Numbers: Fun and Challenge
Leung Yeuk Lam Lecture Series

Ching-Li Chai, August 10, 2007

Throughout history people are interested in *numbers*, for practical purposes and beyond. Perhaps part of the reason is that number is a nearly universal ingredient in human languages.[1] Certain numbers are deemed special. In the western culture, 7 is the "lucky number", while 13 is a number for bad fortune. In the Chinese culture, the even numbers 2, 4, 8 are often associated with good fortune, and the number 95 is associated to the emperor. More mathematically inclined people tend to be attracted to some different aspect of numbers that is difficult to define, and collectively known as " number theory".[2] We would like to share with the reader the romance of numbers, and discuss some of the challenges they pose.

Chronological table

Euclid	∼300 B.C.E.	Galois	1811–1832
Diophantus	∼300 C.E.	Hermite	1822–1901
Brahmagupta	∼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.

To wet our appetite, we begin with a list of some special 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 learns.
- $\frac{1+\sqrt{5}}{2}$, the *golden number*, a root of the quadratic polynomial $x^2 - x - 1$.

[1] The Parahã, a tribe in the Amazon, have no numbers. All known efforts to teach a Parahaã to count in another language failed, unlike other tribes which also have a one-two-many counting system.

[2] In the words of Weil "When I smell number-theory, I think I know it, and when I smell something else, I think I know it too."; see [8].

- $e = \exp(1) = \sum_{n=0}^{\infty} \frac{1}{n!}$, the base of the natural logarithm. It admits the following infinite continuous fraction expansion

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{8 + \cdots}}}}}}}}}}}$$

- π, area of a circle of radius 1. Zu Chungzhi (429–500 C.E.) gave two approximating fractions $\frac{22}{7}$ and $\frac{355}{113}$, and obtained that π is between 3.1415926 and 3.1415927.
- $1729 = 12^3 + 1^3 = 10^3 + 9^3$, 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.
- 30, the largest positive integer m such that every positive integer between 2 and m and relatively prime to m is a prime number.

We will not come back to these numbers, and recommend [1] for amusing digressions.

Next comes some families of numbers.

- $1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, \ldots$, the *triangular numbers*, $\Delta_n = \frac{n(n+1)}{2}$.
- $1, 4, 9, 16, 25, \ldots$, squares of integers.
- $1, 5, 12, 22, 35, \ldots$, the *pentagonal numbers*, $p_n = \sum_{k=1}^{n} (3k-2) = \frac{n(3n-1)}{2}$.
- $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$, the prime numbers.
- $2^p - 1$, the emphMersenne 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]
- $3, 5, 17, 257, 65537, 4294967297$ the *Fermat numbers*, $F_r = 2^{2^r} + 1$.[4]

[3] A perfect number is a positive integer which is equal to the sum of all of its proper divisors. No odd perfect number is known. The 44th known Mersenne prime, $2^{32582657} - 1$, was discovered in 2006; it has 9808358 digits.

[4] Fermat thought that each F_r is a prime, but Euler found in 1732 that F_5 is a composite: $2^{32} + 1 = 4294967297 = 641 \times 6700417$, less than three years since Goldbach asked his opinion about Fermat's statement. No Fermat number F_r with $r > 4$ is known to be a prime.

- $1, 2, 5, 1, \ldots, c_n = \frac{1}{n}\binom{2n}{n}, \ldots$, the *Catalan numbers.*
- The *partition numbers* $p(n)$ with generating series
$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty}(1-x^m)^{-1}$$
The first few of the partition numbers are:$p(0) = 1$, $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$, $p(6) = 11$. Ramanujan gave the asymptotic formula
$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}.$$
- $1, -24, 252, -1472, 4830, -6048, \ldots$ are the first few of the *Ramanujan* numbers, defined by
$$\sum_{n=1}^{\infty} \tau(n)\, x^n = x\left[\prod_{n=1}^{\infty}(1-x^n)\right]^{24} = x\cdot(1-x)^{24}\cdot(1-x^2)^{24}\cdot(1-x^3)^{24}\cdot(1-x^4)^{24}\cdots$$
- The *Bernouli numbers*, defined by
$$\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n\, x^n\,,$$
$B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{12} = -\frac{691}{2730}$, $B_{14} = \frac{7}{6}$.
- The nine *Heegner numbers* $-1, -2, -3, -7, -11, -19, -43, -67, -163$ are the only negative integers $-d$ such that the class number of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ is equal to one. The last few Heegner numbers have the property that $e^{\pi\sqrt{d}}$ is very close to an integer,[5] for instance
$$e^{\pi\sqrt{67}} = 147197952743.99999866,$$
$$e^{\pi\sqrt{163}} = 161537412640768743.99999999999925007$$

Most of the above family of numbers are for historic interest interest only. Only prime numbers, Ramanujan numbers, Bernouli numbers and the Heegner numbers are related to the main themes of this talk.

Primes of the form $Ax^2 + By^2$. Below are some properties about numbers which may excite the budding number theorists.

- (Fermat)
$$p = x^2 + y^2 \iff p \equiv 1 \pmod 4$$
$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod 8$$
$$p = x^2 + 3y^2 \iff p = 3p \text{ or } p \equiv 1 \pmod 3$$

[5] The lattice $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \subset \mathbb{C}$ defines an elliptic curve over $\mathbb{Q}$ of CM-type, whose j-invariant is an integer; $e^{\pi\sqrt{d}}$ is the first term in the q-expansion of the j-invariant, the other terms decay exponentially.

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

Investigations in the direction of the above examples have led to the *class field theory*, a major achievement completed around 1930. We will not be able to go further in this direction in this talk. Rather we will focus our main themes, Diophantine equations, zeta values and modular forms, and illustrate them with some examples. We will indicate how the themes are intertwined, that modular forms and zeta-values come in naturally when we attempt to count the number of solutions. We will not define what an elliptic curve is, although their shadows are everywhere.

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. We will come back to this shortly.
- (Fermat's Last Theorem) $x^p + y^p + z^p = 0$ has no non-trivial integer solution if p is an odd prime number.

  This was proved by A. Wiles in 1994, more than 300 years after Fermat wrote the asserttion 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.
- $\frac{1}{\pi^{2k}}(1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \dots)$ is a rational number for every integer $k \geq 1$.
- $\prod_{n=1}^{\infty} (1 - x^n) = \sum_{n \in \mathbb{Z}} (-1)^n \, x^{n(3n+1)/2}$

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 the following closed formula for $r_2(n)$:

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

  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 the following explicit formula for $r_4(n)$: $r_4(n) = 8\,\sigma'(n)$, where $\sigma'(n)$ is the sum of divisors of n which are not divisible by 4. More explicitly,

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

- 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 $r_3(4^a n) = r_3(n)$. More explicit formulas exists (essentially the class number formula for imaginary quadratic fields, the main part of which is the zeta-value at $s = 1$). 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 we have for instance

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

§2. Fermat's infinite descent

We indicate how Fermat proved that the equation

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

has no non-trivial integer solution, i.e. one with $xy \neq 0$. We may and do assume that $\gcd(x, y, z) = 1$. We have $(x^2 + y^2) \cdot (x^2 - y^2) = z^2$. It is easy to see that 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; the second case is similar. Then there exist integers u, v such that $\gcd(u, v) = 1$, $x^2 + y^2 = 2u^2$, $x^2 - y^2 = 2v^2$ and $z = 2uv$.

Consider the equation $2v^2 = (x + y) \cdot (x - y)$. After suitably adjusting the signs of x and y, there exist integers r, s such that $x + y = r^2$, $x - y = 2s^2$, $v = rs$. An easy computation shows that the original equation $x^4 - y^4 = z^2$ becomes $r^4 + 4s^4 = 4u^2$. Write $r = 2t$, the equation becomes $s^4 + 4t^4 = u^2$, and we have $x = 2t^2 + s^2$, $y = 2t^2 - s^2$, $z = 4tsu$, $\gcd(s, t, u) = 1$.

Consider a non-trivial integer solution of the equation $s^4 + 4t^4 = u^2$ with $\gcd(s,t,u) = 1$. It is easy to see that u and s are both odd. Adjusting the signs, we may assume that $u > 0$. Since $4t^2 = (u-s^2)(u+s^2)$, there exist positive integers a, b such that $u - s^2 = 2b^2$, $u + s^2 = 2a^2$, $t^2 = ab$, $\gcd(a,b) = 1$. From $t^2 = ab$ we see that there exist integers 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 $s^2 = x_1^4 - y_1^4$. Let $z_1 = s$, so (x_1, y_1, z_1) is an integer solution of the original equation $x^4 - y^4 = z^2$, and the absolute value of x_1 is strictly smaller than the absolute value of x in the original non-trivial solution (x,y,z).

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. So we will 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 $|x| > |x_1| > |x_2| > |x_3| > \cdots$, which is impossible. Therefore there is no non-trivial solution. Q.E.D.

Remark. (1) The algebraic variety X_2 defined by the equation $s^4 + 4t^4 = u^2$ is isomorphic to the algebraic variety X_1 defined by the equation $x^4 - y^4 = z^2$ after the base field $\mathbb{Q}$ is extended to $\mathbb{Q}(\sqrt[4]{-4})$. We have a morphism $f : X_1 \to X_2$ given by

$$s \mapsto z,\ t \mapsto xy,\ u \mapsto x^4 + y^4$$

and a morphism $g : X_2 \to X_1$ given by

$$x \mapsto s^2 + 2t^2,\ y \mapsto s^2 - 2t^2,\ z \mapsto 4stu\,.$$

What we showed above is that a nontrivial integral point (x,y,u) on X_1 with x, y odd is the image under g of a non-trivial integer point $(s,t,u$ on X_2, and the latter is the image of another non-trivial integral point on X_1 itself.

(2) After projectivising the two equations above to $(x^4 + y^4 - x^2z^2 = 0$ and $s^4 + 4t^4 - s^2u^2 = 0$ respectively, what we get are two elliptic curves E_1 and E_2 over $\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-1}$. The maps f and g above become multiplication by $1 + \sqrt{-1}$ and $1 - \sqrt{-1}$ respectively over a suitable finite extension field of $\mathbb{Q}$. Of course multiplication by $1 \pm \sqrt{-1}$ are defined over $\mathbb{Q}$. Rather they give a $\mathbb{Q}$-rational map from E_1 to E_2 and a $\mathbb{Q}$-rational map from E_2 to E_1. The composition of the two maps is the $\mathbb{Q}$-rational map "multiplication by 2".

Relation with elliptic integrals

The Italian count Fagnano discovered a remarkable property of 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. He found that the change of variable $\rho^2 = \frac{2\xi^2}{1+\xi^4}$ leads to $\frac{d\rho}{\sqrt{1-\rho^4}} = \sqrt{2}\frac{d\xi}{\sqrt{1+\xi^4}}$ and

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

Similarly the change of variable $\xi^2 = \frac{2\eta^2}{1-\eta^4}$ leads to $\frac{d\xi}{\sqrt{1+\xi^4}} = \sqrt{2}\frac{d\eta}{\sqrt{1-\eta^4}}$ and

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

Combining the two formulas we get a function $r(u)$ $r(u) = \frac{2u\sqrt{1-u^4}}{1+u^4}$ for doubling the arc length of the arc length of the lemniscate, which is a *rational function in u and $\sqrt{1-u^4}$*:

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

We can rewrite the first two formulas with complex number to bring the complex multiplication to focus:

$$\int_0^r \frac{d\rho}{\sqrt{1-\rho^4}} = (1\pm\sqrt{-1})\int_0^v \frac{d\psi}{\sqrt{1-\psi^4}}\,, \qquad r = \frac{\pm 2\sqrt{-1}v^2}{1-v^4}\,.$$

Remark. The parallel between Fermat's infinite descent for $x^4 - y^4 = z^2$ and the above is remarkable. Of course it is not a coincidence. We have $\frac{z}{x^2} = \sqrt{1-(y/x)^4}$, so the curve defined by the algebraic function $\sqrt{1-t^4}$ is isomorphic to E_1 over $\mathbb{Q}$. The curve defined by the algebraic function $\sqrt{1+t^4}$ is isomorphic to E_2 over $\mathbb{R}$ but not over $\mathbb{Q}$, because one has extracted the square root of 2 in the change of variable formula $\rho^2 = \frac{2\xi^2}{\sqrt{1+\xi^4}}$.

In 1751, Fagnano's collection of papers *Produzioni Mathematiche* reached the Berlin Academy, Euler was asked to examine the book and draft a letter to thank Count Fagnano. Soon Euler discovered the addition formula

$$\int_0^r \frac{d\rho}{\sqrt{1-\rho^4}} = \int_0^u \frac{d\eta}{\sqrt{1-\eta^4}} + \int_0^v \frac{d\psi}{\sqrt{1-\psi^4}}\,, \qquad r = \frac{u\sqrt{1-v^4}+v\sqrt{1-u^4}}{1+u^2v^2}\,.$$

and the theory of elliptic functions was born. Notice that r is a *rational function* in u, $\sqrt{1-u^4}$, v and $\sqrt{1-v^4}$. Euler's formula amounts to the group law on the elliptic curve E_1 corresponding to the algebraic function $\sqrt{1-t^4}$ of t.

§3. Zeta and L-values

Euler's evaluation of zeta values. The Riemann zeta function $\zeta(s)$ is defined by the formula

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,.$$

The integral converges absolutely for $\mathrm{Re}(s) > 1$. Euler computed the value of $\zeta(-k)$, $k \in \mathbb{N}_{>0}$ as follows. First he inserts a factor t^k, so that the resulting series converges for $|t| < 1$, then he evaluates it 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

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

Change the variable and set $t = e^x$, so $t\frac{d}{dt} = \frac{d}{dx}$, we see that

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

for $k \in \mathbb{N}_{>0}$ by the definition of Bernouli numbers. In particular $\zeta(-k) \in \mathbb{Q}$ and $\zeta(-2k) = 0$ for all positive integer k.

The standard justification to make sense of values of $\zeta(s)$ for s to the left of $\mathrm{Re}(s) = 1$ is that $\zeta(s)$ 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 which relates $\zeta(s)$ to $\zeta(1-s)$:

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

where $\Gamma(s) = \int_0^\infty e^{-x}x^s\frac{dx}{x}$ is the Gamma function with $\Gamma(n+1) = n!$ for every positive integer n. In particular the values of $\zeta(s)$ at odd negative integers are related to the values at even positive integers.

Some 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. For historical reasons they are also called L-functions because that was the notation used by Dirichlet. 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 $\chi(n_1n_2) = \chi(n_1n_2)$. For instance when $N = 4$, there exists exactly one non-trivial Dirichlet character ϵ_4: $\epsilon_4(1 \pmod 4) = 1$, $\epsilon_4(3 \pmod 4) = -1$. The Dirichlet L-function attached to a Dirichlet character χ modulo N is defined by

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

where we set $\chi(n) = 0$ if n is not prime to N. Just like the Riemann zeta function, the Dirichlet L-functions 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

- $L(1,\epsilon_4) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots = \frac{\pi}{4}$
- $L(3,\epsilon_4) = 1 - \frac{1}{3^3} + \frac{1}{5^3} - \frac{1}{7^3} + \frac{1}{9^3} - \frac{1}{11^3} + \cdots = \frac{\pi^3}{32}$

Magical properties of zeta. Although it is not easy to define what number theory is, there is a sort of "litmus test": number theorists got excited by zeta and L-functions. Many arithmetic properties are encoded in the zeta and L-functions like magic. We illustrate some of them.

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 $\operatorname{Re}(s) = 1$.

Arithmetic properties of special zeta values.

I. We have seen examples that the "essential part" of certain special zeta and L-values are rational number. For instance, the value of the Riemann zeta function at negative integers are rational numbers, while their value at *even* positive integers are rational numbers times suitable powers of π. (These powers of π are the transcendental part of the special value which come from "periods".)

II. The special values often have unexpected ("deep") arithmetic meaning. 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 we saw 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 $\chi(-1) = -1$.

III. The special zeta values have nice p-adic properties. An example is the classical Kummer congruence. Let p be an odd prime number.

(a) For every negative (or non-positive) integer m such that $m \not\equiv 1 \pmod{p-1}$, 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.

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

IV. L-functions are closely related to modular forms. Sometimes special values appear as (the main part of) Fourier coefficients of modular forms; this connection is especially fruitful for investigating p-adic properties of special L-values. Another connection is best viewed through the Langlands program which merges

GRH. Finally we mention one of the great challenges in number theory, the *Riemann Hypothesis*, which asserts that all non-trivial zeroes of $\zeta(s)$ (i.e. those with $0 < \operatorname{Re}(s) < 1$) have $\operatorname{Re}(s) = \frac{1}{2}$. This statement is equivalent to a statement about the error term for the distribution of prime numbers.[6] The *Grand Riemann Hypothesis* is a similar statement for more general zeta and L-functions.

[6] The main term $\log x/x$ is given by the prime number theorem.

§4. Modular forms

Modular forms are very special functions on the upper half plane. They are tightly related to zeta and L-functions one the one hand, and to interesting arithmetic properties on the other hand, especially to elliptic curves. We will only scratch the surface to wrap up this talk and illustrate a key point just mentioned, that modular forms are closely related to Diophantine equations, especially when one studies statical properties. Modular forms occur in many other problems in mathematics as well; we refer the interested readers to [4].

Definition. Let N be a positive integers, and k be either a positive integer or a positive half-integer. A *modular form of weight k and level N* is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ on the upper half plane $\mathbb{H}$ satisfying the following properties.

- For any $\tau \in \mathbb{H}$ and any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_N \subset \mathrm{SL}_2(\mathbb{Z})$ we have
$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k\, f(\tau)\,.$$
- $f(\tau)$ is *holomorphic at infinity.*

Here Γ_N consists of all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $a \equiv d \equiv 1 \pmod N$ and $b \equiv c \equiv 0 \pmod N$. The precise definition of *holomorphic at infinity* is a bit long; we refer the reader to [6]. A modular form $f(\tau)$ as above has a Fourier expansion

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

often called the *q-expansion* of $f(\tau)$, where $q^{n/N} = e^{\frac{2\pi\sqrt{-1}n}{N}}$.

Examples.

- For every positive integer k, let
$$G_{2k}(\tau) = \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(m\tau+n)^{2k}}\,.$$
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 very small number.

- $\Delta = g_2^3 - 27g_3^2$ 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

  $$(2\pi)^{-12}\Delta(\tau) = q\prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n\,,$$

  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 $|\tau(p)| \le 2p^{11/2}$ 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.

- $\theta(\tau) = \sum_{m\in\mathbb{Z}} e^{\pi\sqrt{-1}m^2\tau}$, 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.

- Elliptic curves over $\mathbb{Q}$ provide another source for modular forms. Let E be an elliptic curve over $\mathbb{Q}$. Let $L_E(s)$ be the Dirichlet series

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

  where the integers a_p are determined by[7]

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

[7] Strictly speaking, the formula below is correct only when the elliptic curve E has good reduction at 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 following the same train of ideas.

- Let E be an elliptic curve over $\mathbb{Q}$ as above. Hasse showed that $a_p \leq 2\sqrt{p}$ for each 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.

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

  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.

References

[1] J. Conway & R. Guy. *The Book of Numbers.* Springer-Verlag, 1996.

[2] K. Kato, N. Kurosawa & T. Saito. *Number Theory 1. Fermat's Dream.* Amer. Math. Soc., 2000.

[3] D. Mumford. *Tata Lecture on Theta I.* Birkhäuser, 1983.

[4] P. Sarnak. *Some Applications of Modular Forms.* Cambridge Univ. Press, 1990.

[5] J.-P. Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

[6] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton Univ. Press, 1971.

[7] C. L. Siegel. *Topics in Complex Function Theory.* John Wiley and Sons, 1969.

[8] A. Weil. Two lectures on number theory, past and present. *Enseign. Math.* **20** (1974), 87–110. Œvres Scientifiques, vol. III, 279–310.

[9] A. Weil. *Number Theory. An approach through history from Hammurapi to Legendre.* Birhäuser, 1984.