(\alpha^{(\infty)}) = 0$ and for all primes p there exists an $\alpha^{(p)} \neq 0$ in $\mathbb{Q}_p^m$ such that $f(\alpha^{(p)}) = 0$.*

We postpone the proof of Theorem 3.1 until section 6. Let us see some application first to the classical problem of sums of three squares.

Theorem 3.2. *A nonnegative integer n can be represented by a sum of three squares if and only if n is* not *of the form $4^a(8k + 7)$ $(a, k \in \mathbb{Z}^{\geq 0})$.*

Proof. At first we show that $x^2 + y^2 + z^2 = 4^a(8k + 7)$ has no solutions in $\mathbb{Z}$. If $a \geq 1$ then arguing mod 4 we find that all x, y, z must be even. Therefore we may divide the equation by 4 to represent $4^{a-1}(8k+7)$ as a sum of three squares. Repeating the process we may assume $a = 0$. However, squares have residues $0, 1$, or 4 mod 8, so three squares cannot add up to $8k + 7$.

Step 1: For the converse, we first show that if $n \neq 4^a(8k + 7)$ then n can be written as a sum of the squares of three rational numbers. Consider the quadratic form $x^2 + y^2 + z^2 - nu^2$. We show that it has a local solution at each prime and at infinity. Since $n > 0$, there is a nontrivial root in $\mathbb{R}$. Next we treat $p = 2$:

Lemma 3.3. *Assume $n \not\equiv 0, 4, 7 \pmod 8$, $k \geq 3$. Then there exist $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 + z^2 \equiv n \pmod{2^k}$.*

Proof. Using Proposition 2.7 we may assume $k = 3$. We check $1 = 0^2 + 0^2 + 1^2$, $2 = 0^2 + 1^2 + 1^2$, $3 = 1^2 + 1^2 + 1^2$, $5 = 0^2 + 1^2 + 2^2$, $6 = 1^2 + 1^2 + 2^2$. □

By Lemma 3.3 the form $x^2 + y^2 + z^2 - nu^2$ has a nontrivial zero in $\mathbb{Q}_2$: whenever $4 \mid n$ we may replace $u = \frac{u_1}{2}$ and once $4 \nmid n$ we will have $n \not\equiv 0, 4, 7 \pmod 8$ by our assumption that $n \neq 4^a(8k + 7)$.

Now we turn to the case $p > 2$.

Lemma 3.4. *Assume $p > 2$ and $k \geq 1$. Then the congruence $x^2 + y^2 + z^2 \equiv n \pmod{p^k}$ is solvable for all $n \in \mathbb{Z}$.*

Proof. We take $z = 1$ if $p \mid n$ and $z = 0$ if $p \nmid n$. So it suffices to show that whenever $p \nmid c$ then the congruence $x^2 + y^2 \equiv c \pmod{p^k}$ has a solution (we take $c = n$ or $n - 1$). For the existence of solutions mod p note that the sets $\{c - y^2 \mid y \in \mathbb{F}_p\}$ (resp. $\{x^2 \mid x \in \mathbb{F}_p\}$) have cardinality $\frac{p+1}{2}$, so they cannot be disjoint as $\mathbb{F}_p$ has cardinality $p < \frac{p+1}{2} + \frac{p+1}{2}$. By the multivariate Hensel's Lemma (Thm. 2.4) the mod p solution can be lifted to mod p^k for all $k \geq 1$ since whenever $x_0^2 + y_0^2 \equiv c \not\equiv 0 \pmod p$, we have $(x_0, y_0) \not\equiv (0, 0) \pmod p$ so at least one of the partial derivatives of $x^2 + y^2 - c$ will not vanish mod p at the point (x_0, y_0). □

By Theorem 3.1 there exists a vector $(0, 0, 0, 0) \neq (x_0, y_0, z_0, u_0) \in \mathbb{Q}^4$ such that $x_0^2 + y_0^2 + z_0^2 = nu_0^2$. However, u_0 cannot be 0 as $x_0^2 + y_0^2 + z_0^2$ can only be 0 for $x_0 = y_0 = z_0 = 0$. So putting $x_1 = x_0/u_0$, $y_1 = y_0/u_0$, $z_1 = z_0/u_0$ we find $n = x_1^2 + y_1^2 + z_1^2$.

Step 2: We show that whenever we have rational solutions of $x^2 + y^2 + z^2 = n$, we also have integral solutions. For this we need the following Lemma in elementary geometry due to Cassels and Davenport.

Lemma 3.5. *Assume that we have a rational point $P_1 = (x_1, y_1, z_1) \in \mathbb{Q}^3$ in the Euclidean 3-space with $x_1^2 + y_1^2 + z_1^2 = n \in \mathbb{Z}$ such that the common denominator of (x_1, y_1, z_1) is $t_1 > 1$. Pick an integral vector $P_2 := (x_2, y_2, z_2) \in \mathbb{Z}^3$ by rounding x_1, y_1, z_1, ie. we have $|x_1 - x_2|_\infty, |y_1 - y_2|_\infty, |z_1 - z_2|_\infty \leq \frac{1}{2}$. Then the line connecting P_1 and P_2 intersects the sphere around the origin of radius $\sqrt{n}$ in another rational point $P_3 = (x_3, y_3, z_3) \in \mathbb{Q}^3$ such that $t_1\|P_1 - P_2\|^2(x_3, y_3, z_3) = t_1((x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2)(x_3, y_3, z_3)$ lies in $\mathbb{Z}^3$.*

Proof. Left to the reader. See Lemma B in the Appendix of Chapter I in [4] for a more general statement and proof. □

Note that $t_1\|P_1 - P_2\|^2 \leq t_1(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}) < t_1$ is an integer since we have

$$t_1\|P_1 - P_2\|^2 = t_1\langle P_1 - P_2, P_1 - P_2\rangle = t_1\|P_1\|^2 + t_1\|P_2\|^2 - 2t_1\langle P_1, P_2\rangle = t_1 n + t_1\|P_2\|^2 - 2\langle t_1 P_1, P_2\rangle$$

and $t_1 P_1, P_2 \in \mathbb{Z}^3$. Iterating the above Lemma we end up with an integral point on the sphere of radius $\sqrt{n}$ as desired. □

4. Hilbert symbol and its local properties

In order to uniformize notation we put $\mathbb{Q}_\infty := \mathbb{R}$ and denote by $P \subset \mathbb{N}$ the set of primes such that v (or ℓ) will often run on $P \cup \{\infty\}$. However, p will still denote a (finite) prime.

Definition. Let K be a field (of characteristic different from 2, but for the minicourse always of characteristic 0) and $a, b \in K^\times$. The Hilber symbol $(a, b)_K \in \{\pm 1\}$ is defined to be 1 if the quadratic form $z^2 - ax^2 - by^2$ has a nontrivial root in K and to be -1 otherwise. If the field K is understood from the context we often omit the subscript K. Further, in case $K = \mathbb{Q}_v$ ($v \in P \cup \{\infty\}$) we just put v in the subscript instead of $\mathbb{Q}_v$.

Note that $(a, b)_K = 1$ if and only if the quaternion algebra defined with constants a, b splits over K. We do not need this fact in the sequel, so do not worry if you do not know what a quaternion algebra is.

Proposition 4.1. *Let $a, b \in K^\times$. We have $(a, b) = 1$ if and only if a is a norm of an element in $K(\sqrt{b})$ if and only if b is a norm of an element in $K(\sqrt{a})$.*

Proof. If $b = c^2$ then $K(\sqrt{b}) = K$ whence any $a \in K^\times$ is a norm. Consequently, $x = 0, y = 1, z = c$ is a nontrivial root. Assume now that b is not a square. Then $x_0 = 0$ is not possible for a nontrivial solution $z_0^2 = ax_0^2 + by_1^2$. Therefore $a = (\frac{z_0}{x_0})^2 - b(\frac{y_0}{z_0})^2 = N(\frac{z_0}{x_0} + \sqrt{b}\frac{y_0}{z_0})$. The converse follows similarly. □

The Hilbert symbol has the following basic properties regardless of the field K:

Proposition 4.2. *For all $a, b, c \in K^\times$ we have*

(*i*) $(a, b) = (b, a)$, $(a, bc^2) = (a, b)$;
(*ii*) $(1, a) = (a, -a) = (a, 1 - a) = 1$;
(*iii*) $(a, bc) = (a, b)(a, c)$ *if* $(a, c) = 1$.

Proof. (*i*) and (*ii*) are obvious from the definition. For (*iii*) use Proposition 4.1 and note that the norm is multiplicative. □

So far K could have been an arbitrary field of characteristic different from 2. However, in case $K = \mathbb{Q}_v$ ($v \in P \cup \{\infty\}$) we can say more: the hilbert symbol $(a, b)_v$ is bilinear, ie. property (*iii*) holds without the assumption $(a, c)_v = 1$. In case $v = \infty$ one can see this directly: we have $(a, b)_\infty = -1$ if and only if both a and b are negative therefore we indeed have $(a, bc)_\infty = (a, b)_\infty (a, c)_\infty$. The case of finite primes is more involved, we need a couple of Lemmas.

Lemma 4.3. *Assume $p \neq 2$ and $a, b, c \in \mathbb{Z}_p^\times$. Then the equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial (primitive) solution in $\mathbb{Z}_p$ (hence in $\mathbb{Q}_p$). In particular, we have $(a, b)_p = 1$ if $a, b \in \mathbb{Z}_p^\times$.*

Proof. This is similar to Lemma 3.4, so we leave the details to the reader. We may take $z = 1$. □

Lemma 4.4. *Assume $p \neq 2$ and $u \in \mathbb{Z}_p$ is not a square mod p, ie. $\left(\frac{u}{p}\right) = -1$. Then we have $(u, p)_p = -1$.*

Proof. Assume we have $z^2 - ux^2 - py^2 = 0$ for some $x, y, z \in \mathbb{Q}_p$ not all 0. By rescaling we may assume $x, y, z \in \mathbb{Z}_p$ not all divisible by p. Looking at the equation mod p we find that p must divide x since $\left(\frac{u}{p}\right) = -1$. □

Theorem 4.5. *Assume $p \neq 2$ and put $a = p^\alpha s$, $b = p^\beta t$. Then we have the following formula for the Hilbert symbol at p:*

$$(a,b)_p = (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{s}{p}\right)^\beta \left(\frac{t}{p}\right)^\alpha .$$

In particular, $(\cdot,\cdot)_p \colon \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \to \{\pm 1\}$ is bilinear nondegenerate pairing.

Proof. By Proposition 4.2(i) and Corollary 2.8 we are reduced to a finite computation of Hilbert symbols (among $1, u, p, up$). The statement follows from Lemmas 4.3 and 4.4 by a computation using the properties in Proposition 4.2. □

Theorem 4.6. *Let $a = 2^\alpha s, b = 2^\beta t \in \mathbb{Q}_2$ with $s, t \in \mathbb{Z}_2^\times$. Then we have*

$$(a,b)_2 = (-1)^{\varepsilon(s)\varepsilon(t)+\alpha\omega(t)+\beta\omega(s)}$$

where $\varepsilon(s) \equiv \frac{s-1}{2} \pmod 2$ and $\omega(s) \equiv \frac{s^2-1}{8} \pmod 2$. In particular, $(\cdot,\cdot)_2 \colon \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \times \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \to \{\pm 1\}$ is bilinear and nondegenerate.

Proof. By Corollary 2.8 we only need to check the above identity when $a, b \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ which is a tedious, but finite computation that we omit. □

5. Global properties of the Hilbert symbol

The goal of this section is to formulate relations between $(a,b)_p$ for fixed nonzero rational numbers a, b and varying p. This is closely related to Gauss' quadratic reciprocity law. Further, for fixed $a \in \mathbb{Q}$ and signs $\varepsilon_v \in \{\pm 1\}$ for $v \in P \cup \{\infty\}$ we would like to give necessary and sufficient conditions on the existence of $b \in \mathbb{Q}$ with $(a,b)_v = \varepsilon_v$ for all $v \in P \cup \{\infty\}$. The latter involves the existence of primes in arithmetic progressions due to Dirichlet.

Let $p \neq q$ be odd primes. Then by Lemma 4.4 the Hilbert symbol $(p,q)_p$ is equal to 1 if and only $q$is a square mod p. In other words, we have the identity $(p,q)_p = \left(\frac{q}{p}\right)$. Moreover, by Theorem 4.6 we have $(p,q)_2 = (-1)^{\varepsilon(p)\varepsilon(q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. By the same argument we also have $(-1,p)_p = (-1)^{\frac{p-1}{2}} = (-1,p)_2$. Therefore Gauss' quadratic reciprocity law reads in this language

Theorem 5.1 (quadratic reciprocity law). *For odd primes $p \neq q$ we have*

$$(p,q)_q = \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right) = (p,q)_2(p,q)_p .$$

On the other hand, we have

$$(2,p)_p = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (2,p)_2 .$$

Putting all the above information we deduce

Theorem 5.2 (Hilbert's reciprocity law). *For all $a, b \in \mathbb{Q}^\times$ we have*

(i) $(a,b)_p = 1$ *for all but finitely many primes p;*
(ii) $\prod_{v \in P\cup\{\infty\}} (a,b)_v = 1.$

Proof. Whenever $a, b \in \{-1\} \cup P$, the statement follows from the formulae above for the Hilbert symbol and the quadratic reciprocity law. For general a, b we deduce the statement from the bilinearity of the local Hilbert symbols. □

Theorem 5.3. *Let I be a finite index set and $a_i \in \mathbb{Q}^\times$ a nonzero rational number for each $i \in I$. Assume further we are given signs $\varepsilon_{i,v} \in \{\pm 1\}$ for all $i \in I$ and $v \in P \cup \{\infty\}$. There is an $x \in \mathbb{Q}^\times$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in P \cup \{\infty\}$ if and only if the following three conditions are satisfied:*

(1) $\varepsilon_{i,v} = 1$ *for all but finitely many* $v \in P \cup \{\infty\}$.
(2) *We have* $\prod_{v \in P \cup \{\infty\}} \varepsilon_{i,v} = 1$ *for all* $i \in I$.
(3) *For all* $v \in P \cup \{\infty\}$ *there exists an element* $x_v \in \mathbb{Q}_v^\times$ *such that* $(a_i, x_v) = \varepsilon_{i,v}$ *for all* $i \in I$.

Proof. The necessity of conditions (1) and (2) follow from Hilbert's reciprocity law (Thm. 5.2). Further, if $x \in \mathbb{Q}^\times$ is a global solution then one can take $x_v = x$ in (3).

For the converse assume we are given $a_i \in \mathbb{Q}^\times$ and $\varepsilon_{i,v} \in \{\pm 1\}$ for all $i \in I$ and $v \in P \cup \{\infty\}$ satisfying (1), (2), and (3). We may assume without loss of generality that all a_i are squarefree integers since $(a_i c_i^2, b)_v = (a_i, b)_v$ for all $v \in P \cup \{\infty\}$ and $b, c_i \in \mathbb{Q}^\times$. Put

$$\begin{aligned} S &:= \{\infty, 2\} \cup \{p \in P \mid \exists i \in I \text{ s.t. } p \mid a_i\} \\ T &:= \{v \in P \cup \{\infty\} \mid \exists i \in I \text{ s.t. } \varepsilon_{i,v} = -1 \ . \end{aligned}$$

By our assumptions both S and T are finite subsets of $P \cup \{\infty\}$.

Case 1: $S \cap T = \emptyset$. In particular note that $\infty \notin T$ as $\infty \in S$. Put

$$a := \prod_{\ell \in T} \ell \qquad \text{and} \qquad m := 8 \prod_{p \in S \setminus \{2,\infty\}} p \ .$$

By our assumption $S \cap T = \emptyset$ the integers a and m are coprime, so we may use Dirichlet's theorem to find a prime $q \notin S \cup T$ such that $q \equiv a \pmod{m}$. We claim that $x := aq$ satisfies $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in P \cup \{\infty\}$. We check this case by case:

(1) $v \in S$. In this case we have $\varepsilon_{i,v} = 1$ by the assumption $S \cap T = \emptyset$. For $v = \infty$ we find $(a_i, aq)_\infty = 1$ since $aq > 0$. For $v = p \neq 2 \in S$ we note $q \equiv a \pmod{p}$ as $p \mid m$, so $x = aq \equiv a^2 \pmod{p}$, ie. $\left(\frac{x}{p}\right) = 1$ whence $(a_i, x)_p = 1$ by Theorem 4.5. Similarly, for $v = 2 \in S$ we have $x \equiv a^2 \equiv 1 \pmod{8}$ showing $(x, a_i)_2 = 1$ by Theorem 4.6.

(2) $v = \ell \in T$. So $\ell \notin S$, ie. $\ell \neq \infty, 2$ and $a_i \in \mathbb{Z}_\ell^\times$ for all $i \in I$. Therefore Theorem 4.5 reads in this case

$$(a_i, b)_\ell = \left(\frac{a_i}{\ell}\right)^{v_\ell(b)} \qquad \forall b \in \mathbb{Q}_\ell^\times \ .$$

By condition (3) there exists an $x_\ell \in \mathbb{Q}_\ell^\times$ such that $\left(\frac{a_i}{\ell}\right)^{v_\ell(x_\ell)} = (a_i, x_\ell)_\ell = \varepsilon_{i,\ell}$ for all $i \in I$. Moreover, $\ell \in T$ means there exists an index $i \in I$ with $\varepsilon i, \ell = -1$ showing $v_\ell(x_\ell)$ must be odd. On the other hand, we have $v_\ell(aq) = 1 (\equiv v_\ell(x_\ell) \pmod{2})$ as $q \notin T$ and $\ell \mid a$, but $\ell^2 \nmid a$ by construction. So we have

$$(a_i, x)_\ell = \left(\frac{a_i}{\ell}\right)^{v_\ell(x)} = \left(\frac{a_i}{\ell}\right)^{v_\ell(x_\ell)} = (a_i, x_\ell)_\ell = \varepsilon_{i,\ell}$$

for all $i \in I$ as desired.

(3) $\ell \notin S \cup T \cup \{q\}$. In this case we have $\varepsilon_{i,\ell} = 1$, $a_i \in \mathbb{Z}_\ell^\times$ for all $i \in I$ and $x = aq \in \mathbb{Z}_\ell^\times$, too, whence $(a_i, x)_\ell = 1$ by Lemma 4.3.

By the discussion above the only exception where possibly $(a_i, x)_\ell \neq \varepsilon_{i,\ell}$ is $\ell = q$ not treated by the above 3 cases. This is the point where Dirichlet's Theorem—that we could choose $q \equiv a \pmod m$ to be a prime—comes into force. Indeed, by Hilbert's reciprocity law (Thm. 5.2) and condition (2) the equality $(a_i, x)_\ell = \varepsilon_{i,\ell}$ must fail at an even number of places, so it cannot just be the single place $\ell = q$. This shows we have $(a_i, x)_q = \varepsilon_{i,q}$ proving the result in Case 1.

Case 2: This is the general case where we no longer assume $S \cap T = \emptyset$. By assumption (3) there exists an element $x_v \in \mathbb{Q}_v^\times$ for all $v \in S$ such that $(x_v, a_i)_v = \varepsilon_{i,v}$ for all $i \in I$. In order to proceed further we need the following approximation theorem.

Lemma 5.4. *Assume $S \subset P \cup \{\infty\}$ is a finite set. Then the diagonal embedding $\mathbb{Q} \hookrightarrow \prod_{v \in S} \mathbb{Q}_v$ has dense image where the right hand side is given the product topology of the topologies induced by the v-adic absolute values on $\mathbb{Q}_v$ ($v \in S$).*

Proof. We may increase S to have $\infty \in S$, so we may assume $S = \{\infty, p_1, \dots, p_n\}$. The density in the product topology means that for all $(x_\infty, x_1, \dots, x_n) \in \prod_{v \in S} \mathbb{Q}_v = \mathbb{R} \times \mathbb{Q}_{p_1} \times \dots \times \mathbb{Q}_{p_n}$, $\varepsilon > 0$ and $N \in \mathbb{Z}^{>0}$ there exists a rational number $x \in \mathbb{Q}$ such that $|x - x_\infty|_\infty \leq \varepsilon$ and $v_{p_i}(x - x_i) \geq N$ ($\Leftrightarrow |x - x_i|_{p_i} \leq p^{-N}$) ($i = 1, \dots, n$). Replacing $(x_\infty, x_1, \dots, x_n)$ by $((p_1 \dots p_n)^M x_\infty, (p_1 \dots p_n)^M x_1, \dots, (p_1 \dots p_n)^M x_n)$, ε by $\frac{\varepsilon}{(p_1 \cdots p_n)^M}$ and N by $N+M$ for some large enough M we may assume without loss of generality that x_i belongs to $\mathbb{Z}_{p_i}$ for all $i = 1, \dots, n$. By the Chinese Remainder Theorem there exists an integer $x_0 \in \mathbb{Z}$ such that $x_0 \equiv x_i \pmod{p_i^N}$ for all $i = 1, \dots, n$ as the prime powers p_i^N are pairwise coprime. Pick a prime q different from $p_1, \dots, p_n$ and choose $L > 0$ so that $\frac{(p_1 \cdots p_n)^N}{q^L} < \varepsilon$. Then for any integer $u \in \mathbb{Z}$ and $i = 1, \dots, n$ we have

$$|x_0 + \frac{u(p_1 \dots p_n)^N}{q^L} - x_i|_{p_i} \leq \max(|x_0 - x_i|_{p_i}, |\frac{u(p_1 \dots p_n)^N}{q^L}|_{p_i}) \leq p^{-N} .$$

On the other hand, we may choose $u \in \mathbb{Z}$ such that $|x_0 - x_\infty + \frac{u(p_1 \cdots p_n)^N}{q^L}|_\infty < \varepsilon$ so that $x := x_0 + \frac{u(p_1 \cdots p_n)^N}{q^L}$ satisfies all the required conditions. □

Note that the square elements $(\mathbb{Q}_v^\times)^2$ form an open subset of $\mathbb{Q}_v$: Indeed, in case $v = \infty$ this is obvious as all positive numbers are squares in $\mathbb{R}$. In case $v = p \neq 2$ is a prime this follows from Proposition 2.6 and in case $v = 2$ from Proposition 2.7. So we may apply Lemma 5.4 to find an element $x' \in \mathbb{Q}^\times$ such that $\frac{x'}{x_v}$ is a nonzero square in $\mathbb{Q}_v$ for all $v \in S$. In particular, we deduce $(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in S$. Put $\eta_{i,\ell} := \varepsilon_{i,\ell}(a_i, x')_\ell$ for $\ell \in P \cup \{\infty\}$. The new bunch of signs $(\eta_{i,\ell})_{i \in I, \ell \in P \cup \{\infty\}}$ satisfies (1), (2), (3) by Theorem 5.2 (applied to $(a_i, x')_\ell$) since so does $(\varepsilon_{i,\ell})_{i \in I, \ell \in P \cup \{\infty\}}$. Further, we have $\eta_{i,v} = 1$ for all $v \in S$ by construction. Therefore we may apply Case 1 to find an element $y \in \mathbb{Q}^\times$ satisfying $(a_i, y)_\ell = \eta_{i,\ell}$ for all $i \in I$ and $\ell \in P \cup \{\infty\}$. By the bilinearity of the Hilbert symbol $x := x'y$ satisfies $(a_i, x)_\ell = \varepsilon_{i,\ell}$ for all $i \in I$ and $\ell \in P \cup \{\infty\}$ deducing the theorem in the general case. □

6. Proof of the Hasse–Minkowski Theorem

In order to prove the main theorem in this minicourse we need to recall some generalities on quadratic forms (valid over any field K of characteristic different from 2). Let $f(x_1,\dots,x_n) = \sum_{1\le i\le j\le n} a_{i,j}x_ix_j \in K[x_1,\dots,x_n]$ be a quadratic form, ie. a homogeneous polynomial of degree 2. To f we associate the symmetric matrix $A_f := \begin{pmatrix} a_{1,1} & & & \\ & \ddots & \frac{a_{i,j}}{2} & \\ & \frac{a_{i,j}}{2} & \ddots & \\ & & & a_{n,n}\end{pmatrix}$ so that we have $f(x_1,\dots,x_n) = \begin{pmatrix} x_1 & \cdots & x_n\end{pmatrix} A_f \begin{pmatrix} x_1 \\ \vdots \\ x_n\end{pmatrix}$. We put $\beta_f\colon K^n\times K^n \to K$ for the associated symmetric bilinear form given by the formula $\beta_f(u,w) = u^TA_fw$.

Definition. We call the form β *nondegenerate* if for all $0\neq w\in K^n$ there is a $u\in K^n$ such that $\beta(u,w)\neq 0$. We call a quadratic form f nondegenerate if the associated symmetric bilinear form β_f is nondegenerate.

By quotienting out by the radical $\operatorname{rad}\beta = \{w\in K^n \mid \beta(u,w)=0\ \forall u\in K^n\}$ (or equivalently reducing the number of variables after a suitable change of basis) we may assume from now on that β is nondegenerate.

Definition. We call the symmetric bilinear form β *isotropic* if there exists a nonzero vector $0\neq w\in K^n$ with $\beta(w,w)=0$.

Recall that in this language Theorem 3.1 states that a symmetric bilinear form β over $\mathbb{Q}$ is isotropic over $\mathbb{Q}$ if and only if β is isotropic over $\mathbb{Q}_v$ for all $v\in P\cup\{\infty\}$.

Lemma 6.1. *Assume β is isotropic and nondegenerate. Then for all $a\in K$ there is a vector $w\in K^n$ such that $\beta(w,w)=a$ (we say that a is* represented *by the quadratic form $\beta(u,u)$).*

Proof. Since β is isotropic, there is a vector $u\neq 0\in K^n$ with $\beta(u,u)=0$. On the other hand, β is nondegenerate, so there is a $y\in K^n$ such that $\beta(u,y)\neq 0$. We look for w in the form $w=cu+y$ ($c\in K$ given later). We compute

$$\beta(cu+y,cu+y) = c^2\beta(u,u)+2c\beta(u,y)+\beta(y,y)\ .$$

Therefore $c := \frac{a-\beta(y,y)}{2\beta(u,y)}$ will do as $\operatorname{char} K\neq 2$. □

Proposition 6.2. *Let $f(x_1,\dots,x_n)$ be a nondegenerate quadratic form over K with* $\operatorname{char}K\neq 2$. *Then f represents $a\in K$ if and only if the form $f(x_1,\dots,x_n)-ax_0^2$ (in $n+1$ variables, x_0 being a new variable) is isotropic.*

Proof. Note that $a=0$ is always represented and $f(x_1,\dots,x_n)-0x_0^2$ is indeed isotropic by the choice $x_0=1$, $x_1=\cdots=x_n=0$. Now assume $a\neq 0$. If f is isotropic then by Lemma 6.1 f represents a and in this case $f-ax_0^2$ is also isotropic. So assume f is not isotropic, but $f-ax_0^2$

is. Then there are elements $\alpha_0, \alpha_1, \dots, \alpha_n \in K$, not all zero, such that $f(\alpha_1, \dots, \alpha_n) - a\alpha_0^2 = 0$. Since f is not isotropic, we must have $\alpha_0 \neq 0$ whence $a = f(\frac{\alpha_1}{\alpha_0}, \dots, \frac{\alpha_n}{\alpha_0})$ is represented by f. □

With all this preparation at hand, we can now start the

Proof of Theorem 3.1. Pick a quadratic form f over $\mathbb{Q}$. By the Gram–Schmidt orthogonalization we may assume f is in diagonal form $f = a_1x_1^2 + \dots + a_nx_n^2$ $(a_1 \dots a_n \neq 0)$. Further, by rescaling the variables and multiplying by a constant we may, as well, assume that a_i are square-free integers $(i = 1, \dots, n)$ and $a_1 = 1$. We shall proceed by induction on n, but we need to distinguish all $n \leq 4$. The case $n = 1$ is trivial: in this f cannot be isotropic locally either.

(1) $n = 2$. Then $f = x_1^2 - ax_2^2$ where $a > 0$ since f is isotropic over $\mathbb{R}$. Further, a is a square in $\mathbb{Q}_p$ therefore $v_p(a)$ is even for all primes p. So a is a square in $\mathbb{Q}$ since all primes are on even exponent in the prime decomposition.

(2) $n = 3$, $f = x_1 - ax_2^2 - bx_3^2$ with $a, b \in \mathbb{Z}$ squarefree. We also assume $|a| \leq |b|$ by symmetry. We proceed by induction on $m := |a| + |b|$. The case $m = 2$ is obvious since the form $x_1^2 \pm x_2^2 \pm x_3^2$ has a nontrivial rational root unless both signs are + in which case the form is not isotropic over $\mathbb{R}$, either. So let $m > 2$ whence $|b| \geq 2$. Write $b = \pm p_1 \dots p_k$ in prime decomposition. Since the form $x_1^2 - ax_2^2 - bx_3^2$ is isotropic over $\mathbb{Q}_v$, we have $(a, b)_v = 1$ for all $v \in P \cup \{\infty\}$ by the definition of the Hilbert symbol. So by Theorem 4.5 we have $p_i \mid a$ or $\left(\frac{a}{p_i}\right) = 1$ $(i = 1, \dots, k)$ as we have $v_{p_i}(b) = 1$. Either way the congruence $x^2 \equiv a \pmod{p_i}$ has a solution for all $i = 1, \dots, n$. Hence by the Chinese Remainder Theorem a is a square modulo b, too. In particular there exists an integer t with $|t| \leq \frac{|b|}{2}$ such that $t^2 \equiv a \pmod{b}$, ie. $t^2 = a + bb'$ with $|b'| < |b|$. This equation reads $t^2 - a \cdot 1^2 - bb' \cdot 1^2 = 0$ meaning $(a, bb')_v = 1$ for all $v \in P \cup \{\infty\}$. So by the multiplicativity of the local Hilbert symbols we deduce $(a, b')_v = (a, b^2b')_v = (a, b)_v(a, bb')_v = 1$ for all $v \in P \cup \{\infty\}$. Since $|a| + |b'| < |a| + |b|$, using the induction we deduce that the form $x_1^2 - ax_2^2 - b'x_3^2$ is isotropic over $\mathbb{Q}$. In particular, both b' and bb' are norms of elements of $\mathbb{Q}(\sqrt{a})$ by Proposition 4.1. Therefore their quotient b is also a norm from $\mathbb{Q}(\sqrt{a}$ whence $x_1^2 - ax_2^2 - bx_3^2$ is also isotropic over $\mathbb{Q}$ (using Proposition 4.1 again in the reverse direction).

(3) $n = 4$, $f = (ax_1^2 + bx_2^2) - (cx_3^2 + dx_4^2)$. We need a common value of the binary forms $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$.

Lemma 6.3. *For all $v \in P \cup \{\infty\}$ there exists $0 \neq x_v \in \mathbb{Q}_v$ such that x_v is represented by both forms $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$.*

Proof. There is a common value nontrivially as f is isotropic over $\mathbb{Q}_v$. Now if this common value is 0 then at least one of the two binary forms is isotropic over $\mathbb{Q}_v$ (as it represents 0 nontrivially). By Lemma 6.1 isotropic forms represent any element in $\mathbb{Q}_v$ so we just need to pick a nonzero value of the other form which certainly exists. □

So we pick these elements $x_v \in \mathbb{Q}_v$ for all $v \in P \cup \{\infty\}$. By Proposition 6.2 both forms

$$x_vz^2 - ax_1^2 - bx_2^2 \qquad \text{and} \qquad x_vz^2 - cx_3^2 - dx_4^2$$

are isotropic over $\mathbb{Q}_v$. So we compute

$$1 = \left(\frac{a}{x_v}, \frac{b}{x_v}\right)_v = (ax_v, bx_v)_v = (ax_v, -abx_v^2)_v =$$
$$= (ax_v, -ab)_v = (a, -ab)_v (x_v, -ab)_v = (a, b)_v (x_v, -ab)_v$$

which implies $(x_v, -ab)_v = (a, b)_v$ and by a similar computation $(x_v, -cd)_v = (c, d)_v$ for all $v \in P \cup \{\infty\}$. By Theorem 5.2 we have $\prod_{v \in P\cup\{\infty\}}(a, b)_v = 1 = \prod_{v\in P\cup\{\infty\}}(c, d)_v$ whence we have $\prod_{v\in P\cup\{\infty\}}(x_v, -ab)_v = 1 = \prod_{v\in P\cup\{\infty\}}(x_v, -cd)_v$. Further, $(a, b)_v = -1$ or $(c, d)_v = -1$ for only finitely many places v. Therefore we may apply Theorem 5.3 with $a_1 = -ab$, $a_2 = -cd$, $\varepsilon_{1,v} = (x_v, -ab)_v = (a, b)_v$, $\varepsilon_{2,v} = (x_v, -cd)_v = (c, d)_v$ since condition (3) is also satisfied by the given $x_v \in \mathbb{Q}_v^\times$ ($v \in P \cup \{\infty\}$). So we find an element $x \in \mathbb{Q}^\times$ such that $(x, -ab)_v = (a, b)_v$ and $(x, -cd)_v = (c, d)_v$ for all $v \in P \cup \{\infty\}$. By the same computation as above (x_v replaced by x), we deduce $\left(\frac{a}{x}, \frac{b}{x}\right)_v = 1 = \left(\frac{c}{x}, \frac{d}{x}\right)_v$ for all $v \in P \cup \{\infty\}$. Hence the quadratic forms $ax_1^2 + bx_2^2 - xz^2$ and $cx_3^2 + dx_4^2 - xz^2$ are both isotropic locally everywhere which implies by the case $n = 3$ already proven above that they are also isotropic over $\mathbb{Q}$. By Proposition 6.2 both binary forms $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$ represent $x \neq 0$ showing f is isotropic over $\mathbb{Q}$.

Finally assume $n \geq 5$. In this case we do induction on n. Pick a form

$$f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + \cdots + a_nx_n^2 = h - g$$

where we put $h = a_1x_1^2 + a_2x_2^2$ and $g = -(a_3x_3^2 + \cdots + a_nx_n^2)$ and assume $a_1, \ldots, a_n \in \mathbb{Z}$ are squarefree. As above we look for common values of g and h. Put

$$S := \{\infty, 2\} \cup \{p \in P \mid \exists i \geq 3\colon p \mid a_i\} ,$$

this is a finite set. As in Lemma 6.3, for all $v \in S$ there exists an element $0 \neq a_v \in \mathbb{Q}_v$ such that a_v is represented by both forms g and h, ie. we have $x_1^v, x_2^v, x_3^v, \ldots, x_n^v \in \mathbb{Q}_v$ such that

$$h(x_1^v, x_2^v) = a_v = g(x_3^v, \ldots, x_n^v) .$$

Since $a_v(\mathbb{Q}_v^\times)^2$ is open in $\mathbb{Q}_v$ and $h\colon \mathbb{Q}_v \times \mathbb{Q}_v \to \mathbb{Q}_v$ is continuous (in the v-adic topology), there exist open neighbourhoods $x_1^v \in U_1^v \subset \mathbb{Q}_v$ and $x_2^v \in U_2^v \subset \mathbb{Q}_v$ such that the image of h on $U_1^v \times U_2^v$ is contained in $a_v(\mathbb{Q}_v^\times)^2$. By Lemma 5.4 (applied twice) there exist $x_1, x_2 \in \mathbb{Q}$ such that $x_j \in U_j^v$ for all $v \in S$ and $j = 1, 2$. We put $a := h(x_1, x_2) \neq 0$ and claim that a is a common value of g and h over $\mathbb{Q}$. By construction a is represented by h over $\mathbb{Q}$ so by Proposition 6.2 we are reduced to showing that the $n - 1$-variable form

$$f_1 = az^2 - g(x_3, \ldots, x_n)$$

is isotropic over $\mathbb{Q}$. By induction, we only need to check that f_1 is isotropic locally everywhere. If v lies in S then $\frac{a}{a_v}$ is a square in $a = h(x_1, x_2) \in h(U_1^v, U_2^v) \subseteq a_v(\mathbb{Q}_v^\times)^2$, ie. there exists $u_v \in \mathbb{Q}_v^\times$ such that $a = a_vu_v^2 = g(x_3^v, \ldots, x_n^v)u_v^2 = g(x_3^vu_v, \ldots, x_n^vu_v)$ is represented by g locally at v. On the other hand if $v \in (P \cup \{\infty\}) \setminus S$ then $a_3, \ldots, a_n$ are v-adic units (ie. lie in $\mathbb{Z}_v^\times$) whence g is isotropic locally at v by Lemma 4.3 and represents a by Lemma 6.1. □

Corollary 6.4. *Let a be in $\mathbb{Q}^\times$ and f be a quadratic form over $\mathbb{Q}$. Then f represents a over $\mathbb{Q}$ if and only if it represents a over $\mathbb{Q}_v$ for all $v \in P \cup \{\infty\}$.*

Proof. We apply Theorem 3.1 on the form $az^2 - f$ and deduce the statement from Proposition 6.2. □

Remark. Assume $n \geq 5$ and p is a prime. Then all nondegenerate forms in n variables are isotropic over $\mathbb{Q}_p$. In particular, if f is a nondegenerate quadratic form over $\mathbb{Q}$ in $n \geq 5$ variables then f is isotropic over $\mathbb{Q}$ if and only if it is isotropic over $\mathbb{R}$ (ie. it is indefinite).

Proof. It suffices to treat the case $n = 5$ so let $f = a_1x_1^2 + \cdots + a_5x_5^2$. By rescaling the variables we may assume $a_1, \ldots, a_5$ are all in $\mathbb{Z}_p$ but not divisible by p^2. Further, there are either at least 3 indices $1 \leq i \leq 5$ with $v_p(a_i) = 0$ or at least 3 indices with $v_p(a_i) = 1$. Note that f is isotropic if and only if so is pf, so we may even assume that there are at least 3 indices i with $v_p(a_i) = 0$. In case $p \neq 2$ the remark follows from Lemma 4.3. In case $p = 2$ one checks by a direct computation that all elements mod 8 are represented by any 4-variable form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ where a_1, a_2, a_3 are all odd. Finally one applies Proposition 2.7. □

References

[1] John William Scott Cassels. *Lectures on Elliptic Curves.* Number 24. Cambridge University Press, 1991.

[2] Keith Conrad. Selmer's example. *https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf*, 2017.

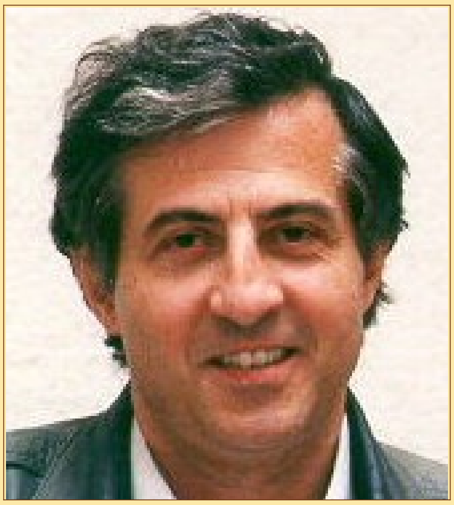
[3] F. Q. Gouvêa. *p-adic Numbers, An Introduction.* Springer, Heidelberg, 1997.

[4] J.-P. Serre. *A course in arithmetic.* Springer, New York, 1993.

Róbert Freud

Gyula Károlyi

Péter Maga



János Pintz

Árpád Tóth

Gergely Zábrádi

SUMMER SCHOOL IN MATHEMATICS

EÖTVÖS LORÁND UNIVERSITY

BUDAPEST, HUNGARY

27. June − 1. July 2022

Topics in Number Theory: Ancient Problems, Recent Results

Budapest, July 2022