Moonshine and the BSD conjecture

These are notes prepared for a talk in the Student Mathematics Colloquium at Columbia, Fall 2018. We explain the monstrous moonshine, and recent new moonshine for O'Nan group and its connection with the BSD conjecture due to Duncan—Mertens—Ono. Our main references are [1],[2],[3], [4], [5] and [6].

Elliptic curves and modular functions

An elliptic curve E over $\mathbb{Q}$ is a smooth cubic curve of the form $E: y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Q}$. The change of variable $x = u^2 x'$, $y \mapsto u^3 y'$ preserves the form of the equation and gives an elliptic curve

$$E': y^2 = x^3 + A'x + B', \quad u^4 A' = A, u^6 B' = B.$$

Then E and E' are isomorphic over the field $\mathbb{Q}(u^2, u^3) = \mathbb{Q}(u)$.

Definition 1 Define the *discriminant* of E to be

$$\Delta(E) = -16(4A^3 + 27B) = (-4A)^3 - 27(4B)^2.$$

Then E is smooth if and only if $\Delta(E) \neq 0$.

Definition 2 Define the j*-invariant* of E to be

$$j(E) = 1728 \cdot \frac{(-4A)^3}{\Delta(E)} = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2}.$$

Then we see that $j(E) = j(E')$. Conversely if $j(E) = j(E')$, then $A^3 B'^2 = A'^3 B^2$, and we may find some $u \in \mathbb{C}$ (actually $u \in \overline{\mathbb{Q}}$) satisfying the desired transformation.

In summary, we may classify elliptic curves over $\mathbb{Q}$ as follows.

Proposition 1

- The isomorphism class of elliptic curve E over $\mathbb{C}$ (or $\overline{\mathbb{Q}}$) is determined by $j(E)$.
- If $AB \neq 0$, then there is a unique elliptic curve $E^{(d)}: y^2 = x^3 + Ad^2 x + Bd^3$ over $\mathbb{Q}$ that is isomorphic to E over $\mathbb{Q}(\sqrt{d})$ but not over $\mathbb{Q}$. We call $E^{(d)}$ the d*-quadratic twist* of E.

There is also an analytic classification of elliptic curves over $\mathbb{C}$. Given any τ in the upper half plane $\mathcal{H} = \{\tau \in \mathbb{C} : \operatorname{im} \tau > 0\}$, we have the associated elliptic curve $E_\tau = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$. Then $E_\tau \cong E_{\tau'}$ if and only if τ, τ' lies in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit. Therefore the j-invariant induces a function $\tau \mapsto j(E_\tau)$ on the upper half plane that is invariant under $\mathrm{SL}_2(\mathbb{Z})$

$$j: \mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{H} \to \mathbb{C}.$$

This is a first example of a modular function (a function with a large group of symmetry given by the modular group $\mathrm{SL}_2(\mathbb{Z})$). Using the Weierstrass $\wp$-function one can write down the coefficients A, B as functions of τ, using Eisenstein series of weight 4 and 6,

$$-4A = \frac{4\pi^4}{3} E_4(\tau), \quad 4B = \frac{8\pi^6}{27} E_6(\tau),$$

where

$$E_4(\tau) = 1 + 240 \sum_{n \geq 1} \sum_{d|n} d^3 q^n, \quad E_6(\tau) = 1 - 504 \sum_{n \geq 1} \sum_{d|n} d^5 q^n, \quad q = e^{2\pi i \tau},$$

and $\Delta(E)$ as Ramanujan's cusp form of weight 12,

$$\Delta(\tau) = (-4A)^3 - 27(4B)^2 = (2\pi)^{12} q \prod_{n \geq 1} (1 - q^n)^{24}.$$

In this way we obtain a nice analytic expression of the j-invariant,

$$j(\tau) = \frac{1}{q} + \sum_{n \geq 0} c_n q^n = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

Links

Chao Li's Homepage

Columbia University

Math Department

Notice the appearance of -16 and 1728 in the definition of Δ and j normalizes their leading coefficients to be $(2\pi)^{12}$ and 1 respectively.

The j-invariant is an example of a *Hauptmodul* (principal modular function), as the modular curve $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \cong \mathbb{A}^1$, and the compactified modular curve $X(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^* \cong \mathbb{P}^1$ is of genus 0 with j a generator of its function field. More generally can can consider quotient by other arithmetic subgroups of $\mathrm{SL}_2(\mathbb{R})$ such as

$$\Gamma_0(p)=\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\in \mathrm{SL}_2(\mathbb{Z}) : p|c\},, \quad \Gamma_0(p)^+=\{\Gamma_0(p), \tfrac{1}{\sqrt{p}}\left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)\}=N_{\mathrm{SL}_2(\mathbb{R})}(\Gamma_0(p)).$$

Theorem 1 (Ogg, 1974) The modular curve $X_0(p) = \Gamma_0(p)\backslash\mathcal{H}^*$ has genus 0 exactly when

$$p = 2, 3, 5, 7, 13$$

(the missing prime $p = 11$ corresponds to the elliptic curve over $\mathbb{Q}$ with smallest conductor $E = X_0(11)$).

The curve $X_0^+(p) = \Gamma_0^+(p)\backslash\mathcal{H}^*$ has genus 0 exactly for the following 15 primes

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71$$

(the missing primes $p = 37, 43, 53, 61, 67$ all correspond to elliptic curves).

Remark 1 Ogg also showed these are exactly the 15 primes p such that all supersingular elliptic curves are defined over $\mathbb{F}_p$ (rather than over $\mathbb{F}_{p^2}$), by looking at the geometry of $X_0(p)$ modulo p and the action of the Atkin—Lehner involution $\left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)$.

Example 1 The Hauptmodul for $X_0(2)$ is given by

$$j_2(\tau) := \frac{\Delta(\tau)}{\Delta(2\tau)} = \frac{1}{q} - 24 + 276q - 2048q^2 + 11202q^3 - 49152q^4 \cdots$$

Monstrous Moonshine

The origin of the mathematical terminology *moonshine* here is the figurative use of the word as foolish talks or ideas (dates back to 15th century: "moonshine in water"), rather than its later use as smuggled alcohol (in 18th century). The "foolish" connection starts with the completely different story of the classification of finite simple groups. Now we know that a finite simple group belongs to one of:

- $\mathbb{Z}/p$,
- A_n,
- 16 infinite families of finite groups of Lie type (such as $\mathrm{PSL}_n(\mathbb{F}_q)$),
- 26 sporadic groups.

The largest sporadic group is known as the *monster group* $\mathbb{M}$, due to its monstrous size and complexity. It has order

$$|\mathbb{M}| = 808017424794512875886459904961710757005754368000000000 \sim 8 \times 10^{53},$$

and has 194 conjugacy classes. The existence of $\mathbb{M}$ was first predicted by Fischer and Griess in 1973, and Griess gave a quite complicated construction in 1980, as the group of linear transformations on a huge vector space (of dimension 196883!) that preserve a certain commutative but nonassociative bilinear product, now known as the Griess product. A total of 20 sporadic groups appear as subquotients of $\mathbb{M}$, known as the *happy family*, and the remaining 6 sporadic group are known as *pariah* (low class of southern India) groups, including the Lyons group, Janko groups J_1, J_3, J_4, Rudvalis group, and O'Nan group.

The first surprise comes from Ogg's observation that

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

The prime factors are exactly those p such that $X_0^+(p)$ with a Hauptmodul! A "moonshine" idea as it may appear to be simply a coincidence of small numbers.

The second surprise comes from the character table of $\mathbb{M}$. Even before the rigorous construction of $\mathbb{M}$, Fischer—Livingstone—Thorne computed the character table of $\mathbb{M}$ in 1978 assuming its existence. The dimension of the representation are quite large, here is the character values of the conjugacy class 1A (trivial) and 2B (order 2) of the first four representations, copied from the ATLAS of finite groups:

χ	1A	2B
χ_1	1	1
χ_2	196883	275
χ_3	21296876	-2324
χ_4	842609326	12974

Now observe the remarkable coincidence (due to McKay and Thompson):

$$196884=196883+1,\quad 276=275+1,$$
$$21493760=21296876+196883+1,\quad -2048=-2324+275+1,$$
$$864299970=842609326+21296876+2\times196883+2\times1,\quad 11202=12974-2324+2\times275+2\times1.$$

In other words, the first four coefficients in $j(\tau)$ and $j_2(\tau)$ exactly matches the character values of the representation χ_1, $\chi_2+\chi_1$, $\chi_3+\chi_2+\chi_1$, $\chi_4+\chi_3+2\chi_2+2\chi_1$ on the conjugacy 1A and 2B respectively, which can no longer be the law of small numbers! This leads to the following *monstrous moonshine conjecture* due to Thompson and Conway—Norton.

Conjecture 1 (Monstrous Moonshine, 1988) There is a naturally defined graded infinite-dimensional module (the *moonshine module*) $V=\bigoplus V_n$ such that for any $g\in\mathbb{M}$ the Mckay—Thompson series

$$T_g(\tau):=\sum_{n\geq -1}\operatorname{tr}(g|V_n)q^n$$

is a Hauptmodul for a discrete subgroup $\Gamma_g\subseteq \mathrm{SL}_2(\mathbb{Z})$ of genus 0.

In fact Conway—Norton gave an explicit recipe for the subgroup Γ_g, which lies between $\Gamma_0(N)$ and its normalizer for some N. Thus the monstrous moonshine provides a natural explanation of Ogg's observation on the order of $\mathbb{M}$.

Example 2 $\Gamma_1=\mathrm{SL}_2(\mathbb{Z})$, $\Gamma_g=\Gamma_0(2)$ for $g\in 2\mathrm{B}$ as suggested by the data above. We have $\Gamma_g=\Gamma_0(2)^+$ for $g\in 2\mathrm{A}$ and the Hauptmodul corresponding to 2A is given by

$$j_2^+=\frac{\Delta(\tau)}{\Delta(2\tau)}+2^{12}\frac{\Delta(2\tau)}{\Delta(\tau)}=\frac{1}{q}-24+4372q+96256q^2+1240002q^3+\cdots.$$

The moonshine module V was constructed by Frenkel—Lepowsky—Meurman in 1983 which has a rich structure of a *vertex operator algebra* (whose automorphism group being $\mathbb{M}$), and they verified the conjecture for $g=1$. The full monstrous moonshine conjecture was later proved by Borcherds.

Theorem 2 (Borcherds, 1992) The Monstrous Moonshine conjecture holds.

Remark 2 Borcherds' proof uses his notion of generalized Kac—Moody algebra (built up from $\mathfrak{sl}_2$ and 3-dimensional Heisenberg algebras), and the construction of the monster Lie algebra from the moonshine module. The key is to prove certain recursive relations of the McKay—Thompson series for $\{T_{g^k}\}$ and reduce the conjecture to a small finite number of identities (the first 7 terms) checkable by hand. The recursive relation finally boils down to the denominator identity for the monster Lie algebra (generalizing the classical Weyl denominator formula for Lie algebras).

O'Nan moonshine

Much work has since been done on the moonshine for other groups in the happy family, which relates the character values of a sporadic group to Hauptmodul of genus 0. For example the Hauptmodul j_2^+ gives the dimension of the irreducible representations of the baby monster group $\mathbb{B}$ (the second largest sporadic). However, there has been no interesting genus 0 moonshine for the remaining six pariah groups. Recently, progress has been made by Duncan—Mertens—Ono on one of the pariah groups, the O'Nan group ON. It has size

$$|\mathrm{ON}|=460815505920=2^9\cdot 3^4\cdot 5\cdot 7^3\cdot 11\cdot 19\cdot 31,$$

and has 30 conjugacy classes. This new O'Nan moonshine has a different flavor: the McKay—Thompson series involve weight 3/2 modular forms, rather than Hauptmoduls (weight 0 modular forms).

Theorem 3 (Duncan—Mertens—Ono, 2017) There is an infinite-dimensional (virtual) graded ON-module $W=\bigoplus_{n>0}W_n$, where $n\equiv 0,3 \pmod 4$, such that for each $g\in\mathrm{ON}$, the McKay—Thompson series

$$F_g(\tau):=-q^{-4}+2+\sum_{n>0}\operatorname{tr}(g|W_n)q^n$$

is a weakly holomorphic modular form of weight 3/2 on $\Gamma_0(4N)$, where N is the order of g.

Example 3 We have

$$F_1(\tau) = -q^{-4} + 2 + 26752q^3 + 143376q^4 + 8288256q^7 + \cdots$$

a generating series of traces of singular of moduli which dates back to Zagier (2002), where

$$26752 = \dim \chi_7, 143376 = 1 + 58311 + 85064 = \dim \chi_1 + \dim \chi_{12} + \dim \chi_{18}, \ldots$$

Remark 3 The proof uses Rademacher sums (low weight analogues of Poincare series) to construct mock modular forms with explicit Fourier expansions (coefficients involve Kloosterman sums). *Mock modular forms* are holomorphic but does not quite satisfy modularity, nevertheless it can be completed to to *harmonic Maass forms*, which are no longer holomorphic but satisfy modularity. One then take certain linear combination of (the Kohnen +space projection of) these explicit harmonic Maass forms and obtain weakly holomorphic modular forms F_g. To relate it to O'Nan, one checks the first few coefficients of these explicit modular forms agree with the desired traces and deduce the rest using the Schur orthogonal relations for characters and certain congruence relations built into the construction of F_g. A natural interesting question is whether one can find more intrinsic definition of the moonshine module W independent of the explicit constructions of F_g (e.g., using vertex operator algebras).

A new feature in the O'Nan moonshine is that the modular forms are of weight 3/2, which encodes even richer arithmetic. It leads to an intriguing relation with the BSD conjecture which we now briefly describe.

Connection with BSD

Come back to the elliptic curve $E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$ (or in Weierstrass form $y^2 = x^3 - 13392x - 1080432$). It has an associated weight 2modular form

$$\begin{aligned} f(\tau) &= \sum_{n\geq 1} a_n q^n = q\prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + \cdots \end{aligned}$$

such that the coefficient $a_p = p + 1 - |E(\mathbb{F}_p)|$ encodes the number of solution of E mod p (when $p \neq 11$).

More generally, the modularity theorem associates a weight 2 modular form $\sum a_n q^n$ to any elliptic curve E over $\mathbb{Q}$. Analogous to the Riemann zeta function, we define the L-function of E to be

$$L(E,s) = \sum_{n\geq 1} \frac{a_n}{n^s},$$

which has analytic continuation to all of $\mathbb{C}$ and satisfies a functional equation relating $L(E,s)$ and $L(E,2-s)$.

Conjecture 2 (Birch and Swinnerton-Dyer)

- (rank) $\operatorname{ord}_{s=1} L(E,s) = \operatorname{rank} E(\mathbb{Q})$.
- (BSD formula) Let $r = \operatorname{ord}_{s=1} L(E,s)$, then

$$\frac{L^{(r)}(E,1)}{r!\Omega(E)R(E)} = \frac{\prod_p c_p(E)\cdot|Ш(E)|}{|E(\mathbb{Q})_{\text{tor}}|^2}.$$

Example 4 For $E = X_0(11)$, $r = 0$ and the BSD formula holds:

$$\frac{0.253841860856\ldots}{1.26920930428\ldots\cdot 1} = \frac{5\cdot 1}{5^2}.$$

The rank part is known when $\operatorname{ord}_{s=1} L(E,s) \leq 1$ due to Gross—Zagier and Kolyvagin in 1980's. Regarding the BSD formula, here is a more recent theorem.

Theorem 4 (2018) For elliptic curves E satisfying some assumptions, there are infinitely many quadratic twists $E^{(d)}$ of rank 0 such that the BSD formula holds for $E^{(d)}$.

Remark 4 The proof is the accumulation of the works of Kato, Skinner—Urban, Skinner, Kobayashi, Wan, Sprung, Zhai, Cai—L.—Zhai...

However, the truth for of BSD formula for all twists is still not known, even for $E = X_0(11)$ (the problem comes from the 11-part and 2-part of the BSD formula).

Theorem 5 (Duncan—Mertens—Ono) Let $E = X_0(11)$. Let $d < -4$ be a fundamental discriminant that is not a square mod 11. Assume (the 11-part of) the BSD formula holds for $E^{(d)}$. Then the followings are equivalent:

- $\operatorname{rank} E^{(d)}(\mathbb{Q}) \geq 2$ or $Ш(E^{(d)})[11] \neq 0$.

- $\dim W_{|d|} \equiv -24h(d) \pmod{11}$. Here $h(d)$ is the class number of $\mathbb{Q}(\sqrt{d})$.

Similar results hold for $E = X_0(19)$ and $p = 19$.

So the O'Nan group knows about solving cubic equations! Naturally one wonders if one can check the second condition in terms of the O'Nan group more intrinsically, which would imply important consequences on the arithmetic of $E^{(d)}$.

Remark 5 To make the connection with BSD less mysterious: a celebrated formula of Waldspurger relates the $|d|$-th coefficient of a weight 3/2 form associated to E to $L(E^{(d)}, 1)$, and a celebrated theorem of Zagier shows that the generating series of (Hurwitz) class numbers and more generally generating series of traces of singular moduli are (mock) modular forms of weight 3/2. The theorem then follows by writing F_g (g of order 11) as an explicit linear combination of weight 3/2 modular forms of Waldspurger's type and Zagier's type and using the congruence between F_1 and F_g mod 11.

References

[1] Conway, J. H. and Norton, S. P., *Monstrous moonshine,* Bull. London Math. Soc. **11** (1979), no.3, 308--339.

[2] Borcherds, Richard E., *Introduction to the Monster Lie algebra,* Groups, combinatorics \& geometry (Durham, 1990), London Math. Soc. Lecture Note Ser., **165** Cambridge Univ. Press, Cambridge, 1992, 99--107.

[3] Borcherds, Richard E., *What is Moonshine?,* Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998), 1998, 607--615.

[4] Gannon, Terry, *Monstrous moonshine: the first twenty-five years,* Bull. London Math. Soc. **38** (2006), no.1, 1--33.

[5] Duncan, John FR and Mertens, Michael H and Ono, Ken, *Pariah moonshine,* Nature communications **8** (2017), no.1, 670.

[6] Duncan, John F.~R. and Mertens, Michael H. and Ono, Ken, *O'Nan moonshine and arithmetic,* arXiv e-prints (2017), arXiv:1702.03516.