A Tour of Fermat's World

Ching-Li Chai

Department of Mathematics
University of Pennsylvania

Philadelphia, March, 2016

Outline

A Tour of Fermat's World
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Some familiar whole numbers

§1. Examples of numbers

- 2, the only even prime number.
- 30, the largest positive integer m such that every positive integer between 2 and m and relatively prime to m is a prime number.
- $1729 = 12^3 + 1^3 = 10^3 + 9^3$,
  the **taxi cab number**. As Ramanujan remarked to Hardy, it is the smallest positive integer which can be expressed as a sum of two positive integers in two different ways.

Some familiar algebraic irrationals

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

- $\sqrt{2}$, the Pythagora's number, often the first irrational numbers one learns in school.
- $\sqrt{-1}$, the first imaginary number one encountered.
- $\frac{1+\sqrt{5}}{2}$, the **golden number**, a root of the quadratic polynomial $x^2 - x - 1$.

Some familiar transcendental numbers

- $1+10+10^{-2}+10^{-6}+10^{-24}+\cdots+10^{-n!}+\cdots$, a *Liouville* number.
- $e=\exp(1)=\sum_{n=0}^{\infty}\frac{1}{n!}$, the base of the natural logarithm.
- π, area of a circle of radius 1. Zu Chungzhi (429–500) gave two approximating fractions,

$$\frac{22}{7} \quad \text{and} \quad \frac{355}{113}$$

(both bigger than π), and obtained

$$3.1415926 < \pi < 3.1415927.$$

Triangular numbers and Mersenne numbers

§2. Some families of numbers

- $1,3,6,10,15,21,28,36,45,55,66,78,91,\ldots$, the triangular numbers, $\Delta_n=\frac{n(n+1)}{2}$.
- $2,3,5,7,11,13,17,19,23,29,31,37,41,\ldots$, the prime numbers.
- 2^p-1 (p is a prime number) are the *Mersenne numbers*. If $M_p := 2^p-1$ is a prime number (a Mersenne prime), then

$$\Delta_M=\frac{1}{2}M(M+1)=2^{p-1}(2^p-1)$$

is an even perfect number. For instance M_p is a Mersenne prime for $p=2,3,5,7,13,17,19,31,61,89,107,127,521$ and 74207281.

Open question: are there infinitely many Mersenne primes?

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Fermat numbers

$3, 5, 17, 257, 65537, 4294967297$ are the first few Fermat numbers,

$$F_r = 2^{2^r} + 1.$$

Not all Fermat numbers are primes; Euler found in 1732 that

$$2^{32} + 1 = 4294967297 = 641 \times 6700417.$$

If a prime number p is a Fermat number, then the regular p-gon's can be constructed with ruler and compass. For instance F_r is a prime number for $r = 0, 1, 2, 3, 4, 5, 65537$.

Open question: are there infinitely many Fermat primes?

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Figure: Fermat

Partition numbers

The partition numbers $p(n)$ is defined as the number of *unordered* partitions of a whole integer n. Its generating series is

$$\sum_{n=0}^{\infty} p(n)\, x^n = \prod_{n=1}^{\infty} (1 - x^m)^{-1}$$

e.g. $(1,1,1,1), (2,1,1,1), (2,2), (3,1), (4)$ are the five ways to partition 4, so $p(4) = 5$.

Ramanujan showed

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}$$

Figure: Ramanujan

A Tour of Fermat's World

Ching-Li Chai

Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Hans Rademacher proved the following exact formula for $p(n)$:

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} k^{1/2} A_k(n) \frac{d}{dn} \frac{\sinh\left(\frac{\pi\sqrt{2n-1/12}}{\sqrt{3}k}\right)}{\sqrt{n-1/24}}$$

where

$$A_k(n) = \sum_{0\leq m<k,(m,k)=1} e^{\pi\sqrt{-1}[s(m,k)-2nm/k]}$$

and the Dedekind sum $s(m,k)$ is by definition

$$s(m,k) = \sum_{1\leq j\leq k-1} \mathrm{sawt}(j/k)\,\mathrm{sawt}(mj/k)$$

$$\mathrm{sawt}(x) = x - \lfloor x \rfloor - \tfrac{1}{2} \ \text{ if } x \notin \mathbb{Z}, \ \ \mathrm{sawt}(x) = 0 \ \text{ if } x \in \mathbb{Z}$$

Figure: Rademacher

A Tour of Fermat's World
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Ramanujan numbers

$1, -24, 252, -1472, 4830, -6048, \ldots$, are the first few Ramanujan numbers, defined by

$$\sum_{n=1}^{\infty} \tau(n)\, x^n = x \left[\prod_{n=1}^{\infty} (1 - x^n) \right]^{24}$$

Ramanujan conjectured that there is a constant $C > 0$ such that

$$\tau(p) \leq C p^{11/2}$$

for every prime number p.

Ramanujan's conjecture was proved by *Deligne* in 1974 (as a consequence of his proof of the *Weil conjecture*) with $C = 2$.

Bernouli numbers

The Bernouli numbers are defined by

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

$B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{12} = -\frac{691}{2730}$, $B_{14} = \frac{7}{6}$.

Remark. The Bernouli numbers are essentially the values of the Riemann zeta function at negative odd integers.

A TOUR OF FERMAT'S WORLD
Ching-Li Chai

Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Heegner numbers

$-1, -2, -3, -7, -11, -19, -43, -67, -163$ are the nine Heegner numbers; they are the only negative integers $-d$ such that the *class number* of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ is equal to one.

For the larger Heegner numbers, $e^{\pi\sqrt{d}}$ is close to an integer; e.g.

$$e^{\pi\sqrt{67}} = 147197952743.99999866$$

$$e^{\pi\sqrt{163}} = 161537412640768743.99999999999925007$$

Two simple diophantine equations

A TOUR OF FERMAT'S WORLD
Ching-Li Chai

§2. Some Diophantine equations

- The equation
$$x^2 + y^2 = z^2$$
has lots of integer solutions. The *primitive* ones with x odd and y even are given by the formula
$$x = st,\ y = \tfrac{s^2-t^2}{2},\ z = \tfrac{s^2+t^2}{2},\ \ s > t \text{ odd},\ \mathrm{gd}(s,t) = 1$$
- (Fermat) The equation
$$x^4 - y^4 = z^2$$
has no non-trivial integer solution.

Primes of the form $Ax^2 + By^2$

- (Fermat)

$$
\begin{aligned}
p = x^2 + y^2 &\iff p \equiv 1 \pmod 4 \\
p = x^2 + 2y^2 &\iff p \equiv 1 \text{ or } 3 \pmod 8 \\
p = x^2 + 3y^2 &\iff p = 3 \text{ or } p \equiv 1 \pmod 3
\end{aligned}
$$

- (Euler)

$$
\begin{aligned}
p = x^2 + 5y^2 &\iff p \equiv 1, 9 \pmod{20} \\
2p = x^2 + 5y^2 &\iff p \equiv 3, 7 \pmod{20}
\end{aligned}
$$

$$
p = x^2 + 14y^2 \text{ or } p = 2x^2 + 7y^2 \iff
$$
$$
p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}
$$

Figure: Euler

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Primes of the form $Ax^2 + By^2$, continued

$$p = x^2 + 27y^2 \iff p \equiv 1 \pmod 3 \text{ and } 2 \text{ is a cubic residue} \pmod p$$

$$p = x^2 + 64y^2 \iff p \equiv 1 \pmod 4 \text{ and } 2 \text{ is a biquadratic residue} \pmod p$$

(Kronecker)

$$p = x^2 + 31y^2 \iff (x^3 - 10x)^2 + 31(x^2 - 1)^2 \equiv 0 \pmod p \quad \text{for some integer } x$$

Some formulas discovered by Euler

- $\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$
- $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \frac{\pi^2}{6}$
- $1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \dots = \frac{\pi^4}{90}$
  - $1 - 2^k + 3^k - 4^k + \dots = -\frac{(1-2^{k+1})}{k+1} B_{k+1}$
    for $k \geq 1$; in particular it vanishes if k is even.
- $\frac{1}{\pi^{2k}}\left(1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \dots\right) \in \mathbb{Q}$ for every integer $k \geq 1$.
- $\prod_{n=1}^{\infty} (1 - x^n) = \sum_{n \in \mathbb{Z}} (-1)^n x^{n(3n+1)/2}$

A Tour of Fermat's World
Ching-Li Chai

Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Prelude to congruent numbers

§3. Congruent numbers.
The equation

$$y^2z = x^3 - n^2xz, \quad n \text{ square free},$$

may or may not have a non-trivial (i.e. $xyz \neq 0$) integer solution—depending on whether n is a *congruent number*, to be discussed next.

Congruent numbers: definition and examples

A Tour of Fermat's World
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

A square free whole number $n > 0$ is a congruent number if there is a *right triangle* with *rational sides* whose area is n.

For instance 5 is a congruent number, because $(20/3)^2 + (3/2)^2 = (41/6)^2$. Similarly 6 is a congruent number because $3^2 + 4^2 = 5^2$.

$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47$ are the beginning of (the sequence of) congruent numbers.

157 as a congruent numbers

The number 157 is a congruent number, but the "simplest" non-trivial rational solution to $a^2+b^2=c^2$ with $a \cdot b = 314$ is

$$a = \frac{157841 \cdot 4947203 \cdot 526771095761}{2 \cdot 32 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441}$$

$$b = \frac{2^2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 526771095761}$$

$$c = \frac{20085078913 \cdot 1185369214457 \cdot 9425458255024420419074801}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 526771095761}$$

The point: although 157 is not a large number, the solution involved may have very large numerators and denominators. In particular it may not be easy to either determine or search for congruent numbers.

Congruent number problem

A TOUR OF FERMAT'S WORLD
Ching-Li Chai

Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Congruence number problem: find an (easily checkable) criterion for a square free positive integer to be a congruence number.

Reformulation in terms of rational points on (a special kind of) elliptic curves: a positive square free integer n is a congruent number if and only if the equation

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

has a solution (x,y) in rational numbers with $y \neq 0$. (Then there are infinitely many such rational solutions.)

Tunnell's theorem on congruent numbers

Theorem (Tunnell 1983) If n is a square free positive congruence number, then

$$\#\{x,y,z\in\mathbb{Z}|n=2x^2+y^2+32z^2\}=(1/2)\cdot\#\{(x,y,z\in\mathbb{Z}|n=2x^2+y^2+8z^2\}$$

if n is odd, and

$$\#\{x,y,z\in\mathbb{Z}|n/2=4x^2+y^2+32z^2\}=(1/2)\cdot\#\{(x,y,z\in\mathbb{Z}|n/2=2x^2+y^2+8z^2\}$$

if n is even. Conversely if the Birch-Swinnerton-Dyer conjecture holds (for the elliptic curve $y^2 = x^3 - n^2 x$), then these equalities imply that n is a congruent number.

Fermat's Last Theorem

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

(Fermat's Last Theorem, now a theorem of Wiles+Taylor-Wiles)

$$x^p + y^p + z^p = 0$$

has no non-trivial integer solution if p is an odd prime number.

Proved by Wiles and Taylor/Wiles in 1994, more than 300 years after Fermat wrote the assertion at the margin of his personal copy of the 1670 edition of *Diophantus*.

Question/Discussion: Why should anyone care?

Fermat's infinite descent illustrated

§4. Fermat's infinite descent
We will explain how to use Fermat's method of infinite descent, which he is jusifiably proud of, to show that the Diophantine equation

$$x^4 - y^4 = z^2$$

has no non-trivial integer solution.

May assume $\gcd(x,y,z) = 1$. The either x, y are both odd, or x is odd and y is even. We will consider only the first case that x, y are **both odd**.

Step 1.

$(x^2+y^2)\cdot(x^2-y^2) = z^2 \Longrightarrow \exists u, v$ such that $\gcd(u,v) = 1$, $x^2+y^2 = 2u^2$, $x^2-y^2 = 2v^2$ and $z = 2uv$.

$2v^2 = (x+y)\cdot(x-y) \Longrightarrow \exists r, s$ such that $x+y = r^2$, $x-y = 2s^2$, $v = rs$ (adjust the signs).

The original equation becomes $r^4 + 4s^4 = 4u^2$. Write $r = 2t$, the equation becomes

$$s^4 + 4t^4 = u^2$$

and we have

$$x = 2t^2 + s^2, \;\; y = 2t^2 - s^2, \;\; z = 4tsu\,,$$

$\gcd(s,t,u) = 1$.

A Tour of Fermat's World
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Step 2.

From $s^4 + 4t^4 = u^2$, $\gcd(s,t,u) = 1$, it is easy to see that u and s are both odd. May assume $u > 0$.

$4t^2 = (u - s^2)(u + s^2) \Longrightarrow \exists a, b$ such that $u - s^2 = 2b^2$, $u + s^2 = 2a^2$, $t^2 = ab$, $\gcd(a,b) = 1$.

$t^2 = ab \Longrightarrow \exists x_1, y_1$ such that $a = x_1^2$, $b = y_1^2$ and $t = x_1 y_1$.. It follows that $u = x_1^4 + y_1^4$ and

$$x_1^4 - y_1^4 = s^2\,.$$

Let $z_1 = s$. Then (x_1, y_1, z_1) is an integer solution of the original equation $x^4 - y^4 = z^2$, with $|x_1|$ strictly smaller.

Fermat's infinite descent, continuted

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Conclusion. Starting with a non-trivial solution, we obtain an infinite sequence of non-trivial solutions $(x,y,z), (x_1,y_1,z_1), (x_2,y_2,z_2), (x_3,y_3,z_3), \ldots$ such that the $|x| > |x_1| > |x_2| > |x_3| > \cdots$. That's impossible. Q.E.D.

(We leave it to the reader to check that if we start with a non-trivial solution of $x^4 - y^4 = z^2$ such that x is odd and y is even, the same argument will also lead us to another non-trivial solution such that the absolute value of x decreases.)

An intrinsic description of infinite descent

Remark. Consider algebraic varieties $X_1 : x^4 - y^4 = z^2$ and $X_2 : s^4 + 4t^4 = u^2$; and maps $f : X_1 \to X_2$

$$f : (x,y,z) \mapsto (s,t,u) = (z, xy, x^4 + y^4)$$

and $g : X_2 \to X_1$

$$g : (s,t,u) \mapsto (s^2 + 2t^2, s^2 - 2t^2, 4stu)$$

The varieties X_1 and X_2 correspond to elliptic curves E_1, E_2 over $\mathbb{Q}$ with **complex multiplication**; they become isomorphic over $\mathbb{Q}(\sqrt[4]{-4})$.

The maps f, g correspond to "multiplication by $(1+\sqrt{-1})$ and $(1-\sqrt{-1})$" respectively. Their composition is "multiplication by 2", defined over $\mathbb{Q}$.

Sum of two squares

§5. Counting solutions.

Notation. For each integer $k \geq 1$, let $r_k(n)$ be the number of k-tuples $(x_1, \ldots, x_n) \in \mathbb{Z}^k$ such that

$$x_1^2 + \ldots + x_k^2 = n\,.$$

Write $n = 2^f \cdot n_1 \cdot n_2$, where every prime divisor of n_1 is $\equiv 1 \pmod 4$ and every prime divisor of n_2 is $\equiv 3 \pmod 4$).

- Fermat showed that $r_2(n) > 0$ (i.e. n is a sum of two squares) if and only if every prime divisor p of n_2 occurs in n_2 to an **even** power.
- Assume this is the case, Jacobi obtained

$$r_2(n) = 4d(n_1)$$

where $d(n_1)$ is the number of divisors of n_1.

Sum of four squares

- Lagrange showed that $r_4(n) > 0$ for every $n \in \mathbb{Z}$.
- Jacobi obtained

$$r_4(n) = 8\,\sigma'(n)$$

where $\sigma'(n)$ is the sum of divisors of n which are not divisible by 4. More explicitly,

$$r_4(n) = \begin{cases} 8 \cdot \sum_{d|n} d & n \text{ odd} \\ 24 \cdot \sum_{d|n,\, d \text{ odd}} d & n \text{ even} \end{cases}$$

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Sum of three squares

- Legendre showed that n is a sum of three squares if and only if n is *not* of the form $4^a(8m+7)$, and $r_3(4^a n) = r_3(n)$.
- Let $R_k(n)$ be the number of **primitive** solutions of $x_1^2 + \cdots + x_k^2 = n$, i.e. $\gcd(x_1, \ldots, x_k) = 1$. Then

$$R_3(n) = \begin{cases} 24 \sum_{s=1}^{\lfloor n/4 \rfloor} \left(\frac{s}{n}\right) & n \equiv 1, 2 \pmod 4 \\ 8 \sum_{s=1}^{\lfloor n/2 \rfloor} \left(\frac{s}{n}\right) & n \equiv 3 \pmod 8 \end{cases}$$

More conceptually, if n is squre free, then

$$r_3(n) = \begin{cases} 24 \cdot h(\mathbb{Q}(\sqrt{-n})) & \text{for } n \equiv 3 \pmod 8 \\ 12 \cdot h(\mathbb{Q}(\sqrt{-n})) & \text{for } n \equiv 1, 2, 5, 6 \pmod 8 \\ 0 & \text{for } n \equiv 7 \pmod 8 \end{cases}$$

where $h(\mathbb{Q}(\sqrt{-n}))$ is the class number of $\mathbb{Q}(\sqrt{-n})$.

Mod p points for a CM elliptic curve

For the elliptic curve E be the elliptic curve $E = \{y^2 = x^3 + x\}$, which hascomplex multiplication by $\mathbb{Z}[\sqrt{-1}]$ with $\sqrt{-1}$ acting by $(x, y) \mapsto (-x, \sqrt{-1}y)$, we have

$$\#E(\mathbb{F}_p) = 1 + p - a_p, \quad -2\sqrt{p} \leq a_p \leq 2\sqrt{p}$$

for all prime numbers p.
(This is a general perperty of elliptic curves, due to Hasse. The CM property allows us to give an explicit formula for a_p's.)

For *odd* p we have

$$\begin{aligned} a_p &= \sum_{u \in \mathbb{F}_p} \left(\frac{u^3 + u}{p} \right) \\ &= \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4 \\ -2a & \text{if } p = a^2 + 4b^2 \text{ with } a \equiv 1 \pmod 4 \end{cases} \end{aligned}$$

The Riemann zeta function

§6. Zeta functions and their special values

The Riemann zeta function $\zeta(s)$ is a meromorphic function on $\mathbb{C}$ with only a simple pole at $s = 0$ (and holomorphic elsewhere),

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_p (1 - p^{-s})^{-1} \qquad \text{for } \operatorname{Re}(s) > 1,$$

such that the function $\xi(s) = \pi^{-s/2} \cdot \Gamma(s/2) \cdot \zeta(s)$ satisfies

$$\xi(1 - s) = \xi(s).$$

Here $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$ for $\operatorname{Re}(s) > 0$, extended to $\mathbb{C}$ by $\Gamma(s + 1) = s\Gamma(s)$.

A Tour of Fermat's World
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Figure: Riemann

Dirichlet L-functions

Similar properties hold for the Dirichlet L-function

$$L(\chi,s) = \sum_{n\in N,\,(n,N)=1} \chi(n)\cdot n^{-s} \qquad \mathrm{Re}(s)>1$$

for a *primitive* Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}_1^\times$.

(Here $\mathbb{C}_1^\times$ denotes the set of all complex numbers with absolute value 1, $(\mathbb{Z}/N\mathbb{Z})^\times$ is the set of all integers modulo N which are prime to N, and χ is a function compatible with the rules of multiplication for both its source and target.)

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Figure: Dirichlet

L-functions and distribution of prime numbers

Theme. Zeta and L-values often contain deep arithmetic/geometric information.

- Dirichlet's theorem for primes in arithmetic progression
  $\leftrightarrow\ L(\chi,1)\neq 0\ \ \forall$ Dirichlet character χ.
- The prime number theorem
  $\leftrightarrow$ zero free region of $\zeta(s)$ near $\{\mathrm{Re}(s)=1\}$.
- Riemann's hypothesis $\leftrightarrow$ (estimate of) the second term in the asymptotic expansion of
  $$\pi(x) := \#\{p \text{ prime} \,|\, p\leq x\}$$
  Note: the first/main term in expansion of $\pi(x)$ is
  $$\mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2x}{(\log x)^3} + \frac{6x}{(\log x)^4} + \cdots$$

A Tour of Fermat's World
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

More magical properties of zeta values

- Certain values of zeta or L-functions tend to be rational or algebraic numbers, or becomes rational/algebraic after suitable transcendental factors are removed.
- These special zeta values contains deep information such as class numbers, Mordell-Weil group, Selmer group, Tate-Shafarevich group, etc.

Examples. (a) Leibniz's formula: $\mathbb{Z}[\sqrt{-1}]$ is a PID (because the formula implies that the class number $h(\mathbb{Q}(\sqrt{-1}))$ is 1).

(b) B_k/k appears in the formula for the number of (isomorphism classes of) exotic $(4k-1)$-spheres.

Bernouli numbers as zeta values

A TOUR OF FERMAT'S WORLD
Ching-Li Chai

Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Recall that the Bernoulli numbers B_n are defined by

$$\frac{x}{e^x - 1} = \sum_{n\in\mathbb{N}} \frac{B_n}{n!} \cdot x^n$$

$B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, $B_8 = -1/30$, $B_{10} = 5/66$, $B_{12} = -691/2730$.

(i) (Euler) $\zeta(1-k) = -B_k/k \quad \forall$ even integer $k > 0$.

(ii) (Leibniz's formula, 1678; Madhava, ~ 1400)
$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}$

Euler's evaluation of zeta values.

Insert a factor t^k into the fomal infinite series for $\zeta(-n)$ and evaluate at $t=1$: $\zeta(-k) = \sum_{n=1}^{\infty} n^k = \left(\sum_{n=1}^{\infty} n^k t^n\right)\Big|_{t=1}$

From $\left(t\frac{d}{dt}\right)^k t^n = n^k t^n$, we get

$$\zeta(-k) = \left(t\frac{d}{dt}\right)^k \left(\sum_{n=1}^{\infty} t^n\right)\Bigg|_{t=1} = \left(t\frac{d}{dt}\right)^k \left(\frac{t}{1-t}\right)\Bigg|_{t=1}$$

Let $t = e^x$, so $t\frac{d}{dt} = \frac{d}{dx}$ and

$$\zeta(-k) = \left(\frac{d}{dx}\right)^k \left(\frac{e^x}{1-e^x}\right)\Bigg|_{x=0} = -\frac{B_{k+1}}{k+1}$$

for $k > 0$. Esp. $\zeta(-k) \in \mathbb{Q}$, $\zeta(-2k) = 0 \ \forall\, k > 0$.

Congruence of zeta values

Theme. Special zeta or L-values satisfy strong congruence properties—causing them to have p-adic avatars (called p-adic L-functions) which interpolate complex L-functions

Example. (Kummer congruence)

(i) $\zeta(m) \in \mathbb{Z}_{(p)}$ for $m \le 0$ with $m \not\equiv 1 \pmod{p-1}$

(ii) $\zeta(m) \equiv \zeta(m') \pmod{p}$ for all $m, m' \le 0$ with $m \equiv m' \not\equiv 1 \pmod{p-1}$.

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Examples of p-adic properties of zeta values

EXAMPLES OF KUMMER CONGRUENCE.

- $\zeta(-1) = -\dfrac{1}{2^2\cdot 3}$; $-1 \equiv 1 \pmod{p-1}$ only for $p = 2, 3$.
- $\zeta(-11) = \dfrac{691}{2^3\cdot 3^2\cdot 5\cdot 7\cdot 13}$; $-11 \equiv 1 \pmod{p-1}$ holds only for $p = 2, 3, 5, 7, 13$.
- $\zeta(-5) = -\dfrac{1}{2^2\cdot 3^2\cdot 7} \equiv \zeta(-1) \pmod{5}$, and we have $-1 \equiv -5 \pmod{5}$.
  (This congruence holds because $3\cdot 7 \equiv 1 \pmod{5}$.)

EXAMPLE. (Kummer's criterion) The prime factor 691 of the numerator of $\zeta(-11)$ implies that 691 divides the class number of $\mathbb{Q}(e^{2\pi\sqrt{-1}/691})$. (One such congruence for a $\zeta(m)$, e.g. $m = -11$, sufficies.)

Figure: Kummer

A TOUR OF FERMAT'S WORLD
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Modular forms and Hecke symmetry

§7. Modular forms and L-functions

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, i.e. Γ contains all elements which are $\equiv \mathrm{I}_2 \pmod{N}$ for some N.

(a) A holomorphic function $f(\tau)$ on the upper half plane $\mathbb{H}$ is said to be a *modular form* of weight k and level Γ if

$$f((a\tau+b)(c\tau+d)^{-1}) = (c\tau+d)^k \cdot f(\tau) \;\; \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

and has *moderate growth* at all cusps.

Modular forms and L-functions

(c) The L-function

$$L_f(s) = \sum_{n\geq 1} a_n n^{-s}$$

attached to a cusp form

$$f = \sum_{n\geq 1} a_n e^{2\pi\sqrt{-1}\tau} \quad \forall \tau \in \mathbb{H}$$

of weight k for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, which is a *common eigenvector* of all Hecke correspondences, admits an Euler product

$$L_f(s) = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1}$$

The Ramanujan τ function

Example. Weight 12 cusp forms for $\mathrm{SL}_2(\mathbb{Z})$ are constant multiples of

$$\Delta = q \cdot \prod_{m\geq 1} (1-q^m)^{24} = \sum_n \tau(n)\, q^n$$

and

$$T_p(\Delta) = \tau(p)\cdot\Delta \quad \forall p,$$

where T_p is the Hecke operator represented by $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

Let $L(\Delta, s) = \sum_{n\geq 1} a_n \cdot n^{-s}$. We have

$$L(\Delta, s) = \prod_p (1-\tau(p)\, p^{-s} + p^{11-2s})^{-1}.$$

How to count number of sum of squares

A Tour of Fermat's World
Ching-Li Chai

Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Method. Explicitly identify k-th power the theta series

$$\theta^k(\tau) = \Big(\sum_{m\in\mathbb{N}} q^{m^2}\Big)^k \qquad \text{where } q = e^{2\pi\sqrt{-1}\,\tau} = \sum_{n\in\mathbb{N}} r_k(n)\, q^n$$

with a modular form obtained in a different way, such as Eisenstein series.
(Because $\theta(\tau)$ is a modular form of weight $1/2$, its k-th power is a modular form of weight $k/2$. Modular forms of a given weight for a given congruence subgroup form a finite dimensional vector space.)

Counting congruence solutions

(a) Count the number of congruence solutions of a given diophantine equation modulo a (fixed) prime number p

(b) Identify the L-function for a given diophantine equation (basically the generating function for the number of *congruence solutions* modulo p as p varies)

with

an L-function coming from harmonic analysis. (The latter is associated to a modular form).

Remark. (b) is an essential aspect of the Langlands program.

Elliptic curves basics

A Tour of Fermat's World
Ching-Li Chai

Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

§9. Elliptic curves, complex multiplication and L-functions

Equivalent definitions of an `elliptic curve` E:

- a projective curve with an algebraic group law;
- a projective curve of genus one together with a rational point (= the origin);
- over $\mathbb{C}$: a complex torus of the form $E_\tau = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$, where $\tau \in \mathfrak{H} :=$ upper-half plane;
- over a field F with $6 \in F^\times$: given by an affine equation

$$y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in F.$$

Weistrass theory

For $E_\tau = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$, let

$$\begin{aligned} x_\tau(z) &= \wp(\tau, z) \\ &= \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left(\frac{1}{(z - m\tau - n)^2} - \frac{1}{(m\tau + n)^2} \right) \end{aligned}$$

$y_\tau(z) = \frac{d}{dz}\wp(\tau, z)$

Then E_τ satisfies the Weistrass equation

$$y_\tau^2 = 4x_\tau^3 - g_2(\tau)x_\tau - g_3(\tau)$$

with

- $g_2(\tau) = 60 \displaystyle\sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \frac{1}{(m\tau+n)^4}$
- $g_3(\tau) = 140 \displaystyle\sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \frac{1}{(m\tau+n)^6}$

The j-invariant

Elliptic curves are classified by their j-invariant

$$j = 1728 \frac{g_2^3}{g_2^3 - 27g_3^2}$$

Over $\mathbb{C}$, $j(E_\tau)$ depends only on the lattice $\mathbb{Z}\tau + \mathbb{Z}$ of E_τ. So $j(\tau)$ is a `modular function` for $\mathrm{SL}_2(\mathbb{Z})$:

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau)$$

for all $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$.

We have a Fourier expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884\,q + 21493760\,q^2 + \cdots,$$

where $q = q_\tau = e^{2\pi\sqrt{-1}\,\tau}$.

A Tour of Fermat's World
Ching-Li Chai
Samples of numbers
More samples in arithemetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Elliptic curves with complex multiplication

An elliptic E over $\mathbb{C}$ is said to have complex multiplication if its endomorphism algebra $\mathrm{End}^0(E)$ is an imaginary quadratic field.

Example. Consequences of

- $j(\mathbb{C}/\mathscr{O}_K)$ is an algebraic integer
- $K \cdot j(\mathbb{C}/\mathscr{O}_K)$ = the Hilbert class field of K.

$$e^{\pi\sqrt{67}} = 147197952743.9999986624542245068292613\cdots$$
$$j\left(\frac{-1+\sqrt{-67}}{2}\right) = -147197952000 = -2^{15}\cdot 3^3\cdot 5^3\cdot 11^3$$

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007259719\ldots$$
$$j\left(\frac{-1+\sqrt{-163}}{2}\right) = -262537412640768000 =$$
$$-2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3$$

A CM curve and its associated modular form

We have seen that the number of congruent points on the elliptic curve $E = y^2 = x^3 + x$ is given by

$$\#E(\mathbb{F}_p) = 1 + p - a_p$$

and for *odd* p we have

$$a_p = \sum_{u\in\mathbb{F}_p}\left(\frac{u^3+u}{p}\right)$$
$$= \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4 \\ -2a & \text{if } p = a^2 + 4b^2 \text{ with } a \equiv 1 \pmod 4 \end{cases}$$

A CM curve and its associated modular form, continued

The L-function $L(E,s)$ attached to E with

$$\prod_{p \text{ odd}} (1 - a_p p^{-s} + p^{1-2s})^{-1} = \sum_n a_n \cdot n^{-s}$$

is equal to a Hecke L-function $L(\psi,s)$, where the Hecke character ψ is the given by

$$\psi(\mathfrak{a}) = \begin{cases} 0 & \text{if} \quad 2|\mathrm{N}(\mathfrak{a}) \\ \lambda & \text{if} \quad \mathfrak{a} = (\lambda),\ \lambda \in 1 + 4\mathbb{Z} + 2\mathbb{Z}\sqrt{-1} \end{cases}$$

The function $f_E(\tau) = \sum_n a_n \cdot q^n$ is a modular form of weight 2 and level 4, and

$$f_E(\tau) = \sum_{\mathfrak{a}} \psi(\mathfrak{a}) \cdot q^{\mathrm{N}(\mathfrak{a})} = \sum_{\substack{a \equiv 1 \pmod 4 \\ b \equiv 0 \pmod 2}} a \cdot q^{a^2+b^2}$$

Estimates of Fourier coefficients by Weil conjecture

§10. Weil conjecture and equidistribution
Let $\Delta(\tau) = \sum_{n\geq 1} \tau(n)\, e^{2\pi\sqrt{-1}}$ be the normalized cusp form of weight 12 whose Fourier coefficients are the Ramanujan numbers $\tau(n)$; they are eigenvalues of Hecke operators T_n.

- (Eichler & Shimura) $\tau(p) = \alpha_p + \overline{\alpha_p}$ for each prime number p, where α_p is the eigenvalues of a "Frobenius operator for p".
- (Deligne) Deligne showed that the Ramanujan conjecture $|\tau(p)| \leq C \cdot p^{11/2}$ is a consequence of Weil's conjecture (which asserts that $|\alpha_p| = p^{11/2}$ in this case). Then he proved Weil's conjecture in 1974.

A Tour of Fermat's World
Ching-Li Chai

Samples of numbers
More samples in arithmetic
Congruent numbers
Fermat's infinite descent
Counting solutions
Zeta functions and their special values
Modular forms and L-functions
Elliptic curves, complex multiplication and L-functions
Weil conjecture and equidistribution

Equidistribution

Remark. Similar estimates of Fourier coefficients of modular forms also follows from Weil's conjecture. This gives the best possible estimates of Fourier coefficients by algebraic methods. (Estimates obtained by analytic methods so far are very far off.)

Question In what sense is the above estimate "best possible"?

ANSWER. The family of real numbers $\{\tau(p)/\sqrt{p}\}$ is equidistributed in $[-2,2]$ with respect to the measure $\frac{1}{2\pi}\sqrt{4-t^2}dt$, i.e.

$$\lim_{x\to\infty} \frac{1}{\#\{p : p \leq x\}} \sum_{p\leq x} f(a_p/\sqrt{p}) = \frac{1}{2\pi}\int_{-2}^{2} f(t)\sqrt{4-t^2}dt$$

for every continuous function $f(t)$ on $[-2,2]$.