Algebraic Methods in Number Theory and Combinatorics (lecture notes of 2021)

MARTIN KLAZAR

Preface

The name of this course, which I am teaching in the Computer Science Section of the Faculty of Mathematics and Physics of Charles University in Prague for many years, is for technical reasons *Algebraic Number Theory*, in Czech *Algebraická teorie čísel* (NDMI066). Years ago, for example in the summer term of 2005/6 or in the winter term of 2007/8, I indeed lectured on the classical algebraic number theory, which is mostly concerned with arithmetic questions in the framework of number fields. Recall that a *number field* K is any field extension $K \supset \mathbb{Q}$ such that the vector space K over $\mathbb{Q}$ has finite dimension. Then I was following the nice book *Number Fields* [15] by D. Marcus. Topics I have been lecturing on in the course more recently are better captured by the above umbrella title of the lecture notes. If it is not said else, results presented are not original. I always try to give proper attributions, if I remember them, and apologize for possible omissions.

January 2022, Prague M. Klazar

Contents

Chapter 1

Lecture 1. *abc* conjectures: in $\mathbb{Z}$ and in $\mathbb{C}[t]$

We begin the course with a conjecture.

The *abc* conjecture

The most important open problem in number theory today is the so called *abc conjecture*. To state it we define for any nonzero integer n its *radical* $r(n)$ as

$$r(n) := \prod_{p,\, p \,|\, n} p \,.$$

It is the product of all prime factors p of n, i.e., of all prime numbers p dividing n. We set $r(\pm 1) := 1$. It is clear that for any $a, b \in \mathbb{Z} \setminus \{0\}$ and any $k \in \mathbb{N} := \{1, 2, \dots\}$,

$$r(ab^k) = r(ab) \,.$$

Also, always $r(a) \le |a|$. Numbers $a_1, a_2, \dots, a_k \in \mathbb{Z}$ are *coprime* if the maximum $d \in \mathbb{Z}$ dividing them all is $d = 1$. They are *pairwise coprime* if each pair a_i, a_j for $1 \le i < j \le k$ is coprime.

Conjecture 1.1 (*abc* conjecture).

$$\forall\, \varepsilon > 0\ \exists\, M = M(\varepsilon) > 0 :\ a, b, c \in \mathbb{N} \text{ pairwise coprime and } a + b = c \Rightarrow$$
$$\Rightarrow\ c < M \cdot r(abc)^{1+\varepsilon} \,.$$

Nothing changes if one replaces "pairwise coprime" with "coprime", and/or $\mathbb{N}$ with $\mathbb{Z} \setminus \{0\}$ and the last bound with

$$\max(|a|,\, |b|,\, |c|) < M \cdot r(abc)^{1+\varepsilon} \,.$$

The *abc* conjecture is not very old: it was proposed by the British mathematician D. Masser [17] in 1985, and independently by the French mathematician J. Oesterlé [23] in 1988. In August 2012, the Japanese mathematician

S. Mochizuki posted on the arXiv preprint server `https://arxiv.org/` several long articles which, as he claimed and claims, prove the *abc* conjecture. In 2021 he supported this claim by turning his preprints in the publications [18, 19, 20, 21]. Currently the majority consensus of the mathematical community, with the exception of several people, is that these articles still do not prove the *abc* conjecture. This is somewhat embarrassing, both for mathematics and for mathematicians.

The *abc* conjecture posits that if $a, b, c \in \mathbb{N}$ are coprime and $a + b = c$, then the prime factorizations of a, b and c cannot involve high powers. For example, we show below that the *abc* conjecture implies that each equation $x^n + y^n = z^n$, $n \in \mathbb{N}$ with $n \geq 4$, has in $\mathbb{N}$ only finitely many coprime solutions. This is a weaker form of the famous FLT, *Fermat's Last Theorem*, that $x^n + y^n = z^n$ has in fact no solution $x, y, z, n \in \mathbb{N}$ with $n \geq 3$, which was proved by A. Wiles and R. Taylor in [28, 27] in 1995. But one does not have to restrict to equal exponents:

Proposition 1.2 (weak generalized FLT in $\mathbb{Z}$). *If the abc conjecture holds then for any triple of numbers $k, l, m \in \mathbb{N}$ with $1/k+1/l+1/m < 1$ the equation*

$$x^k + y^l = z^m$$

has only finitely many coprime solutions $x, y, z \in \mathbb{N}$.

Proof. Suppose that k, l and m are as stated. We fix sufficiently small $\varepsilon > 0$ such that still

$$d := (1 + \varepsilon) \cdot (1/k + 1/l + 1/m) < 1 \, .$$

By the *abc* conjecture there is a constant $M > 0$ such that for any coprime numbers $a, b, c \in \mathbb{N}$ with $a^k + b^l = c^m$ one has the following three bounds (logarithmic forms of the bound in the *abc* conjecture):

$$k \log a, \, l \log b, \, m \log c < (1 + \varepsilon) \log(r(abc)) + \log M \leq (1 + \varepsilon) S + \log M \, ,$$

where $S := \log a + \log b + \log c$. Dividing by k, l and m and adding the three resulting bounds we get that

$$S < (1 + \varepsilon) \cdot (1/k + 1/l + 1/m) \cdot S + (1/k + 1/l + 1/m) \log M \, .$$

So $S < d \cdot S + \log M$. Since $d \in (0, 1)$, this inequality becomes impossible once any of a, b and c is large enough. Thus the above equation has only finitely many coprime solutions in $\mathbb{N}$. □

In a similar way one can easily deduce by the *abc* conjecture the Darmon–Granville theorem [4] that if $A, B, C \in \mathbb{Z} \setminus \{0\}$ and $k, l, m \in \mathbb{N}$ are such that $1/k + 1/l + 1/m < 1$ then the equation

$$Ax^k + By^l = Cz^m$$

has only finitely many coprime solutions in $\mathbb{Z} \setminus \{0\}$. Their theorem is proven also in [3, Chapter 12.6], and the proof uses the difficult theorem of G. Faltings [6, 7] on finiteness of rational points on curves with genus at least 2.

Proposition 1.3 (weak FLT in $\mathbb{Z}$). *If the abc conjecture holds then for any integer $n \geq 4$ the equation*

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

has only finitely many coprime solutions $x, y, z \in \mathbb{N}$.

Proof. Just set $k = l = m := n$ in the previous proposition. □

These are obvious applications of the *abc* conjecture. A non-obvious application is mentioned in the fascinating book [3] *Heights in Diophantine Geometry* by E. Bombieri and W. Gubler. Chapter 12 is devoted to the *abc* conjecture and explains besides other results a derivation from the *abc* conjecture of *Roth's theorem on Diophantine approximation* [25]. Recall that this theorem says that for any real irrational algebraic number α and any $\varepsilon > 0$ there is a constant $c = c(\alpha, \varepsilon) > 0$ such that $|\alpha - p/q| > c/q^{2+\varepsilon}$ holds for any fraction p/q with $q > 0$.

We show that in the *abc* conjecture one cannot take M to be a fixed constant, for $\varepsilon \to 0$ the required $M = M(\varepsilon)$ has to go to $+\infty$. In particular, also the ε cannot be omitted.

Proposition 1.4 (on ε and M). *No matter how large $M > 0$ is, there exist a small $\varepsilon > 0$ and coprime numbers $a, b, c \in \mathbb{N}$ such that*

$$a + b = c \quad \textit{and} \quad c > M \cdot r(abc)^{1+\varepsilon} \ .$$

Proof. For any $n \in \mathbb{N}$ we define the numbers $x_n, y_n \in \mathbb{N}$ by the equation

$$x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n \ .$$

So $(x_1, y_1) = (3, 2)$, $(x_2, y_2) = (17, 12)$, $(x_3, y_3) = (99, 70)$ and so on. It follows that also

$$x_n - y_n\sqrt{2} = (3 - 2\sqrt{2})^n \ .$$

Thus

$$x_n^2 - 2y_n^2 = (x_n + y_n\sqrt{2})(x_n - y_n\sqrt{2}) = \left(3^2 - 2 \cdot 2^2\right)^n = 1$$

— x_n, y_n are solutions of the Pell equation $x^2 - 2y^2 = 1$. In fact, the list of all integral solutions of this equation is

$$\{(\pm 1,\, 0)\} \cup \{(\pm x_n,\, \pm y_n) \mid n \in \mathbb{N}\} \ ,$$

but we do not need this fact. We use that for every even $n = 2m$,

$$x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^{2m} = (x_m + y_m\sqrt{2})^2 = x_m^2 + 2y_m^2 + 2x_m y_m\sqrt{2} \ .$$

Thus $y_n = 2x_m y_m$. It follows that if $n = 2^m$ then 2^{m+1} divides y_n. We set

$$n := 2^m \text{ for } m = 1, 2, \ldots, \ a := 1, \ b := 2y_n^2 \text{ and } c := x_n^2 \ .$$

Then a, b and c are coprime natural numbers and $a+b=c$. For any $\varepsilon>0$ and any $m\in\mathbb{N}$ we have, since y_n is a multiple of 2^{m+1} and $r(uv^k)=r(uv)$, that

$$\frac{c}{r(abc)^{1+\varepsilon}}=\frac{x_n^2}{r(x_ny_n/2^m)^{1+\varepsilon}}\geq\frac{x_n^2\cdot 2^{(1+\varepsilon)m}}{(x_ny_n)^{1+\varepsilon}}>\frac{2^m}{x_n^{2\varepsilon}}\,,$$

where the first inequality follows from $r(u)\leq|u|$, and the next one from $y_n<x_n$ and $2^{\varepsilon m}>1$. Let an $M>0$ be given. We take an $m\in\mathbb{N}$ so large that $2^m>M$, and then an $\varepsilon>0$ so small that still $2^m/x_n^{2\varepsilon}>M$. Then ε and the numbers $a=1$, $b=2y_n^2$ and $c=x_n^2$ corresponding to the $n=2^m$ enjoy the stated properties. □

The previous proof is taken from the book [5, pp. 169–170] *Analytic Number Theory* by J.-M. De Koninck and F. Luca. Chapter 11 of it is devoted to the *abc* conjecture and its corollaries.

The Stothers–Mason theorem

In the second half of the lecture I discuss — and prove in Theorem 1.6 — a form of the *abc* conjecture for the ring $\mathbb{C}[t]$ of univariate polynomials with complex coefficients. In $\mathbb{C}[t]$ the situation is much nicer than in $\mathbb{Z}$: one does not need the constants M and ε and the polynomial *abc* conjecture has a simple and surprising proof. The *radical* $r(a)=r(a(t))$ of a nonzero polynomial $a\in\mathbb{C}[t]$ is now defined as

$$r(a):=|\{\alpha\in\mathbb{C}\mid a(\alpha)=0\}|\,,$$

which is the number of distinct roots of $a(t)$. Analogues to the above properties of integral radicals hold: for any nonzero $a,b\in\mathbb{C}[t]$ and any $k\in\mathbb{N}$,

$$r(ab^k)=r(ab)\ \text{ and }\ r(a)\leq\deg a\,.$$

The crucial tool available in $\mathbb{C}[t]$ but lacking in $\mathbb{Z}$ is *formal differentiation*. For $a=a(t)=\sum_{i=0}^n a_it^i\in\mathbb{C}[t]$ we set

$$a'=a(t)'=\frac{d\,a(t)}{d\,t}:=\sum_{i=0}^n ia_it^{i-1}=\sum_{i=1}^n ia_it^{i-1}=na_nt^{n-1}+\cdots+2a_2t+a_1\,.$$

Obviously, $a'=0$ iff a is a constant polynomial. One easily verifies two properties of this unary operation on $\mathbb{C}[t]$: the linearity

$$\forall\,\alpha,\,\beta\in\mathbb{C}\,\forall\,a,\,b\in\mathbb{C}[t]:\ (\alpha a+\beta b)'=\alpha a'+\beta b'$$

and the *Leibniz identity*

$$\forall\,a,\,b\in\mathbb{C}[t]:\ (ab)'=a'b+ab'\,.$$

But we need to work in a wider domain, in the field of fractions of the ring $\mathbb{C}[t]$. It is the field

$$\mathbb{C}(t)=\{a/b\mid a,\,b\in\mathbb{C}[t],\,b\neq0\}$$

of so called *(complex) rational functions*. We extend formal differentiation to $\mathbb{C}(t)$ by the formula

$$\left(\frac{a}{b}\right)' := \frac{a'b - ab'}{b^2} \ .$$

It is not hard to check that this is a correct definition (if $a/b = c/d$ then $(a/b)' = (c/d)'$), that it is indeed an extension of the formal differentiation in $\mathbb{C}[t]$, that the extension preserves the field of constants $\mathbb{C}$ (the elements with zero derivative), and that the linearity and the Leibniz identity still hold.

Proposition 1.5 (logdif identity). *If $a_1, \ldots, a_k \in \mathbb{C}(t)$ are non-zero rational functions and $a := a_1 a_2 \ldots a_k$, then*

$$\frac{a'}{a} = \sum_{i=1}^{k} \frac{a_i'}{a_i} \ .$$

Proof. We expand $(a_1 a_2 \ldots a_k)'$ by iterating the Leibniz identity and get that

$$\frac{a'}{a} = \frac{\sum_{i=1}^{k} a_1 \ldots a_{i-1} a_i' a_{i+1} \ldots a_k}{a_1 a_2 \ldots a_k} = \sum_{i=1}^{k} \frac{a_i'}{a_i} \ .$$

□

For nonzero $a \in \mathbb{C}(t)$ we call the fraction a'/a the *logarithmic derivative* of a. This term is motivated by the calculus formula $(\log(a(t)))' = a(t)'/a(t)$. We apply the logdif identity to factorization of any nonzero rational function in linear factors: if

$$0 \neq \frac{a}{b} = \frac{a(t)}{b(t)} = \alpha \prod_{i=1}^{k} (t - \alpha_i)^{m_i} \ ,$$

where $\alpha \in \mathbb{C}^\times := \mathbb{C} \setminus \{0\}$, $k \in \mathbb{N}_0 := \{0, 1, \ldots\}$, $\alpha_i \in \mathbb{C}$ are mutually distinct numbers and $m_i \in \mathbb{Z} \setminus \{0\}$, then one quickly computes by the logdif identity that

$$\frac{(a/b)'}{(a/b)} = \sum_{i=1}^{k} \frac{m_i}{t - \alpha_i} \ , \qquad (*)$$

where for $k = 0$ the above product is defined as 1, and the above sum as 0.

Now we state and prove the polynomial *abc* conjecture/theorem. Recall that some polynomials in $\mathbb{C}[t]$ are *coprime* if they have no common (complex) root. The theorem is due independently to W. W. Stothers [26] in 1981 and R. C. Mason [16] in 1984.

Theorem 1.6 (Stothers–Mason). *If $a(t), b(t), c(t) \in \mathbb{C}[t]$ are (pairwise) coprime nonzero polynomials that are not all constant, then*

$$a + b = c \Rightarrow \max(\deg a, \deg b, \deg c) \leq r(abc) - 1 \ .$$

Proof. Let a, b and c be as stated. We compute:

$$a+b=c \rightsquigarrow \frac{a}{c}+\frac{b}{c}=1 \rightsquigarrow (a/c)'+(b/c)'=0 \rightsquigarrow \frac{a}{b}=-\frac{(b/c)'/(b/c)}{(a/c)'/(a/c)}\ . \qquad (\rightsquigarrow)$$

Suppose that the factorizations of a, b and c in linear factors are

$$a(t)=\alpha\prod_{i=1}^{k}(t-\alpha_i)^{r_i},\ b(t)=\beta\prod_{i=1}^{l}(t-\beta_i)^{s_i}\ \text{ and }\ c(t)=\gamma\prod_{i=1}^{m}(t-\gamma_i)^{t_i}\ ,$$

where $\alpha,\beta,\gamma\in\mathbb{C}^\times$, $k,l,m\in\mathbb{N}_0$, $\alpha_i,\beta_i,\gamma_i\in\mathbb{C}$ (by the assumption on a, b and c, the numbers α_i, β_i and γ_i are mutually distinct) and $r_i,s_i,t_i\in\mathbb{N}$. Substituting the sums of equation $(*)$ in the right-hand side of the last equation in $(\rightsquigarrow)$ we get that

$$\frac{a(t)}{b(t)}=-\frac{\sum_{i=1}^{l}s_i/(t-\beta_i)-\sum_{i=1}^{m}t_i/(t-\gamma_i)}{\sum_{i=1}^{k}r_i/(t-\alpha_i)-\sum_{i=1}^{m}t_i/(t-\gamma_i)}=:-\frac{P(t)}{Q(t)}=\frac{-d(t)P(t)}{d(t)Q(t)}\ ,$$

where $d(t):=\prod_{i=1}^{k}(t-\alpha_i)\cdot\prod_{i=1}^{l}(t-\beta_i)\cdot\prod_{i=1}^{m}(t-\gamma_i)$. Clearly, $-dP, dQ\in\mathbb{C}[t]$. Since the polynomials a and b are coprime, $a(t)/b(t)$ is in lowest terms and

$$\deg a\le\deg(-dP)\le r(abc)-1\ \text{ and }\ \deg b\le\deg(dQ)\le r(abc)-1\ .$$

From $c=a+b$ we get that also $\deg c\le r(abc)-1$. □

We have the following corollaries.

Proposition 1.7 (generalized FLT for polynomials). *If $k,l,m\in\mathbb{N}$ are numbers and $a,b,c\in\mathbb{C}[t]$ are (pairwise) coprime nonzero polynomials that are not all constant, then*

$$a^k+b^l=c^m \Rightarrow \frac{1}{k}+\frac{1}{l}+\frac{1}{m}>1\ .$$

Proof. Suppose that a, b and c are as stated and satisfy the hypothesis of the implication. By the previous theorem we then get three bounds

$$k\deg a,\ l\deg b,\ m\deg c\le r(abc)-1\le\deg a+\deg b+\deg c-1=:S-1\ .$$

Dividing by k, l and m and adding the three resulting bounds we get that

$$S\le S\cdot(k^{-1}+l^{-1}+m^{-1})-(k^{-1}+l^{-1}+m^{-1})\ .$$

Dividing by $S\ge 1$ we get that

$$k^{-1}+l^{-1}+m^{-1}\ge 1+\frac{k^{-1}+l^{-1}+m^{-1}}{S}>1\ .$$

□

In other words, if the sum of reciprocals of $k,l,m\in\mathbb{N}$ does not exceed 1 then the equation $x^k+y^l=z^m$ has no coprime and nonzero solution in $\mathbb{C}[t]$ such that the three polynomials $x(t)$, $y(t)$ and $z(t)$ are not all constant.

Proposition 1.8 (FLT for polynomials). *If $n \geq 3$ is an integer then the equation*

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

has no solution in coprime and nonzero polynomials $x(t), y(t), z(t) \in \mathbb{C}[t]$ that are not all constant.

Proof. Just set $k = l = m := n$ in the previous proposition. □

Later we will see another proof of this proposition.

Chapter 2

Lecture 2. Existence of $\sqrt[n]{z}$ for complex z

We remind an important family of complex numbers.

Roots of unity

For $m \in \mathbb{N}$ and $\alpha \in \mathbb{C}$, we say that α is an *m-th root of* 1 if

$$\alpha^m = 1 \, .$$

Let α be an m-th root of 1. The *order of* α is the minimum $n \in \mathbb{N}$ such that $\alpha^n = 1$. It is easy to see that n divides m. If $n = m$, we say that α is a *primitive m-th root of* 1. For example, i has order 4, 1 is an m-th root of 1 for every m, and -1 is a $2m$-th root of 1 for every m and is a primitive 2nd root of 1.

We can express roots of 1 by means of the complex exponential function $\exp(z)$ and/or the real trigonometric functions $\cos t$ and $\sin t$: the m-th roots of 1 are exactly the m complex numbers

$$\alpha_j := \exp((j/m)2\pi i) = \cos((j/m)2\pi) + i \sin((j/m)2\pi) \qquad \text{(RU)}$$

where $j \in [m] := \{1, \ldots, m\}$. In particular, $\alpha_m = 1$. Instead of $[m]$ the number j may run through any set $X \subset \mathbb{Z}$ representing all m residues modulo m, and one often takes $X = \{0, 1, \ldots, m-1\}$. The m-th roots of 1 form the m vertices of the regular m-gon that is inscribed in the *(complex) unit circle*

$$S := \{z \in \mathbb{C} \mid |z| = 1\}$$

and has vertex 1. The primitive m-th roots of 1 correspond to the $j \in [m]$ coprime to m. In other words, to the j when the fraction j/m is in lowest terms. For any $n \in \mathbb{N}$ we define

$$\mathrm{RU}_n := \{\alpha \in \mathbb{C} \mid \alpha \text{ is an } n\text{-th root of } 1\}$$

and

$$\mathrm{PRU}_n := \{\alpha \in \mathbb{C} \mid \alpha \text{ is a primitive } n\text{-th root of } 1\} \ .$$

The cardinalities, i.e., numbers of elements, of these sets are $|\mathrm{RU}_n| = n$ and $|\mathrm{PRU}_n| = \varphi(n)$, where

$$\varphi(n) := |\{m \in [n] \mid m \text{ and } n \text{ are coprime}\}| \ .$$

The function $\varphi\colon \mathbb{N} \to \mathbb{N}$ is called *Euler's (totient) function.* For any $n \in \mathbb{N}$, any number $z \in \mathbb{C}^\times$ has exactly n distinct *n-th roots*

$$u = |z|^{1/n} \cdot \alpha_j, \ j = 0, 1, \ldots, n-1 \ . \tag{NR}$$

Here $|z|^{1/n}$ is the unique nonnegative real n-th root of $|z|$ and the α_j are defined in equation (RU); recall from the course of mathematical analysis that

$$|z|^{1/n} = \sup(\{x \in \mathbb{R} \mid x \geq 0 \wedge x^n \leq |z|\}) \ .$$

These are exactly the n complex solutions u of the equation $u^n = z$. For $z = 0$ all its n-th roots coincide and are equal to 0.

Existence of n-th roots in $\mathbb{C}$

One of the fundamental mathematical results is the *Fundamental Theorem of Algebra* (FTAlg): every non-constant complex polynomial has at least one complex root. Most proofs of it rely on the fact that every complex number has at least one n-th root for every n, and usually gloss over it by referring to equation (NR). The goal of this lecture is to present my purely topological proof of existence of complex n-th roots.

So we prove purely topologically that

$$\forall\, u \in \mathbb{C}\ \forall\, n \in \mathbb{N}\ \exists\, v \in \mathbb{C} :\ v^n = u \ , \tag{nR}$$

without using either of the functions $\exp(\cdot)$, $\cos(\cdot)$ and $\sin(\cdot)$. Instead we use connected and disconnected subsets of $\mathbb{C}$. Why we bind our hands and do not want to use these nice special functions? The proof of existence of n-th roots is simpler without them, both conceptually and technically. To establish all necessary properties of the exponential function and/or the trigonometric functions takes time if one gives all details. The existence of n-th roots based on cosine and sine looks simple exactly because these details are usually not given.

For my proof of claim (nR) we need the property of connectedness of sets of complex numbers and some further properties of these sets. A set $X \subset \mathbb{C}$ is *open* if

$$\forall\, u \in X\ \exists\, r > 0 :\ B(u, r) \subset X \ .$$

Here $B(u, r) := \{z \in \mathbb{C} \mid |z - u| < r\}$ is the *open ball (with center u and radius r).* As is well known, $\emptyset$, $\mathbb{C}$ and every $B(u, r)$ are open sets, any union of

open sets is an open set and any finite intersection of open sets is an open set. For $X \subset \mathbb{C}$ we say that a function $f\colon X \to \mathbb{C}$ is *continuous* if

$$\forall\, u \in X\ \forall\, \varepsilon > 0\ \exists\, \delta > 0 :\ f[B(u,\, \delta) \cap X] \subset B(f(u),\, \varepsilon)\ .$$

Here the notation $g[X]$ means, for a function $g\colon A \to B$ and a set $X \subset A$, the *image of X by g*, the set

$$g[X] := \{g(a) \mid a \in X\} \subset B\ .$$

Similarly, for $X \subset B$ the set

$$g^{-1}[X] := \{a \in A \mid g(a) \in X\} \subset A$$

is the *inverse image of X by g*. An equivalent definition of continuity is that for $X \subset \mathbb{C}$ a function $f\colon X \to \mathbb{C}$ is continuous if

$$\forall\, \text{open set } A \subset \mathbb{C}\ \exists\, \text{an open set } B \subset \mathbb{C} :\ f^{-1}[A] = B \cap X\ .$$

We say that a set $X \subset \mathbb{C}$ is *disconnected* if there exist two open sets $A, B \subset \mathbb{C}$ such that

$$(X \subset A \cup B) \wedge (A \cap X \neq \emptyset \neq B \cap X) \wedge (A \cap B \cap X = \emptyset)\ .$$

In this situation we say that *A and B tear X*. If no such two open sets A and B exist, we say that the set X is *connected*. Proofs of the following three useful results on connectedness are left to the reader as exercises.

1. If $X, Y \subset \mathbb{C}$ are connected sets and $X \cap Y \neq \emptyset$ then $X \cup Y$ is connected.
2. Any real interval $I \subset \mathbb{C}$ — we regard $\mathbb{R}$ as a subset of $\mathbb{C}$ — is connected.
3. For any connected set $X \subset \mathbb{C}$ and any continuous function $f\colon X \to \mathbb{C}$ the set $f[X]$ is connected.

Proposition 2.1 (connectedness of S). *The unit circle*

$$S = \{z \in \mathbb{C} \mid |z| = 1\} \subset \mathbb{C}$$

is a connected set.

Proof. We express S as the union $S = S^- \cup S^+$ with the sets $S^- = f^-[I]$ and $S^+ = f^+[I]$ (S^-, resp. S^+, is the lower, resp. upper, semicircle of S), where $I = [-1, 1] \subset \mathbb{C}$ is a real interval and the functions

$$f^-,\ f^+\colon I \to \mathbb{C}$$

are given by

$$f^-(t) = t - i\sqrt{1 - t^2} \ \text{ and } \ f^+(t) = t + i\sqrt{1 - t^2}\ .$$

It is clear that f^- and f^+ are continuous and that $S^- \cap S^+ = \{-1, 1\}$. Hence the above properties 1–3 show that S is a connected set. □

The function $\sqrt{\cdot}$ used in the proof is the root of a nonnegative real number, which we mentioned above. A simpler proof of connectedness of S uses the representation $S = f[J]$, where $J = [0, 2\pi]$ and $f(t) = \cos t + i \sin t$. But recall that we do not want to use trigonometric functions.

We also need an extension of the root function $\sqrt{\cdot}$ to the complex domain. Another exercise for the reader is to establish the following result:

$$\forall\, a + bi \in \mathbb{C}\ \exists\, c + di \in \mathbb{C} :\ (c + di)^2 = a + bi\ . \qquad (\sqrt{\cdot})$$

(Hint: use the quadratic formula.) Using this and the previous proposition we easily prove claim (nR).

Theorem 2.2 (existence of n-th roots in $\mathbb{C}$). *For every $n \in \mathbb{N}$ and every $u \in \mathbb{C}$ there is a $v \in \mathbb{C}$ such that*

$$v^n = u\ .$$

Proof. We may assume that u is nonzero, so let $u \in \mathbb{C}^\times$ and $n \in \mathbb{N}$. Since $|\frac{1}{|u|} \cdot u| = 1$ and we can take n-th root of any nonnegative real number, we may assume that $|u| = 1$, i.e., $u \in S$. Since $n = 2^j k$ for a $j \in \mathbb{N}_0$ and an odd $k \in \mathbb{N}$ and by claim $(\sqrt{\cdot})$ we can take repeatedly roots of complex numbers, we may assume that n is an odd number. Thus we assume that $u \in S$ and that $n \in \mathbb{N}$ is odd and look for a $v \in S$ such that $v^n = u$. So we need to show that the function

$$f\colon S \to S,\ f(z) = z^n\ ,$$

is onto, $f[S] = S$. The key property of f is that $f(-z) = -f(z)$ because n is odd.

For contradiction, let $w \in S \setminus f[S]$. Then also $-w \in S \setminus f[S]$. We take the line $\ell \subset \mathbb{C}$ going through the antipodal points $-w$ and w on S and partition $\mathbb{C}$ in the disjoint union

$$\mathbb{C} = A \cup \ell \cup B\ ,$$

where A and B are the two open half-planes determined by ℓ. These sets are open not only by name but they are really open sets. It is easy to see that

$$(A \cup B) \cap S = S \setminus \{-w, w\},\ A = -B := \{-z \mid z \in B\}$$

and that $\{-1, 1\} \subset (A \cup B) \cap f[S]$. It follows that A and B tear $f[S]$ and the set $f[S]$ is disconnected. On the other hand, f is continuous and S is connected by Proposition 2.1, so by the above property 3 the set $f[S]$ is connected. This is the desired contradiction. □

The 1st application of roots of unity: primes $\equiv 1$ mod m

We prove that for every $m \in \mathbb{N}$ there exist infinitely many prime numbers congruent to 1 modulo m. *Dirichlet's theorem on primes in arithmetic progression* is the deep generalization that

$$\forall \text{ coprime } m, a \in \mathbb{N} \; \exists \infty \text{ many primes } p : \; p \equiv a \pmod{m} \; .$$

All known proofs are analytic and difficult. The proof of the special case for $a = 1$, given here, is simple and algebraic. It is based on the *cyclotomic polynomials*

$$\Phi_n(x) := \prod_{\alpha \in \mathrm{PRU}_n} (x - \alpha) \in \mathbb{C}[x], \; n \in \mathbb{N} \; .$$

In the next lecture we show that $\Phi_n(x) \in \mathbb{Z}[x]$. The factorization

$$x^n - 1 = \prod_{\alpha \in \mathrm{RU}_n} (x - \alpha)$$

and the disjoint union

$$\mathrm{RU}_n = \bigcup_{d \,|\, n} \mathrm{PRU}_d$$

(we say more on it below) give the factorization

$$x^n - 1 = \prod_{d \,|\, n} \Phi_d(x) \; .$$

For example, $x^4 - 1 = (x-1) \cdot (x+1) \cdot (x^2+1)$, corresponding to the divisors $d = 1, 2$ and 4 of the number $n = 4$. Comparing degrees of polynomials on both sides we get the following identity; in the proof we restate the argument in elementary terms.

Proposition 2.3 (an identity for φ). *For every $n \in \mathbb{N}$,*

$$n = \sum_{d \in \mathbb{N},\, d \,|\, n} \varphi(d) \; .$$

Proof. For any given $n \in \mathbb{N}$ and any divisor $d \in \mathbb{N}$ of n we define the sets of fractions

$$A := \{ j/n \mid j \in [n] \} \text{ and } B_d := \{ j/d \mid j \in [d] \text{ and is coprime with } d \} \; .$$

Thus in each set B_d the fractions are in lowest terms. If d and d' are distinct divisors of n then $B_d \cap B_{d'} = \emptyset$ because for any $\frac{j}{d} \in B_d$ and any $\frac{j'}{d'} \in B_{d'}$ one has that $\frac{j}{d} = \frac{j'}{d'} \iff jd' = j'd \iff j = j' \wedge d = d'$. Also, the union of all B_d equals A because every fraction $\frac{j}{d} \in B_d$ can be extended as $j/d = j \cdot \frac{n}{d}/n \in A$

and every fraction $\frac{j}{n} \in A$ can be brought to lowest terms as $\frac{j}{n} = \frac{j'}{d} \in B_d$ for some divisor d of n. So

$$n = |A| = \sum_{d \mid n} |B_d| = \sum_{d \mid n} \varphi(d) \ .$$

□

For example, $12 = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12) = 1+1+2+2+2+4$. We mention the well known formula

$$\varphi(n) = n \cdot \prod_{p \mid n} \left(1 - p^{-1}\right) \ .$$

It can be proven combinatorially by inclusion–exclusion, or by algebraic arguments.

Theorem 2.4 (∞ many primes $\equiv 1 \pmod m$). *For any number $m \in \mathbb{N}$ the sequence*

$$P(m) := (1 + m,\ 1 + 2m,\ 1 + 3m,\ \dots)$$

contains infinitely many prime numbers.

Interestingly, it suffices to establish existence of only one prime in $P(m)$.

Theorem 2.5 (one prime $\equiv 1 \pmod m$). *For any number $m \in \mathbb{N}$ the sequence*

$$P(m) = (1 + m,\ 1 + 2m,\ 1 + 3m,\ \dots)$$

contains at least one prime number.

We show that Theorem 2.5 $\Rightarrow$ Theorem 2.4. For any $m \in \mathbb{N}$, let $p_m \in P(m)$ be one prime number congruent to 1 modulo m. Clearly, $P(km) \subset P(m)$ for every $k \in \mathbb{N}$. Also, $p_m > m$ and therefore

$$\lim_{k \to \infty} p_{km} = +\infty \ .$$

Hence $\{p_{km} \mid k \in \mathbb{N}\}$ give infinitely many different primes in $P(m)$. We prove Theorem 2.5 in the next lecture.

Chapter 3

Lecture 3. Prime numbers $p = 1 + mn$ and FLT in $\mathbb{C}[t]$

In this lecture we prove

Theorem 3.1 (Theorem 2.5).

$$\forall\, m \in \mathbb{N}\ \exists\, p:\ p \equiv 1 \pmod{m}\ .$$

Last time we saw how this implies that for any $m \in \mathbb{N}$ there exist even infinitely many primes of the form $p = 1 + mn$, $n \in \mathbb{N}$.

First we show that cyclotomic polynomials have integral coefficients. From the definition it is clear that each polynomial $\Phi_n(x)$ is *monic*, has leading coefficient 1.

Lemma 3.2. *For every $n \in \mathbb{N}$,*

$$\Phi_n(x) = \prod_{\alpha \in \mathrm{PRU}_n} (x - \alpha) \in \mathbb{Z}[x]\ .$$

More precisely, each $\Phi_n(x)$ is integral (has integral coefficients) and has constant coefficient $\Phi_n(0) = \pm 1$.

Proof. We proceed by induction on n. For $n = 1$ it all holds as $\Phi_1(x) = x - 1$. Let $n > 1$, $m := \varphi(n)$,

$$\Phi_n(x) =: \sum_{j=0}^{m} a_j x^j \quad \text{and} \quad \Psi_n(x) := \prod_{d \,|\, n,\, d<n} \Phi_d(x) =: \sum_{j=0}^{n-m} b_j x^j\ .$$

Comparing the coefficients of x^j, $j = 0, 1, 2, \ldots$, on both sides of the equation

$$x^n - 1 = \Phi_n(x) \cdot \Psi_n(x)$$

we get the system of equations

$$-1 = a_0 b_0,\ 0 = a_0 b_1 + a_1 b_0,\ c_2 := [x^2](x^n - 1) = a_0 b_2 + a_1 b_1 + a_2 b_0,\ \dots\ ,$$

where by the inductive assumption the b_i are integers (they are coefficients in a polynomial obtained as a product of integral polynomials), the a_i are the unknowns and $[x^j]\dots$ denotes the coefficient of x^j in the expression $\dots$. Since $b_0 = \pm 1$ by the inductive assumption (it is a product of $\pm$1s), $a_0 = -1/b_0 = \pm 1$ too. By solving for the a_i,

$$a_1 = (1/b_0)(-a_0 b_1),\ a_2 = (1/b_0)(c_2 - a_0 b_2 - a_1 b_1),\ \dots\ ,$$

we see that each $a_i \in \mathbb{Z}$ because $1/b_0 = \pm 1$, each b_i and each c_i is an integer and so is each already obtained a_j for $j < i$. □

Proof of Theorem 3.1. Let $m \in \mathbb{N}$. We produce a prime p of the form $p = 1 + mn$. Consider the polynomials

$$f(x) := \Phi_m(x) \ \text{ and } \ g(x) := \prod_{d \mid m,\, d<m} \Phi_d(x)$$

(for $m = 1$ we set $g(x) := 1$). By the previous lemma we know that $f, g \in \mathbb{Z}[x]$ and from the previous lecture we know that

$$x^m - 1 = f(x) \cdot g(x)\ . \tag{fg}$$

By the definition of f and g, the roots of f are exactly the primitive m-th roots of 1 and the roots of g are all remaining m-th roots of 1. Thus the polynomials f and g have no common complex root and therefore are coprime as elements of the polynomial ring $\mathbb{Q}[x]$, in other words if $h \in \mathbb{Q}[x]$ divides both f and g then h is a unit of the ring, $h \in \mathbb{Q}^\times$. Hence there exist polynomials $\alpha, \beta \in \mathbb{Q}[x]$ such that

$$\alpha f + \beta g = 1\ .$$

Below we explain how this identity, called Bézout's in the polynomial case but Bachet's for general rings, follows from the fact that the ring $\mathbb{Q}[x]$ is Euclidean, i.e., division with remainders works in it. Multiplying by an appropriate $c \in \mathbb{N}$ we get the identity

$$a(x) \cdot f(x) + b(x) \cdot g(x) = c \tag{Bézout}$$

where now $a, b \in \mathbb{Z}[x]$ and we may assume that $c \geq 3$. From the definition of f and since $c \geq 3$, it follows that

$$\mathbb{N} \ni |f(c)| \geq 2$$

and there exists a prime number p dividing $f(c) \in \mathbb{Z}$ (we excluded that $f(c) = \pm 1$).

We show that p is the desired prime congruent to 1 modulo m. Equation (fg) gives that $c^m - 1 = f(c) \cdot g(c)$ and therefore p divides $c^m - 1$. We show

that p does not divide $c^d - 1$ for any divisor $d < m$ of m. For contradiction, let $p \,|\, c^d - 1$ where $d \in \mathbb{N}$ divides m and is smaller than m. From

$$c^d - 1 = \prod_{e \,|\, d} \Phi_e(c)$$

and the definition of g it follows that $c^d - 1$, and so also p, divides $g(c)$. But then by setting $x = c$ in identity (Bézout) we see that p divides c and (since $p \,|\, c^m - 1$) also 1, which is a contradiction. We have shown that the multiplicative order of c modulo p is m, the number m is the minimum $j \in \mathbb{N}$ such that $c^j \equiv 1$ modulo p. The Little Theorem of Fermat says that also $c^{p-1} \equiv 1$ modulo p. It follows that the order m divides $p - 1$, which is exactly what we wanted to show. □

This proof is taken from the book [22] by W. Narkiewicz.

The 2nd application of roots of unity: FLT in $\mathbb{C}[t]$

We give another (and somewhat more complicated) proof of FLT in $\mathbb{C}[t]$. We assume that a number $n \in \mathbb{N}$ with $n \geq 3$ and three coprime nonzero polynomials $a, b, c \in \mathbb{C}[t]$, not all of them constant, are such that

$$a(t)^n + b(t)^n = c(t)^n \ ,$$

and deduce a contradiction. The contradiction will consist in producing another three coprime nonzero polynomials $\alpha(t)$, $\beta(t)$ and $\gamma(t)$, not all of them constant, solving the equation and such that

$$\max(\deg \alpha, \deg \beta, \deg \gamma) < \max(\deg a, \deg b, \deg c) \ .$$

This results in an *infinite descent*, an infinite strictly descending sequence of natural numbers. It does not exist and we have a contradiction. Arguments of this kind, showing insolubility of certain Diophantine equations, go back to P. de Fermat in the 17th century .

So let n and polynomials a, b and c be as stated. Then

$$a(t)^n = c(t)^n - b(t)^n = \prod_{j=0}^{n-1} (c(t) - \xi^j \cdot b(t)) \ , \qquad \text{(fact.)}$$

where $\xi = \exp(2\pi i/n)$ is a primitive n-th root of 1. This identity follows from the already mentioned factorization

$$x^n - 1 = \prod_{\alpha \in \mathrm{RU}_n} (x - \alpha) = \prod_{j=0}^{n-1} (x - \xi^j)$$

by substituting $x := c/b$ and then multiplying by b^n. The polynomial ring $\mathbb{C}[t]$, where we now work, is Euclidean and — we review it now — therefore is a UFD, a *unique factorization domain.*

A review of divisibility in rings

To continue cogently in the proof we need some notions and results in ring theory. Let R be a commutative ring with 1_R. We say that it is an *integral domain* if for every $a, b \in R$ one has that $ab = 0_R \Rightarrow a = 0_R \vee b = 0_R$. An element $a \in R$ is a *unit* if $ab = 1_R$ for some $b \in R$. The units in R form a group $R^\times = (R^\times, 1_R, \cdot)$. A non-zero and non-unit element $a \in R$ is *irreducible (in R)* if $a = bc$ with $b, c \in R$ is possible only when b or c is a unit. R is a *field* if every nonzero element in R is a unit, $R^\times = R \setminus \{0_R\}$. Elements $a, b \in R$ are *coprime (in R)* if their common divisors in R are only units. An integral domain R is a UFD if every non-zero and non-unit element in it factorizes uniquely in a product of irreducible elements. By *uniqueness of irreducible factorizations* in R we mean that if $b_i, c_i \in R$ are such that

$$b_1 b_2 \dots b_k = c_1 c_2 \dots c_l$$

and every b_i and every c_i is irreducible, then $k = l$ and there exist a bijection $\pi\colon [k] = [l] \to [k] = [l]$ and units $d_1, \dots, d_k \in R$ such that

$$b_i = d_i \cdot c_{\pi(i)},\ i = 1,\, 2,\, \dots,\, k\ .$$

For example, the UFD of integers $\mathbb{Z}$ has units $\{-1, 1\}$, irreducible elements

$$\{\pm p \mid p \text{ is a prime number}\}$$

and unique irreducible factorizations like

$$-12 = 3 \cdot (-2) \cdot 2 = (-2) \cdot (-2) \cdot (-3) = \dots\ .$$

A property of an integral domain R that implies uniqueness of irreducible factorizations is that R is a PID, a *principal ideal domain*. It means that every ideal $I \subset R$ is generated by a single element, there is a $g \in I$ such that $I = \{ag \mid a \in R\}$. Recall that an *ideal* in a ring R is any set $I \subset R$ such that $a, b \in I \Rightarrow a - b \in I$ and $a \in R, b \in I \Rightarrow ab \in I$. Every PID R enjoys *Bachet's identity* that

$$a, b \in R \text{ are coprime} \Rightarrow \exists\, c,\, d \in R\colon\ ca + bd = c \cdot_R a +_R b \cdot_R d = 1_R\ .$$

Indeed, the ideal $I := \{ca + db \mid c, d \in R\}$ is generated by some $g \in I$, which means that g divides both $a \in I$ and $b \in I$ and therefore g must be a unit with an inverse $h \in R$, and $1_R = hg \in I$. C. G. Bachet de Méziriac (1581–1638) established the identity for the ring $\mathbb{Z}$ and E. Bézout (1730–1783) proved it for a polynomial ring. Thus we think that the terminology we use here (sometimes the identity is completely attributed to Bézout) is fair. Now to establish uniqueness of irreducible factorizations, it clearly suffices to prove the implication

$$a, b, c \in R,\ a \text{ is irreducible and divides } bc \Rightarrow a \text{ divides } b \text{ or } c\ .$$

With Bachet's identity it is easy. Suppose that a is irreducible, divides bc and does not divide b. Thus a and b are coprime and

$$a'a + b'b = 1_R$$

for some $a', b' \in R$ by Bachet's identity. Multiplying by c we get the identity

$$ca'a + b'bc = c$$

showing that a divides c.

A stronger property of an integral domain R implying that it is a PID is that R is *Euclidean*. It means that

$$\begin{aligned} &\exists \text{ a function } |\cdot| \colon R \setminus \{0_R\} \to \mathbb{N}_0 \; \forall\, a,\, b \in R,\, b \neq 0_R \; \exists\, c,\, r \in R : \\ &: \; a = bc + r \wedge (r = 0_R \vee |r| < |b|) \; . \end{aligned} \tag{Eucl.}$$

We show that any Euclidean R is a PID. Suppose that $I \subset R$ is an ideal. We take a nonzero element $a \in I$ with the minimum value of $|a|$. Then we write according to property (Eucl.) any $x \in I$ as

$$x = ab + r,\; b,\, r \in R,\; r = 0_R \vee |r| < |a| \; .$$

But $r = x - ab \in I$ and the minimality of $|a|$ implies that $r = 0_R$. Thus $x = ab$ and I is generated by a.

It is well known that the ring $\mathbb{C}[t]$ is Euclidean, with the function $|\cdot|$ being the degree of a nonzero polynomial. By the above review this means that irreducible factorizations in $\mathbb{C}[t]$ are unique, in the above explained sense, whenever they exist. But do they exist? They do and the most straightforward argument showing it relies on the FTAlg. We already used in the first lecture that every non-constant polynomial $a \in \mathbb{C}[t]$ factorizes as

$$a(t) = \alpha \prod_{i=1}^{n} (t - \alpha_i) \; ,$$

where $\alpha \in \mathbb{C}^\times$, all $\alpha_i \in \mathbb{C}$ and are not necessarily distinct and $n = \deg a \in \mathbb{N}$. Clearly, α is a unit ($\mathbb{C}^\times$ equals to the units of $\mathbb{C}[t]$) and each factor $t - \alpha_i$ is irreducible. A more elementary argument, which does not need the FTAlg and which works more generally for any polynomial ring $F[t]$ where F is a field, uses additivity of the degree function: for every two nonzero polynomials a and b in $F[t]$,

$$\deg(ab) = \deg a + \deg b \; .$$

Also, $\deg a = 0$ iff a is a unit in $F[t]$ (a nonzero constant polynomial). Thus if polynomials $a, b, c \in F[t]$, $a \neq 0$, are such that $a = bc$ and neither of b and c is a unit, then $\max(\deg b, \deg c) < \deg a$. This descent shows that every nonzero and non-unit polynomial in $F[t]$ is a product of irreducible polynomials. Hence we can conclude that $\mathbb{C}[t]$, and more generally any $F[t]$ (since $F[t]$ is Euclidean), is a UFD. We summarize this review in a proposition.

Proposition 3.3 (on polynomials over F). *For every field F the ring of polynomials $F[t]$ with coefficients in F is Euclidean and is a* UFD.

Back to the proof of FLT in $\mathbb{C}[t]$

Having recalled all this we resume the proof of FLT in $\mathbb{C}[t]$ and invoke the next result whose proof we leave to the reader as an exercise.

Proposition 3.4 (on n-th powers). *Suppose that R is a* UFD*, $n \in \mathbb{N}$, $a \in R$ is nonzero and $a_1, \ldots, a_k \in R$ are pairwise coprime elements such that*

$$a_1 a_2 \ldots a_k = a^n \ .$$

Then there exist units $b_i \in R$ and pairwise coprime elements $c_i \in R$ such that

$$a_i = b_i \cdot c_i^n, \ i = 1, 2, \ldots, k \ .$$

We apply the proposition to the above factorization (fact.) — the n factors on the right-hand side are pairwise coprime, for else we could linearly combine two of them and show that $c(t)$ and $b(t)$ are not coprime — and get polynomials $w_j \in \mathbb{C}[t]$ such that

$$c(t) - \xi^j \cdot b(t) = w_j(t)^n, \ j = 0, 1, \ldots, n-1 \ .$$

Why are there no units on the right-hand side? Due to the nice property of the ring $\mathbb{C}[t]$ (not shared by the ring $\mathbb{Z}$) that any unit, i.e., any $c \in \mathbb{C}^\times$, is an n-th power; we saw a proof of it in the previous lecture. Thus we absorbed the units in the powers $w_j(t)^n$. The crucial step in obtaining an infinite descent is the next identity expressing the linear dependence of the three factors for $j = 2, 0, 1$ on the left-hand side (now we need that $n \geq 3$):

$$c(t) - \xi^2 \cdot b(t) + \xi \cdot (c(t) - b(t)) = (1 + \xi) \cdot (c(t) - \xi \cdot b(t)) \ .$$

Substituting the n-th powers $w_j(t)^n$ we get the equation

$$\underbrace{w_2(t)^n}_{\alpha(t)^n} + \underbrace{(\psi \cdot w_0(t))^n}_{\beta(t)^n} = \underbrace{(\eta \cdot w_1(t))^n}_{\gamma(t)^n} \ ,$$

where $\psi, \eta \in \mathbb{C}$ are such that $\psi^n = \xi$ and $\eta^n = 1 + \xi$ (we again use existence of n-th roots in $\mathbb{C}$). We already know that the polynomials α, β and γ are nonzero and pairwise coprime. No two of them are constant, for else a liner combination would show that b and c, and thus also a, is constant. We have a new (coprime, nonzero and non-constant) solution

$$\alpha(t)^n + \beta(t)^n = \gamma(t)^n$$

of Fermat's equation. Clearly,

$$\begin{aligned} \max(\deg \alpha, \deg \beta, \deg \gamma) &\leq \frac{1}{n} \max(\deg a, \deg b, \deg c) \\ &< \max(\deg a, \deg b, \deg c) \end{aligned}$$

because $\max(\deg a, \deg b, \deg c) > 0$. An infinite descent was established. $\square$

The previous proof of FLT in $\mathbb{C}[t]$ is taken from the book [24, p. 7] of A. van der Poorten; we corrected some typographical and other errors in it and supplied the review of divisibility in rings.

The 3rd application of roots of unity: the regular 17-gon

A classical problem that originated in antiquity was — and still is — to determine all $n \in \mathbb{N}$ such that the regular n-gon can be constructed by straightedge and compass. The following classical characterization is well known.

Theorem 3.5 (Gauss–Wantzel). *The regular n-gon can be constructed by straightedge and compass $\iff$ n has the form*

$$n = 2^k p_1 p_2 \dots p_r \ ,$$

where $k, r \in \mathbb{N}_0$ (for $r = 0$ we define the product of primes p_i as 1) and $p_1 < p_2 < \cdots < p_r$ are distinct Fermat primes*, prime numbers of the form*

$$F_m := 2^{2^m} + 1, \ m \in \mathbb{N}_0 \ .$$

The sufficiency part $\Leftarrow$ in the theorem is due to C. F. Gauss, and the necessity part $\Rightarrow$ to P. Wantzel. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are all prime numbers and this is the complete list of *currently known* Fermat primes. It is not known if these are already all Fermat primes or if there exist some more. The Wikipedia page [9] states: "As of 2014, it is known that F_m is composite for $5 \le m \le 32$". The ancient problem of constructing regular n-gons remains wide open because we are (currently) unable to determine all Fermat primes. A nice book on the numbers F_m is [14] by M. Křížek, F. Luca and L. Sommer. In the next lecture we show that the regular 17-gon, corresponding to the Fermat prime F_2, can be constructed by straightedge and compass.

Chapter 4

Lecture 4. Gauss and the regular 17-gon

In today's lecture we show that the real number

$$z_1 := 2\cos(2\pi/17)$$

is *constructible*: z_1 can be obtained from the numbers in $\mathbb{Q}$ (or, equivalently, just from the number 1) by repeated applications of the arithmetic operations $+$, $-$,$\times$, : and the operation $\sqrt{\cdot}$ of square root extraction. Hence the regular 17-gon, associated to the Fermat prime F_2, can be constructed by straightedge and compass because

$$\alpha := 2\pi/17$$

is its central angle. It was discovered by the 19 years old C. F. Gauss in 1796.

We begin with two detours, and give one more after the construction. The first detour is a nice application of Bachet's identity.

Proposition 4.1 (m-gon and n-gon give mn-gon). *If $m, n \in \mathbb{N}$ are coprime numbers and both the regular m-gon and the regular n-gon can be constructed by straightedge and compass, then so can be the regular mn-gon. In fact, then the regular mn-gon can be constructed only by compass.*

Proof. Bachet's identity for the ring $\mathbb{Z}$ tells us that for some $r_1, r_2 \in \mathbb{Z}$ one has that $r_1 m + r_2 n = 1$. Thus

$$r_2 \cdot \frac{2\pi}{m} + r_1 \cdot \frac{2\pi}{n} = 2\pi \cdot \frac{r_2 n + r_1 m}{mn} = \frac{2\pi}{mn}$$

is the central angle of the regular mn-gon. It is clear that if the central angles of the regular m-gon and n-gon are given, say determined by pairs of radii in the unit circle, then their above linear combination can be constructed only by compass. □

The second detour concerns moduli $m \in \mathbb{N}$ possessing so called primitive roots. A *primitive root* modulo m is a residue class a modulo m that is coprime with m and is such that

$$\begin{aligned}&\{a^i \bmod m \mid i = 1, 2, \ldots, \varphi(m)\}\\ &= \mathbb{Z}_m^\times = \{x \bmod m \mid x \in [m] \text{ and is coprime with } m\}\ .\end{aligned}$$

In algebraic terms, a modulo m is a generator of the multiplicative group $\mathbb{Z}_m^\times = (\mathbb{Z}_m^\times, 1, \cdot)$. So m possesses a primitive root iff the group $\mathbb{Z}_m^\times$ is cyclic. For example, $m = 4$ has the primitive root $a = 3$, but $m = 8$ does not have any primitive root because all squares 1^2, 3^2, 5^2 and 7^2 are 1 modulo 8. A known theorem says that

$$m \text{ has a primitive root } \iff m = 1, 2, 4, p^k \text{ and } 2p^k\ ,$$

where $k \in \mathbb{N}$ and $p > 2$ is a prime number, but we only prove the case $m = p$. This was done by the 24 years old C. F. Gauss in his tract *Disquisitiones Arithmeticae* (Arithmetical Investigations) in 1801.

Theorem 4.2 (primitive roots of p). *Every prime number has a primitive root.*

Proof. Recall that the *multiplicative order* of an $a \in \mathbb{Z}$ modulo $m \in \mathbb{N}$, where a and m are coprime, is the minimum $e \in \mathbb{N}$ such that $a^e \equiv 1$ modulo m. By Euler's generalization of Fermat's Little Theorem, $a^{\varphi(m)} \equiv 1$ modulo m and therefore e divides $\varphi(m)$. If a and m are not coprime then there is no such e.

Let p be a prime number. For every $d \in \mathbb{N}$ dividing $\varphi(p) = p - 1$ we define the set of nonzero residues modulo p

$$A_d := \{a \bmod p \mid a \text{ has multiplicative order } d \text{ modulo } p\}\ .$$

It follows from the definition of multiplicative order that (i) the sets

$$\{A_d \mid d \text{ divides } p - 1\}$$

form a partition of $\mathbb{Z}_p^\times$ (in a moment we show that each A_d is nonempty). It suffices to prove (ii) the implication

$$A_d \neq \emptyset \Rightarrow |A_d| = \varphi(d)\ .$$

The facts (i), (ii) and the identity

$$|\mathbb{Z}_p^\times| = p - 1 = \sum_{d \,|\, p-1} \varphi(d)$$

of Proposition 2.3 imply that $|A_d| = \varphi(d)$ for every divisor d of $p - 1$. In particular, $|A_{p-1}| = \varphi(p - 1) > 0$, in the group $\mathbb{Z}_p^\times$ there exist elements with the maximum possible multiplicative order $p - 1$ and $\mathbb{Z}_p^\times$ is cyclic.

We prove the implication (ii). Let d be a divisor of $p-1$ and let $a \in A_d$ (so $A_d \neq \emptyset$). We define

$$B := \{a \bmod p,\, a^2 \bmod p,\, \ldots,\, a^d \bmod p\}$$

and

$$R := \{x \bmod p \mid x^d - 1 \equiv 0 \bmod p\}\ .$$

Then (iii) $|B| = d$ because for $|B| < d$ the element a would have multiplicative order smaller than d. Also, (iv) $B \subset R$ and (v) $|R| \leq d$. The fact (iv) follows from $a \in A_d$ and the fact (v) follows from the bound on the number of roots of a polynomial (here $x^d - 1$) over a field (here $\mathbb{Z}_p$) in that field. (We use that $\mathbb{Z}_p = (\mathbb{Z}_p, 0, 1, +, \cdot)$ is a field.) The facts (iii), (iv) and (v) imply that (vi) $R = B$. Clearly, (vii) $A_d \subset R$. The facts (vi) and (vii) imply that (viii) $A_d \subset B$ and so every $x \in A_d$ has the form $x = a^i$ for a unique $i \in [d]$. Finally, it follows that (ix) for every $i \in [d]$ one has that $a^i \in A_d$ iff i and d are coprime. By the facts (viii) and (ix), $|A_d| = \varphi(d)$ and the implication (ii) is proven. □

The proof is like a chess miniature, black mates in nine moves. We not only proved that the group $\mathbb{Z}_p^\times$ is cyclic, but we even got the formula $\varphi(p-1)$ for the number of its generators. For example, modulus 17 has $\varphi(16) = 16/2 = 8$ primitive roots, i.e., every other nonzero residue class is a primitive root. One of them is 3, which will be used in the next Gaussian construction:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^m	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

where $3^m =: k$ is reduced mod 17. We let m run in $0, 1, \ldots, 15$ rather than in $1, 2, \ldots, 16$ because we are following the construction in the book [11].

Theorem 4.3 (Gaussian construction of the reg. 17-gon). *Suppose that $\alpha = 2\pi/17$, $z_1 = 2\cos\alpha$ and $z_2 := 2\cos(4\alpha)$. The number z_1 is constructible because the real numbers $z_1 > z_2$ are solutions of the quadratic equation*

$$z^2 - y_1 z + y_3 = 0\ ,$$

where the four real numbers y_1, y_2, y_3 and y_4 are determined by the conditions that $y_1 > y_2$ are solutions of the quadratic equation

$$y^2 - x_1 y - 1 = 0$$

and $y_3 > y_4$ are solutions of the quadratic equation

$$y^2 - x_2 y - 1 = 0\ ,$$

where the real numbers $x_1 > x_2$ are solutions of the quadratic equation

$$x^2 + x - 4 = 0\ .$$

Thus the regular 17-gon can be constructed by straightedge and compass.

Proof. For $k = 1, 2, \ldots, 16$ we set $\varepsilon_k := \cos(k\alpha) + i\sin(k\alpha)$. These are the roots of the polynomial $p(x) := 1 + x + x^2 + \cdots + x^{16} = \frac{x^{17}-1}{x-1}$. Recall that $k = 3^m$ modulo 17; according to the above table we set

$$x_1 := \sum_{m \text{ is even}} \varepsilon_k = \varepsilon_1 + \varepsilon_9 + \varepsilon_{13} + \varepsilon_{15} + \varepsilon_{16} + \varepsilon_8 + \varepsilon_4 + \varepsilon_2$$

and

$$x_2 := \sum_{m \text{ is odd}} \varepsilon_k = \varepsilon_3 + \varepsilon_{10} + \varepsilon_5 + \varepsilon_{11} + \varepsilon_{14} + \varepsilon_7 + \varepsilon_{12} + \varepsilon_6 \ .$$

From $\varepsilon_k + \varepsilon_{17-k} = 2\cos(k\alpha)$, $k = 1, 2, \ldots, 16$, we get that

$$x_1 = 2(\cos\alpha + \cos(8\alpha) + \cos(4\alpha) + \cos(2\alpha))$$

and

$$x_2 = 2(\cos(3\alpha) + \cos(7\alpha) + \cos(5\alpha) + \cos(6\alpha)) \ .$$

Since $(x-u)(x-v) = x^2 - (u+v)x + uv$, to show that x_1 and x_2 are root of a monic integral quadratic polynomial it suffices to compute $x_1 + x_2$ and $x_1 x_2$. As for the sum,

$$x_1 + x_2 = 2\sum_{k=1}^{8} \cos(k\alpha) = \sum_{k=1}^{16} \varepsilon_k = -[x^{15}]p(x) = -1 \ .$$

For the product we need the identity

$$2\cos u \cos v = \cos(u+v) + \cos(u-v) \ . \qquad \text{(id.)}$$

Using it, the fact that $\cos(k\alpha) = \cos((17-k)\alpha)$, $k = 1, 2, \ldots, 16$, and using multiset notation, we get that

$$\begin{aligned}
x_1 x_2 &= 4 \cdot (\cos\alpha + \cos(8\alpha) + \cos(4\alpha) + \cos(2\alpha)) \cdot (\cos(3\alpha) + \cos(7\alpha) + \\
&+ \cos(5\alpha) + \cos(6\alpha)) \\
&= 2 \sum_{r \in \{4,8,6,7,11,15,13,14,7,11,9,10,5,9,7,8\}} \cos(r\alpha) + \\
&+ 2 \sum_{r \in \{2,6,4,5,5,1,3,2,1,3,1,2,1,5,3,4\}} \cos(r\alpha) \\
&= 8\sum_{r=1}^{8} \cos(r\alpha) = 4(x_1 + x_2) \\
&= -4 \ .
\end{aligned}$$

Thus x_1 and x_2 are the roots of $x^2 + x - 4$. Since $\cos\alpha + \cos(2\alpha) > 2\cos(\pi/4) > -\cos(8\alpha)$ and $\cos(4\alpha) > 0$, we have that $x_1 > 0$ and hence (from $x_1 + x_2 = -1$) $x_1 > x_2$. Such inequalities (we have similar ones for the y_i and z_i) are needed for telling apart the roots of each quadratics.

We set

$$\begin{aligned}
y_1 &:= \sum_{m\equiv 0 \pmod 4} \varepsilon_k = \varepsilon_1+\varepsilon_{13}+\varepsilon_{16}+\varepsilon_4 = 2(\cos\alpha+\cos(4\alpha)) \ , \\
y_2 &:= \sum_{m\equiv 2 \pmod 4} \varepsilon_k = \varepsilon_9+\varepsilon_{15}+\varepsilon_8+\varepsilon_2 = 2(\cos(8\alpha)+\cos(2\alpha)) \ , \\
y_3 &:= \sum_{m\equiv 1 \pmod 4} \varepsilon_k = \varepsilon_3+\varepsilon_5+\varepsilon_{14}+\varepsilon_{12} = 2(\cos(3\alpha)+\cos(5\alpha)) \ \text{ and} \\
y_4 &:= \sum_{m\equiv 3 \pmod 4} \varepsilon_k = \varepsilon_{10}+\varepsilon_{11}+\varepsilon_7+\varepsilon_6 = 2(\cos(7\alpha)+\cos(6\alpha)) \ .
\end{aligned}$$

Clearly, $y_1+y_2=x_1$. By (id.),

$$y_1y_2 = 2\sum_{r\in\{9,3,12,6\}}\cos(r\alpha)+2\sum_{r\in\{7,1,4,2\}}\cos(r\alpha) = 2\sum_{r=1}^{8}\cos(r\alpha) = -1 \ .$$

Thus y_1 and y_2 are the roots of y^2-x_1y-1. It is clear that $y_1>y_2$ because cos decreases on $[0,\pi]$. Similarly, $y_3+y_4=x_2$,

$$y_3y_4 = 2\sum_{r\in\{10,9,12,11\}}\cos(r\alpha)+2\sum_{r\in\{4,3,2,1\}}\cos(r\alpha) = 2\sum_{r=1}^{8}\cos(r\alpha) = -1 \ ,$$

y_3 and y_4 are the roots of y^2-x_2y-1 and $y_3>y_4$.

Finally, $z_1+z_2=y_1$ and (by (id.)) $z_1z_2 = 4\cos\alpha\cos(4\alpha) = 2\cos(5\alpha)+2\cos(3\alpha)=y_3$. Thus z_1 and z_2 are the roots of $z^2-y_1z+y_3$. It is clear that $z_1>z_2$. □

The previous proof and the proof of Proposition 4.1 are taken from the classical book [11] by G. H. Hardy and E. M. Wright. They mention the explicit formula

$$\begin{aligned}
z_1 = 2\cos(2\pi/17) &= \frac{1}{8}\Big(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\Big)+ \\
&+\frac{1}{8}\sqrt{68+12\sqrt{17}-16\sqrt{34+2\sqrt{17}}-2(1-\sqrt{17})\sqrt{34-2\sqrt{17}}} \ .
\end{aligned}$$

The third detour concerns irreducibility of the polynomial $p(x)=1+x+x^2+\cdots+x^{16}$ in $\mathbb{Z}[x]$. We prove more generally that every polynomial $\frac{x^p-1}{x-1} = 1+x+\cdots+x^{p-1}$ is irreducible in $\mathbb{Z}[x]$.

Theorem 4.4 (Eisenstein's). *Every integral polynomial*

$$a(x) := a_nx^n+\cdots+a_1x+a_0, \ n\in\mathbb{N} \ ,$$

such that for some prime p the coefficient a_n is not divisible by p, each of the coefficients $a_{n-1},\ldots,a_1,a_0$ is divisible by p and the coefficient a_0 is not divisible by p^2 is irreducible in $\mathbb{Z}[x]$.

Proof. Suppose for contradiction that $a(x)$ is as stated and

$$a(x) = \sum_{i=0}^{n} a_i x^i = \sum_{j=0}^{k} b_j x^j \cdot \sum_{j=0}^{l} c_j x^j =: b(x) \cdot c(x)$$

for some $b_j, c_j \in \mathbb{Z}$ and $k, l \in \mathbb{N}$ with $b_k c_l \neq 0$. Reducing this equality modulo p we see that $b(x)$ (resp. $c(x)$) has a unique coefficient not divisible by p, namely b_k (resp. c_l). This follows from the fact that (coefficient-wise) reduction modulo p is a ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}_p[x]$. But then $a_0 = b_0 c_0$ is divisible by p^2, contrary to the assumption. □

Corollary 4.5 (on $\frac{x^p-1}{x-1}$). *For every prime number p, the polynomial*

$$a(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$$

is irreducible in $\mathbb{Z}[x]$.

Proof. Let p be a prime number. To make Eisenstein's theorem applicable to $a(x)$ we change the variable by setting $x := y + 1$. It is easy to check that the new polynomial

$$b(y) := a(y+1) = \frac{(y+1)^p - 1}{(y+1) - 1} = \sum_{j=1}^{p} \binom{p}{j} y^{j-1} \in \mathbb{Z}[y]$$

satisfies for the prime p the hypothesis of Theorem 4.4. Therefore $b(y)$ is irreducible in $\mathbb{Z}[y]$ and $a(x)$ is irreducible in $\mathbb{Z}[x]$. □

Chapter 5

Lecture 5. Non-commutativity: Wedderburn's theorem and Alimov's theorem

The 4th application of roots of unity: Wedderburn's theorem

(November 11, 2021) The most famous result in algebra on non-existence of an algebraic structure is the *Feit–Thompson theorem* [8]:

No finite non-commutative simple group G with odd order exists.

Explicitly, in set-theoretic terms, the theorem says the following. There does not exist any triple

$$G = (G, 1_G, \cdot_G)$$

of a set G, its element $1_G \in G$ and a map (an operation on G)

$$\cdot_G \colon G \times G \to G$$

such that

1. G is finite and has cardinality $|G| \equiv 1 \pmod 2$,
2. 1_G is the neutral element of the operation: $1_G \cdot_G g = g \cdot_G 1_G = g$ for every $g \in G$,
3. the operation is associative: $(g \cdot_G h) \cdot_G i = g \cdot_G (h \cdot_G i)$ for every $g, h, i \in G$,
4. every element $g \in G$ has an inverse $h \in G$ in the operation: $g \cdot_G h = h \cdot_G g = 1_G$,

5. there exist two elements $g, h \in G$ such that $g \cdot_G h \neq h \cdot_G g$ and

6. G has no nontrivial normal subgroup.

Property 5 accounts for non-commutativity of G and property 6 for its "simplicity". We review definition of normal subgroups and do it for any group, that is, any triple $G = (G, 1_G, \cdot_G)$ with properties 2–4. A subset $H \subset G$ is a *normal subgroup of* G if $1_G \in H$, the set H is closed to $\cdot_G$ and to taking inverses, and for every $g \in G$ one has that

$$\{g \cdot_G h \mid h \in H\} =: gH = Hg := \{h \cdot_G g \mid h \in H\}.$$

For example, $H = \{1_G\}$ and $H = G$ are always normal subgroups of G. These are the *trivial normal subgroups*, any other normal subgroup of G is *nontrivial*. We call a group *simple* if it has no nontrivial normal subroup.

The Feit–Thompson theorem says that the above properties 1–6 of a triple $(G, 1_G, \cdot_G)$ are altogether contradictory and no triple satisfying them simultaneously can exist. In [8] it takes over 250 pages to bring the conjunction of properties 1–6 to contradiction. Fortunately, thanks to formalized mathematics and to (a team led by) G. Gonthier [10], nowadays (unlike, say, in 1963 or in 2010) we possess absolute certainty that the Feit–Thompson theorem holds and that its proof is correct.

Unfortunately, in the case of the *Wiles–Taylor theorem* [27, 28] (earlier, as a conjecture, called FLT)

$$\textit{No quadruple } x, y, z, n \in \mathbb{N} \textit{ exists such that } x^n + y^n = z^n \textit{ and } n \geq 3.$$

we are not yet in this desirable state, no formalization of it is (as far as I know) in sight. Note that the two articles [27, 28] comprise together of 129 pages, which amount to about a half of [8]. I think that until a proof of the Wiles–Taylor theorem is formalized, we cannot be completely sure of its correctness. Certainly not with the degree of certainty comparable to that we enjoy with regard to the Feit–Thompson theorem. I know that not everybody shares this opinion ([12]).

But let us proceed to the main topic of today's lecture, which is another result on non-existence of a non-commutative algebraic structure. A *skew field* K is a quintuple

$$K = (K, 0_K, 1_K, +_K, \cdot_K)$$

of a set K, its two distinct elements $0_K, 1_K \in K$ and two operations $+_K$ and $\cdot_K$ on K such that

SF1 0_K (resp. 1_K) is the neutral element of $+_K$ (resp. of $\cdot_K$),

SF2 both operations are associative and $+_K$ is commutative,

SF3 $\forall x \in K$ (resp. $\forall x \in K \setminus \{0_K\}$) $\exists y \in K$ such that $x + y := x +_K y = 0_K$ (resp. $xy := x \cdot_K y = yx = 1_G$),

SF4 $\forall\, x, y, z \in K:\ x(y+z) = (xy) + (yz) =: xy + xz$ and $(y+z)x =: yx + zx$ and

SF5 $\exists\, x, y \in K:\ xy \neq yx$.

The additive (resp. multiplicative) inverse y in axiom SF3 is denoted, as usual, by $-x$ (resp. by x^{-1}). A skew field K is (in)finite if the underlying set K is (in)finite. Infinite skew fields exist: an example are *rational quaternions*

$$Q = (Q,\, 0,\, 1,\, +,\, \cdot) \ \text{ with } \ Q = \{a + bi + cj + dk \mid a,\, b,\, c,\, d \in \mathbb{Q}\}\ ,$$

where $i, j, k \in Q$ (we identify i with $0 + 1i + 0j + 0k$ etc.) are three distinct *imaginary units*, $0 := 0+0i+0j+0k$, $1 := 1+0i+0j+0k$, $+$ is coordinate-wise addition in $\mathbb{Q}^4$, and $\cdot$ is defined via both distributive laws in axiom SF4 and via the products of the imaginary units ($i^2 = ii$ etc.)

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i \ \text{ and } \ ik = -j\ .$$

One can check that Q is a skew field. However, finite skew fields — unlike finite fields where axiom SF5 is replaced with commutativity of $\cdot_K$ — do not exist. We begin the proof of this fact with a lemma on divisibility in $\mathbb{Z}$.

Lemma 5.1. *Let $m, n, q \in \mathbb{N}$ with $q \geq 2$ be such that $q^m - 1 \,|\, q^n - 1$. Then in fact $m \,|\, n$.*

Proof. Let $m, n, q \in \mathbb{N}$ be as stated. We divide n by m with remainder:

$$n = ma + b \ \text{ where } \ a,\, b \in \mathbb{N}_0 \wedge 0 \leq b < m\ .$$

Since $q^m - 1$ divides $q^n - 1 = q^n - q^m + q^m - 1 = q^m(q^{n-m} - 1) + q^m - 1$, it follows that $q^m - 1$ divides $q^{n-m} - 1$. Iterating this a times we get that $q^m - 1$ divides $q^b - 1$. Thus $b = 0$ and m divides n. □

Now we prove the promised theorem on nonexistence of finite skew fields.

Theorem 5.2 (Wedderburn's). *No finite skew field K exists.*

Proof. Let K be a finite skew field. We deduce a contradiction (no worry, in much less than 250 pages). We set $K^\times := K \setminus \{0_K\}$, and similarly for other subsets of K. It is not hard to see that the *conjugation relation* $\sim$ on $K^\times$, given by

$$x \sim y \iff \exists\, s \in K^\times:\ s^{-1}xs = y\ ,$$

is an equivalence relation (i.e., is reflexive, symmetric and transitive). For any $x \in K^\times$ we define its *conjugation class*

$$A_x := \{y \in K^\times \mid x \sim y\}\ .$$

Since $\sim$ is an equivalence, these sets form a partition of $K^\times$: they are nonempty ($x \in A_x$), their union is $K^\times$ and any two of them either coincide or are disjoint.

We call A_x *nontrivial* if $|A_x| \geq 2$, and *trivial* if $A_x = \{x\}$. It follows from axiom SF5 that there is at least one nontrivial conjugation class.

For any $x \in K$ we define its *centralizer*

$$C_x := \{y \in K \mid xy = yx\} .$$

We show that for any $x \in K^\times$,

$$|K^\times| = |C_x^\times| \cdot |A_x| . \tag{c}$$

For any fixed $x \in K^\times$ we consider the surjective map

$$f\colon K^\times \to A_x,\ f(s) = s^{-1}xs .$$

We fix an $s \in K^\times$ and count the $s_1 \in K^\times$ such that $f(s_1) = f(s)$. This equality means that

$$s_1^{-1}xs_1 = s^{-1}xs \iff xs_1s^{-1} = s_1s^{-1}x \iff s_1s^{-1} \in C_x^\times \iff s_1 \in C_x^\times s ,$$

where $C_x^\times s := \{ys \mid y \in C_x^\times\}$. It is easy to see that $|C_x^\times s| = |C_x^\times|$. Thus f always maps $|C_x^\times|$ elements to a single element, and we get equation (c).

We define the *center* of K as

$$Z := \{x \in K \mid \forall\, y \in K :\ xy = yx\} .$$

We have that $q := |Z| \geq 2$ because $0_K, 1_K \in Z$. It is easy to see that Z is closed to both operations $+_K$ and $\cdot_K$ and to taking both inverses to its elements. Hence

$$Z = (Z,\, 0_K,\, 1_K,\, +_K,\, \cdot_K)$$

is a (commutative!) field.

The key insight of the proof is that

K and every centralizer C_x is a (finite) vector space over the field Z .

The addition of vectors is just $+_K$, and multiplication by a scalar in Z is via $\cdot_K$. It is easy to see that every centralizer C_x is closed to these operations. By the elementary linear algebra,

$$|K| = q^n \ \text{ and } \ |C_x| = q^{n_x} , \tag{d}$$

where $n \in \mathbb{N}$ (resp. $n_x \in \mathbb{N}$) is the dimension of the vector space K (resp. C_x) over Z. Axiom SF5 implies that $K \neq Z$ and thus $n \geq 2$.

Let $A_{x_1}, A_{x_2}, \ldots, A_{x_t}$, where $t \in \mathbb{N}$, be the list of all nontrivial conjugation classes. Note that the union of the remaining trivial conjugation classes is exactly $Z^\times$. Thus we have the partition

$$K^\times = Z^\times \cup \bigcup_{i=1}^{t} A_{x_i} .$$

From it we get by equations (c) and (d) the equality

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1} \ ,$$

where n_i is the dimension of the vector space C_{x_i} over Z. For any $i = 1, 2, \ldots, t$ we have that $q^{n_i} - 1 \,|\, q^n - 1$ and that $n_i < n$ (since $|A_{x_i}| \geq 2$). By Lemma 5.1, each n_i divides n.

Now comes the time of cyclotomic polynomials $\Phi_d(x)$. We use the factorization

$$x^m - 1 = \prod_{d \,|\, m} \Phi_d(x) \ .$$

Thus we transform the above equality to

$$\prod_{d \,|\, n} \Phi_d(q) = q - 1 + \sum_{i=1}^{t} \frac{\prod_{d \,|\, n} \Phi_d(q)}{\prod_{e \,|\, n_i} \Phi_e(q)} \ .$$

Since every cyclotomic polynomial is integral (Lemma 3.2), all $\Phi_d(q), \Phi_e(q) \in \mathbb{Z}$. Since $n_i \,|\, n$ and $n_i < n$, every number $\Phi_e(q)$ in the denominator of the fraction appears in the product in the numerator, but differs from $\Phi_n(q)$. It follows that $\Phi_n(q) \in \mathbb{Z}$ divides $q - 1$. But this is impossible because

$$|\Phi_n(q)| = \prod_{\alpha \in \mathrm{PRU}_n} |q - \alpha| > \prod_{\alpha \in \mathrm{PRU}_n} (q - 1) = (q - 1)^{\varphi(n)} \geq q - 1 \ .$$

The crucial strict inequality follows from the facts that $q \geq 2$ and that $n \geq 2$ (so always $\alpha \neq 1$). We have a contradiction (after 2 pages). □

Alimov's theorem: commutativity and infinitesimals

One of the simplest frameworks where one can talk about *infinitesimals*, positive quantities q that are infinitely close to 0 (so that $0 < q < 1/n$ for every $n \in \mathbb{N}$), are *ordered semigroups* $A = (A, +, <)$. Here A is a set, $+$ is an associative (but not necessarily commutative) operation on A and $<$ is a strict linear order on A such that $+$ is monotonous with respect to it. In more details, $< \subset A \times A$ is a transitive and irreflexive relation on A and for any $a, b, c \in A$ we have that

$$a < b \Rightarrow a + c < b + c \wedge c + a < c + b \ .$$

An *anomalous pair* $a, b \in A$ (necessarily $a \neq b$) in an ordered semigroup A satisfies

$$\forall\, n \in \mathbb{N} : \ na < nb < (n+1)a \ \text{ or } \ \forall\, n \in \mathbb{N} : \ na > nb > (n+1)a \ ,$$

where

$$na := \underbrace{a + a + \cdots + a}_{n \text{ summands}} \ .$$

One can view it so that the distinct elements a and b are infinitely close each to the other: if the first system of inequalities holds then $(0 <)\ a < b$ but the "distance" from a to b cannot be magnified to exceed a no matter by which $n \in \mathbb{N}$ we multiply it. In a way this "distance" is positive but at the same time is infinitely close to zero. We illustrate anomalous pairs with two examples.

Example 1. Consider the ordered semigroup $((0, +\infty), +, <)$ of positive real numbers with usual addition and ordering. This semigroup is commutative and has no anomalous pair because for $0 < a < b$ one has that

$$nb > (n+1)a \ \text{ for any } \ n > \frac{a}{b-a}\ ,$$

and that $na < (n+1)a$ for any n — neither the first nor the second system of inequalities can hold.

Example 2. Consider the ordered semigroup $(\{a, b\}^*, +, <)$ where $\{a, b\}^*$ is the set of all nonempty words over the two-element alphabet $\{a, b\}$, the operation $+$ is concatenation of words (for example, $abba + ab = abbaab$) and $<$ compares words first by their length, and for equal lengths lexicographicly with $a < b$ (for example, $bbab < bbba$ but $bbba < bbaba$). This semigroup is not commutative (for example, $a + b \neq b + a$) and has many anomalous pairs, for instance

$$a < b < aa < bb < aaa < bbb < aaaa < \dots\ .$$

Interestingly, non-commutativity forces appearance of anomalous pairs (infinitesimals):

Theorem 5.3 (Alimov's). *Any ordered semigroup A without anomalous pairs is commutative.*

We prove the theorem next time.

Chapter 6

Lecture 6. Proof of Alimov's theorem. The Chevalley–Warning theorem

(November 18, 2021) In fact, no student appeared. Here is what I prepared for the lecture.

We prove Alimov's theorem that if the ordered semigroup $A = (A, +, <)$ has no anomalous pair, i.e., no pair of elements $a, b \in A$ such that

$$\forall\, n \in \mathbb{N}:\ na < nb < (n+1)a \ \text{ or } \ \forall\, n \in \mathbb{N}:\ na > nb > (n+1)a\ ,$$

then A is commutative, $a + b = b + a$ for any $a, b \in A$.

Since $+$ is monotonous with respect to $<$ and $<$ is trichotomic, in A we have the *cancellation law*

$$\forall\, a,\, b,\, c \in A:\ a + c < b + c \Rightarrow a < b\ ,$$

and the same holds when c is added from the left and/or $<$ is replaced with $=$.

Let $a, b \in A$ be arbitrary. Then exactly one of $b + a > b$, $b + a = b$ and $b + a < b$ holds. In the first case associativity and monotonicity of $+$ and the cancellation law give that

$$\forall\, c \in A:\ b + (a + c) \overset{\text{asoc.}}{=} (b + a) + c \overset{\text{monot.}}{>} b + c \overset{\text{canc.}}{\rightsquigarrow} \forall\, c \in A:\ a + c > c\ .$$

In the 2nd, resp. the 3rd, case we similarly get that

$$\forall\, c \in A:\ a + c = c, \ \text{ resp. } \ \forall\, c \in A:\ a + c < c\ .$$

Thus for any $a \in A$ exactly one of the following three cases occurs:

$$\underbrace{\forall\, c \in A:\ a + c > c}_{a \text{ is ``positive''}}, \ \underbrace{\forall\, c \in A:\ a + c = c}_{a \text{ is a ``zero element''}} \ \text{ and } \ \underbrace{\forall\, c \in A:\ a + c < c}_{a \text{ is ``negative''}}\ .$$

So A is partitioned in positive, zero and negative elements; each of these classes may be empty. In the three above formulas we add a from the left, but the same partition of A results from adding a from the right. For example, if a is positive, then for the same b as above we have $a+b>b$ and

$$\forall\, c\in A:\ (c+a)+b=c+(a+b)>c+b\rightsquigarrow\forall\, c\in A:\ c+a>c\ .$$

Similarly for zero and negative elements.

In particular, if $a,b\in A$ are zero elements then $a+b=a$ and $a+b=b$, hence $a=b$. Thus A has at most one zero element, which will be denoted as 0. We may assume that $0\in A$ exists; if not we simply add 0 to A and define $0+a=a+0:=a$ for any $a\in A$ and $a>0$ (resp. $a<0$) for any positive (resp. negative) $a\in A$. Using 0 we may equivalently define the positive, zero and negative elements of A as, respectively,

$$\{a\in A\mid a>0\},\ \{a\in A\mid a=0\}\ \text{ and }\ \{a\in A\mid a<0\}\ .$$

Indeed, if a is in the first set then, by monotonicity of $+$, $a+c>c$ for any c and a is positive. If a is positive then in particular $a=a+0>0$. Similarly in the other two cases.

We start the proof of Alimov's theorem proper. We assume that there is no anomalous pair in A and show that

$$\forall\, a,\, b\in A:\ a+b=b+a\ .$$

If $a=0$ or $b=0$ then it certainly holds. Thus we need to distinguish only three cases, according to whether a and b are positive or negative.

(i) $a,b>0$. We show that if $a+b\neq b+a$ then $a+b, b+a$ is an anomalous pair. Indeed if, say, $a+b<b+a$ then for any $n\in\mathbb{N}$ we have that

$$(n+1)(a+b)\overset{\text{asoc.}}{=}a+n(b+a)+b\overset{a>0}{>}n(b+a)+b\overset{b>0}{>}n(b+a)\overset{\text{L}}{>}n(a+b)\ ,$$

so $n+1)(a+b)>n(b+a)>n(a+b)$. We used lemma L:

$$r,\, s,\, t,\, u\in A,\, r<s,\, t<u\Rightarrow r+t<s+u\ .$$

Thus $a+b=b+a$.

(ii) $a,b<0$. We proceed as in the previous case; we only start with $a+b>b+a$ and revert the inequalities in the previous computation.

(iii) $a<0<b$. Now we have three sub-cases.

(a) $a+b=0$. By associativity of $+$,

$$a+(b+a)=(a+b)+a=0+a=a+0\overset{\text{canc.}}{\rightsquigarrow}b+a=0$$

and $a+b=b+a=0$.

(b) $a+b>0$. Also $b>0$. For $a+b\neq b+a$, say $a+b<b+a$, we get the contradiction

$$\begin{aligned}2(b+a)&\overset{\text{asoc.}}{=}(b+(a+b))+a\overset{\text{case (i) for } b,\ a+b}{=}((a+b)+b)+a\\&\overset{\text{asoc.}}{=}(a+b)+(b+a)\overset{\text{monot.}}{<}(b+a)+(b+a)\\&=2(b+a)\ .\end{aligned}$$

For $a+b > b+a$ we get a similar contradiction, only the last inequality is reverted. Thus $a+b = b+a$.

(c) $a+b < 0$. Also $a < 0$. For $a+b \neq b+a$, say $a+b < b+a$, we get the same contradiction

$$\begin{aligned} 2(b+a) &\overset{\text{asoc.}}{=} b+((a+b)+a) \overset{\text{case (ii) for } a,\ a+b}{=} b+(a+(a+b)) \\ &\overset{\text{asoc.}}{=} (b+a)+(a+b) \overset{\text{monot.}}{<} (b+a)+(b+a) \\ &= 2(b+a)\ . \end{aligned}$$

Similarly for $a+b > b+a$. Again $a+b = b+a$. □

This proof is taken from [1]. Who was N. G. Alimov? In [1] we read that the paper was received on March 8, 1949, and that it was presented by the member of the Academy of Sciences A. N. Kolmogorov, but there is no address or affiliation of the author. I found the anonymous document [13] in Russian, with the head "Department of mathematical analysis". It describes the history of the Department, a part of the Faculty of Physics and Mathematics (which was founded, as we read at the start, on July 1, 1917) of Tomsk State University. The section "They were the first" mentions on p. 6 Nikolai Grigor'evich Alimov who almost surely was N. G. Alimov of [1]. We read, for example, that he was born on April 2, 1900, started to work in Tomsk State University as a docent since 1934 (more precisely and significantly, "he was fulfilling duties of a docent"), that since 1938 he worked in the Department as a senior lecturer and that in 1939 he left the Department as he was transferred to the Pedagogical Institute in Yaroslavl. At this point [13] leaves him; the date of his death is not given. His another publication referenced in *Mathematical Reviews* is [2].

The Chevalley–Warning theorem

Lemma 6.1 *If F is a finite field and $n \in \mathbb{N}$ is not divisible by $|F|-1$ or $n = 0$ (and $0_F^0 := 1_F$), then*

$$\sum_{a \in F} a^n = 0_F\ .$$

Proof. For $n = 0$ the result holds, the sum then equals $|F|_F = 0_F$ (see the notation in the next proof) because the characteristic p of F divides $|F|$.

We assume that $n > 0$ and is not divisible by $|F|-1$. It is true that the multiplicative group $F^\times = (F^\times, 1_F, \cdot)$ of F is cyclic (we proved it only for $F = \mathbb{Z}_p$) and thus any generator $g \in F^\times$ of this group has the property that $g^n \neq 1_F$. But then from the equation

$$\sum_{a \in F} a^n = \sum_{a \in F} (ga)^n = g^n \sum_{a \in F} a^n$$

it follows that the sum has to be 0_F. □

Theorem 6.2 (Chevalley–Warning) *Let p be a prime number, $m, n \in \mathbb{N}$, F be a finite field with characteristic p and $P_1, \ldots, P_m \in F[x_1, \ldots, x_n]$ be nonzero polynomials such that*

$$\sum_{i=1}^{m} \deg P_i < n \, .$$

Then

$$N := |\{\overline{x} := (x_1, \ldots, x_n) \in F^n \mid P_1(\overline{x}) = \cdots = P_m(\overline{x}) = 0_F\}| \equiv 0 \pmod{p} \, .$$

In particular, if each polynomial P_i has zero constant term then $N \geq 2$ and the system

$$P_1(\overline{x}) = \cdots = P_m(\overline{x}) = 0_F$$

has a non-trivial (non-zero) solution.

Proof. For $k \in \mathbb{N}_0$ we denote by $k_F \in F$ the element of the field obtained as

$$k_F := \underbrace{1_F + 1_F + \cdots + 1_F}_{k \text{ summands}} \, .$$

It is clear that $k_F = 0_F$ iff $k \equiv 0$ modulo p. We see that

$$E := \sum_{\overline{x} \in F^n} \prod_{i=1}^{m} \left(1_F - P_i(\overline{x})^{|F|-1}\right) = N_F$$

because $P_i(\overline{x})^{|F|-1} \in \{0_F, 1_F\}$ and vanishes iff $P_i(\overline{x}) = 0_F$. It suffices to show that the expression E on the left-hand side vanishes, equals 0_F. By expanding the $|F|-1$-th powers, multiplying out and regrouping the summands, we write it as (we set $D := (|F|-1)\sum_{i=1}^{m} \deg P_i$)

$$E = \sum_{\substack{\overline{k} \in \mathbb{N}_0^n \\ k_1 + \cdots + k_n \leq D}} c(\overline{k}) \prod_{i=1}^{n} \sum_{x_i \in F} x_i^{k_i} \, ,$$

where $c(\overline{k}) \in F$ and D is an upper bound on the degrees of monomials in E. By the assumption, $D < (|F|-1)n$. Thus for every $\overline{k}$ in the sum there is an $i \in [n]$ such that $0 \leq k_i < |F| - 1$. By the previous lemma, the corresponding inner sum is 0_F and so $E = 0_F$.

The second claim follows from the fact that if every P_i has zero constant term, then the system has always the trivial zero solution and thus it has at least $p \geq 2$ solutions. □

Corollary 6.3 (on multigraphs) *Every loop-less multigraph M that is obtained from a 4-regular multigraph (a multigraph where every vertex is incident with four edges) by adding one edge contains a non-empty 3-regular submultigraph.*

Proof. Let $M = (V, E)$ be the described multigraph. We associate with it the polynomial system of $|V|$ quadratic equations over $F := \mathbb{Z}_3$:

$$\sum_{e \in E} a(e,\, v) \cdot x_e^2 = 0_F,\ v \in V\ ,$$

where the x_e are $|E|$ unknowns and the coefficient $a(e, v) \in \{0_F, 1_F\}$, with $a(e, v) = 1_F$ iff $v \in e$. The condition on degrees of equations in the previous theorem is satisfied because

$$|E| = 1 + 4|V|/2 = 1 + 2|V| > 2|V|\ .$$

By the theorem there exist $y_e \in F$, $e \in E$, which are not all zero and solve the system. Let $E' := \{e \in E \mid y_e \neq 0_F\}$. Then $E' \neq \emptyset$ and if we set

$$V' := \bigcup E' \subset V\ ,$$

also $V' \neq \emptyset$. We claim that the submultigraph $M' := (V', E')$ of $M = (V, E)$ is 3-regular. Indeed, for any vertex $v \in V'$ we have that (by $\deg_{M'}(v)$ we denote the number of edges in M' incident with the vertex v)

$$(\deg_{M'}(v))_F = \sum_{e \in E'} a(e,\, v) = \sum_{e \in E} a(e,\, v) \cdot y_e^2 = 0_F$$

because $y_e^2 = 1_F$ for $y_e \neq 0_F$, and of course $y_e^2 = 0_F$ for $y_e = 0_F$. So $\deg_{M'}(v)$ is divisible by 3 and because it lies in the set $\{1, 2, 3, 4, 5\}$, it equals 3. □

Chapter 7

N. Alon's Combinatorial Nullstellensatz

A monomial (or a term) $cx_1^{k_1} \dots x_n^{k_n}$ in a non-zero polynomial $f \in F[x_1, \dots, x_n]$ is a *maximal monomial* if $c \neq 0_F$ and $k_1 + \dots + k_n = \deg f$.

Theorem 7.1 (N. Alon) *Let F be an integral domain, $n \in \mathbb{N}$,*

$$f \in F[x_1, \dots, x_n]$$

be a nonzero polynomial and let $cx_1^{k_1} \dots x_n^{k_n}$ be a maximal monomial in f. Then for every n-tuple of sets $A_i \subset F$ with $|A_i| > k_i$ there exist elements $a_i \in A_i$ such that

$$f(a_1, \dots, a_n) \neq 0_F \, .$$

Proof. We proceed by induction on $\deg f \in \mathbb{N}_0$. For $\deg f = 0$, so $f = c \in F^\times$, the claim holds trivially: $k_1 = \dots = k_n = 0$, the $A_i \neq \emptyset$ and f has the only value $c \neq 0_F$.

Let $d := \deg f > 0$, $cx_1^{k_1} \dots x_n^{k_n}$ be a maximal monomial in f and let $A_i \subset F$ be n sets with $|A_i| > k_i$ elements. We may assume that $k_1 > 0$. We take any element $a_1 \in A_1$ and express f as

$$f(x_1, \dots, x_n) = (x_1 - a_1) \cdot g(x_1, \dots, x_n) + h(x_2, \dots, x_n) \, .$$

This identity was obtained by dividing the polynomial $f \in F[x_2, \dots, x_n][x_1] =: G[x_1]$ by the polynomial $x_1 - a_1$. So $g \in G[x_1]$, $\deg g = d - 1$,

$$cx_1^{k_1 - 1} x_2^{k_2} \dots x_n^{k_n}$$

is a maximal monomial in g and h is a constant polynomial in $G[x_1]$, i.e., $h \in G = F[x_2, \dots, x_n]$.

If $h(a_2, \dots, a_n) \neq 0_F$ for some elements $a_2 \in A_2, \dots, a_n \in A_n$ then

$$f(a_1, a_2, , \dots, , a_n) = (a_1 - a_1) \cdot g(a_1, \dots, a_n) + h(a_2, \dots, a_n) \neq 0_F$$

and we are done.

Else, if $h(a_2, \ldots, a_n) = 0_F$ for any choice of elements $a_2 \in A_2, \ldots, a_n \in A_n$, we apply to g (and the sets $A_1 \setminus \{a_1\}$, A_2, $\ldots$, A_n and the displayed maximal monomial in g) the inductive assumption, pick appropriate elements $a \in A_1$, $a \neq a_1$, $a_2 \in A_2$, $\ldots$, $a_n \in A_n$ such that $g(a, a_2, \ldots, a_n) \neq 0_F$ and get again that

$$f(a, a_2, , \ldots, , a_n) = (a - a_1) \cdot g(a, a_2, \ldots, a_n) + h(a_2, \ldots, a_n) \neq 0_F \ .$$

□

Corollary 7.2 (on hyperplanes) *In $\mathbb{R}^n$, it is not possible to cover all vertices of the (discrete) cube $\{0,1\}^n$ but one with less than n hyperplanes.*

Proof. Suppose for the contrary that $H_i \subset \mathbb{R}^n$, $i = 1, \ldots, m$, $m < n$, are m hyperplanes in $\mathbb{R}^n$ such that they cover all vertices of the cube but the origin $(0, \ldots, 0)$. Thus they have equations

$$p_i(x_1, \ldots, x_n) = \alpha_{i,1}x_1 + \cdots + \alpha_{i,n}x_n + \beta_i, \ i \in [m] \ ,$$

where every $\beta_i \neq 0$ and for every $\overline{v} \in \{0,1\}^n \setminus \{(0, \ldots, 0)\}$ there is an $i \in [m]$ such that $p_i(\overline{v}) = 0$. We consider the polynomial

$$f(x_1, \ldots, x_n) := \prod_{i=1}^{m} \beta_i \cdot (1 - x_1) \ldots (1 - x_n) - \prod_{i=1}^{m} p_i(x_1, \ldots, x_n) \ .$$

Since $m < n$, it has degree n and has the maximal monomial

$$(-1)^n \beta_1 \ldots \beta_m \, x_1 \ldots x_n \ .$$

By our assumptions, $f(\overline{v}) = 0$ for every $\overline{v} \in \{0,1\}^n$. But the previous theorem, applied to f and to the sets $A_1 = \cdots = A_n = \{0,1\}$, gives us a $\overline{v} \in \{0,1\}^n$ such that $f(\overline{v}) \neq 0$. We got a contradiction. □

Bibliography

[1] N. G. Alimov, Ob uporyadochennyx polugruppax, *Izvestiya Akademii Nauk SSSR, Ser. Matem.*, **14** (1950), 569–576 (in Russian, title: On ordered semigroups).

[2] N. G. Alimov, Quantity and ratio in Euclid. (Russian), *Istor.-Mat. Issled.*, **8** (1955), 573–619.

[3] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, Cambridge, UK, 2006.

[4] H. Darmon and A. Granville, On the equation $z^m = F(x, y)$ and $Ax^p + by^q = Cz^r$, *Bull. London Math. Soc*, **27** (1995), 513–543.

[5] J. M. De Koninck and F. Luca, *Analytic Number Theory*, American Mathematical Society, Providence, RI, 2012.

[6] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Inventiones Mathematicae*, **73** (1983), 349–366 (in German, title: Finiteness theorems for abelian varieties over number fields).

[7] G. Faltings, Erratum: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Inventiones Mathematicae*, **75** (1984), 381 (in German).

[8] W. Feit and J. G. Thompson, Solvability of groups of odd order, *Pacific J. of Math.*, **13** (1963), 775–1029.

[9] Fermat number, Wikipedia article, `https://en.wikipedia.org/wiki/Fermat_number#Primality_of_Fermat_numbers`.

[10] G. Gonthier, A. Asperti, J. Avigad, Y. Bertot, C. Cohen, F. Garillot, S. Le Roux, A. Mahboubi, R. O'Connor, S. Ould Biha, I. Pasca, L. Rideau, A. Solovyev, E. Tassi and L. Théry, A Machine-Checked Proof of the Odd Order Theorem, *Interactive Theorem Proving. 4th International Conference, ITP 2013, Rennes, France, July 22–26, 2013. Proceedings*, 163–179.

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 1978 (5th edition).

[12] M. Harris, Why the Proof of Fermat's Last Theorem Doesn't Need to Be Enhanced, *Quantamagazine*, June 3, 2019,
https://www.quantamagazine.org/
why-the-proof-of-fermats-last-theorem-doesnt-need-to-be-enhanced-20190603/

[13] Kafedra matematicheskogo analiza, http://math.tsu.ru/sites/default/files/mmf2/staff/kratkaya%20istoriya%20kma.pdf , 14 pp.

[14] M. Křížek, F. Luca and L. Sommer, *17 Lectures on Fermat Numbers. From Number Theory to Geometry*, Springer, New York, 2001.

[15] D. Marcus, *Number Fields*, Springer, Berlin, 1977.

[16] R. C. Mason, *Diophantine Equations over Function Fields*, London Mathematical Society Lecture Note Series, 96, Cambridge University Press, Cambridge, UK, 1984.

[17] D. W. Masser, Open problems. In: W. W. L. Chen (ed.), *Proceedings of the Symposium on Analytic Number Theory*, Imperial College, London, 1985.

[18] S. Mochizuki, Inter-universal Teichmüller theory IV: Log-volume computations and set-theoretic foundations, *Publ. Res. Inst. Math. Sci.*, **57** (2021), 627–723.

[19] S. Mochizuki, Inter-universal Teichmüller theory III: Canonical splittings of the log-theta-lattice, *Publ. Res. Inst. Math. Sci.*, **57** (2021), 403–626.

[20] S. Mochizuki, Inter-universal Teichmüller theory II: Hodge-Arakelov-theoretic evaluation, *Publ. Res. Inst. Math. Sci.*, **57** (2021), 209–401.

[21] S. Mochizuki, Inter-universal Teichmüller theory I: Construction of Hodge theaters, *Publ. Res. Inst. Math. Sci.*, **57** (2021), 3–207.

[22] W. Narkiewicz, *The Development of Prime Number Theory. From Euclid to Hardy and Littlewood*, Springer, Berlin, 2000.

[23] J. Oesterlé, Nouvelles approches du "théorème" de Fermat, *Séminaire Bourbaki*, Exposé 694, Vol. 1987/88, Astérisque **161/162** (1988), 165–186 (in French, title: New approches to the "theorem" of Fermat).

[24] A. van der Poorten, *Notes on Fermat's Last Theorem*, Wiley, New York, 1996.

[25] K. F. Roth, Rational approximations to algebraic numbers, *Mathematika*, **2** (1955) 1–20, 168.

[26] W. W. Stothers, Polynomial identities and hauptmoduln, *Quarterly J. Math. Oxford 2*, **32** (1981), 349–370.

[27] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. Math.*, **141** (1995), 553–572.

[28] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.*, **141** (1995), 443–551.

Index