NUMBERS: FUN AND CHALLENGE

LEUNG YEUK LAM LECTURE SERIES

Ching-Li Chai

Hong Kong, August 10, 2007

Chronological table

Euclid	$\sim$300 B.C.E.	Galois	1811–1832
Diophantus	$\sim$300 C.E.	Hermite	1822–1901
Brahmagupta	$\sim$600 C.E.	Eisenstein	1823–1852
Qin Jiushao	1202–1261	Kronecker	1823–1891
Fermat	1601–1665	Riemann	1826–1866
Euler	1707–1783	Dedekind	1831–1916
Lagrange	1736–1813	Weber	1842–1913
Legendre	1752–1833	Hensel	1861–1941
Gauss	1777–1855	Hilbert	1862–1943
Abel	1802–1829	Takagi	1875–1960
Jacobi	1804–1851	Hecke	1887–1947
Dirichlet	1805–1859	Artin	1898–1962
Kummer	1810–1893	Hasse	1898–1979

§1. Examples

Some numbers

- 2, the only even prime number.

- $\sqrt{2}$, 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 $x^2 - x - 1$.

- $e = \exp(1) = \sum_{n=0}^{\infty} \frac{1}{n!}$, the base of the natural logarithm.

- π, area of a circle of radius 1. Zu Chungzhi (429–500) gave two approximating fractions,

$$\frac{22}{7} \qquad \frac{355}{113}$$

and obtained that

$$3.1415926 < \pi < 3.1415927$$

- $1729 = 12^3 + 1^3 = 10^3 + 9^3$,

the **taxi cab 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.

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**.

- $2^p - 1$, the **Mersenne numbers**. If $M = 2^p - 1$ 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**.

- $3, 5, 17, 257, 65537, 4294967297$

the **Fermat numbers**,

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

Euler found in 1732 that

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

- The **partition numbers** $p(n)$ with generating series

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

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

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

- $1, -24, 252, -1472, 4830, -6048, \ldots,$

the first few of the **Ramanujan numbers**, defined by

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

- The **Bernouli numbers**, defined by

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

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

- $-1, -2, -3, -7, -11, -19, -43, -67, -163,$

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.

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

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007$$

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

- (Fermat)

$$p = x^2 + y^2 \iff p \equiv 1 \pmod 4$$

$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod 8$$

$$p = x^2 + 3y^2 \iff p = 3p \text{ or } p \equiv 1 \pmod 3$$

- (Euler)

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$$

$$2p = x^2 + 5y^2 \iff p \equiv 3, 7 \pmod{20}$$

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

- $p = x^2 + 27y^2 \iff p \equiv 1 \pmod 3$ and 2 is a cubic residue modulo p.

- $p = x^2 + 64y^2 \iff p \equiv 1 \pmod 4$ and 2 is a biquadratic residue modulo p.

- (Kronecker)
$p = x^2+31y^2 \iff (x^3-10x)^2+31(x^2-1)^2 \equiv 0 \pmod p$ has an integer solution

I. 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

$$x = s^2 - t^2,\ y = 2st,\ z = s^2 + t^2$$

- (Fermat) The equation

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

has no non-trivial integer solution.

- (Fermat's Last Theorem)

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

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

Proved by A. 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*.

II. Some formulas discovered by Euler

- $\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$

- $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \frac{\pi^2}{2}$

- $1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \dots = \frac{\pi^4}{90}$

- $1 - 2^k + 3^k - 4^k + \dots = -\frac{(1-2^{k+1})}{k+1} B_{k+1}$

for $k \geq 1$; in particular it vanishes if k is even.

- $\frac{1}{\pi^{2k}}(1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \dots) \in \mathbb{Q}$

for every integer $k \geq 1$.

III. Counting solutions.

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

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

- Sum of two squares.

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

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.

- 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

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

§2. Fermat's infinite descent

Fermat's proof that

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

has no non-trivial integer solution.

May assume $\mathrm{gcd}(x, y, z) = 1$. 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

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

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

Step 2. $s^4 + 4t^4 = u^2, \ \gcd(s, t, u) = 1$

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.

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.)

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 $\mathbb{Q}$.

Relation with elliptic integrals

- Fagnano considered the arc length integral

$$\int_0^r \frac{d\rho}{\sqrt{1-\rho^4}}$$

of the lemniscate

$$[(x-\frac{1}{\sqrt{2}})^2+y^2]\cdot[(x+\frac{1}{\sqrt{2}})^2+y^2]=\frac{1}{2}\,,$$

using $\rho=\sqrt{x^2+y^2}$ as the parameter.

1. $\rho^2=\frac{2\xi^2}{1+\xi^4}$ leads to $\frac{d\rho}{\sqrt{1-\rho^4}}=\sqrt{2}\frac{d\xi}{\sqrt{1+\xi^4}}$,

$$\int_0^r \frac{d\rho}{\sqrt{1-\rho^4}}=\sqrt{2}\int_0^t \frac{d\xi}{\sqrt{1+\xi^4}}\,,$$

where $r^2=\frac{2t^2}{1+t^4}$

2. $\xi^2 = \frac{2\eta^2}{1-\eta^4}$ leads to $\frac{d\xi}{\sqrt{1+\xi^4}} = \sqrt{2}\frac{d\eta}{\sqrt{1-\eta^4}}$,

$$\int_0^t \frac{d\xi}{\sqrt{1+\xi^4}} = \sqrt{2}\int_0^u \frac{d\eta}{\sqrt{1-\eta^4}}\,,$$

where $t^2 = \frac{2u^2}{1-u^4}$

3. $r(u) = \frac{2u\sqrt{1-u^4}}{1+u^4}$ doubles the arc length

$$2\int_0^u \frac{dt}{\sqrt{1-t^4}} = \int_0^{r(u)} \frac{dt}{\sqrt{1-t^4}}\,,$$

where $r^2 = \frac{4u^2(1-u^4)}{(1+u^4)^2}$

4. Rewrite:

$$\int_0^r \frac{d\rho}{\sqrt{1-\rho^4}} = (1 \pm \sqrt{-1})\int_0^v \frac{d\psi}{\sqrt{1-\psi^4}}$$

where $r = \frac{\pm 2\sqrt{-1}v^2}{1-v^4}$.

• In 1751, inspired by Fagnano, Euler discovered the addition formula

$$\int_0^r \frac{d\rho}{\sqrt{1-\rho^4}} = \int_0^u \frac{d\eta}{\sqrt{1-\eta^4}} + \int_0^v \frac{d\psi}{\sqrt{1-\psi^4}}$$

where $r = \frac{u\sqrt{1-v^4}+v\sqrt{1-u^4}}{1+u^2v^2}$, and the theory of elliptic functions was born.

Notice that r is a **rational function** in u, $\sqrt{1-u^4}$, v and $\sqrt{1-v^4}$.

S3. Zeta and L-values

Euler's evaluation of zeta values.

The Riemann zeta function $\zeta(s)$ is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,, \quad \mathrm{Re}(s) > 1$$

Insert a factor t^k and evaluate at $t = 1$:

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

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

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

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

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

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

Remark. $\zeta(s)$ extends to a meromorphic function on the whole complex plane $\mathbb{C}$ with $s = 1$ as the only pole. Moreover $\zeta(s)$ satisfies a function equation

$$\pi^{-s/2}\,\Gamma(s/2)\,\zeta(s) = \pi^{-(1-s)/2}\,\Gamma((1-s)/2)\,\zeta((1-s)/2)\,,$$

where $\Gamma(s) = \int_0^\infty e^{-x} x^s \frac{dx}{x}$ is the Gamma function with $\Gamma(n+1) = n!$ for each positive integer n.

In particular the values of $\zeta(s)$ at odd negative integers are related to the values at even positive integers.

Numerical examples.

- $\zeta(0) = -\frac{1}{2}$
- $\zeta(-1) = -\frac{1}{2^2 \times 3}$
- $\zeta(-3) = -\frac{1}{2^3 \times 3 \times 5}$
- $\zeta(-11) = \frac{691}{2^3 \times 3^2 \times 5 \times 7 \times 13}$

L-functions. The Riemann zeta function has many cousins. Let N be a positive integer, and let

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

be a *Dirichlet character* modulo N. That means χ is a function from integers prime to N to $\mathbb{C}^\times$ such that $\chi(n_1) = \chi(n_2)$ if $n_1 \equiv n_2 \pmod{N}$ and $\chi(n_1 n_2) = \chi(n_1 n_2)$.

For instance when $N = 4$, there is exactly one non-trivial Dirichlet character ϵ_4:

$$\epsilon_4(1\ (\mathrm{mod} 4)) = 1, \ \ \epsilon_4(3\ (\mathrm{mod} 4)) = -1$$

The **Dirichlet L-function** attached to χ is

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where we set $\chi(n) = 0$ if n is not prime to N.

The Dirichlet L-functions also have meromorphic continuation and functional equations relating $L(s,\chi)$ to $L(1-s,\chi)$. Their values at non-positive integers and positive integers k such that $\chi(-1)=(-1)^k$ can be computed by Euler's method.

For instance when the **conductor** $N=4$, we have

$$L(1,\epsilon_4) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots = \frac{\pi}{4}$$

$$L(3,\epsilon_4) = 1 - \frac{1}{3^3} + \frac{1}{5^3} - \frac{1}{7^3} + \frac{1}{9^3} - \cdots = \frac{\pi^3}{32}$$

Magical properties of zeta.

I. Non-vanishing of zeta functions.

- Dirichlet's famous theorem that there are infinitely many prime numbers in any arithmetic progression amounts to $L(1,\chi) \neq 0$.

- Similarly the *Prime number theorem*, which asserts that the number of prime numbers up to a real number x is asymptotic to $\frac{x}{\log x}$ amounts to the non-vanishing of $\zeta(s)$ at the critical line $\mathrm{Re}(s) = 1$.

II. Rationality The "essential part" of certain special zeta and L-values are rational number.

E.g. $\zeta(0), \zeta(-1), \zeta(-3), \zeta(-5), \ldots \in \mathbb{Q}$,
$\zeta(2), \zeta(4), \zeta(6), \ldots \in \pi^{2\mathbb{N}}\mathbb{Q}$.

III. Arithmetic info encoded in special values.

- For instance, the special value $L(1, \epsilon_4)$ tells us that the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ is a unique factorization domain.

- The formula for $R_3(n)$, the number of primitive solutions of the Diophantine equation $x_1^2 + x_2^2 + x_3^3 = n$, is closely related to the values $L(1, \chi)$ for Dirichlet characters χ such that $\chi^2 = 1$ and $\chi(-1) = -1$.

IV. p-adic properties of special values.

EXAMPLE 1. (Kummer congruence)

(a) For every non-positive integer m with $m \not\equiv 1 \pmod{p-1}$, the denominator of $\zeta(m)$ is prime to p.

ILLUSTRATION. The prime factors of the denominators of $\zeta(-11)$ are $2, 3, 5, 7, 13$, exactly those primes p such that $-11 \equiv 1 \mod p-1$.

(b) If m_1, m_2 are non-positive integers such that $m_1 \equiv m_2 \not\equiv 1 \pmod{p-1}$, then the numerator of $\zeta(m_1) - \zeta(m_2)$ is divisible by p.

EXAMPLE 2. The prime factor 691 of the numerator of $\zeta(-11)$ implies that 691 divides the class number of $\mathbb{Q}(e^{2\pi\sqrt{-1}/691})$.

V. Close relation to modular forms

(a) Sometimes special values appear as (the main part of) Fourier coefficients of modular forms—fruitful for p-adic properties of special L-values.

(b) This connection is part of the **Langlands program**.

Challenge: GRH.

Riemann Hypothesis: All non-trivial zeroes of $\zeta(s)$ (i.e. those with $0 < \mathrm{Re}(s) < 1$) have $\mathrm{Re}(s) = \frac{1}{2}$

(Equivalent to a statement about the error term for the distribution of prime numbers.)

The **Grand Riemann Hypothesis** is a similar statement for more general zeta and L-functions.

S4. Modular forms.

Definition. Let $N \in \mathbb{N}_+$, $k \in (1/2)\mathbb{N}_+$. A **modular form of weight k and level N** is a holomorphic function $f : \mathbb{H} \longrightarrow \mathbb{C}$ on the upper half plane $\mathbb{H}$ s.t.

- $\forall\ \tau \in \mathbb{H}$ and $\forall\ a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$, $a \equiv d \equiv 1 \pmod{N}$ and $b \equiv c \equiv 0 \pmod{N}$, we have

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k\, f(\tau)\,.$$

- $f(\tau)$ is *holomorphic at infinity*.

Such a modular form $f(\tau)$ has a q**-expansion**

$$f(\tau) = \sum_{n=0}^{\infty} a_n\, e^{\frac{2\pi\sqrt{-1}n}{N}} = \sum_{n=0}^{\infty} a_n\, q^{n/N}\,,$$

where $q^{n/N} = e^{\frac{2\pi\sqrt{-1}n}{N}}$.

Examples.

- For every positive integer k, let

$$G_{2k}(\tau)=\sum\nolimits'_{m,n\in\mathbb{Z}} \frac{1}{(m\tau+n)^{2k}}\ .$$

This Eisenstein series is a modular form of weight $2k$ and level 1, whose q-expansion is

$$G_{2k}(\tau)=2\zeta(2k)+2\frac{(2\pi\sqrt{-1})^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)\,q^n\ ,$$

where $\sigma_{2k-1}(n)=\sum_{d|n} d^{2k-1}$.

Notice that the constant term of G_{2k} is a zeta-value.

- Put $g_2 = 60G_2\ ,\quad g_3 = 140G_3$,

$\Delta = g_2^3 - 27g_3^2$. The classical j-invariant is

$$j(\tau) = (12)^3 g_2^3/\Delta = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n)q^n$$

where every $c(n) \in \mathbb{Z}$.

- For the Heegner numbers $-d = -67, -163$, the theory of complex multiplications tells us that $j\left(\frac{1+\sqrt{-d}}{2}\right) \in \mathbb{Z}$. The q-expansion of $j(\tau)$ tells us that the difference between $e^{\pi\sqrt{d}}$ and the nearest integer is $\sum_{n=1}^{\infty}(-1)^n c(n) e^{-n\pi\sqrt{d}}$, a pretty small number.

- $\theta(\tau) = \sum_{m\in\mathbb{Z}} e^{\pi\sqrt{-1}m^2\tau}$, the Jacobi theta series. It is a modular form of weight $1/2$ and level 4. We have

$$\theta(\tau)^k = \sum_{n\in\mathbb{Z}} r_k(n)\, e^{\pi\sqrt{-1}n\tau}$$

where $r_k(n)$ is the number of ways to represent n as a sum of k squares. Explicit formulas for $r_2(n)$, $r_4(n)$ and $r_3(n)$ can be obtained by expressing $\theta(\tau)^k$ in terms of other modular forms.

- $\Delta = g_2^3 - 27g_3^2$ vanishes at infinity; i.e. it is a **cusp form** of weight 12, and it is up to constant the unique cusp form of weight 12.

- The normalized cusp form $\Delta' = (2\pi)^{-12}\Delta$ admits a product expansion

$$\Delta'(\tau) = q \prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n\,,$$

where $\tau(n)$ are the Ramanujan numbers.

The theory of Hecke operators give

$$\tau(mn) = \tau(m)\tau(n) \qquad \text{if } \gcd(m,n) = 1$$

and $\tau(p^n)$ can be computed from $\tau(p)$ by recursion

$$\tau(p)\tau(p^n) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1})$$

if p is a prime number.

- Ramanujan conjectured that $|\tau(p)| \leq 2p^{11/2}$ for every prime number p. This was proved by Deligne in 1974 when he proved the Weil conjecture; it is one of the great achievements in the 20th century.

- The L-function attached to the cusp form Δ' admits an Euler product decomposition

$$L_{\Delta'}(s) := \sum_{n=1}^{\infty} \tau(n) n^{-s} = \prod_p \frac{1}{(1 - \tau(p) p^{-s} + p^{11-2s})} \,.$$

Moreover it extends to an entire function on $\mathbb{C}$ and

$$(2\pi)^{-s}\,\Gamma(s)\,L_{\Delta'}(s) = (2\pi)^{12-s}\,\Gamma(12-s)\,L_{\Delta'}(12-s)\,.$$

Similar properties hold for more general primitive cusp forms.

- Elliptic curves over $\mathbb{Q}$ provide another source for modular forms.

Let E be an elliptic curve over $\mathbb{Q}$. Let

$$L_E(s) := \prod_p \frac{1}{(1 - a_p p^{-s} + p^{1-2s})} = \sum_{n \geq 1} a_n\, n^{-s}$$

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

Let

$$f_E(\tau) = \sum_{n \geq 1} a_n\, q^n\,.$$

The **modularity conjecture** asserts that f_E is a modular form of weight 2.

In 1994 A. Wiles and R. Taylor proved the modularity conjecture when E has semistable reduction, from which Fermat's Last Theorem follows. The modularity conjecture was subsequently settled by C. Breuil, B. Conrad, F. Diamond and R. Taylor.

- Let E be an elliptic curve over $\mathbb{Q}$ **without complex multiplication**.

(Hasse): $a_p \leq 2\sqrt{p}$ $\forall$ prime number p

The **Sato-Tate conjecture** asserts that the family of real numbers $\{a_p/\sqrt{p}\}$ 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 $[-2, 2]$.

This statement was not known for a **single** elliptic curve over $\mathbb{Q}$ until the Sato Tate conjecture was proved by R. Taylor in 2006.

Number theory is not standing still!

Further Challenge. The key to the proof of the modularity conjecture and the Sato-Tate conjecture is to show certain families of Dirichlet series come from modular forms. Extending the method to other more general Dirichlet series is another great challenge in number theory.