The shoulders we stand on

Clay lecture I

Hendrik Lenstra

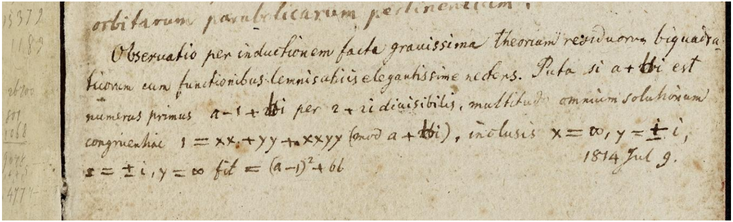
Mathematisch Instituut
Universiteit Leiden

with the assistance of Daan van Gent

Carl Friedrich Gauss (1777–1855)

From 1796 to 1814, Gauss kept a mathematical diary.
It was only published in 1897, by Felix Klein.
By that time, the *last entry* was not yet superseded.

The last entry



orbitarum parabolicarum pertinentium.

Obseruatio per inductionem facta grauissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ est numerus primus $a-1+bi$ per $2+2i$ diuisibilis, multitudo omnium solutionum congruentiae $1 = xx+yy+xxyy \pmod{a+bi}$, inclusis $x=\infty, y=\pm i$, $x=\pm i, y=\infty$ fit $=(a-1)^2+bb$

1814 Jul 9.

The Latin text

Observatio per inductionem facta gravissima theoriam biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a + b\mathrm{i}$ est numerus primus $a - 1 + b\mathrm{i}$ per $2 + 2\mathrm{i}$ divisibilis, multitudo omnium solutionum congruentiae $1 = xx + yy + xxyy \pmod{a + b\mathrm{i}}$, inclusis $x = \infty$, $y = \pm\mathrm{i}$, $x = \pm\mathrm{i}$, $y = \infty$ fit $= (a - 1)^2 + bb$

1814 Jul 9.

A literal English version

Observation empirically rendered extremely serious, most elegantly linking the theory of biquadratic residues with lemniscatic functions. Namely, if $a + b\mathrm{i}$ is a prime number, $a - 1 + b\mathrm{i}$ divisible by $2 + 2\mathrm{i}$, the number of all solutions to the congruence $1 = x^2 + y^2 + x^2y^2 \pmod{a + b\mathrm{i}}$, including $x = \infty$, $y = \pm\mathrm{i}$; $x = \pm\mathrm{i}$, $y = \infty$, becomes equal to $(a-1)^2 + b^2$. July 9, 1814.

The first sentence

Observatio per inductionem facta gravissima theoriam biquadraticorum cum functionibus lemniscaticis elegantissime nectens.

Observation empirically rendered extremely serious, most elegantly linking the theory of biquadratic residues with lemniscatic functions.

A primary prime element

Puta si $a+b\mathrm{i}$ est numerus primus $a-1+b\mathrm{i}$ per $2+2\mathrm{i}$ divisibilis,

Namely, if $a+b\mathrm{i}$ is a prime number, $a-1+b\mathrm{i}$ divisible by $2+2\mathrm{i}$,

Clearly, $\pi = a+b\mathrm{i}$ should be a prime element of $\mathbf{Z}[\mathrm{i}]$, and $\pi \equiv 1 \bmod (2+2\mathrm{i})$.

A primary prime element

Puta si $a + b\mathrm{i}$ est numerus primus $a - 1 + b\mathrm{i}$ per $2 + 2\mathrm{i}$ divisibilis,

Namely, if $a + b\mathrm{i}$ is a prime number, $a - 1 + b\mathrm{i}$ divisible by $2 + 2\mathrm{i}$,

Clearly, $\pi = a + b\mathrm{i}$ should be a prime element of $\mathbf{Z}[\mathrm{i}]$, and $\pi \equiv 1 \bmod (2 + 2\mathrm{i})$.

Note: $(2 + 2\mathrm{i}) = (1 + \mathrm{i})^3$ (as ideals). Elements of $\mathbf{Z}[\mathrm{i}]$ that are 1 mod $(2 + 2\mathrm{i})$ are called *primary*.

Primary elements

Exercise. *The natural map* $\mathbf{Z}[\mathrm{i}] \to \mathbf{Z}[\mathrm{i}]/(2+2\mathrm{i})$ *induces an* isomorphism $\mathbf{Z}[\mathrm{i}]^* \cong (\mathbf{Z}[\mathrm{i}]/(2+2\mathrm{i}))^*$ *of unit groups.*

Primary elements

Exercise. *The natural map* $\mathbf{Z}[\mathrm{i}] \to \mathbf{Z}[\mathrm{i}]/(2+2\mathrm{i})$ *induces an* isomorphism $\mathbf{Z}[\mathrm{i}]^* \cong (\mathbf{Z}[\mathrm{i}]/(2+2\mathrm{i}))^*$ *of unit groups.*

Hence every element of $\mathbf{Z}[\mathrm{i}]$ that is coprime to $1+\mathrm{i}$ can in a unique way be written as a unit times a primary element.

Counting solutions

multitudo omnium solutionum congruentiae $1 = xx + yy + xxyy \pmod{a + b\mathrm{i}}$, inclusis $x = \infty$, $y = \pm\mathrm{i}$, $x = \pm\mathrm{i}$, $y = \infty$ fit $= (a-1)^2 + bb$

the number of all solutions to the congruence $1 = x^2 + y^2 + x^2y^2 \pmod{a + b\mathrm{i}}$, including $x = \infty$, $y = \pm\mathrm{i}$; $x = \pm\mathrm{i}$, $y = \infty$, becomes equal to $(a-1)^2 + b^2$.

Changing notation

If $\pi \in \mathbf{Z}[\mathrm{i}]$ is a primary prime element, then the number of solutions to $1 = x^2 + y^2 + x^2y^2$ in $\mathbf{Z}[\mathrm{i}]/(\pi)$, including $(x, y) = (\infty, \pm\mathrm{i})$, $(\pm\mathrm{i}, \infty)$, equals $(\pi - 1)(\bar{\pi} - 1)$.

Changing notation

If $\pi \in \mathbf{Z}[\mathrm{i}]$ is a primary prime element, then the number of solutions to $1 = x^2 + y^2 + x^2y^2$ in $\mathbf{Z}[\mathrm{i}]/(\pi)$, including $(x, y) = (\infty, \pm\mathrm{i}), (\pm\mathrm{i}, \infty)$, equals $(\pi - 1)(\bar{\pi} - 1)$.

Points at infinity
$(x^2 + 1)(y^2 + 1) = 2$, so if one of x, y becomes infinite, the other becomes ±i.

Gauss considers the *normalization* of the projective closure of the curve $1 = x^2 + y^2 + x^2y^2$.

A modern reformulation

Observation. *If* $\pi \in \mathbf{Z}[\mathrm{i}]$ *is a primary prime element, and* E *denotes the normalization of the projective closure of the curve*

$$1 = x^2 + y^2 + x^2y^2,$$

then $\#E(\mathbf{Z}[\mathrm{i}]/(\pi)) = (\pi - 1)(\bar{\pi} - 1)$.

A Weierstrass equation

Over any field K in which $2 \neq 0$, the curve E is irreducible of genus 1, and one can give it by the Weierstrass equation

$$v^2 = u^3 + 4u.$$

A Weierstrass equation

Over any field K in which $2 \neq 0$, the curve E is irreducible of genus 1, and one can give it by the Weierstrass equation

$$v^2 = u^3 + 4u.$$

If $\mathrm{i} \in K$, then all 2-torsion of E is rational, and $(u, v) = (2, 4)$ has order 4, so $E(K)$ has a subgroup of order 8; in addition, E has complex multiplication by $\mathbf{Z}[\mathrm{i}]$.

We shall take $K = \mathbf{Z}[\mathrm{i}]/(\pi) = \mathbf{F}_{\pi\bar{\pi}}$.

A modern proof

The endomorphism ring $\mathrm{End}_K(E)$ contains the Frobenius $\varphi\colon (u,v) \mapsto (u^{\#K}, v^{\#K})$ and the complex multiplication element $\mathrm{i}\colon (u,v) \mapsto (-u, \mathrm{i}v)$.

Since φ and i commute, and $\mathbf{Z}[\mathrm{i}]$ is a maximal commutative subring of $\mathrm{End}_K(E)$, one has $\varphi \in \mathbf{Z}[\mathrm{i}]$.

A modern proof

The endomorphism ring $\mathrm{End}_K(E)$ contains the Frobenius $\varphi\colon (u,v) \mapsto (u^{\#K}, v^{\#K})$ and the complex multiplication element $\mathrm{i}\colon (u,v) \mapsto (-u, \mathrm{i}v)$.

Since φ and i commute, and $\mathbf{Z}[\mathrm{i}]$ is a maximal commutative subring of $\mathrm{End}_K(E)$, one has $\varphi \in \mathbf{Z}[\mathrm{i}]$.

Because $\#E(K) = (\varphi - 1)(\bar{\varphi} - 1)$ is 0 mod 8, the Frobenius φ is primary.

Also $\varphi\bar{\varphi} = \#K = \pi\bar{\pi}$, so $\varphi \in \{\pi, \bar{\pi}\}$. (In fact $\varphi = \pi$.) Thus $\#E(K) = (\pi - 1)(\bar{\pi} - 1)$, as Gauss observed.

More on the endomorphism ring

There are two cases: $\pi\bar{\pi} = p$ or p^2.

Case I: $\pi\bar{\pi} = p$, a prime that is 1 mod 4.
Then E is *ordinary*, $K = \mathbf{F}_p$, and $\mathrm{End}_K(E) = \mathbf{Z}[\mathrm{i}]$.

More on the endomorphism ring

There are two cases: $\pi\bar{\pi} = p$ or p^2.

Case I: $\pi\bar{\pi} = p$, a prime that is 1 mod 4.
Then E is *ordinary*, $K = \mathbf{F}_p$, and $\mathrm{End}_K(E) = \mathbf{Z}[\mathrm{i}]$.

Case II: $\pi = -p$, with p a prime that is 3 mod 4.
Then E is *supersingular*, $K = \mathbf{F}_{p^2}$, and $\mathrm{End}_K(E) = \mathbf{Z}[\mathrm{i}, (1 + \mathrm{i}\sqrt{-p})/2]$ with $\mathrm{i} \cdot \sqrt{-p} = -\sqrt{-p} \cdot \mathrm{i}$
and $\sqrt{-p}$ equal to the Frobenius of E over $\mathbf{F}_p$.

More on the endomorphism ring

There are two cases: $\pi\bar{\pi} = p$ or p^2.

Case I: $\pi\bar{\pi} = p$, a prime that is 1 mod 4.
Then E is *ordinary*, $K = \mathbf{F}_p$, and $\mathrm{End}_K(E) = \mathbf{Z}[\mathrm{i}]$.

Case II: $\pi = -p$, with p a prime that is 3 mod 4.
Then E is *supersingular*, $K = \mathbf{F}_{p^2}$, and $\mathrm{End}_K(E) = \mathbf{Z}[\mathrm{i}, (1 + \mathrm{i}\sqrt{-p})/2]$ with $\mathrm{i} \cdot \sqrt{-p} = -\sqrt{-p} \cdot \mathrm{i}$
and $\sqrt{-p}$ equal to the Frobenius of E over $\mathbf{F}_p$.

All of the literature I have seen on the last entry disregards Case II.

Literature on the last entry

The first published proof is due to Gustav Herglotz (1921). He included a second proof using results of Gauss himself. A third early proof uses Jacobi sums.

Writing $z = (1 + x^2) \cdot y$ in $1 = x^2 + y^2 + x^2y^2$, one reduces to the diagonal equation $z^2 = 1 - x^4$.

All these proofs restrict to Case I. Do they carry over to Case II?

For references, see Franz Lemmermeyer, *Reciprocity laws* (2000), Chapter 10.

Disregarding the supersingular case

Two of our lecture series concentrate on supersingular elliptic curves, so it would be a pity to disregard them.

In addition, in the case $p \equiv 3 \bmod 4$, Gauss's last entry has great interest for the early history of finite fields.

Of course, finite fields are omnipresent in cryptography.

The early history of finite fields

Caveat: before the 1870's, "sets" did not exist yet!

Still, Fermat, Euler, Lagrange, Legendre, and Gauss worked with the prime fields we now call $\mathbf{F}_p$. They used ordinary integers, replacing equality by congruences modulo p.

Galois introduced non-prime finite fields in 1830, using *imaginaries*.

Dedekind justified this in 1857, replacing $\mathbf{Z}$ by $\mathbf{Z}[X]$, and "$\bmod p$" by "$\bmod (p, F)$".

Gauss's role

In his *eighth chapter*, excluded from his Disquisitiones Arithmeticae (1801) and published only in 1876, Gauss studied what *we* call finite fields, but he explicitly avoided introducing them.

Apparently, Gauss preferred to work exclusively with entities whose genuine existence was beyond any reasonable doubt. Finite non-prime fields do not occur in this eighth chapter.

Changing his mind

In the last entry Gauss works very clearly with the concrete finite non-prime fields $\mathbf{Z}[\mathrm{i}]/(p)$, for primes $p \equiv 3 \bmod 4$! This occurred in 1814, when Galois (1811–1832) was only two years of age.

Clearly, Gauss felt just as comfortable with $\mathbf{Z}[\mathrm{i}]/(a+b\mathrm{i})$ as with $\mathbf{Z}/(p)$. He must have changed his opinion on “imaginary zeroes” since writing his eighth chapter.

Changing his mind

Clearly, Gauss felt just as comfortable with $\mathbf{Z}[\mathrm{i}]/(a+b\mathrm{i})$ as with $\mathbf{Z}/(p)$. He must have changed his opinion on “imaginary zeroes” since writing his eighth chapter.

Note that in the last entry Gauss wrote

$$1 = xx + yy + xxyy \pmod{a+b\mathrm{i}},$$

using an *equality* sign instead of a *congruence* sign!

Two take-home messages

Conclusion. *Elliptic curves over finite fields are just as old as finite fields themselves.*

Two take-home messages

Conclusion. *Elliptic curves over finite fields are just as old as finite fields themselves.*

Our next subject:

Likewise, polynomial-time algorithms in number theory are just as old as polynomial-time algorithms.

Again starting from Gauss

In connection with Euler's criterion

$$\left(\tfrac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p,$$

Gauss wrote (Disquis. Arithm., Art. 106):

"as soon as the numbers we are examining are even moderately large, this criterion is practically useless, because of the amount of calculation involved."

Did Gauss not realize that this "amount of calculation" is only $O((\log p)^3)$?

History of complexity theory

Polynomial-time algorithms and NP-completeness became popular in the early 1970's, in the context of theoretical computer science and optimization.

Later it was discovered that John Nash had written about exponential algorithms in 1955, and that Kurt Gödel speculated on "P versus NP" in 1956.

History of complexity theory

Polynomial-time algorithms and NP-completeness became popular in the early 1970's, in the context of theoretical computer science and optimization.

Later it was discovered that John Nash had written about exponential algorithms in 1955, and that Kurt Gödel speculated on "P versus NP" in 1956.

But already in 1910, Henry Cabourn Pocklington clearly expressed the difference between polynomial-time and exponential algorithms.

History of complexity theory

But already in 1910, Henry Cabourn Pocklington clearly expressed the difference between polynomial-time and exponential algorithms.

Eric Bach, Jeffrey Shallit,
Algorithmic number theory (1996).

Pocklington (1910)

In a context closely resembling Euler's criterion:

"We notice that the labour required here is proportional to a power of the logarithm of the modulus, not to the modulus itself or its square root as in the indirect processes, and hence see that in the case of a large modulus the direct process will be much quicker than the indirect."

He made similar comments in papers published in 1914 and 1917.

A brief biography

Henry Cabourn Pocklington (1879–1952) was an English high school teacher of physics and a Fellow of the Royal Society. He was a solitary and happy person, and his writings, if "addressed to anybody, were intended for those likely to understand".

His most important discoveries were said to be in physics, and "number-theory was more of a side-line".

A brief biography

His most important discoveries were said to be in physics, and “number-theory was more of a side-line”.

Once, during an electrical experiment, he “received a severe shock and was thrown across the room”, and “he refused to have electricity supplied to his home”.

All four together

René Schoof (1955–) in his PhD thesis (1985):

Theorem. *There is a polynomial-time algorithm that given a finite field K and an elliptic curve E over K, computes $\#E(K)$.*

This was the first time that polynomial-time algorithms occurred in the theory of elliptic curves.

The basic method

Let $\varphi \in \mathrm{End}_K(E)$ again be the Frobenius endomorphism of E over K, and put $q = \#K$.

Then $t = \varphi + \bar{\varphi}$ satisfies

$$\begin{gathered} t \in \mathbf{Z},\ |t| \leq 2\sqrt{q}, \\ \varphi^2 - t\varphi + q = 0 \text{ in } \mathrm{End}_K(E), \\ \#E(K) = q - t + 1. \end{gathered}$$

For $l \in \mathbf{Z}_{>0}$ and $P \in E[l]$, the relation $\varphi^2(P) + q \cdot P = t \cdot \varphi(P)$ determines $(t \bmod l)$.

Use this for small prime numbers l.

Back to Gauss

Corollary. *There is a polynomial-time algorithm that given a prime number p that is* $1 \bmod 4$*, computes a square root of* $(-1 \bmod p)$.

Proof. Let $K = \mathbf{F}_p$ and let E be Gauss's elliptic curve. If $p = a^2 + b^2$ with $a + b\mathrm{i}$ primary, then $\#E(K) = p - 2a + 1$. Hence Schoof's algorithm finds a. Compute b from $p = a^2 + b^2$, then one has $(a/b)^2 \equiv -1 \bmod p$.

Elementary number theory

Corollary. *There is a polynomial-time algorithm that given a prime number* p *that is* $1 \bmod 4$, *computes a square root of* $(-1 \bmod p)$.

This was the first algorithmic application of elliptic curves to elementary number theory.

“The rest is history”

After René Schoof, elliptic curves soon found many other applications: primality testing, factoring integers, and cryptography.

“The rest is history”

After René Schoof, elliptic curves soon found many other applications: primality testing, factoring integers, and cryptography.

And, yes, his method was also used for computing coefficients of modular forms:

Bas Edixhoven, Jean-Marc Couveignes (eds),
Computational aspects of modular forms and Galois representations (2011).

“The rest is history”

After René Schoof, elliptic curves soon found many other applications: primality testing, factoring integers, and cryptography.

And, yes, his method was also used for computing coefficients of modular forms:

Bas Edixhoven, Jean-Marc Couveignes (eds),
Computational aspects of modular forms and Galois representations (2011).

I thank you for your attention!