Algebraic Number Theory
(lecture notes)

Martin Klazar

This course does not deal with the classical algebraic number theory, concerned with finite extensions of the field of fractions $\mathbf{Q}$ and arithmetic in them (in the past the course was oriented this way, and I was using the books of Marcus [22] and Stillwell [29]), but instead I present a variety of topics devoted to interesting number-theoretic facts obtained by *algebraic* methods. As the course developed, at the end much of it revolved around bounds on sizes on zero sets of polynomial equations and their applications. Eventually, the following topics were covered.

Contents

Notation. $|X|$ or $\#X$ denotes the cardinality of a set X. $\mathbf{N} = \{1, 2, \dots\}$ are the natural numbers; $\mathbf{N}_0 = \{0, 1, 2, \dots\}$. $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ are the integers and $\mathbf{Q}$ denotes the set of fractions (rational numbers). $\mathbf{R}$ is the set of real numbers and $\mathbf{C}$ are the complex numbers. The symbols p and q usually but not always denote prime numbers. $\mathbf{Z}_p$ is the finite field of residues modulo a prime p and $\mathbf{F}_q$ is the finite field with q elements, where q is power of a prime p. $F^\times$ refers to the set (or multiplicative group) of nonzero elements of a field F. $F[t]$ or $F[x_1, \dots, x_n]$ denotes the ring of polynomials in variable t or in n variables $x_1, \dots, x_n$, with coefficients in F; $F(t)$ or $F(x_1, \dots, x_n)$ are the fields of fractions of these rings (that is, ratios of polynomials). By (a, b) we often denote the greatest common divisor of the integers a and b; for $m \in \mathbf{N}$, $\varphi(m)$ denotes the number of $n \in \mathbf{N}$ with $n \le m$ and $(n, m) = 1$. $\Phi_n(x)$ is

the n-th cyclotomic polynomial. Two acronyms: PID stands (besides 'Pražská integrovaná doprava') for the 'principal ideal domain' — each ideal in the ring is generated by a single element — and UFD is the 'unique factorization domain' — each element in the ring has a unique, up to reordering and multiplying by units, factorization into a product of irreducible elements.

Lecture 1, October 9, 2012

The abc conjecture and the Stothers–Mason theorem

We state the famous *abc conjecture*, proposed by Oesterlé in 1988 [27] and Masser in 1985 [24]. Currently this is one of the most important open problems in number theory, which we demonstrate by deducing from it validity of *Fermat's last theorem* for all sufficiently large exponents. Then we state and prove the polynomial version of the abc conjecture, which in fact motivated it, and deduce, unconditionally, the FLT for polynomials. Finally, we prove that both the constant ε in the exponent and the dependence of the constant M on ε in the abc conjecture are necessary.

For any nonzero $n \in \mathbf{Z}$, we denote by

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

the *radical of* n, the product of all prime divisors of n. Clearly, $1 \le r(n) \le |n|$ and $r(mn^k) = r(mn)$ for any nonzero $m, n \in \mathbf{Z}$ and $k \in \mathbf{N}$.

Conjecture (the abc conjecture). *For every $\varepsilon > 0$ there is a constant $M = M(\varepsilon) > 0$ such that if $a, b, c \in \mathbf{Z}$ are coprime integers satisfying relation*

$$a + b = c \,,$$

then

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

In other words, for any $\varepsilon > 0$ only finitely many triples of coprime natural numbers a, b, c exist such that $a + b = c$ and $c > r(abc)^{1+\varepsilon}$.

Corollary (asymptotic FLT). *If the abc conjecture holds then there is an $n_0 \in \mathbf{N}$ such that the equation*

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

has no solution $x, y, z, n \in \mathbf{N}$ with $n > n_0$.

Proof. If we have a solution $x, y, z, n \in \mathbf{N}$ of the equation, the abc conjecture (with $\varepsilon = 1$) implies that

$$z^n < M \cdot r(x^n y^n z^n)^2 = M \cdot r(xyz)^2 \leq M(xyz)^2 \leq Mz^6 \ ,$$

for a constant $M > 0$, and therefore $n < (\log M / \log z) + 6 < M + 6$ (we may assume that $z \geq 3$). □

Recently (August 2012), "Shinichi Mochizuki released a paper with a serious claim to a proof of the abc conjecture. Mochizuki calls the theory on which this proof is based inter-universal Teichmüller theory (...)", see [36] and the references therein, especially [37].

If $a \in \mathbf{C}[t]$ is a nonzero polynomial then $r(a)$, the *radical number of* a, denotes the number of distinct roots of a. So, again, $r(a) \leq \deg a$ and $r(ba^n) = r(ba)$ for every $a, b \in \mathbf{C}[t]$ and $n \in \mathbf{N}$. In the ring $\mathbf{C}[t]$ we have the (formal) derivative

$$(a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0)' = n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \cdots + a_1$$

($a' = 0$ if a is constant). It is characterized by linearity, $(\alpha a + \beta b)' = \alpha a' + \beta b'$, and the Leibniz identity, $(ab)' = a'b + ab'$ ($\alpha, \beta \in \mathbf{C}$ and $a, b \in \mathbf{C}[t]$). Setting $(1/a)' = -a'/a^2$, we extend the derivative to the field $\mathbf{C}(t)$ of fractions of $\mathbf{C}[t]$. If $f = f_1 f_2 \dots f_k$, $f_i \in \mathbf{C}(t)$, the Leibniz identity implies the *logarithmic derivative identity*

$$\frac{f'}{f} = \frac{(f_1 f_2 \dots f_k)'}{f_1 f_2 \dots f_k} = \frac{f_1 f_2 \dots f_k (f_1'/f_1 + f_2'/f_2 + \cdots + f_k'/f_k)}{f_1 f_2 \dots f_k} = \sum_{i=1}^{k} \frac{f_i'}{f_i} \ .$$

It is crucial for the proof of the polynomial version of the abc conjecture.
Theorem (the abc conjecture for polynomials; the Stothers–Mason theorem). *Suppose that three polynomials $a, b, c \in \mathbf{C}[t]$ satisfy relation*

$$a + b = c \ ,$$

are coprime and not all constant. Then

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

Proof. Dividing $a + b = c$ by c ($c \neq 0$ by coprimality), setting $f = a/c$, $g = b/c$ and differentiating, we get the equations

$$f + g = 1 \ \text{ and } \ f' + g' = f \cdot \frac{f'}{f} + g \cdot \frac{g'}{g} = 0 \ ,$$

which gives

$$-\frac{f'/f}{g'/g} = \frac{b}{a} \ .$$

We split a, b, c in linear factors:

$$f = \frac{a}{c} = \frac{\alpha \prod (t-\alpha_i)^{m_i}}{\gamma \prod (t-\gamma_i)^{o_i}} \quad \text{and} \quad g = \frac{b}{c} = \frac{\beta \prod (t-\beta_i)^{n_i}}{\gamma \prod (t-\gamma_i)^{o_i}} \ ,$$

where $\alpha, \beta, \gamma \in \mathbf{C}$ are nonzero, the α_i are distinct roots of a with multiplicities $m_i \in \mathbf{N}$, and similarly for the β_i and γ_i. Expressing f'/f and g'/g by the logarithmic derivative identity mentioned above, we get

$$\frac{b}{a} = -\frac{\sum m_i/(t-\alpha_i) - \sum o_i/(t-\gamma_i)}{\sum n_i/(t-\beta_i) - \sum o_i/(t-\gamma_i)} \ .$$

If we multiply the denominator and the numerator on the right side by

$$N = \prod (t-\alpha_i) \cdot \prod (t-\beta_i) \cdot \prod (t-\gamma_i) \ ,$$

we get

$$\frac{b}{a} = -\frac{N\left(\sum m_i/(t-\alpha_i) - \sum o_i/(t-\gamma_i)\right)}{N\left(\sum n_i/(t-\beta_i) - \sum o_i/(t-\gamma_i)\right)} = \frac{Q}{P} \ ,$$

where the polynomials $P, Q \in \mathbf{C}[t]$ have degrees at most $\deg N - 1 = r(abc) - 1$. Since a, b are coprime, $\deg a \leq \deg P \leq r(abc) - 1$ and $\deg b \leq \deg Q \leq r(abc) - 1$. From $a + b = c$ we deduce that $\deg c \leq \max(\deg a, \deg b) \leq r(abc) - 1$ too. □

The theorem was obtained, independently, by Stothers [30] and Mason [23], and our proof is taken from Lang [17, p. 194] who writes that it is due to Mason. Using the theorem it is an easy matter to show that Fermat's last theorem holds for polynomials.

Corollary. *Suppose that three polynomials $a, b, c \in \mathbf{C}[t]$, not all constant, satisfy relation*

$$a^n + b^n = c^n, \ n \in \mathbf{N} \ .$$

Then $n \leq 2$.

Proof. We may assume that the polynomials a, b, c are coprime. Let $d \geq 1$ be their maximum degree. The S.–M. theorem: $nd = \max(\deg a^n, \deg b^n, \deg b^n) \leq r(a^n b^n c^n) - 1 = r(abc) - 1 \leq \deg(abc) - 1 \leq 3d - 1$. So $n \leq 2$. □

For $n = 1$, there are very many solution, and the same for $n = 2$: specializing the polynomial identity $(x^2 - y^2)^2 + (2xy)^2 = (x^2 + y^2)^2$ holding in $\mathbf{C}[x, y]$, we get many solutions (pythagorean triples) in $\mathbf{C}[t]$.

Lecture 2, October 16, 2012

As we promised, we show that in contrast with the neat polynomial version, the abc conjecture for integers can only hold if it involves an ε in the exponent and a multiplicative constant depending on ε.

Proposition. *No matter how large $M > 0$ is, there exists an $\varepsilon > 0$ and a triple a, b, c of coprime integers such that*

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

Proof. For $n = 1, 2, \ldots$ let $x_n, y_n \in \mathbf{N}$ be defined by

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

for example, $(x_1, y_1) = (3, 2)$, $(x_2, y_2) = (17, 12)$ and $(x_3, y_3) = (99, 70)$. It follows by induction that

$$x_n^2 - 2y_n^2 = 1$$

for every n; these are solutions of the Pell equation $x^2 - 2y^2 = 1$. Also, for any even $n = 2m$ we have

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

which gives that $y_n = 2x_m y_m$ and shows that if $n = 2^m$ then 2^{m+1} divides y_n. Thus setting $n = 2^m$ for $m = 1, 2, \ldots$ and

$$a = 1, \ b = 2y_n^2, \ c = x_n^2 \ ,$$

we have that $a + b = c$, a, b, c are coprime and, for any $\varepsilon > 0$,

$$\frac{\max(|a|, |b|, |c|)}{r(abc)^{1+\varepsilon}} = \frac{x_n^2}{r(x_n y_n/2^m)^{1+\varepsilon}} \geq \frac{x_n^2 2^{(1+\varepsilon)m}}{(x_n y_n)^{1+\varepsilon}} > \frac{2^m}{x_n^{2\varepsilon}} \ ,$$

which proves the claim. □

This proof is taken from de Koninck and Luca [16, Theorem 11.2]. Lang [17, p. 196] suggests a similar proof, based on the identity $(3^{2^n} - 1) + 1 = 3^{2^n}$ and the observation that the number in brackets is divisible by 2^n.

Roots of unity and cyclotomic polynomials

The next topic is applications of roots of unity to number theory; we will give four. For $m \in \mathbf{N}$, the number $\alpha \in \mathbf{C}$ is an *m-th root of* 1 *(unity)* if $\alpha^m = 1$. There are exactly m of them and they form vertices, one of them being the number 1 itself, of a regular plane m-gon inscribed in the unit circle in the complex plane centered at the origin:

$$\alpha = \exp(2\pi i k/m) = \cos(2\pi k/m) + i\sin(2\pi k/m), \ k = 1, 2, \ldots, m \ .$$

If $(k, m) = 1$, α is called a *primitive m-th root of* 1: the order of α is m as $\alpha^j \neq 1$ for any $j < m$. In general the order of an m-th root of 1 is a divisor d of m, obtained as $k/m = l/d$, $(l, d) = 1$, by bringing the fraction k/m to lowest

terms. There are exactly $\varphi(m)$ primitive m-th roots of 1. For example, if $m = p$ is a prime number then $\zeta = \exp(2\pi ik/p)$ for $k = 1, 2, \ldots, p-1$ are the $p-1$ primitive p-th roots of 1 and $1 = \exp(2\pi ip/p)$ is the only p-th root of 1 with order 1, corresponding to the divisor 1 of p.

For $n \in \mathbf{N}$, we denote the $\varphi(n)$-element set of primitive n-th roots of 1 by $\mathrm{pr}(n)$. Since the set of all n-th roots of 1 is partitioned in the sets $\mathrm{pr}(d)$ for d running over the divisors of n,

$$\{\mathrm{e}^{2\pi ik/n} \mid k = 1, 2, \ldots, n\} = \bigcup_{d \mid n} \mathrm{pr}(d) \; ,$$

comparison of cardinalities gives the identity

$$n = \sum_{d \mid n} \varphi(d) \; .$$

The n-th *cyclotomic polynomial* $\Phi_n(x) \in \mathbf{C}[x]$ is defined by

$$\Phi_n(x) = \prod_{\alpha \in \mathrm{pr}(n)} (x - \alpha) \; .$$

Thus $\deg \Phi_n = \varphi(n)$. The partition gives besides the identity also the factorization

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

Lemma. *For every $n \in \mathbf{N}$, the polynomial $\Phi_n(x)$ is monic, has integral coefficients and constant term ± 1.*

Proof. It is clear that each Φ_n is monic. We prove the other two claims by induction on n. For $n = 1$ they hold as $\Phi_1(x) = x - 1$. If $n > 1$, $m = \varphi(n)$, $\Phi_n(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ and $\Psi_n(x) = \prod_{d \mid n,\, d<n} \Phi_d(x) = x^{n-m} + b_{n-m-1}x^{n-m-1} + \cdots + b_1 x + b_0$, then by induction we have that $b_i \in \mathbf{Z}$ and $b_0 = \pm 1$. Comparison of coefficients in

$$\begin{aligned} x^n - 1 &= \prod_{d \mid n} \Phi_d(x) = \Phi_n(x)\Psi_n(x) \\ &= (x^m + \cdots + a_1 x + a_0)(x^{n-m} + \cdots + b_1 x + b_0) \end{aligned}$$

yields the system of equations

$$-1 = a_0 b_0, \; 0 = a_0 b_1 + a_1 b_0, \; \ldots \; .$$

It can be solved for each a_i in terms of the b_j, $j \le i$, and the a_k, $k < i$, with dividing only by b_0: $a_0 = 1/b_0 = \pm 1$, $a_1 = -a_0 b_1 / b_0 = \pm a_0 b_1 \in \mathbf{Z}$, $\ldots$, hence $a_i \in \mathbf{Z}$ for every i. □

Application 1: primes of the form $1 + m$, $1 + 2m$, ...

Proposition. *Let $m \in \mathbf{N}$. Then*

$$p = 1 + mn,\ n \in \mathbf{N}\ ,$$

is a prime number for infinitely many n.

Proof. First note that it suffices to exhibit just one prime number of this form. Indeed, if this prime is $p(m)$ then $p(km)$, $k = 1, 2, \ldots$, is a sequence of primes, all congruent to 1 modulo m, containing infinitely many distinct primes because $p(km) > km$ for every k.

Let $m \in \mathbf{N}$; we may assume that $m \geq 3$. We consider the two polynomials

$$\begin{aligned} f(x) &= \Phi_m(x) \ \text{ and} \\ g(x) &= \prod_{d\,|\,m,\,d<m} \Phi_d(x)\ , \ \text{ so} \\ f(x)g(x) &= x^m - 1\ . \end{aligned}$$

By the above lemma, $f(x)$ and $g(x)$ have integral coefficients. Since they have no common root (the roots of $f(x)$ are exactly the primitive m-th roots of 1 and the roots of $g(x)$ are the remaining m-th roots of 1), there exist polynomials $a, b \in \mathbf{Z}[x]$ and a number $c \in \mathbf{N}$ such that

$$a(x)f(x) + b(x)g(x) = c\ .$$

(The ring $\mathbf{Q}[x]$ is a PID and f, g are coprime in it, thus the ideal $\langle f, g\rangle = \langle 1\rangle$ and we have the Bachet identity $\alpha f + \beta g = 1$ for some $\alpha, \beta \in \mathbf{Q}[x]$. Multiplying by a common multiple of the denominators of the coefficients of $\alpha(x)$ and $\beta(x)$, we get the stated identity.) By the definition of $\Phi_m(x)$, we have $|f(x)| > 1$ for any $x \geq 2$ ($|x - \alpha| > 1$ for every $\alpha \in \mathrm{pr}(m)$ as $m > 2$). Thus there exist a prime number p dividing the integer $f(2c)$ as $|f(2c)| \geq 2$. Since $f(2c)$ divides $(2c)^m - 1$, so does p. If d is a divisor of m, smaller than m, then p does not divide $(2c)^d - 1 = \prod_{e,\,e\,|\,d} \Phi_e(2c)$, because otherwise it would divide $g(2c)$, hence (by the above identity) c and 1. Thus the multiplicative order of $2c$ modulo p is m. Little Fermat's theorem gives $(2c)^{p-1} \equiv 1$ modulo p and therefore m divides $p - 1$, and we are done. □

This proves a particular case of famous Dirichlet's theorem (1837), which asserts that for any two coprime numbers $a, m \in \mathbf{N}$ the number $a + mn$ is a prime number for infinitely many $n \in \mathbf{N}$, and is proved by analytic means. As discussed in Narkiewicz [26], the algebraic arguments probably cannot be extended to yield the general case.

Lecture 3, October 23, 2012

The previous proof is taken from Narkiewicz [26, p. ???] who took it from Wendt [34] and simplified it. (And we simplified the proof further a tiny bit: [26] considers the values $f(kc)$, $k = 1, 2, \ldots$, but this is unnecessary as $f(2c)$ always works.) In the lecture I gave a quite cumbersome presentation of the proof by means of the next result, which I keep in the lecture notes for its intrinsic interest.

Proposition. *Let $a \in \mathbf{Z}[x]$ be a nonconstant polynomial. Then infinitely many prime numbers p divide a nonzero value $a(n)$, $n \in \mathbf{N}$.*

Proof. Let $S = \{p_1, p_2, \ldots, p_r\}$ be a finite set of primes. We show that there is an $n \in \mathbf{N}$ such that $a(n) \neq 0$ and is divisible by a prime not in S.

A combinatorial argument. We consider the two sets

$$X = \{p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} \mid a_i \in \mathbf{N}_0\} \quad \text{and} \quad Y = \{|a(n)| \in \mathbf{N}\backslash\{1\} \mid n \in \mathbf{N}\} .$$

We claim that for $x \to +\infty$, denoting by $d = \deg a \geq 1$,

$$|X(x)| = |X \cap [1, x]| = O(\log^r x) \quad \text{and} \quad |Y(x)| = |Y \cap [1, x]| = \Omega(x^{1/d}) .$$

The first bound folows from the fact that for any $n \in \mathbf{N}$, $n \geq 2$, there are at most $\log x / \log 2 + 1$ powers $1, n, n^2, n^3, \ldots$ not exceeding x (and, of course, from the uniqueness of prime factorizations). The second bound follows from the facts that for each $m \in \mathbf{Z}$, the equation $a(x) = m$ has at most d solutions $x \in \mathbf{Z}$ (even in $\mathbf{C}$) and that $a(n) = O(n^d)$ for $n \in \mathbf{N}$. Thus for large x, the set $Y(x)$ is much larger than $X(x)$ and, in particular, $Y\backslash X \neq \emptyset$. So any $m \in Y\backslash X$ has the property that $m = |a(n)| \neq 0, 1$ for some $n \in \mathbf{N}$ and is divisible by a prime not in S.

An algebraic argument. Let $a(x) = a_d x^d + \cdots + a_1 x + a_0$ with $a_i \in \mathbf{Z}$, $d \geq 1$ and $a_d \neq 0$. The claim holds if $a_0 = 0$ because then n divides $a(n)$ for every $n \in \mathbf{N}$. Thus we assume $a_0 \neq 0$. We set $m = p_1 p_2 \ldots p_r$ and for $k = 1, 2, \ldots$ have

$$a(kma_0) = \sum_{i=0}^{d} a_i (kma_0)^i = a_0 \left(1 + \sum_{i=1}^{d} a_i (km)^i a_0^{i-1} \right) .$$

For any k, the integer in brackets is 1 modulo m and, if distinct from ± 1, it is divisible by a prime not in S and so is $a(kma_0)$. As we know, $a(n) = b$ has at most $\deg a = d$ solutions $n \in \mathbf{Z}$, and so we may select a $k \in \mathbf{N}$ with $a(kma_0) \neq 0, \pm a_0$; the value $a(kma_0)$ has then the required properties. □

The combinatorial argument reveals that polynomiality of the function

$$a : \mathbf{N} \to \mathbf{Z}$$

is in fact irrelevant for the result; what only matters is the degree of its non-injectivity and its growth. For example, by the combinatorial argument, the proposition holds for any strictly increasing function $a(x)$ such that $a(x) = O(x^c)$ as $x \to +\infty$, with a constant $c > 0$. See Elsholtz [10] for such results.

But the algebraic argument has its merit too. It is easy to come up with functions $a : \mathbf{N} \to \mathbf{Z}$ growing too quickly to satisfy the growth condition, hence the combinatorial argument does not apply to them, but for which the algebraic argument works. For example, consider

$$a(x) = b(2^{2^x}),\ b \in \mathbf{Z}[x] \text{ with } \deg b \geq 1 .$$

Application 2: Wedderburn's theorem on skew fields

It is easy to show (by linear algebra) that each finite field F has p^k elements, where p is a prime and $k \in \mathbf{N}$, and it is not too hard to prove that for each prime power p^k there is (up to isomorphism) exactly one finite field F with this number of elements; F is obtained either as $\mathbf{Z}_p[x]/(a)$ for an irreducible polynomial $a \in \mathbf{Z}_p[x]$ with degree k or as the set of roots (in the algebraic closure of $\mathbf{Z}_p$) of the polynomial $x^{p^k} - x$.

In contrast, no finite skew field ('noncommutative field'), which is a noncommutative ring in which each nonzero element is a unit, exists. The next proof of this interesting fact relies on cyclotomic polynomials and is taken from the nice book of Aigner and Ziegler [1, Chapter 5].

Theorem (Wedderburn [32], Dickson [9]). *There is no finite skew field.*

Proof (Witt [35]). Let T be a finite skew field that is not a field: $xy \neq yx$ for some $x, y \in T$; we derive a contradiction. We partition $T^\times = T\backslash\{0\}$ by the conjugation relation $\sim$: for $x, y \in T^\times$ we have $x \sim y \iff x = sys^{-1}$ for some $s \in T^\times$. This is an equivalence relation, and we denote the equivalence classes by

$$A_x = \{y \in T^\times \mid x \sim y\} = \{sxs^{-1} \mid s \in T^\times\},\ x \in T^\times .$$

So we have the partition

$$T^\times = \bigcup_{x \in T^\times} A_x$$

— if $A_x \cap A_{x'} \neq \emptyset$ then $A_x = A_{x'}$. For $x \in T^\times$ we consider also the centralizer C_x of x,

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

This is the set of elements in T commuting with x; it contains 0 and 1 and is a skew subfield of T. The centre Z of T are the elements in T that commute with every element in T:

$$Z = \bigcup_{x \in T^\times,\ |A_x| = 1} A_x \cup \{0\} = \bigcup_{x \in T^\times,\ |A_x| = 1} \{x\} \cup \{0\} = \bigcap_{x \in T} C_x .$$

Z is a (commutative) subfield of T.

For every $x \in T^\times$,

$$|T^\times| = |C_x^\times| \cdot |A_x| \ .$$

This follows from the fact that, given $x \in T^\times$, the mapping from $T^\times$ to $T^\times$ that sends s to sxs^{-1} is onto A_x and $|C_x^\times|$-to-1: $s_1 x s_1^{-1} = s_2 x s_2^{-1}$ iff $s_2^{-1} s_1 \in C_x$ iff $s_1 \in s_2 C_x$.

T and every C_x are vector spaces over the field Z. Denoting $q = |Z|$, and the respective dimensions of T and C_x by n and n_x, we get

$$|T| = q^n \ \text{ and } \ |C_x| = q^{n_x} \ .$$

By our initial assumption, there is at least one class A_x with more than one element. Let all the distinct non-singleton classes be $A_{x_1}, A_{x_2}, \ldots, A_{x_t}$, $t \geq 1$, and let n_i be the dimension of C_{x_i} over Z. By the above relation, $|A_{x_i}| = |T^\times|/|C_{x_i}^\times|$. Thus

$$q^n - 1 = |T^\times| = |Z^\times| + \sum_{x \in T^\times,\ |A_x| \geq 2} |A_x| = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1} \ .$$

We show that this identity,

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1},\ (q^{n_i} - 1) \,|\, (q^n - 1),\ n_i < n,\ q \geq 2$$

$(t, q, n_i, n \in \mathbf{N})$, is contradictory. First we show that the divisibility assumption implies that each n_i divides n. Indeed, if $q^m - 1$ divides $q^n - 1$, $q, m, n \in \mathbf{N}$ and $q \geq 2$, then we write $n = am + b$ with $0 \leq b < m$ and

$$q^n - 1 = q^{am+b} - 1 - (q^m - 1) = q^m (q^{(a-1)m+b} - 1)$$

shows that $q^m - 1$ divides $q^{(a-1)m+b} - 1$; iterating we get that $q^m - 1$ divides $q^b - 1$, hence $b = 0$ and m divides n. So we have the identity

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

where q, n, n_i are positive integers, $q \geq 2$ and each n_i is a divisor of n smaller than n.

We deduce contradiction by means of cyclotomic polynomials. Factorizing $x^n - 1$ and $x^{n_i} - 1$ by them, the identity gives

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

which implies, since each n_i divides n but $n_i < n$, that the integer $\Phi_n(q)$ divides $q - 1$. This is impossible:

$$|\Phi_n(q)| = \prod_{\alpha} |q - \alpha| > \prod_{\alpha} |q - 1| = (q-1)^{\varphi(n)} \geq q - 1 \ ,$$

where the product is taken over all $\varphi(n) \geq 1$ primitive n-th roots of unity $\alpha \in \mathbf{C}$, because $q \geq 2$ and each α has real part smaller than 1. □

Lecture 4, October 30, 2012

Application 3: euclidean constructions of the regular plane 5-gon, 17-gon, 257-gon and 65537-gon

The well-known characterization of regular plane n-gons constructible by an euclidean construction — a construction using only an unmarked ruler and a compass — says that this is possible $\iff$ n factorizes to

$$n = 2^l p_1 p_2 \dots p_j \ ,$$

where $l \in \mathbf{N}_0$ and the p_i are mutually distinct primes of the form $2^k + 1$, $k \in \mathbf{N}_0$. The implication $\Rightarrow$ was proved by Gauss and the opposite implication $\Leftarrow$ by Wantzel.

From the factorization $x^r + y^r = (x+y)(x^{r-1} - x^{r-2}y + x^{r-3}y^2 - \dots + y^{r-1})$ for odd r it follows that necessary condition for primality of $2^k + 1$ is that k is a power of 2. The primes of the form $2^{2^t} + 1$, $t \in \mathbf{N}_0$, are called *Fermat primes* because Fermat conjectured that all of them are primes; this turned out to be quite wrong. To date only five Fermat primes are known:

$$2^1 + 1 = 3,\ 2^2 + 1 = 5,\ 2^4 + 1 = 17,\ 2^8 + 1 = 257 \ \text{ and } \ 2^{16} + 1 = 65537 \ .$$

The next number $2^{32} + 1$ was shown to be divisible by 641 and thus composite by Euler. A more recent conjecture says that no Fermat prime besides these five exists. In the lecture I will prove the following particular case of Gauss' result.

Theorem (Gauss). *If $p = 2^k + 1$, $k \in \mathbf{N}$, is a prime number, then the regular plane p-gon can be obtained by euclidean construction.*

(We put aside the prime $p = 3 = 2^0 + 1$ which is kind of exceptional; the equilateral triangle is clearly constructible.) I will follow the proof in Davenport [8, p. 20–21].

We start with some auxiliary results. The next is known as *Eisenstein's irreducibility criterion.*

Proposition (Eisenstein). *If p is a prime and $f(x) = a_n x^n + \dots + a_1 x + a_0$ is an integral polynomial such that p does not divide a_n, p divides each a_i with $i < n$ and p^2 does not divide a_0, then $f(x)$ is irreducible in $\mathbf{Z}[x]$.*

Proof. Note two easy results. First, the reduction mapping from $\mathbf{Z}[x]$ to $\mathbf{Z}_p[x]$ sending a polynomial $p(x)$ to its reduction $\overline{p(x)}$, in which each coefficient is reduced mod p, is a ring homomorphism. Second, if R is an integral domain,

e.g. $\mathbf{Z}_p$, and $a \in R^\times$, then the only factorizations $ax^k = g(x)h(x)$ in $R[x]$ are $g(x) = bx^l$ and $h(x) = cx^m$, where $b, c \in R$ with $bc = a$ and $l, m \in \mathbf{N}_0$ with $l + m = k$. (This follows either from the fact that $R[x]$ is a UFD or can be seen directly.)

Now suppose for contradiction that $f(x) = g(x)h(x)$ in $\mathbf{Z}[x]$ with $\deg g, \deg h \geq 1$. Reducing this mod p we get, by the assumption on the coefficients a_i,

$$\overline{a_n}x^n = \overline{g(x)} \cdot \overline{h(x)}, \ \overline{a_n} \neq 0 \ .$$

So, as we noted, $\overline{g(x)} = bx^l$ and $\overline{h(x)} = cx^m$ where $b, c \in \mathbf{Z}_p$ with $bc = \overline{a_n}$ and $l, m \in \mathbf{N}_0$ with $l + m = n$. In fact, $l = \deg g \geq 1$ and $m = \deg h \geq 1$ or vice versa. This means that the constant terms in both $g(x)$ and $h(x)$ are divisible by p. Thus their product a_0 is divisible by p^2, in contradiction with the assumption. □

Corollary. *If p is a prime, the cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbf{Z}[x]$.*

Proof. Clearly, $\Phi_p(x)$ is irreducible in $\mathbf{Z}[x]$ if and only if $f(y)$ is irreducible in $\mathbf{Z}[y]$, where $f(y) = \Phi_p(y + 1)$. But

$$f(y) = \Phi_p(y+1) = \frac{(y+1)^p - 1}{(y+1) - 1} = y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{p-1}$$

is irreducible by Eisenstein's criterion, because $\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i!}$ is divisible by p for $0 < i < p$ and $\binom{p}{p-1} = p$. □

It is well known by the Gauss lemma, which we will neither state nor prove here, that irreducibility in $\mathbf{Z}[x]$ is equivalent with irreducibility in $\mathbf{Q}[x]$.

For $m \in \mathbf{N}$, we denote by

$$\mathbf{Z}_m^\times = \{i \mid i = 1, 2, \ldots, m, \ (i, m) = 1\}$$

the set of residues modulo m coprime to m, and also the multiplicative group $(\mathbf{Z}_m^\times, \cdot)$. We say that $g \in \mathbf{Z}_m^\times$ is a *primitive root modulo m* if $(\mathbf{Z}_m^\times, \cdot)$ is cyclic and g generates it. Then $i \mapsto g^i$ gives an isomorphism of the groups $(\mathbf{Z}_{\varphi(m)}, +)$ and $(\mathbf{Z}_m^\times, \cdot)$. Every residue $n \in \mathbf{Z}_m^\times$ then can be written as

$$n \equiv g^i \pmod{m} \ ,$$

where the exponent $i \in \mathbf{Z}$ is unique modulo $\varphi(m)$. We write

$$i = \operatorname{ind}(n) = \operatorname{ind}_g(n)$$

for the inverse isomorphism. Clearly,

$$\operatorname{ind}(mn) \equiv \operatorname{ind}(m) + \operatorname{ind}(n) \pmod{\varphi(m)} \ .$$

Moduli with primitive roots therefore possess a discrete logarithm function ind_g. The next result is due to Gauss.

Proposition. *Every prime modulus p has a primitive root.*

Proof. We consider the finite field $\mathbf{Z}_p = (\mathbf{Z}_p, +, \cdot)$ and for any divisor d of $\varphi(p) = p - 1$ denote by A_d the set of $a \in \mathbf{Z}_p^\times$ with order d and by R_d the set of $a \in \mathbf{Z}_p$ with $a^d - 1 = 0$. We want to show that $A_{p-1} \neq \emptyset$. For any $m \in \mathbf{N}$ we have the elementary identity

$$\sum_{d \mid m} \varphi(d) = m \ ,$$

which follows by partitioning the numbers $1, 2, \ldots, m$ by the equivalence relation $\sim$ defined by $i \sim j \iff (i, m) = (j, m) = d$. We show that

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

which due to the identity (with $m = p - 1$) gives that always $|A_d| = \varphi(d)$. In particular, $A_{p-1} \neq \emptyset$ because $|A_{p-1}| = \varphi(p-1) \geq 1$, and there are $\varphi(p-1)$ primitive roots modulo p.

So let $a \in A_d$. The powers $a, a^2, \ldots, a^d$ are all distinct modulo p, for else a would have order smaller than d. Also, $\{a, a^2, \ldots, a^d\} \subset R_d$. Since $|R_d| \leq d$ (by the bound on the number of roots of a polynomial), we have that $R_d = \{a, a^2, \ldots, a^d\}$. But $A_d \subset R_d$, and we see that each element of A_d is a power a^i, $1 \leq i \leq d$. Clearly, $a^i \in A_d$ iff i is coprime to d, and $|A_d| = \varphi(d)$. □

In the following, p is a prime number, ζ is a primitive p-th root of 1 — a complex number of the form $\zeta = \exp(2\pi i k/p)$ with $k \in \{1, 2, \ldots, p-1\}$ — and g is a primitive root modulo p. Note that then

$$1, \ \zeta, \ \zeta^2, \ \ldots, \ \zeta^{p-1}$$

is the list of all p p-th roots of unity, where the last $p-1$ ones are the primitive roots with order p and 1 is the p-th root of unity with order 1.

Proposition. *Let p be a prime and $f \in \mathbf{Z}[x]$. Then there exist unique integers $a_1, a_2, \ldots, a_{p-1}$ such that for every primitive p-th root of unity ζ we have*

$$f(\zeta) = a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} \ .$$

Proof. Using the identity $\zeta^p = 1$ we reduce each power of ζ in $f(\zeta)$ to one with the exponent in $0, 1, \ldots, p-1$. If a term $a\zeta^0 = a$, $a \in \mathbf{Z}$ nonzero, is present, we get rid of it using the identity

$$\zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1 \ ,$$

which follows from the fact that the sum of all p-th roots of 1 is 0 (minus coefficient of x^{p-1} in $x^p - 1$). This gives the required expression of $f(\zeta)$ as a linear integral combination of all primitive p-th roots of 1. If

$$a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} = a'_1\zeta + a'_2\zeta^2 + \cdots + a'_{p-1}\zeta^{p-1}$$

for two distinct $(p-1)$-tuples of integers $a_1, \ldots, a_{p-1}$ and $a'_1, \ldots, a'_{p-1}$, by substraction and taking out a power of ζ we deduce that ζ is a root of a nonzero integral polynomial with degree smaller than $p-1$, which contradicts the above proved irreducibility of $\Phi_p(x)$. Thus the tuple $a_1, \ldots, a_{p-1}$ is unique. $\square$

If p is a prime and

$$p - 1 = ef, \ e, f \in \mathbf{N} \ ,$$

is a factorization, we define for $j \in \mathbf{Z}$ the *e-th Gauss period* $\eta_j \in \mathbf{C}$ by

$$\eta_j = \sum_{\mathrm{ind}(n) \equiv j \pmod{e}} \zeta^n \ ,$$

that is, we keep in the sum $\sum_{n=1}^{p-1} \zeta^n = -1$ only the exponents n whose index $\mathrm{ind}_g(n)$ is j modulo e. Each η_j is a sum of f summands and since η_j is periodic in j modulo e, we have e (potentially) distinct Gauss periods and may take $j = 1, 2, \ldots, e$. Also,

$$\eta_1 + \eta_2 + \cdots + \eta_e = -1 \ .$$

The value of η_j depends on the choice of the primitive root ζ of 1 and also on the choice of the primitive root g modulo p. But the replacement of ζ with ζ^n for n coprime to p and g with g^i for i coprime to $p-1$ only results in permuting the indices of $\eta_1, \eta_2, \ldots, \eta_e$, and thus makes no difference for symmetric expressions in periods, that is, expressions that are invariant upon permuting the indices (e.g., the identity $\eta_1 + \eta_2 + \cdots + \eta_e = -1$). We make use of Gauss periods to prove euclidean constructibility of regular $p = (2^k + 1)$-gons.

Lecture 5, November 6, 2012

We assume that $p > 2$ is an odd prime and look first at the two Gauss periods η_1 and η_2 for $e = 2$.

Lemma. *If $p > 2$ is a prime number and $e = 2$ then the two corresponding Gauss periods satisfy*

$$(\eta_2 - \eta_1)^2 = \begin{cases} -p & \ldots \quad p \equiv 3 \pmod 4 \\ p & \ldots \quad p \equiv 1 \pmod 4 \end{cases}$$

Consequently, both periods are quadratic irrationalities, $\eta_{1,2} = \frac{1}{2}(1 \pm i\sqrt{p})$ in the former case and $\eta_{1,2} = \frac{1}{2}(1 \pm \sqrt{p})$ in the latter.

Proof. We denote by QR the quadratic residues modulo p and by NR the quadratic nonresidues. It is easy to see that the former are exactly the elements in $\mathbf{Z}_p^\times$ with an even index and the latter are those with an odd index. Thus

$$G = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \zeta^m = \sum_{m \in \mathbf{Z}_p^\times, m \in \mathrm{QR}} \zeta^m - \sum_{m \in \mathbf{Z}_p^\times, m \in \mathrm{NR}} \zeta^m = \eta_2 - \eta_1 \ .$$

Squaring, substituting $m_2 \equiv m_1 n$ modulo p and using properties of Legendre's symbol $(\frac{n}{p})$, we get

$$\begin{aligned} G^2 &= \sum_{m_1,m_2=1}^{p-1} \left(\frac{m_1 m_2}{p}\right) \zeta^{m_1+m_2} = \sum_{m_1=1}^{p-1}\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^{m_1+m_1 n} \\ &= \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \sum_{m_1=1}^{p-1} \zeta^{m_1(1+n)} \ . \end{aligned}$$

If $n = p-1$, the inner sum equals $p-1$, and else it is -1 for then the exponent runs through all residues in $\mathbf{Z}_p^\times$. Hence

$$G^2 = \left(\frac{p-1}{p}\right)(p-1) - \sum_{n=1}^{p-2} \left(\frac{n}{p}\right) = \left(\frac{-1}{p}\right) p \ ,$$

because the full sum $\sum_{n=1}^{p-1}(\frac{n}{p}) = 0$ (there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues). Thus, by the 1st supplement to the quadratic reciprocity law, $G^2 = -p$ for $p \equiv 3 \bmod 4$ and $G^2 = p$ for $p \equiv 1 \bmod 4$, and this is the stated formula. Thus $\eta_2 - \eta_1 = \pm i\sqrt{p}$ in the former case and $\eta_2 - \eta_1 = \pm\sqrt{p}$ in the latter, which together with $\eta_1 + \eta_2 = -1$ enables us to express η_1 and η_2, up to the undetermined sign. □

What about the undetermined sign in the expressions for η_1 and η_2? Since $\sum_{m=0}^{p-1} \zeta^m = 0$, we get that also

$$\eta_2 - \eta_1 = 1 + 2 \sum_{m \in \mathbf{Z}_p^\times, m \in \mathrm{QR}} \zeta^m = \sum_{m=0}^{p-1} \zeta^{m^2} \ .$$

To speak about a concrete sign, first one has to fix a specific ζ. So let $\zeta = \exp(2\pi i/p)$. Davenport [8, pp. 12–16] gives a (cool) proof, due to Dirichlet in 1835, of the more general result that for any $N \in \mathbf{N}$,

$$\sum_{n=0}^{N-1} \exp(2\pi i n^2/N) = \begin{cases} (1+i)\sqrt{N} & \ldots \quad N \equiv 0 \pmod 4, \\ \sqrt{N} & \ldots \quad N \equiv 1 \pmod 4, \\ 0 & \ldots \quad N \equiv 2 \pmod 4 \text{ and} \\ i\sqrt{N} & \ldots \quad N \equiv 3 \pmod 4 \ . \end{cases}$$

The next general proposition is a tool enabling to relate Gauss periods for e to those for $e/2$.

Proposition. *Let $p > 2$ be a prime, $p - 1 = ef$ for $e, f \in \mathbf{N}$, ζ be a primitive p-th root of 1 and let*

$$f(x,t) \in \mathbf{Z}[x,t]$$

be a polynomial with the property that for any $m \in \mathbf{Z}$ coprime to p but divisible by e we have

$$f(x,\zeta) = f(x,\zeta^m) \ .$$

Then there exist polynomials $b_j \in \mathbf{Z}[x]$, $1 \le j \le e$, such that for every primitive p-th root of unity ζ we have

$$f(x,\zeta) = \sum_{j=1}^{e} b_j(x)\eta_j \ .$$

Proof.

□

Proposition. *Let $p = 2^k + 1$, $k \in \mathbf{N}$, be a prime number, that is to say, $p = 5, 17, 257$ or 65537 ($k = 2, 4, 8$ or 16), and ζ be a primitive p-th root of 1. Then*

$$\zeta \in \mathbf{Q}_k \ ,$$

where $\mathbf{Q}_0 = \mathbf{Q}$ and $\mathbf{Q}_j = \mathbf{Q}_{j-1}(\sqrt{\alpha_{j-1}})$ for $j = 1, 2, \dots, k$ with $\alpha_{j-1} \in \mathbf{Q}_{j-1}$ and $\mathbf{Q}_{j-1} \subset \mathbf{R}$. In other words, ζ can be obtained from fractions by using rational operations and taking k times a square root, so that all involved square roots except the last one taken are real numbers.

Proof.

□

Lecture 6, November 13, 2012

Application 4: a particular case of Weil's theorem on the number of solutions of polynomial congruences

In 1948, A. Weil [33] obtained a strong bound on the number of points on curves defined over finite fields. To state it, we say that a polynomial $F \in K[x_1, \dots, x_n]$ over a field K is *absolutely irreducible* if it is irreducible in $\overline{K}[x_1, \dots, x_n]$ where $\overline{K}$ is the algebraic closure of K.

Theorem (Weil, 1948). *Suppose $F \in \mathbf{F}_q[x, y]$ is an absolutely irreducible polynomial over a finite field $\mathbf{F}_q$ with $q = p^k$ elements. Then*

$$N = \#\{(a, b) \in \mathbf{F}_q^2 \mid F(a, b) = 0 \ \} = q + O(\sqrt{q}) \ .$$

Weil conjectured and partially proved more general and detailed results which we do not state here. It turns out that building on the case $n = 2$, one can extend Weil's bound to $n \ge 2$ variables. Thus Lang and Weil [18] proved that if $F \in \mathbf{F}_q[x_1, \dots, x_n]$ is an absolutely irreducible polynomial in $n \ge 2$ variables, then the equation $F(x_1, \dots, x_n) = 0$ has in $\mathbf{F}_q$

$$q^{n-1} + O(q^{n-3/2})$$

solutions.

In the course I will prove two particular cases of this bound: for the polynomials

$$F(x_1,\dots,x_n) = a_1x_1^{r_1} + \cdots + a_nx_n^{r_n} \quad \text{and} \quad F(x,y) = y^2 - ax^3 - bx^2 - cx - d\,,$$

with integral coefficients and just for the field $\mathbf{F}_q = \mathbf{Z}_p$ of residues modulo a prime p, when the equation can be viewed as a congruence modulo p.

For the diagonal polynomials in the first case we will count the solutions by means of complex roots of 1; the method in the second case will be totally different. The result and its proof are taken from the book of Borevič and Šafarevič [5, Section 1.2]. We will prove the following.

Proposition. *Let p be a prime, $a_1,\dots,a_n \in \mathbf{Z}$, $n \ge 3$, numbers not divisible by p, $r_1,\dots,r_n \in \mathbf{N}$ and $d_i = (r_i, p-1)$. Then the number N of solutions of the congruence*

$$a_1x_1^{r_1} + a_2x_2^{r_2} + \cdots + a_nx_n^{r_n} \equiv 0 \pmod p$$

satisfies the estimate

$$|N - p^{n-1}| \le (d_1-1)\dots(d_n-1)(p-1)p^{n/2-1} = O(p^{n/2})\,.$$

The estimate is in fact valid also for $n \le 2$ but then it is trivial and gives no information; for $n \le 2$ variables it is easy to resolve the congruence directly. For $n = 3$ we get Weil's bound and for $n \ge 4$ an even stronger bound. If an exponent r_i is coprime to $p-1$, the estimate yields $N = p^{n-1}$. This can be seen directly: we write the congruence as $x_i^{r_i} \equiv -y/a_i$, where y is the rest of the left side, and (as we show in a lemma below) for any fixed mod p residue y given by each of the p^{n-1} choices of values for the unknowns distinct from x_i there is exactly one solution x_i.

To prove the Proposition, we derive for N an explicit formula. By $\sum_x \dots$ we denote summation over all p residues modulo p, and by $\sum'_x \dots$ summation over the $p-1$ nonzero residues mod p. Also, for each prime p we fix $\zeta \in \mathbf{C}$, a primitive p-th root of 1, and $g \in \mathbf{Z}_p^\times$, a primitive root modulo p.

Lemma. *Let p be a prime and $F \in \mathbf{Z}[x_1,\dots,x_n]$ an integral polynomial. The number N of solutions of the congruence $F(x_1,\dots,x_n) \equiv 0$ modulo p is given by the formula*

$$N = p^{n-1} + \frac{1}{p}\sum_x{}' \sum_{x_1,\dots,x_n} \zeta^{xF(x_1,\dots,x_n)}\,.$$

Proof. For any $y \in \mathbf{Z}$ we have

$$\sum_x \zeta^{xy} = \begin{cases} p & \dots \quad y \equiv 0 \pmod p \\ 0 & \dots \quad y \not\equiv 0 \pmod p\,. \end{cases}$$

Indeed, the former case is clear and in the latter xy runs through all residues mod p, and we get the sum of all p p-th roots of 1, which is 0. Thus

$$N = \frac{1}{p} \sum_{x_1,\ldots,x_n} \sum_x \zeta^{xF(x_1,\ldots,x_n)} = \frac{1}{p} \sum_x \sum_{x_1,\ldots,x_n} \zeta^{xF(x_1,\ldots,x_n)} ,$$

which gives the stated formula after taking out the terms with $x = 0$. □

To make the formula more explicit if $F(x_1, \ldots, x_n) = a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n}$, we find the number of solutions y of the congruence $y^r \equiv x$. Recall that for $x \in \mathbf{Z}_p^\times$, the index $\mathrm{ind}(x)$ is the mod $p-1$ unique residue i such that $g^i \equiv x \bmod p$ (g is the fixed primitive root modulo p).

Lemma. *Let p be a prime, $r \in \mathbf{N}$, $x \in \mathbf{Z}$, $d = (r, p-1)$ and $m(x)$ be the number of solutions y of the congruence $y^r \equiv x$ modulo p. Then*

$$m(x) = \begin{cases} 1 & \ldots \quad x \equiv 0 \pmod{p} \\ 0 & \ldots \quad x \not\equiv 0 \pmod{p} \ \&\ \mathrm{ind}(x) \not\equiv 0 \pmod{d} \\ d & \ldots \quad x \not\equiv 0 \pmod{p} \ \&\ \mathrm{ind}(x) \equiv 0 \pmod{d} . \end{cases}$$

In particular, if $d = 1$ then $m(x) = 1$ for every $x \in \mathbf{Z}$.

Proof. If $x \equiv 0 \bmod p$, there is exactly one solution, $y \equiv 0$. If $x \not\equiv 0 \bmod p$, then so is y and in terms of indices the congruence is equivalent with

$$r \cdot \mathrm{ind}(y) \equiv \mathrm{ind}(x) \pmod{p-1} .$$

The left side and the modulus are divisible by d, and if the right side is not, there is no solution. So we assume that d divides $\mathrm{ind}(x)$ and get the equivalent congruence

$$(r/d) \cdot \mathrm{ind}(y) \equiv \mathrm{ind}(x)/d \pmod{(p-1)/d} .$$

Now $(r/d, (p-1)/d) = 1$ and thus the last congruence has exactly one solution for $\mathrm{ind}(y)$ modulo $(p-1)/d$. It gives all $\frac{p-1}{(p-1)/d} = d$ solutions for $\mathrm{ind}(y)$ modulo $p-1$. □

To express the quantity $m(x)$ in an algebraicly convenient form, we resort to the d mappings $\chi_s : \mathbf{Z} \to \mathbf{C}$, $s = 0, 1, \ldots, d-1$, given for $x \in \mathbf{Z}$ not divisible by p as

$$\chi_s(x) = \varepsilon^{s \cdot \mathrm{ind}(x)} ,$$

where ε is a fixed primitive d-th root of 1, and by $\chi_s(x) = 0$ if p divides x.

Lemma. *Let p be a prime, $x \in \mathbf{Z}$, $r \in \mathbf{N}$, $d = (r, p-1)$ and $m(x)$ be the number of solutions y of the congruence $y^r \equiv x$ modulo p. Then*

$$m(x) = 1 + \sum_{s=1}^{d-1} \chi_s(x) .$$

Proof. If p divides x then each sumand is 0 and we get $m(x) = 1$, as we should. Else the right side equals

$$\sum_{s=0}^{d-1} \chi_s(x) \ .$$

Here if d divides $\mathrm{ind}(x)$ then each summand is 1 and the sum is d. If d does not divide $\mathrm{ind}(x)$, then the last sum equals

$$\sum_{s=0}^{d-1} \varepsilon^{s\cdot \mathrm{ind}(x)} = \frac{\varepsilon^{d\cdot \mathrm{ind}(x)} - 1}{\varepsilon^{\mathrm{ind}(x)} - 1} = \frac{1-1}{\varepsilon^{\mathrm{ind}(x)} - 1} = 0 \ .$$

For any x we have agreement with the previous lemma. □

For p a prime, $\chi : \mathbf{Z} \to \mathbf{C}$ a p-periodic mapping and $a \in \mathbf{Z}$, we denote

$$\tau_a(\chi) = \sum_x \chi(x)\zeta^{ax} \ .$$

If $F(x_1, \ldots, x_n) = a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n}$, we transform the formula for the number of solutions stated in the first lemma for general polynomial in a more explicit form involving the quantities $\tau_a(\chi)$.

Lemma. *If p is a prime, $a_1, \ldots, a_n \in \mathbf{Z}$, $n \geq 1$, numbers not divisible by p, $r_1, \ldots, r_n \in \mathbf{N}$, $d_i = (r_i, p-1)$ and N is the number of solutions of the congruence $a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n} \equiv 0$ modulo p, then*

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} \tau_{a_i x}(\chi_{i,s}) \ ,$$

where $\chi_{i,s}(x) = \varepsilon_i^{s\cdot \mathrm{ind}(x)}$ and ε_i is a fixed primitive d_i-th root of 1.

Proof. For $F(x_1, \ldots, x_n) = a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n}$ the formula for N stated in the first lemma becomes

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \sum_{x_1, \ldots, x_n} \zeta^{x(a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n})} = p^{n-1} + \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum_{x_i} \zeta^{x a_i x_i^{r_i}} \ .$$

Denoting $a = x a_i$, $r = r_i$ and $y = x_i$, the inner sum equals

$$\sum_y \zeta^{a y^r} = \sum_x m(x) \zeta^{ax} \ ,$$

where as before $m(x)$ counts solutions y of $y^r \equiv x$ modulo p. Denoting $d = d_i = (r, p-1) = (r_i, p-1)$ and replacing $m(x)$ by the expression of the previous lemma, we get

$$\sum_y \zeta^{a y^r} = \sum_x \left(1 + \sum_{s=1}^{d-1} \chi_s(x)\right) \zeta^{ax} = \sum_x \zeta^{ax} + \sum_{s=1}^{d-1} \sum_x \chi_s(x) \zeta^{ax} = \sum_{s=1}^{d-1} \tau_a(\chi_s)$$

because $a \not\equiv 0$ modulo p. Thus the inner sum equals to the sum of the quantities $\tau_a(\chi_s)$ for $s = 1, 2, \ldots, d-1$, and we get the stated formula. □

Note that we may assume that each $d_i \geq 2$, because $d_i = 1$ makes the whole error term correctly 0, as we observed above.

In the next lecture we will prove that the quantities $\tau_a(\chi_s)$, called *Gauss sums*, involved in the formula all have modulus $\sqrt{p}$. This gives the bound in the Proposition at once:

$$\begin{aligned} |N - p^{n-1}| &= \left| \frac{1}{p} {\sum_x}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} \tau_{a_i x}(\chi_{i,s}) \right| \leq \frac{1}{p} {\sum_x}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} |\tau_{a_i x}(\chi_{i,s})| \\ &= \frac{1}{p} {\sum_x}' \prod_{i=1}^{n} (d_i - 1)\sqrt{p} \\ &= (p-1)(d_1 - 1) \ldots (d_n - 1) p^{n/2 - 1} \, . \end{aligned}$$

Lecture 7, November 20, 2012

To complete the proof of the Proposition, we prove that Gauss sums have modulus $\sqrt{p}$.

Lemma. *Let p be a prime number, ε a primitive d-th root of 1, where $d \geq 2$ and is a divisor of $p-1$, $\chi = \chi_s : \mathbf{Z} \to \mathbf{C}$ be given by $\chi(x) = \varepsilon^{s \cdot \mathrm{ind}(x)}$ for some $s \in \{1, 2, \ldots, d-1\}$ if $x \in \mathbf{Z}$ with $(x, p) = 1$ ($\chi(x) = 0$ if p divides x) and $a \in \mathbf{Z}$ be a number not divisible by p. Then*

$$|\tau_a(\chi)| = \left| \sum_x \chi(x) \zeta^{ax} \right| = \sqrt{p} \, .$$

Proof. The properties of $\chi = \chi_s$ important for the proof, easily folowing from ther definition, are that χ is periodic modulo p, $\chi(ab) = \chi(a)\chi(b)$ for any two numbers $a, b \in \mathbf{Z}$ and that $\chi(c) \neq 1$ for some $c \in \mathbf{Z}_p^{\times}$ (set $c = g$, then $\chi(c) = \varepsilon^s \neq 1$ as $d \geq 2$ and $s \neq 0$).

If $f, g : \mathbf{Z} \to \mathbf{C}$ are p-periodic functions, the formula

$$\langle f, g \rangle = \frac{1}{p} \sum_x f(x) \overline{g(x)}$$

defines a hermitian scalar product on the p-dimensional complex vector space of p-periodic and complex-valued functions on $\mathbf{Z}$. The set of p functions

$$f_b(x) = \zeta^{bx}, \ b \in \mathbf{Z}_p \, ,$$

is an orthonormal basis: $\langle f_b, f_{b'} \rangle = 1$ if $b = b'$, and $= 0$ if $b \neq b'$, by the evaluation of $\sum_x \zeta^{xy}$ above. We expand χ in terms of this basis,

$$\chi(x) = \sum_b \alpha_b f_b(x), \ \alpha_b \in \mathbf{C} \ ,$$

multiply the expansion by $\chi(c)$ for a nonzero mod p residue c and change the summation variable b to bc:

$$\chi(cx) = \chi(c)\chi(x) = \sum_b \chi(c)\alpha_b f_b(x) = \sum_{bc} \chi(c)\alpha_{bc} f_{bc}(x) = \sum_{bc} \chi(c)\alpha_{bc} f_b(cx) \ .$$

This shows that $\alpha_b = \chi(c)\alpha_{bc}$ and, setting $b = 1$, $|\alpha_c| = |\alpha_1|$ for any $c \in \mathbf{Z}_p^\times$. Setting $b = 0$ we get the equation $\alpha_0 = \chi(c)\alpha_0$, thus $\alpha_0 = 0$ (as we remarked above, we can select c so that $\chi(c) \neq 0, 1$). So for any $a \in \mathbf{Z}_p^\times$,

$$\langle \chi, \chi \rangle = \sum_b |\alpha_b|^2 = (p-1)|\alpha_a|^2 = \frac{(p-1)|\tau_a(\chi)|^2}{p^2} \ ,$$

because

$$\alpha_{-a} = \langle \chi, f_{-a} \rangle = \frac{1}{p} \sum_x \chi(x)\zeta^{ax} = \frac{\tau_a(\chi)}{p} \ .$$

But by definition also

$$\langle \chi, \chi \rangle = \frac{1}{p} \sum_b \chi(b)\overline{\chi(b)} = \frac{1}{p} \sum_b |\chi(b)|^2 = \frac{p-1}{p} \ ,$$

and we get that $|\tau_a(\chi)|^2 = p$. □

The proof of the Proposition is now complete.

Another particular case of Weil's theorem: Hasse's theorem

In 1936, H. Hasse [15] proved a conjecture, stated by E. Artin in 1924, on the number of points on elliptic curves over finite fields. In terms of congruences his result, which we do not state in details, gives the following bound.

Theorem (Hasse, 1936). *Let p be a prime number, $a, b, c, d \in \mathbf{Z}$ be numbers with $a \neq 0$ and N be the number of solutions of the congruence*

$$y^2 \equiv ax^3 + bx^2 + cx + d \pmod{p} \ .$$

Then

$$N = p + O(\sqrt{p}) \ ,$$

with an absolute implicit constant in the O.

Instead of congruences we will use the language of finite fields $\mathbf{Z}_p$; we may and will assume that $p > 5$. The proof we present is taken from Baker and Wüstholz [4, Section 1.6] (who in turn write that they follow Baker [3]). Let

$$f(x) = ax^3 + bx^2 + cx + d \in \mathbf{Z}_p[x] \quad \text{and} \quad g(x) = f(x)^{(p-1)/2} \in \mathbf{Z}_p[x] \ .$$

Recall Euler's criterion: if $\alpha \in \mathbf{Z}_p$ is nonzero, then $\alpha^{(p-1)/2} = \pm 1$ and for value 1 the equation $y^2 = \alpha$ has exactly 2 solutions and for value -1 it has 0 solutions. If $\alpha = 0$ then $y^2 = \alpha$ has 1 solution. (In the above lemma we actually proved a more general result.) Thus if

$$n = \#\{\alpha \in \mathbf{Z}_p \mid g(\alpha) = 1\} \quad \text{and} \quad n' = \#\{\alpha \in \mathbf{Z}_p \mid g(\alpha) = -1\} \ ,$$

then $p - 3 \le n + n' \le p$ and $2n \le N \le 2n + 3$. It suffies to show that

$$n, n' < \frac{p}{2} + O(\sqrt{p}) \ ,$$

for then $n = p/2 + O(\sqrt{p})$ and hence $N = 2n + O(1) = p + O(\sqrt{p})$.

We prove that

$$n < \frac{p}{2} + O(\sqrt{p}) \ ;$$

as we will see, the same bound for n' can be proven almost with no change. To this end, we construct an auxiliary polynomial

$$\varphi(x) = \sum_{j=0}^{J-1} (u_j(x) + v_j(x)g(x))x^{pj} = \sum_{j=0}^{J-1} u_j(x)x^{pj} + v_j(x)g(x)x^{pj} \ ,$$

where $J \in \mathbf{N}$ and $u_j, v_j \in \mathbf{Z}_p[x]$ are polynomials with degrees at most $(p-5)/2$ each. Their coefficients and the value of J will be specified later.

Lemma. *If at least one of the polynomials $u_j(x)$ and $v_j(x)$, $0 \le j < J$, is nonzero, then so is the whole $\varphi(x)$.*

Proof. Let $d_{j0} = \deg u_j$ and $d_{j1} = \deg v_j$. We show that the degrees of any two (nonzero) summands of the $2J$ summands in the last sum defining $\varphi(x)$ are distinct; this shows that there is no cancellation and proves the claim. Suppose two of the degrees are equal:

$$d_{jk} + pj + k(3/2)(p-1) = d_{j'k'} + pj' + k'(3/2)(p-1) \ ,$$

where $0 \le j, j' < J$ and $k, k' \in \{0, 1\}$. This equation is equivalent with

$$2(d_{jk} - d_{j'k'}) + 3(k' - k) = p(2(j' - j) + 3(k' - k)) \ .$$

The integer on the left side is in absolute value at most $2(p-5)/2+3 = p-2 < p$ (for this step to work we need $p > 5$), and the right side is divisible by p. Thus their common value is 0, which implies that $k = k'$ and $j = j'$. □

Next we consider derivatives of $\varphi(x)$. Since we differentiate polynomials with coefficients in the field $\mathbf{Z}_p$ of characteristic p, things sometimes go differently than in the more familiar case of characteristic 0.

Lemma. *For every $l = 0, 1, 2, \dots$ we have the representation*

$$\varphi(x)^{(l)} = \frac{1}{f(x)^l} \sum_{j=0}^{J-1} (u_{jl}(x) + v_{jl}(x)g(x))x^{pj} \ ,$$

where $u_{jl}, v_{jl} \in \mathbf{Z}_p[x]$ are polynomials with degrees less than $2l + p/2$ each. Moreover, for each j, each coefficient of $u_{jl}(x)$ expresses as a linear combination (with coefficients in $\mathbf{Z}_p$) of the coefficients of $u_j(x)$, and similarly for $v_{jl}(x)$ and $v_j(x)$.

Proof. We proceed by induction on l. For $l = 0$ the claim holds. Since $\varphi(x)^{(l+1)} = (\varphi(x)^{(l)})'$ and $(x^{pj})' = 0$, we have

$$\varphi(x)^{(l+1)} = \frac{1}{f(x)^{l+1}} \sum_{j=0}^{J-1} (-l)f(x)'(\dots)x^{pj} + \frac{1}{f(x)^l} \sum_{j=0}^{J-1} (\dots)'x^{pj} \ .$$

From $g(x)' = \frac{p-1}{2} g(x)f(x)'/f(x)$ we get

$$(\dots)' = \frac{u_{jl}(x)'f(x) + v_{jl}(x)'f(x)g(x) + \frac{p-1}{2} v_{jl}(x)f(x)'g(x)}{f(x)} \ .$$

Hence

$$\varphi(x)^{(l+1)} = \frac{1}{f(x)^{l+1}} \sum_{j=0}^{J-1} (u_{j,l+1}(x) + v_{j,l+1}(x)g(x))x^{pj} \ ,$$

where

$$\begin{aligned} u_{j,l+1}(x) &= (-l)f(x)'u_{jl}(x) + u_{jl}(x)'f(x) \text{ and} \\ v_{j,l+1}(x) &= (-l)f(x)'v_{jl}(x) + v_{jl}(x)'f(x) + \tfrac{p-1}{2} v_{jl}(x)f(x)' \end{aligned}$$

are polynomials with degrees by at most 2 larger than $u_{jl}(x)$ and $v_{jl}(x)$ because $\deg f = 3$. The claim on the form of the coefficients in $u_{jl}(x)$ and $v_{jl}(x)$ is also clear from the recurrence. □

We set up $\varphi(x)$ so that it vanishes on each solution of $g(x) = 1$ in $\mathbf{Z}_p$ to a high order, which will provide the above upper bound on the number n of these solutions. One can control the vanishing by a simpler polynomial:

Lemma. *We associate with $\varphi(x)^{(l)}$ the polynomial*

$$\psi_l(x) = \sum_{j=0}^{J-1} (u_{jl}(x) + v_{jl}(x))x^j \ .$$

It has degree less than $2l + \frac{p}{2} + J - 1$ *and has this property: if (the coefficients in* $u_j(x)$ *and* $v_j(x)$ *were selected so that)* $\psi_l(x)$ *is a zero polynomial, then* $g(\alpha) = 1$, $\alpha \in \mathbf{Z}_p$, *implies that* $\varphi^{(l)}(\alpha) = 0$.

Proof. If $u, v \in \mathbf{Z}_p[x]$ are two polynomials that are congruent modulo the ideal generated by $\{x^p - x, g(x) - 1\}$, then $u(\alpha) = v(\alpha)$ whenever $\alpha \in \mathbf{Z}_p$ is such that $g(\alpha) = 1$; the reduction of x^p follows from the fact that $\alpha^p = \alpha$ for every $\alpha \in \mathbf{Z}_p$ (by little Fermat's theorem). And this is exactly the case for the numerator of $\varphi(x)^{(l)}$ and $\psi_l(x)$. Thus $\varphi(\alpha)^{(l)} = \psi_l(\alpha) = 0$ whenever $g(\alpha) = 1$. □

To specify the coefficients of $u_j(x)$ and $v_j(x)$, we use the simple but useful fact that any system of linear homogeneous equations with more unknowns than equations has a nontrivial solution.

Lemma. *If* F *is a field and* $a_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \in F^n$, $i = 1, 2, \ldots, m$, *are* m n*-tuples of elements of* F *and* $m < n$, *then there exist* $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, *not all of them* 0, *such that*

$$a_{i1}\alpha_1 + a_{i2}\alpha_2 + \cdots + a_{in}\alpha_n = 0, \ i = 1, 2, \ldots, m \ .$$

Proof. In a vector space V, if $U, U' \subset V$ are subspaces then the codimensions ($\operatorname{codim} U = \dim V - \dim U$) satisfy

$$\operatorname{codim}(U \cap U') \leq \operatorname{codim} U + \operatorname{codim} U' \ .$$

Each of the m hyperplanes in $\mathbf{Z}_p^n$ given by $\sum_j a_{ij}x_j = 0$ has codimension at most 1, and thus their intersection has codimension at most m and dimension at least $n - m \geq 1$. In particular, the intersection contains a nonzero vector. □

We want to specify the coefficients of the polynomials $u_j(x)$ and $v_j(x)$, $j = 0, 1, \ldots, J-1$, defining $\varphi(x)$ so that some of them and hence $\varphi(x)$ is not a zero polynomial, but each $\psi_l(x)$, $l = 0, 1, \ldots, L-1$, is a zero polynomial; the value of $L \in \mathbf{N}$ will be specified later. The number of unknown coefficients equals $2J(\frac{p-5}{2} + 1) = J(p-3)$. We have one homogeneous linear equation for each coefficient of each $\psi_l(x)$, $l = 0, 1, \ldots, L-1$, which we require to be 0 (recall that each coefficient of $\psi_l(x)$ is a linear combination of the coefficients in $u_j(x)$ and $v_j(x)$). We have $\deg \psi_l < 2l + \frac{p}{2} + J - 1 \leq 2L + \frac{p}{2} + J - 1$ and thus the number of equations is less than $L(2L + \frac{p}{2} + J)$. To summarize, in view of the previous lemmas we get the following.

Lemma. *If* $p > 5$ *is a prime number and* $J, L \in \mathbf{N}$ *are such that*

$$L(2L + \frac{p}{2} + J) < J(p-3) \ ,$$

then one can select the polynomials $u_j, v_j \in \mathbf{Z}_p[x]$, *where* $j = 0, 1, \ldots, J-1$ *and* $\deg u_j, \deg v_j \leq \frac{p-5}{2}$, *so that the above defined polynomial* $\varphi \in \mathbf{Z}_p[x]$ *is nonzero and*

$$\varphi^{(l)}(\alpha) = 0, \ l = 0, 1, \ldots, L-1 \ ,$$

for every $\alpha \in \mathbf{Z}_p$ *with* $g(\alpha) = 1$.

Lecture 8, November 27, 2012

We set $L = \lfloor \sqrt{p} \rfloor$ and $J = L/2 + c$ for a constant $c > 0$. The inequality in the previous lemma then becomes

$$(5/2)L^2 + pL/2 + cL < pL/2 + cp - 3L/2 - 3c \iff (5/2)L^2 + (c+3/2)L + 3c < cp\,,$$

which is satisfied if $(c + 3/2)\sqrt{p} + 3c < (c - 5/2)p$. This holds for any $p \geq 7$ if $c = 20$ and larger, so we may set $J = L/2 + 20$ (plus $\frac{1}{2}$ for odd L, to make J an integer). The choice

$$L = \lfloor \sqrt{p} \rfloor,\ J = \frac{\lfloor \sqrt{p} \rfloor}{2} + 20\ (+1/2 \text{ for odd } L)$$

therefore satisfies for any prime $p > 5$ the inequality in the previous lemma.

Finally, we apply the next well-known fact.

Lemma. *If* $u \in \mathbf{Z}_p[x]$ *is a nonzero polynomial,* $S \subset \mathbf{Z}_p$ *and* $u^{(l)}(\alpha) = 0$ *for every* $\alpha \in S$ *and* $l = 0, 1, \ldots, L-1$, *where* $L \in \mathbf{N}$ *and* $L \leq p$, *then*

$$u(x) = v(x) \prod_{\alpha \in S} (x - \alpha)^L, v \in \mathbf{Z}_p[x]\,.$$

In particular, $\deg u \geq |S|L$.

Proof. It suffices to prove this for $S = \{\alpha\}$. ($\mathbf{Z}_p[x]$ is a UFD and the polynomials $(x-\alpha)^r$ and $(x-\beta)^s$ are coprime if $\alpha \neq \beta$, thus if both divide $u(x)$ then so does their product.) We proceed by induction on L. For $L = 0$ the claim holds trivially, with $u = v$. For $L \geq 1$ we have by induction $u(x) = (x-\alpha)^{L-1}t(x)$ for some $t \in \mathbf{Z}_p[x]$, which after $L-1$ differentiations yields the expression $u(x)^{(L-1)} = (L-1)!t(x) + (x-\alpha)w(x)$ for some $w \in \mathbf{Z}_p[x]$. As $(L-1)! \neq 0$ in $\mathbf{Z}_p$, setting $x = \alpha$ we get $t(\alpha) = 0$. Thus, by the division algorithm in $\mathbf{Z}_p[x]$, $t(x) = (x-\alpha)v(x)$ and $u(x) = (x-\alpha)^{L-1}t(x) = (x-\alpha)^L v(x)$. □

The lemma does not hold for $L > p$.

We finish the proof of Hasse's theorem. In view of the last two lemmas and the above choice of J and L, we get for the number n of solutions of $g(x) = 1$ the inequalities

$$nL \leq \deg \varphi \ \text{ and } \ n < \frac{pJ + \frac{p-5}{2} + \frac{3(p-1)}{2}}{L} < \frac{p}{2} + \frac{23p}{L} < \frac{p}{2} + 46\sqrt{p}\,.$$

This is the required bound on n. To prove the same bound on n' — literally the same, $p/2 + 46\sqrt{p}$ — it suffices to change the + sign in the definition of the polynomials $\psi_l(x)$ in the above lemma to − (the reduction polynomial $g(x) - 1$

is replaced with $g(x)+1$). Since $2n \le N \le 2n+3$ and $n \ge p - n' - 3 > p/2 - 46\sqrt{p} - 3$, we get the explicit bound

$$|N - p| < 92\sqrt{p} + 6 < 95\sqrt{p} \quad (p \ge 7) \; .$$

Clearly, the bound $|N-p| < 95\sqrt{p}$ holds for the primes $p = 2, 3, 5$ too. The constant in the $O(\sqrt{p})$ error term for N is indeed absolute, independent of the coefficients a, b, c, d. The proof of Hasse's theorem is complete. □

Another elementary proof of Hasse's theorem was given by Manin [21], see the book of Gel'fond and Linnik [13, Chapter 10]. Manin's proof uses the group structure of points on elliptic curves and works with the solutions of $y^2 = ax^3 + bx^2 + cx + d$ in the field of rational functions $\mathbf{C}(t)$.

The Chevalley–Warning theorem and Alon's combinatorial Nullstellensatz

In one of the lemmas above we proved that any system of m homogeneous linear equations with n unknowns, $n > m$, has a nontrivial solution $(s_1, \ldots, s_n)$ with at least one $s_i \neq 0$. In fact, if the coefficient field (finite or infinite) is K, there exist at least $|K|$ distinct solutions, obtained by multiplying the nontrivial solution by elements of K. The next theorem is a generalization to higher degree systems.

Theorem (Chevalley–Warning). *Suppose that $P_1, \ldots, P_m \in \mathbf{F}_q[x_1, \ldots, x_n]$ are m nonzero polynomials with coefficients in the finite field $\mathbf{F}_q$ with $q = p^k$ elements and*

$$\deg P_1 + \cdots + \deg P_m < n \; .$$

Then

$$\#\{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{F}_q^n \mid P_1(\alpha) = \cdots = P_1(\alpha) = 0\} \equiv 0 \pmod{p} \; .$$

This was proved by Chevalley [7] and Warning [31]. If the polynomials have zero constant terms then the system of equations has always the trivial all-zeros solution, and the theorem implies that there must be another solution:

Corollary. *If the polynomials P_i are as in the theorem and have zero constant terms, then the system of equations $P_1 = \cdots = P_m = 0$ has a solution with at least one nonzero coordinate.*

Before proving the theorem we present a nice combinatorial application.

Corollary. *Any finite loopless multigraph $G = (V, E)$ (multiple edges are allowed) that arises from a 4-regular multigraph (each vertex incides with four edges) by adding one edge contains a nonempty 3-regular submultigraph G'.*

Proof. We associate with each vertex $v \in V$ of G the equation

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

where $a(e, v) = 1$ if $v \in e$ and is 0 else and the coefficients are understood as elements of the field $\mathbf{Z}_3$. G has $(4|V| + 2)/2 = 2|V| + 1$ edges. This is also the number of unknowns, which thus exceeds the sum of degrees $2|V|$ of the equations. By the previous Corollary, the system of equations has a solution $(\alpha_e, \ e \in E) \in \mathbf{Z}_3^{|E|}$ with at least one nonzero coordinate. We set

$$E' = \{e \in E \mid \alpha_e \neq 0\} \text{ and } \ V' = \bigcup E' \subset V \, .$$

This gives a nonempty submultigraph $G' = (V', E')$. Since $\alpha^2 = 1$ for every $\mathbf{Z}_3^\times$, we get that the degree of any vertex $v' \in V'$ in G' is divisible by 3, because $\sum_{e \in E'} a(e, v')$ is 0 in $\mathbf{Z}_3$. But the degrees in G' lie in the set $\{1, 2, 3, 4, 5\}$, and thus are all equal to 3. □

Lecture 9, December 4, 2012

We prove the Chevalley–Warning theorem and then deduce by means of it another interesting result. Let N be the number of solutions of the system $P_1 = P_2 = \cdots = P_m = 0_F$ in the finite field $F = \mathbf{F}_q$ with characteristic p. Then

$$N_F = \sum_{\alpha \in F^n} \prod_{i=1}^{m} \left(1_F - P_i(\alpha)^{|F|-1}\right) \, ,$$

where N_F is the sum of N elements 1_F in the field F. This follows from the fact that $0_F^{|F|-1} = 0_F$ and $\beta^{|F|-1} = 1_F$ if $\beta \in F$ is nonzero. We show that the sum is in fact 0_F. Thus $N_F = 0_F$, which implies that N is a multiple of p.

Let $D = (|F| - 1)(\deg P_1 + \cdots + \deg P_m)$. Expanding the powers and the product, we get the expression

$$N_F = \sum_{\alpha \in F^n} \sum_{k \in \mathbf{N}_0^n, \ k_1 + \cdots + k_n \leq D} c_k \prod_{i=1}^{n} \alpha_i^{k_i}, \ \ c_k \in F \, ,$$

which is the same as the expression

$$N_F = \sum_{k \in \mathbf{N}_0^n, \ k_1 + \cdots + k_n \leq D} c_k \prod_{i=1}^{n} \sum_{\alpha_i \in F} \alpha_i^{k_i} \, .$$

Since, by the assumption, $D < (|F|-1)n$, from $k_1 + \cdots + k_n \le D$ it follows that each n-tuple $k = (k_1, \ldots, k_n)$ in the sum contains a coordinate k_j that is smaller than $|F| - 1$. If $k_j = 0$, it follows from the former expression that the sum $\sum_{\alpha_j \in F} \alpha_j^{k_j}$ is to be interpreted as $1_F + \cdots + 1_F$ with $|F|$ summands 1_F (in question is the value of 0_F^0), and so it equals $|F|_F = 0_F$, as $|F| \equiv 0 \bmod p$. If $1 \le k_j < |F| - 1$, again

$$\sum_{\alpha_j \in F} \alpha_j^{k_j} = 0_F \ .$$

This follows from the fact that the group $(F^\times, \cdot)$ is cyclic, with a generator g — we proved this fact in the fifth lecture in the case of $F = \mathbf{Z}_p$, but the proof works without change for any finite field — and therefore for any nonzero number $r \in \mathbf{Z}$ not divisible by $|F| - 1$ we have

$$\sum_{\gamma \in F} \gamma^r = \sum_{\gamma \in F} (g\gamma)^r = g^r \sum_{\gamma \in F} \gamma^r = 0_F \ ,$$

as $g^r \ne 1_F$. Thus each product is 0_F and so is the whole sum. □

The following result was proved by Erdős, Ginzburg and Ziv [11] fifty years ago.

Theorem (Erdős–Ginzburg–Ziv). *Let $n \in \mathbf{N}$. Among every $2n-1$ (not necessarily distinct) integers some n of them sum up to a multiple of n.*

Proof. We give proof only for prime modulus $n = p$, and leave extension to arbitrary n as an exercise. Suppose $a_1, \ldots, a_{2p-1}$ are the given integers. We consider in the field $\mathbf{Z}_p$ the two equations

$$\sum_{i=1}^{2p-1} a_i x_i^{p-1} = \sum_{i=1}^{2p-1} x_i^{p-1} = 0 \ .$$

The system has the trivial all-zeros solution. By the Ch.–W. theorem it has also a nontrivial solution $s_1, \ldots, s_{2p-1}$, because the number of unknowns $2p-1$ exceeds the sum of degrees $(p-1) + (p-1) = 2p-2$. Let I be the set of $i \in \{1, 2, \ldots, 2p-1\}$ with nonzero s_i; $I \ne \emptyset$. Since $\alpha^{p-1} = 1$ for any $\alpha \in \mathbf{Z}_p^\times$, after setting $x_i = s_i$ the two equations give, respectively,

$$\sum_{i \in I} a_i = 0 \quad \text{and} \quad \sum_{i \in I} 1 = 0 \ .$$

Thus both $\sum_{i \in I} a_i$ and $|I|$ is divisible by p and, since $0 < |I| < 2p$, $|I| = p$. □

The $(2n-2)$-tuple of $n-1$ 0s and $n-1$ 1s shows that the value $2n-1$ in the theorem cannot be decreased.

The next theorem was proved by Alon [2], who in his article obtains by means of it many interesting combinatorial results. Of these we present below just one, a geometric result on cube and hyperplanes.

Theorem (combinatorial Nullstellensatz). *Suppose $n \in \mathbf{N}$, F is a field (or even an integral domain),*

$$f \in F[x_1, x_2, \ldots, x_n]$$

is a nonzero polynomial and $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$, $k_i \in \mathbf{N}_0$, is a maximum degree monomial in f (i.e., $k_1 + \cdots + k_n = \deg f$) with nonzero coefficient. Then for any n-tuple of subsets $A_i \subset F$ with $|A_i| \geq k_i + 1$ there exist elements $a_i \in A_i$ such that

$$f(a_1, a_2, \ldots, a_n) \neq 0 \, .$$

Proof. By induction on $\deg f$. For $\deg f = 0$ the result is trivial. Let $\deg f > 0$ and the $k_i \in \mathbf{N}_0$ and $A_i \subset F$ be given. We may assume that $k_1 \geq 1$ and take an arbitrary element $a_1 \in A_1$. We express f as

$$f = (x_1 - a_1)g + h \, ,$$

where $g \in F[x_1, x_2, \ldots, x_n]$ with $\deg g = \deg f - 1$ and $h \in F[x_2, x_3, \ldots, x_n]$. This follows from the division algorithm in the ring $R[x_1]$, $R = F[x_2, \ldots, x_n]$: we divide by the monic polynomial $x_1 - a_1$ and get a remainder h with degree 0 in x_1. Clearly, in g the maximum degree monomial $x_1^{k_1 - 1} x_2^{k_2} \ldots x_n^{k_n}$ has nonzero coefficient.

We distinguish two cases: (i) $h(a_2, \ldots, a_n) \neq 0$ for some $a_2 \in A_2, \ldots, a_n \in A_n$ and (ii) $h(a_2, \ldots, a_n) = 0$ for every $a_2 \in A_2, \ldots, a_n \in A_n$. If (i) occurs, we are done:

$$f(a_1, a_2, \ldots, a_n) = h(a_2, \ldots, a_n) \neq 0 \, .$$

In the case (ii) we apply inductive assumption to g, the exponents $k_1 - 1, k_2, \ldots, k_n$ and sets $A_1 \backslash \{a_1\}, A_2, \ldots, A_n$: there exist elements $b_i \in A_i$, $b_1 \neq a_1$, such that $g(b_1, \ldots, b_n) \neq 0$. Then

$$f(b_1, b_2, \ldots, b_n) = (b_1 - a_1) g(b_1, \ldots, b_n) \neq 0 \, ,$$

and we are done as well. □

The proof of Alon's theorem was simplified in several articles and the above, in our opinion ultimately simple, proof is due to Michałek [25]; we smoothed his presentation further a tiny bit. In retrospect, the proof is such a straightforward generalization of the argument in the univariate case that no nonzero polynomial $f \in F[x]$ with degree d vanishes identically on a $(d+1)$-element set $A \subset F$ — express f as $f = (x - a)g + h$, where $a \in A$, $g \in F[x]$ has degree by 1 less than f and $h \in F$, and apply induction to g — that one wonders why this proof was not found (much) earlier.

Proposition. *In the n-dimensional Euclidean space $\mathbf{R}^n$, one cannot cover all 2^n vertices of the unit cube but one by less than n hyperplanes.*

Proof. Let $H_i \subset \mathbf{R}^n$, $i = 1, 2, \ldots, m$, be some m hyperplanes, H_i given by the equation

$$p_i(x) = p_i(x_1, \ldots, x_n) = \alpha_{i,1}x_1 + \cdots + \alpha_{i,n}x_n + \beta_i = 0,\ \alpha_{i,j}, \beta_i \in \mathbf{R}\ .$$

Suppose that their union contains each of the 2^n vectors $\{0,1\}^n$ except the origin $(0, 0, \ldots, 0)$. Thus every β_i is nonzero. We show that $m \geq n$.

Let us suppose for contradiction that $m < n$. Consider the polynomial

$$f(x) = \beta_1 \ldots \beta_m (1 - x_1) \ldots (1 - x_n) - p_1(x) \ldots p_m(x) \in \mathbf{R}[x_1, \ldots, x_n]\ .$$

Since the subtracted term has degree $m < n$, it follows that $f(x)$ has degree n and the monomial $x_1 x_2 \ldots x_n$ has in $f(x)$ nonzero coefficient, namely $(-1)^n \beta_1 \ldots \beta_m$. The polynomial $f(x)$ vanishes at each of the 2^n vectors $\{0,1\}^n$: at the origin it gives value $\beta_1 \ldots \beta_m - \beta_1 \ldots \beta_m = 0$, and at each $(v_1, \ldots, v_n)$ with $v_i \in \{0,1\}$ and at least one $v_i = 1$ both terms in the difference are zero. But by Alon's c. N., with $A_i = \{0,1\}$ for $i = 1, 2, \ldots, n$, there exists a vector in $\{0,1\}^n$ on which $f(x)$ has nonzero value. This is a contradiction. □

We remark that just two hyperplanes $x_1 = 0$ and $x_1 = 1$ cover all 2^n vertices of the unit cube, and n hyperplanes $x_1 = 1, x_2 = 1, \ldots, x_n = 1$ cover all vertices but the origin.

Lecture 10, December 11, 2012

The Skolem–Mahler–Lech theorem on zero sets of recurrence sequences

If F is a field, by a *recurrence sequence (in F)* — the precise denomination would be a *sequence satisfying a homogeneous linear recurrence relation with constant coefficients* — we mean a sequence

$$a = (a_n) = (a_0, a_1, a_2, \ldots) \subset F$$

such that for some $k \geq 1$ elements $\alpha_0, \ldots, \alpha_{k-1} \in F$, not all of them zero, we have $\sum_{i=0}^{k-1} \alpha_i a_{n+i} = 0$ for every $n \in \mathbf{N}_0$. In other words, there exist $\alpha_1, \ldots, \alpha_k \in F$, $\alpha_k \neq 0$, such that

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k},\ n \geq k\ .$$

If $(a_n) \subset F$ is any sequence, $m \in \mathbf{N}$ and $i \in \{0, 1, \ldots, m-1\}$, the *$i$-th m-section of* (a_n) is the subsequence

$$(a_{i+mn})_{n \geq 0} = (a_i, a_{i+m}, a_{i+2m}, \ldots)$$

of terms in (a_n) with the index $n \equiv i \bmod m$. We will prove a particular case of the next theorem that characterizes occurrences of zeros in recurence sequences.

Theorem (Skolem–Mahler–Lech). *Suppose F is a field of characteristic 0 and $(a_n) \subset F$ is a recurrence sequence. Then there exists an $m \in \mathbf{N}$ such that each of the m-sections of (a_n) is either identically zero or contains only finitely many zeros: for each $i \in \{0, 1, \dots, m-1\}$,*

$$a_{i+mn} = 0$$

holds either for all $n \in \mathbf{N}_0$ or for only finitely many $n \in \mathbf{N}_0$.

We will prove the theorem only for the field of fractions $F = \mathbf{Q}$. It turns out that the general case reduces to this one by certain algebraic specialization arguments, which we will not have time to present. The theorem was proved first for $F = \mathbf{Q}$ by Skolem [28], for F being a number field (i.e., when F has finite dimension as a vector space over $\mathbf{Q}$) by Mahler [20] and in the general case by Lech [19]. Below we give an example (due to Lech) showing that in fields with positive characteristic the theorem no longer holds.

Before we begin with the proof we reformulate the theorem and give a few remarks and examples. For a sequence $a = (a_n)$ we denote by

$$Z(a) = \{n \in \mathbf{N}_0 \mid a_n = 0\}$$

the zero set of the sequence. The SML theorem says, equivalently, that the zero set of any recurrence sequence in a field with characteristic 0 has form

$$Z(a) = S \cup A_1 \cup A_2 \cup \cdots \cup A_t,\ t \in \mathbf{N}_0\ ,$$

where $S \subset \mathbf{N}_0$ is a finite set and each $A_i \subset \mathbf{N}_0$ is an infinite arithmetic progression $j + d\mathbf{N}_0 = \{j, j+d, j+2d, \dots\}$ with $j \in \mathbf{N}_0$ and $d \in \mathbf{N}$ (possibly depending on i).

Speaking of recurrence sequences, multiplication of rabbits and the *Fibonacci sequence* come in mind, our **first example:** $F = \mathbf{Q}$ and

$$a = (a_n) = (1, 1, 2, 3, 5, 8, 13, 21, 34, \dots)\ ,$$

given by

$$a_n = a_{n-1} + a_{n-2},\ a_0 = a_1 = 1\ .$$

Thus, clearly (since the a_n strictly increase) $Z(a) = \emptyset$.

Somebody might object that according to her/his definition of Fibonacci numbers, the initial values are $a_0 = 0$, $a_1 = 1$ and the sequence starts $a = (a_n) = (0, 1, 1, 2, 3, 5, 8, \dots)$, hence $Z(a) = \{0\}$. Should the very size of the zero set of the Fibonacci sequence depend on reglementing where it starts? This trouble is resolved by regarding recurrence sequences as defined on $\mathbf{Z}$, rather

than $\mathbf{N}_0$. We revert the recurrence and by running the sequence backwards extend it from $\mathbf{N}_0$ to $\mathbf{Z}$:

$$\begin{aligned} & a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k},\ \alpha_k \neq 0 \\ \iff & a_{n-k} = -\alpha_k^{-1}\alpha_{k-1}a_{n-k+1} - \cdots - -\alpha_k^{-1}\alpha_1 a_{n-1} - \alpha_k^{-1} a_n\ . \end{aligned}$$

For the Fibonacci sequence, $a_{n-2} = -a_{n-1} + a_n$ gives the extension

$$a = (a_n)_{n\in\mathbf{Z}} = (\dots, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, \dots)\ .$$

Now it is easy to see that $|Z(a)| = 1$, no matter where the sequence exactly 'begins'.

Nevertheless, we will stick to sequences defined on $\mathbf{N}_0$. It is not too hard to prove that the SML theorem for recurrence sequences of the type $(a_n)_{n\in\mathbf{N}_0}$ is equivalent to the version for recurrence sequences of the type $(a_n)_{n\in\mathbf{Z}}$. We prove equivalence of both versions at the end.

In the **second example,** $F = \mathbf{Q}$ and

$$a_n = (n-6)(1+(-1)^n)\ .$$

Then

$$Z(a) = \{6\} \cup (1 + 2\mathbf{N}_0)\ .$$

Since $a_n - a_{n-2} = 2(1+(-1)^n)$, we see that (a_n) is indeed a recurrence sequence:

$$a_{n+2} - 2a_n + a_{n-2} = (a_{n+2} - a_n) - (a_n - a_{n-2}) = 0,\ n \geq 2\ .$$

The **third example** demonstrates that zero sets of recurrence sequences in fields with characteristic p need not have form described in the SML theorem.

Proposition. *Let p be a prime number and $F = \mathbf{Z}_p(x)$, the field of rational functions with coefficients in the finite field $\mathbf{Z}_p$. The sequence $a = (a_n) \subset F$, given by*

$$a_n = (1+x)^n - 1 - x^n,\ n \in \mathbf{N}_0\ ,$$

has zero set

$$Z(a) = \{1, p, p^2, p^3, p^4, \dots\}\ ,$$

and is a recurrence sequence: there exist coefficients $\alpha, \beta, \gamma, \delta \in F$, not all four zero, such that

$$\alpha a_{n+3} + \beta a_{n+2} + \gamma a_{n+1} + \delta a_n = 0,\ n \geq 0\ .$$

Proof. In any field F with $\mathrm{char}(F) = p$,

$$\binom{p}{i_1, i_2, \dots, i_k} = \frac{p!}{i_1! i_2! \dots i_k!} \in \{0, 1\}\ ,$$

with the value 1 iff some $i_j = p$ (and $i_{j'} = 0$ for $j' \neq j$); this follows from the fact that if no $i_j = p$, then the multinomial coefficient is divisible by p. It folows that for any $\alpha_1, \dots, \alpha_k \in F$ and $r \in \mathbf{N}$,

$$(\alpha_1 + \cdots + \alpha_k)^{p^r} = \alpha_1^{p^r} + \cdots + \alpha_k^{p^r} \ .$$

Thus for $n \in \mathbf{N}$ in the form $n = mp^k$, $k \in \mathbf{N}_0$, $m \in \mathbf{N}$ and $(m, p) = 1$,

$$(1+x)^n = (1 + mx + \cdots + x^m)^{p^k} = 1 + (mx)^{p^k} + \cdots + x^n \neq 1 + x^n \ \text{ if } \ m > 1 \ .$$

For $m = 1$ we have $(1+x)^n = 1 + x^n$. So $a_n = 0$ exactly if n is a power of p.

To show that (a_n) is a recurrence sequence, consider the system of three homogeneous linear equations with four unknowns α, β, γ and δ:

$$\begin{aligned} \alpha(1+x)^3 + \beta(1+x)^2 + \gamma(1+x) + \delta &= 0 \\ \alpha + \beta + \gamma + \delta &= 0 \\ \alpha x^3 + \beta x^2 + \gamma x + \delta &= 0 \ . \end{aligned}$$

As we know from the above Proposition (in lecture 7), this system has a non-trivial solution $\alpha, \beta, \gamma, \delta \in F$. But $a_{n+k} = (1+x)^k(1+x)^n - 1 - x^k x^n$, and using this for $k = 0, 1, 2, 3$ we get, for every $n \in \mathbf{N}_0$,

$$\alpha a_{n+3} + \beta a_{n+2} + \gamma a_{n+1} + \delta a_n = 0(1+x)^n - 0 \cdot 1 - 0x^n = 0 \ .$$

□

Now, to begin with the proof of the SML theorem, we derive for any recurrence sequence $a = (a_0, a_1, a_2, \dots) \subset F$ a matrix representation. The recurrence

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \cdots + \alpha_k a_{n-k}, \ n \geq k \ ,$$

can be equivalently written as

$$\begin{pmatrix} a_n \\ a_{n-1} \\ a_{n-2} \\ \vdots \\ a_{n-k+1} \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_{k-1} & \alpha_k \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ a_{n-3} \\ \vdots \\ a_{n-k} \end{pmatrix}, \ n \geq k \ .$$

We call the square $k \times k$ matrix $M \in F^{k \times k}$ on the right side the *matrix of the recurrence*. It is regular:

$$\det M = (-1)^{k+1} \alpha_k \neq 0 \ .$$

Iterating the relation and using associativity of matrix multiplication, we get a quasi-explicit formula for a_n:

$$a_n = u M^{n-k+1} v = u M^n w, \ n \in \mathbf{N}_0 \ ,$$

where $M \in F^{k\times k}$ is the matrix of the recurrence, $u = (1, 0, \dots, 0) \in F^{1\times k}$ is a row vector and $v = (a_{k-1}, a_{k-2}, \dots, a_0)^t \in F^{k\times 1}$ and $w = M^{1-k}v \in F^{k\times 1}$ are column vectors.

This matrix formula for a_n works in any field F but from now we confine to fractions, $F = \mathbf{Q}$. First we reduce the problem to the situation when all entries in the matrix formula are integers.

Lemma. *If $a = (a_0, a_1, \dots) \subset \mathbf{Q}$ is a recurrence sequence given by*

$$a_n = \sum_{i=1}^{k} \alpha_i a_{n-i},\ \alpha_i \in \mathbf{Q},\ \alpha_k \neq 0\ ,$$

then there exist a $d \in \mathbf{N}$, integral vectors $u = (1, 0, \dots, 0) \in \mathbf{Z}^{1\times k}$ and $w \in \mathbf{Z}^{k\times 1}$ and a regular integral matrix $M \in \mathbf{Z}^{k\times k}$ such that

$$d^{n+1}a_n = uM^n w \in \mathbf{Z},\ n \in \mathbf{N}_0\ .$$

Proof. We have the matrix formula $a_n = u(M')^n w'$, where $u = (1, 0, \dots, 0)$, M' is the matrix of the recurrence and the entries of M' and w' lie in $\mathbf{Q}$. We take a common multiple $d \in \mathbf{N}$ of the denominators of the entries in M' and w', and set $M = dM'$ (each entry in M' is multiplied by d) and $w = dw'$. Then $M \in \mathbf{Z}^{k\times k}$ and is regular, $w \in \mathbf{Z}^{k\times 1}$ and

$$\mathbf{Z} \ni uM^n w = d^{n+1}u(M')^n w' = d^{n+1}a_n\ .$$

□

Of course, the point is that the two sequences $a'_n = d^{n+1}a_n$ and a_n have the same zero set:

$$Z(a') = Z(a)\ .$$

Next, we transform the integral matrix formula into an expansion of each m-section, for some $m \in \mathbf{N}$, of the sequence to powers of a prime p.

Proposition. *Suppose that $u \in \mathbf{Z}^{1\times k}$, $w \in \mathbf{Z}^{k\times 1}$, $M \in \mathbf{Z}^{k\times k}$ is a regular matrix,*

$$a_n = uM^n v,\ n = 0, 1, \dots\ ,$$

and p is a prime number not dividing $\det M$. Then there exists a number $m \in \mathbf{N}$ such that for each $i \in \{0, 1, \dots, m-1\}$ there is a sequence $(b_0, b_1, b_2, \dots) \subset \mathbf{Z}$ such that

$$a_{i+ml} = \sum_{j=0}^{l} \binom{l}{j} p^j b_j,\ l = 0, 1, 2, \dots\ .$$

Proof. We claim that there is an $m \in \mathbf{N}$ such that

$$M^m = I + pN$$

where I is the identity $k \times k$ matrix and $N \in \mathbf{Z}^{k\times k}$. Indeed, if we reduce the entries in M mod p, we get a matrix $\overline{M} \in \mathbf{Z}_p^{k\times k}$ that is still regular because $\det \overline{M} = \overline{\det M} \neq 0$. Thus for m we may take the order of $\overline{M}$ in the (finite and noncommutative) multiplicative group of regular matrices in $\mathbf{Z}_p^{k\times k}$, or we may set m to be the order of this group. Anyway, $m < p^{k^2}$. Writing $n = i + ml$, $0 \leq i < m$, we get by the binomial formula that

$$a_{i+ml} = uM^i(I + pN)^l w = \sum_{j=0}^{l} \binom{l}{j} p^j (uM^i N^j w) = \sum_{j=0}^{l} \binom{l}{j} p^j b_j \ ,$$

where $b_j = uM^i N^j w \in \mathbf{Z}$. Eventhough the matrix ring is noncommutative, we may use the binomial formula as in the commutative case because the matrices I and N commute. □

Now it is clear that the SML theorem for $F = \mathbf{Q}$ follows from the previous lemma and proposition and the next proposition.

Proposition. *Suppose p is a prime with $p > 2$ and $(b_0, b_1, b_2, \dots) \subset \mathbf{Z}$ is a sequence of integers, not all of them zero. Then the equation*

$$\sum_{j=0}^{l} \binom{l}{j} p^j b_j = 0$$

has only finitely many solutions $l \in \mathbf{N}_0$.

The last proposition does not hold for $p = 2$: Since

$$1 = (2-1)^l = \sum_{j=0}^{l} \binom{l}{j} 2^j (-1)^{l-j} = (-1)^l \sum_{j=0}^{l} \binom{l}{j} 2^j (-1)^j \ ,$$

for $p = 2$ and $(b_0, b_1, b_2, \dots) = (0, -1, 1, -1, 1, \dots)$ the equation is solved by every even number $l = 0, 2, 4, 6, \dots$.

Lecture 11, December 18, 2012

It remains to prove the last proposition. We deduce it as a corollary of a more general result on infinite systems of polynomial congruences. For a prime p, we call a fraction $\frac{a}{b} \in \mathbf{Q}$ *p-integral* if $\operatorname{ord}_p(a/b) = \operatorname{ord}_p(a) - \operatorname{ord}_p(b) \geq 0$, that is, $\frac{a}{b}$ in lowest terms has denominator coprime to p. It is easy to see that the product and sum of two p-integral fractions is again p-integral. Thus

$$\mathbf{Q}_{(p)} := \{\alpha \in \mathbf{Q} \mid \ \alpha \text{ is } p\text{-integral}\}$$

contains $\mathbf{Z}$ and forms a subring of the field $\mathbf{Q}$. The notion of congruence to a power of p extends from $\mathbf{Z}$ to $\mathbf{Q}_{(p)}$: if $r \in \mathbf{N}_0$ and $\alpha, \beta \in \mathbf{Q}_{(p)}$, we define

$$\alpha \equiv \beta \pmod{p^r} \iff \operatorname{ord}_p(\alpha - \beta) \geq r \ .$$

A *Skolem system* $\mathcal{S}$, for a given prime p, is an infinite sequence of polynomial congruences

$$p_j(x) \equiv 0 \pmod{p^{i_j}}, \ j = 0, 1, 2, \dots \ ,$$

such that each $p_j \in \mathbf{Q}_{(p)}[x]$, $0 \leq i_1 \leq i_2 \leq \dots$ and i_j go to $+\infty$, and the coefficients of the polynomials p_j satisfy the *coherence condition*

$$p_j(x) \equiv p_{j+1}(x) \pmod{p^{i_j}} \ ,$$

meaning that for each $n \in \mathbf{N}_0$ the coefficient of x^n in p_j is modulo p^{i_j} the same as in p_{j+1} (hence $p_j(x) \equiv p_{j'}(x) \pmod{p^{i_j}}$ for each $j' \geq j$); powers x^n with n exceeding the degree have zero coefficient by default. A *solution of* $\mathcal{S}$ is any $\alpha \in \mathbf{Q}_{(p)}$ satisfying each of the congruences:

$$p_j(\alpha) \equiv 0 \pmod{p^{i_j}}, \ j \in \mathbf{N}_0 \ .$$

The coherence condition implies that if α solves the j-th congruence, then it solves each earlier congruence with index j', $0 \leq j' \leq j$.

For a given Skolem system $\mathcal{S}$, we denote by $\overline{p_j}(x) \in \mathbf{Z}_{p^{i_j}}[x]$ the polynomial obtained from $p_j(x)$ by the mod p^{i_j} reduction, that is, we replace each coefficient by its residue modulo p^{i_j}. If at least one polynomial $\overline{p_j}(x)$ is nonzero, we call $\mathcal{S}$ a *nonzero Skolem system*. Clearly, zero Skolem systems (with all polynomials $\overline{p_j}(x)$ being zero) are solved by every $\alpha \in \mathbf{Q}_{(p)}$. We are going to show that any nonzero Skolem system has only finitely many solutions. The coherence condition implies that if x^n has in $\overline{p_j}(x)$ nonzero coefficient, then this coefficient remains nonzero in every $\overline{p_{j'}}(x)$ with $j' \geq j$. Thus if $\mathcal{S}$ is nonzero and $j_0 \in \mathbf{N}_0$ is the first index with $\overline{p_{j_0}}(x) \neq 0$, then $\overline{p_j}(x) \neq 0$ for every $j \geq j_0$ and

$$\deg \overline{p_{j_0}}(x) \leq \deg \overline{p_{j_0+1}}(x) \leq \deg \overline{p_{j_0+2}}(x) \leq \dots \ .$$

We define $\deg \mathcal{S}$, the *degree of the (nonzero) Skolem system* S, to be the degree $\deg \overline{p_{j_0}}$ of the first nonzero reduction in $\mathcal{S}$.

Proposition. *Let p be a prime and $\mathcal{S}$ be a nonzero Skolem system of polynomial congruences*

$$\mathbf{Q}_{(p)}[x] \ni p_j(x) \equiv 0 \pmod{p^{i_j}}, \ j = 0, 1, 2, \dots \ ,$$

with degree d. $\mathcal{S}$ has at most d solutions in p-integral fractions $x = \alpha \in \mathbf{Q}_{(p)}$.

We give the proof in the next (and final) lecture and conclude this one by showing how this result implies finiteness of the solution set for $l \in \mathbf{N}_0$ of the binomial equation

$$\sum_{j=0}^{l} \binom{l}{j} p^j b_j = 0 \ ,$$

where $p > 2$ is a prime and the $b_j \in \mathbf{Z}$ are given coefficients, not all zero.

First, there is a nondecreasing sequence $i_0 \le i_1 \le \dots$ of $i_j \in \mathbf{N}_0$ such that $\lim_j i_j = +\infty$ and

$$\mathrm{ord}_p(p^j/j!) \ge i_j,\ j = 0, 1, \dots \ .$$

Indeed, by the old result of Legendre on prime factorization of factorials,

$$\mathrm{ord}_p(p^j/j!) = j - \sum_{k\ge 1} \left\lfloor \frac{j}{p^k} \right\rfloor \ge j\left(1 - \sum_{k=1}^{\infty} \frac{1}{p^k}\right) = \frac{(p-2)j}{p-1} \ge 0 \text{ and } \to +\infty$$

for $j \to \infty$, because $p > 2$. Thus for $j = 0, 1, \dots$ we may set

$$i_j = \left\lfloor \frac{(p-2)j}{p-1} \right\rfloor \ .$$

For $j = 0, 1, \dots$, we consider the sequence $\mathcal{S}$ of congruences

$$p_j(x) := \sum_{k=0}^{j} \binom{x}{k} p^k b_k = \sum_{k=0}^{j} \frac{p^k}{k!} x(x-1)\dots(x-k+1) b_k \equiv 0 \pmod{p^{i_j}} \ .$$

We claim that $\mathcal{S}$ is a nonzero Skolem system and that each solution $l \in \mathbf{N}_0$ of the above binomial equation solves $\mathcal{S}$ too. By the last proposition, the above binomial equation has therefore only finitely many solutions.

By the above inequality and definition of the exponents i_j, the coefficients of $p_j(x)$ are p-integral and those of $\binom{x}{j} p^j b_j$ are zero modulo p^{i_j}, let alone modulo $p^{i_j - 1}$. Thus $p_j(x)$ lie in $\mathbf{Q}_{(p)}[x]$ and satisfy the coherence condition. Suppose that $b_0 = b_1 = \dots = b_{r-1} = 0$ but $b_r \ne 0$. Since the roots of $\binom{x}{j}$ are exactly $0, 1, \dots, j-1$, we see that

$$p_j(r) = p_r(r) = \binom{r}{r} p^r b_r = p^r b_r \ne 0 \text{ for every } j \text{ with } j \ge r \ .$$

We take j large enough so that $j \ge r$ and $i_j > \mathrm{ord}_p(p^r b_r)$. It follows that for each such j the reduction $\overline{p_j}(x)$ is nonzero (as $p_j(x)$ attains on r a value that is nonzero mod p^{i_j}) and thus $\mathcal{S}$ is a nonzero Skolem system. Finally, suppose that $l \in \mathbf{N}_0$ is such that

$$\sum_{j=0}^{l} \binom{l}{j} p^j b_j = 0 \ .$$

We claim that $p_j(l) \equiv 0 \mod p^{i_j}$ for every $j \in \mathbf{N}_0$. Indeed, for $j = l$ this holds even as an equality, hence for $j < l$ it holds by the coherence condition satisfied by $\mathcal{S}$, and for $j > l$ it holds by the fact that each $\binom{x}{k}$, $k > l$, vanishes at $x = l$. Hence l solves $\mathcal{S}$.

This concludes, modulo the proof of the last proposition, the proof of the SML theorem for fractions.

Lecture 12, January 8, 2013

We prove the last proposition, which bounds the number of solutions of a nonzero Skolem system. Let us first recall the proof of the more elementary but basic result that each polynomial equation

$$F[x] \ni p(x) = 0 \ ,$$

where $p(x)$ is a nonzero polynomial with coefficients in a field F and degree d, has at most d solutions $x = \alpha \in F$. It goes by induction on d. If $d = 0$, there is no solution ($p(x)$ is a nonzero constant). Let $d > 0$ and $\alpha \in F$ be a solution (if there is still no solution, the claim holds trivially). Write, by the division algorithm,

$$p(x) = (x - \alpha)q(x) + p(\alpha) = (x - \alpha)q(x) \ ,$$

where $q \in F[x]$ is nonzero and of degree $d - 1$. If $\beta \in F$, $\beta \neq \alpha$, is another solution, then $0 = p(\beta) = (\beta - \alpha)q(\beta)$ and $q(\beta) = 0$. Thus β is also a solution of the equation $q(x) = 0$, and there are at most $d - 1$ of these, by induction. Thus in total $p(x) = 0$ has at most $1 + (d - 1) = d$ solutions.

We will mimick this proof for Skolem systems. We already extended it to multivariate polynomials, when proving (after Michałek) the Combinatorial Nullstellensatz in lecture 9.

Proof of the last proposition. Suppose p is a prime and

$$p_j(x) \equiv 0 \pmod{p^{i_j}}, \ j = 0, 1, 2, \dots \ ,$$

is a nonzero Skolem system $\mathcal{S}$. We may assume that already $\overline{p_0}(x)$ is nonzero and thus $\deg \mathcal{S} = \deg(\overline{p_0}) = d \in \mathbf{N}_0$. We prove by induction on d that $\mathcal{S}$ has at most d solutions $\alpha \in \mathbf{Q}_{(p)}$. This is true if $d = 0$, for then already the first congruence $p_0(x) \equiv 0 \pmod{p^{i_0}}$ has no solution. We therefore assume that $d > 0$ and $\mathcal{S}$ has a solution $\alpha \in \mathbf{Q}_{(p)}$. Using the division algorithm, we express

$$p_j(x) = (x - \alpha)q_j(x) + p_j(\alpha), \ j = 0, 1, \dots \ ,$$

where $q_j \in \mathbf{Q}_{(p)}[x]$ and has degree by 1 less than p_j. (Since we divide by a monic polynomial, namely $x - \alpha$, the partial ratio $q_j(x)$ automatically remains in $\mathbf{Q}_{(p)}[x]$.) We claim that (i)

$$q_j(x) \equiv 0 \pmod{p^{i_j}}, \ j = 0, 1, 2, \dots \ ,$$

is a nonzero Skolem system $\mathcal{S}'$ with degree $d - 1$ and (ii) any other solution $\beta \in \mathbf{Q}_{(p)}$, $\beta \neq \alpha$, of $\mathcal{S}$ solves $\mathcal{S}'$ as well. Induction then gives that $\mathcal{S}$ has at most $1 + (d - 1) = d$ solutions.

To show that $q_j(x)$ satisfy the coherence condition, we express their coefficients in terms of those of $p_j(x)$. Let $\deg p_j = d_j$ and the coefficient of x^n in $p_j(x)$ be $a_{j,n}$. Then

$$q_j(x) = \sum_{n=1}^{d_j} a_{j,n} \frac{x^n - \alpha^n}{x - \alpha} = \sum_{n=1}^{d_j} a_{j,n}(x^{n-1} + x^{n-2}\alpha + \cdots + x\alpha^{n-2} + \alpha^{n-1}) \ .$$

The coherence condition for $\mathcal{S}$ implies that modulo p^{i_j} this expression is identical to that for $j+1$ and thus, modulo p^{i_j}, the polynomials $q_j(x)$ and $q_{j+1}(x)$ have identical coefficients. Setting $j = 0$ and reducing mod p^{i_0}, we get

$$\overline{p_0}(x) = (x - \overline{\alpha})\overline{q_0}(x) \; .$$

Thus $\overline{q_0}(x)$ is nonzero and has degree $\deg \overline{p_0} - 1 = d - 1$. We have proven the claim (i).

To prove the crucial claim (ii), we take a $\beta \in \mathbf{Q}_{(p)}$ distinct from α that solves $\mathcal{S}$. We need to show that $q_j(\beta) \equiv 0 \bmod p^{i_j}$ for each $j \in \mathbf{N}_0$. Let $j \in \mathbf{N}_0$ be given. We take $k \in \mathbf{N}_0$ large enough so that $k \geq j$ and

$$i_k - \mathrm{ord}_p(\beta - \alpha) \geq i_j$$

(which is possible as $\beta - \alpha \neq 0$ and $i_k \to +\infty$). We set $x = \beta$ in the equality defining $q_k(x)$:

$$p_k(\beta) = (\beta - \alpha)q_k(\beta) + p_k(\alpha) \; .$$

From this equality it follows that $\mathrm{ord}_p(q_k(\beta))$ is at least

$$\min(\mathrm{ord}_p(p_k(\beta)), \mathrm{ord}_p(p_k(\alpha))) - \mathrm{ord}_p(\beta - \alpha) \geq i_k - \mathrm{ord}_p(\beta - \alpha) \geq i_j \; .$$

That is, $q_k(\beta) \equiv 0 \bmod p^{i_j}$. Since $q_k(\beta) \equiv q_j(\beta) \bmod p^{i_j}$ by the coherence condition for $\mathcal{S}'$, we conclude that $q_j(\beta) \equiv 0 \bmod p^{i_j}$, which we needed to prove. □

We conclude with giving several remarks on the (previous proof of the) SML theorem.

1. The proof we just completed is inspired by Hansel [14] and Fischer [12].

References

[1] M. Aigner and G. Ziegler, *Proofs from THE BOOK*, Springer, 2001 (2nd edition).

[2] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.*, **8** (1999), 7–29. (Presented at 'Recent trends in combinatorics', Mátraháza, 1995.)

[3] A. Baker, Some aspects of transcendence theory, *Astérisque*, **24–25** (1975), 169–175.

[4] A. Baker and G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, Cambridge University Press, 2007.

[5] З. И. Боревич и И. Р. Шафаревич, *Теория чисел*, Издательство Наука, Москва, 1985 (издание третье, дополненное). [Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Publishing House Nauka, Moscow, 1985 (3rd, extended edition).]

[6] J. W. S. Cassels, *Local Fields*, Cambridge University Press, Cambridge (UK), 1986.

[7] C. Chevalley, Démonstration d'une hypothèse de M. Artin, *Abh. Math. Semin. Hamb. Univ.*, **11** (1935), 73–75.

[8] H. Davenport, *Multiplicative Number Theory*, Springer, 2000 (3rd edition, revised by H. L. Montgomery).

[9] L. E. Dickson, On finite algebras, *Nachrichten der Akad. Wissenschaften Göttingen Math.-Phys. Klasse* (1905), 1–36.

[10] Ch. Elsholtz, Prime divisors of thin sequences, *Amer. Math. Monthly*, **119** (2012), 331–333.

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

[12] I. Fischer, *Der Satz von Skolem, Mahler, Lech — ein Ergebnis über die Nullstellen linearer Rekursionsfolgen*, Master thesis, University of Vienna, 1997.

[13] А. О. Гельфонд и Ю. В. Линник, *Элементарные методы в аналитической теории чисел*, Государственное Издательство Физико-математической Литературы, Москва, 1962. [A. O. Gel'fond and Yu. V. Linnik, *Elementary methods in analytic number theory*, State Publishing House of Physico-Mathematical Literature, Moscow, 1962.]

[14] G. Hansel, A simple proof of the Skolem–Mahler–Lech theorem, *Automata, languages and programming (Nafplion, 1985)*, Lecture Notes in Comput. Sci., 194, Springer, Berlin, 1985, 244–249.

[15] H. Hasse, Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II & III, *J. Reine Angew. Math.*, **175** (1936), 55–62, 69–88 and 193–208.

[16] J.-M. de Koninck and F. Luca, *Analytic Number Theory. Exploring the Anatomy of Integers*, AMS, 2012.

[17] S. Lang, *Algebra*, Springer, 2002 (revised 3rd edition).

[18] S. Lang and A. Weil, Number of points of varieties in finite fields, *Amer. J. Math.*, **76** (1954), 819–827.

[19] C. Lech, A note on recurring series, *Arkiv der Mathematik*, **2** (1953), 417–421.

[20] K. Mahler, Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen, *Akad. Wetensch. Amsterdam*, **38** (1935), 50–60.

[21] Ю. И. Манин, О сравнениях третьей степени по простому модулю, *ИАН, сер. матем.*, **20** (1956), 673–678. [Yu. I. Manin, On third degree congruences to prime modulus, *Proc. Acad. Sci., math. ser.*, **20** (1956), 673–678.]

[22] D. A. Marcus, *Number Fields*, Springer, 1977 (3rd corrected printing, 1995).

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

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

[25] M. Michałek, A short proof of combinatorial Nullstellensatz, *Amer. Math. Monthly*, **117** (2010), 821–823.

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

[27] J. Oesterlé, Nouvelles approches du 'théorème' de Fermat, *Astérisque*, **161–162** (1988), 165–186 (published 1989).

[28] Th. Skolem, Ein Varfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen, *C. r. 8 congr. scand. à Stockholm*, (1934), 163–188.

[29] J. Stillwell, *Elements of Number Theory*, Springer, 2003.

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

[31] E. Warning, Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, *Abh. Math. Semin. Hamb. Univ.*, **11** (1935), 76–83.

[32] J. H. M. Wedderburn, A theorem on finite algebras, *Trans. Amer. Math. Soc.* **6** (1905), 349–352.

[33] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann et Cie., Paris, 1948.

[34] E. Wendt, Elementarer Beweis des Satzes, dass in jeder unbegrenzten arithmetischen Progression $my + 1$ unendlich viele Primzahlen vorkommen, *J. Reine Angew. Math.*, **115** (1895), 85–88.

[35] E. Witt, Über die Kommutativität endlicher Schiefkörper, *Abh. Math. Sem. Univ. Hamburg*, **8** (1931), 413.

[36] Wikipedia, abc conjecture,
http://en.wikipedia.org/wiki/Abc_conjecture

[37] Polymath, ABC conjecture,
http://michaelnielsen.org/polymath1/index.php?title=ABC_conjecture