Higher-dimensional reciprocity laws

Dr Ana Caraiani

Imperial College London

September 10, 2020

Perfect squares and quadratic residues

Question: What are the last digits of perfect squares? 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169...

The pattern is 0, 1, 4, 5, 6, 9, but never 2, 3, 7 or 8. We say that 0, 1, 4, 5, 6, 9 are *quadratic residues* modulo 10.

Perfect squares and quadratic residues

Question: What are the last digits of perfect squares? 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169...
The pattern is 0, 1, 4, 5, 6, 9, but never 2, 3, 7 or 8. We say that 0, 1, 4, 5, 6, 9 are *quadratic residues* modulo 10.

Harder question: For what prime numbers p is 3 a quadratic residue modulo p? In other words, for what prime numbers p does the equation

$$x^2 \equiv 3 \pmod{p}$$

have any whole number solutions?

Quadratic reciprocity

Let p and q be prime numbers. The law of quadratic reciprocity, first proved by Gauss in 1792, relates whether

- p is a quadratic residue modulo q

to whether

- q is a quadratic residue modulo p.

Quadratic reciprocity

Let p and q be prime numbers. The law of quadratic reciprocity, first proved by Gauss in 1792, relates whether

- p is a quadratic residue modulo q

to whether

- q is a quadratic residue modulo p.

Consequence: whether 3 is a quadratic residue modulo p only depends on $p \pmod{12}$.

The answer is no for $p = 5, 17, 29, 41$ and yes for $p = 13$.

Primes and quadratic extensions

Quadratic reciprocity is intimately connected to the behavior of prime numbers in quadratic extensions of $\mathbb{Q}$.

Primes and quadratic extensions

Quadratic reciprocity is intimately connected to the behavior of prime numbers in quadratic extensions of $\mathbb{Q}$.

For example, when $p \geq 5$ is prime, the number of solutions of

$$x^2 \equiv 3 \pmod{p}$$

depends on whether p *stays prime* in $\mathbb{Q}(\sqrt{3})$ or *splits* into a product of two primes. We know that $5, 17, 29$ and 41 all stay prime, whereas $13 = (4 - \sqrt{3}) \cdot (4 + \sqrt{3})$.

Primes and quadratic extensions

Quadratic reciprocity is intimately connected to the behavior of prime numbers in quadratic extensions of $\mathbb{Q}$.

For example, when $p \geq 5$ is prime, the number of solutions of

$$x^2 \equiv 3 \pmod{p}$$

depends on whether p *stays prime* in $\mathbb{Q}(\sqrt{3})$ or *splits* into a product of two primes. We know that $5, 17, 29$ and 41 all stay prime, whereas $13 = (4 - \sqrt{3}) \cdot (4 + \sqrt{3})$.

The interaction between prime numbers and the group of symmetries $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{\pm 1\}$ governs this behavior.

A 2-dimensional reciprocity law

Quadratic reciprocity is an example of a one-dimensional reciprocity law. More reciprocity laws like this were discovered through the first half of the 20th century, under the framework of *class field theory*.

A 2-dimensional reciprocity law

Quadratic reciprocity is an example of a one-dimensional reciprocity law. More reciprocity laws like this were discovered through the first half of the 20th century, under the framework of *class field theory*.

In 1954, Eichler wrote down a reciprocity law for cubic equations in two variables. Say that the equation

$$y^2 + y \equiv x^3 - x^2 \pmod{p}$$

has N_p solutions.

A 2-dimensional reciprocity law

Quadratic reciprocity is an example of a one-dimensional reciprocity law. More reciprocity laws like this were discovered through the first half of the 20th century, under the framework of *class field theory*.

In 1954, Eichler wrote down a reciprocity law for cubic equations in two variables. Say that the equation

$$y^2 + y \equiv x^3 - x^2 \pmod{p}$$

has N_p solutions.

For example, the solutions modulo 5 are $(0,0),(1,0),(0,4),(1,4)$, so $N_5 = 4$.

Similarly, $N_7 = 9, N_{11} = 10, N_{13} = 9 \ldots$

A 2-dimensional reciprocity law

The difference $p - N_p$ tends to be small compared to p:

p	2	3	5	7	11	13
$p - N_p$	-2	-1	1	-2	1	4

.

The number of solutions is roughly equal to p.

A 2-dimensional reciprocity law

The difference $p - N_p$ tends to be small compared to p:

p	2	3	5	7	11	13
$p - N_p$	-2	-1	1	-2	1	4

The number of solutions is roughly equal to p.

Miracle: the error term can be recovered from the power series expansion of the following infinite product

$$q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2$$

$$= q + (-2) \cdot q^2 + (-1) \cdot q^3 + 2q^4 + 1 \cdot q^5 + \dots .$$

Elliptic curves

The cubic equation

$$y^2 + y = x^3 - x^2,$$

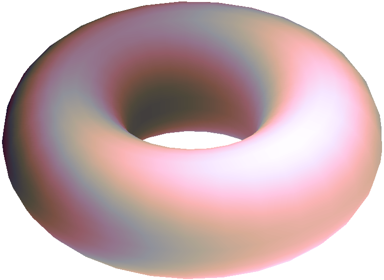
is really an *elliptic curve* $E/\mathbb{Q}$. This is a smooth, projective curve of genus one.

Elliptic curves

The cubic equation

$$y^2 + y = x^3 - x^2,$$

is really an *elliptic curve* $E/\mathbb{Q}$. This is a smooth, projective curve of genus one.

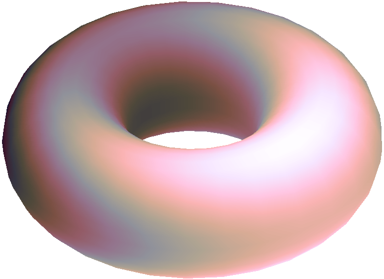


Elliptic curves

The cubic equation

$$y^2 + y = x^3 - x^2,$$

is really an *elliptic curve* $E/\mathbb{Q}$. This is a smooth, projective curve of genus one.



The elliptic curve lives in the world of *arithmetic algebraic geometry*.

Modular forms

A modular form lives in the world of *harmonic analysis*. This is the modern approach to Fourier theory, developed to study planetary orbits and vibrating strings.

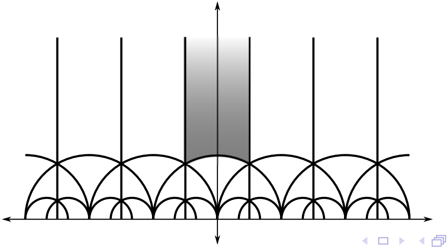
Modular forms

A modular form lives in the world of *harmonic analysis*. This is the modern approach to Fourier theory, developed to study planetary orbits and vibrating strings.

More precisely, a modular form is a very special kind of function on the upper half plane

$$\mathcal{H} = \{z = x + y\sqrt{-1} \mid x, y \in \mathbb{R}, y > 0\}.$$

It satisfies many symmetries, coming from the symmetries of the upper-half plane: horizontal translations and inversions about circles.



Hyperbolic geometry

- The upper-half plane can be identified with 2-dimensional hyperbolic (rather than Euclidean) space.

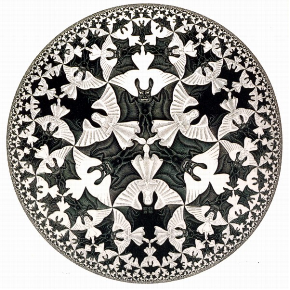
[1] *Circle Limit IV*, M.C. Escher, from wikiart.org

Hyperbolic geometry

- The upper-half plane can be identified with 2-dimensional hyperbolic (rather than Euclidean) space.

- The Escher drawing on the right is another model of the hyperbolic plane, this time using the unit disk.

[1]



[1] *Circle Limit IV*, M.C. Escher, from wikiart.org

Consequences of higher reciprocity

For harmonic analysis:

- The Ramanujan conjecture and its generalisations. Proved by Deligne (1974): given

$$q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2=\sum_{n=1}^{\infty}a_nq^n,$$

and p a prime number, the Fourier coefficient a_p satisfies

$$|a_p|\leq 2\sqrt{p}.$$

Consequences of higher reciprocity

For harmonic analysis:

- The Ramanujan conjecture and its generalisations. Proved by Deligne (1974): given

  $$q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2=\sum_{n=1}^{\infty}a_nq^n,$$

  and p a prime number, the Fourier coefficient a_p satisfies

  $$|a_p|\leq 2\sqrt{p}.$$

- This has applications to computer science by constructing Ramanujan graphs.

Pythagorean triples and Fermat's Last Theorem

A central question in number theory is finding whole number solutions to polynomial equations.

Pythagorean triples and Fermat's Last Theorem

A central question in number theory is finding whole number solutions to polynomial equations.

For example, the equation

$$x^2 + y^2 = z^2$$

has solutions of the form $(x, y, z) = (2mn, m^2 - n^2, m^2 + n^2)$.

Pythagorean triples and Fermat's Last Theorem

A central question in number theory is finding whole number solutions to polynomial equations.

For example, the equation

$$x^2 + y^2 = z^2$$

has solutions of the form $(x, y, z) = (2mn, m^2 - n^2, m^2 + n^2)$.

A question first asked about Pierre de Fermat in 1637 is to show that the more general equation

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

has no non-trivial whole-number solutions when $n \geq 3$.

Consequences of higher reciprocity

For number theory:

Theorem (Wiles, 1995)

If $n \geq 3$ is any integer, the equation

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

has no non-trivial whole-number solutions.

Consequences of higher reciprocity

For number theory:

Theorem (Wiles, 1995)

If $n \geq 3$ is any integer, the equation

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

has no non-trivial whole-number solutions.

- Prove that all elliptic curves over $\mathbb{Q}$ come from modular forms.

Consequences of higher reciprocity

For number theory:

Theorem (Wiles, 1995)

If $n \geq 3$ is any integer, the equation

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

has no non-trivial whole-number solutions.

- Prove that all elliptic curves over $\mathbb{Q}$ come from modular forms.
- (Frey, 1985) Use a non-trivial solution $a^\ell + b^\ell = c^\ell$ to cook up an elliptic curve

  $$y^2 = x(x - a^\ell)(x + b^\ell)$$

  which can't possibly be related to a modular form!

Current research

Are there reciprocity laws for elliptic curves over imaginary quadratic fields, like the Gaussian numbers $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$?

$$y^2 + (i+1)\,xy + y = x^3 + ix^2 + (-i-1)\,x$$

Current research

Are there reciprocity laws for elliptic curves over imaginary quadratic fields, like the Gaussian numbers $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$?

$$y^2 + (i+1)\,xy + y = x^3 + ix^2 + (-i-1)\,x$$

These should be encoded in the symmetries of hyperbolic 3-space.

Current research

Are there reciprocity laws for elliptic curves over imaginary quadratic fields, like the Gaussian numbers $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$?

$$y^2 + (i+1)\,xy + y = x^3 + ix^2 + (-i-1)\,x$$

These should be encoded in the symmetries of hyperbolic 3-space. In 2018, we obtained "potential" reciprocity laws:

- *Potential automorphy over CM fields*, Allen, Calegari, C., Gee, Helm, Le Hung, Newton, Scholze, Taylor, and Thorne.
- *Abelian surfaces over totally real fields are potentially modular*, Boxer, Calegari, Gee, and Pilloni.

Current research

Are there reciprocity laws for elliptic curves over imaginary quadratic fields, like the Gaussian numbers $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$?

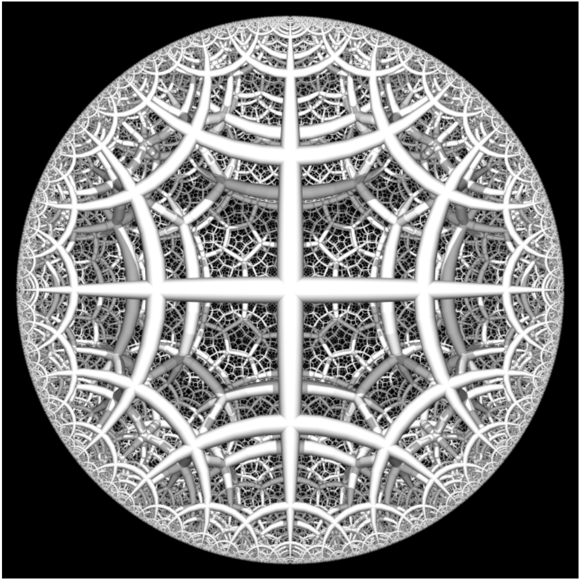
$$y^2 + (i+1)\,xy + y = x^3 + ix^2 + (-i-1)\,x$$

These should be encoded in the symmetries of hyperbolic 3-space. In 2018, we obtained "potential" reciprocity laws:

- *Potential automorphy over CM fields*, Allen, Calegari, C., Gee, Helm, Le Hung, Newton, Scholze, Taylor, and Thorne.
- *Abelian surfaces over totally real fields are potentially modular*, Boxer, Calegari, Gee, and Pilloni.

These ideas are part of the *Langlands program*, an incredible network of conjectures that bridge number theory with other parts of pure maths.

Hyperbolic 3-space



2

[2] http://kim.oyhus.no/icosians.html

The London School of Geometry and Number Theory

There are many potential supervisors at LSGNT working on topics related to higher reciprocity!

- Imperial College London: Toby Gee, David Helm
- University College London: Sarah Zerbes
- King's College London: Fred Diamond, Payman Kassaei, James Newton

The end

Thank you!