On the equation $x^2 + dy^6 = z^p$

Primeiro Encontro Portugûes de Teoria dos Números

Franco Golfieri

November 2, 2022

Universidade de Aveiro

Fermat's equation

Fermat's Last Theorem

The equation $x^n + y^n = z^n$ does not have primitive non-trivial solutions for $n \geq 3$.

- The cases $n = 3, 4$ were done by Euler and Fermat respectively.
- It is enough to prove it for primes $p \geq 5$ and for primitive solutions, i.e. solutions (a, b, c) with $\gcd(a, b, c) = 1$.

(a, b, c) non-trivial primitive solution to $x^p + y^p = z^p$ for $p \geq 5$

$$\Downarrow$$

$$E_{a,b} : y^2 = x(x - a^p)(x + b^p)$$

$$\Downarrow$$

This curve cannot exist

Elliptic Curves

$$E_{a,b} : y^2 = x(x - a^p)(x + b^p)$$

In general:

$$E : y^2 = f(x) := x^3 + ax^2 + bx + c$$
$$\Delta(E) := 2^4 \cdot \mathsf{disc}(f) = 2^4 \cdot \prod_{i<j} (x_i - x_j)^2.$$

Theorem

(Mordell) $E(\mathbb{Q})$ has a structure of finitely generated abelian group.

If p is an odd prime, then

$$E_p := y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c}.$$

It is an elliptic curve over $\mathbb{F}_p$ if and only if $p \nmid \Delta(E)$.

$$N(E) = \prod_{p|\Delta_E} p^{f_p}.$$

Elliptic Curves

We define the a_p coefficient of E by $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$.

$$E[n] = \{P \in E(\bar{\mathbb{Q}}) : [n]P = \mathcal{O}\}.$$

- $\mathsf{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. Then it defines a continuous representation

$$\bar{\rho}_{E,n} : \mathsf{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

- Also, $\mathsf{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathsf{Ta}_\ell(E) = \varprojlim_n \{E[\ell^n]\}$. Then it defines a continuous representation

$$\rho_{E,n} : \mathsf{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell).$$

When $p \nmid \ell N$, then

$$a_p(E) = \mathsf{Tr}(\bar{\rho}_{E,\ell}(\mathsf{Frob}_\mathfrak{p})).$$

for $\mathfrak{p} \subset \overline{\mathbb{Z}}$ a prime ideal over p.

Modular Forms

We define the Hecke subgroup of level N as

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \text{ mod } \mathrm{N} \right\}$$

Let denote $\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$.

A function $f : \mathcal{H} \to \mathbb{C}$ is said to be a **weight 2 modular form of level N** if the following conditions are satisfied:

- f is holomorphic on $\mathcal{H}$,
- $f(\gamma\tau) = (c\tau + d)^2 f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and $\tau \in \mathcal{H}$,
- f is holomorphic at the cusps.

$$(c\tau + d)^{-2} f(\beta\tau) = \sum_{n=-\infty}^{\infty} c_n^{(\beta)} q_N^n \quad \text{with} \quad q_N = e^{\frac{2\pi i z}{N}}.$$

The last conditions means that $c_n^{\beta} = 0$ for all $n < 0$, for the cusps $\beta(\infty)$.

Modular Forms

- We say that a modular form is **cuspidal** if $c_0^\beta = 0$ for the cusps. We denote the space of weight 2 cuspidal forms of level N by $S_2(\Gamma_0(N))$.
- If $f \in S_2(\Gamma_0(N))$ then

$$f(z) = \sum_{n=1}^{\infty} a_n(f) q_N^n \quad \text{with} \quad q_N = e^{\frac{2\pi i z}{N}}.$$

- If $M|N$ then $\Gamma_0(N) \subset \Gamma_0(M)$. A cuspidal form is **new** if it does not come from lower levels.

We say that an elliptic curve E is **modular** if there exists a cuspidal newform $f \in S_2(\Gamma_0(N_E)))$ such that $a_p(E) = a_p(f)$ for all prime p.

Theorem (Wiles, Taylor-Wiles)

The semiestable rational elliptic curves are modular

The curve $E_{a,b}$ is one of these curves, and hence we have a cuspidal form $f_{a,b} \in S_2(\Gamma_0(N_{a,b}))$.

Conclusion

$$\Delta(E_{a,b}) = 16(abc)^{2p}.$$
$$N(E_{a,b}) = \prod_{q|abc} q.$$

Obstacle: $N(E_{a,b})$ depends on a and b so we cannot study specifically the space $S_2(\Gamma_0(N_{a,b}))$.

Theorem (Mazur-Ribet)

There exists a cuspidal form $f \in S_2(\Gamma_0(2))$ such that

$$a_\ell(E_{a,b}) \equiv a_\ell(f) \text{ (mód } p), \text{ for all } \ell \neq 2, p.$$

However, $S_2(\Gamma_0(2)) = \{0\}$, so we get a contradiction.

Generalised Fermat's equations

$$Ax^p + By^q = Cz^r \tag{1}$$

Darmon & Granville (1986): If

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1,$$

then equation (1) has finitely many primitive non-trivial solutions.

ABC conjecture: The equation (1) has finetely many solutions even if we allow the parameters to vary. In particular, if we fix A, B, C, p, q and vary r.

Expected result: Prove the non-existance of primitive solutions (a, b, c) to the equation:

$$x^2 + dy^6 = z^p$$

for p greater enough. It was first studied by Benntet and Chen for $d = 1$, by Koutsianas for $d = 3$ and later by Pacetti and Villagra for $d = 2$ and 6.

Modularity Method

1. Construction of the curve From a putative solution (a, b, c) we construct a curve $E_{(a,b,c)}$ such that $\Delta(E_{(a,b,c)}) = c \cdot D^p$, where c depends on the equation and D on the solution. Furthermore, we want that the primes p that divide D are of multiplicative reduction.
2. Modularity of the curve: To relate to our curve a cuspidal form of level the same as the conductor of the curve.
3. Lower the level: To determine a cuspidal form of a lower level that does not deppend on the solution
4. Discard the possible modular forms to arrive to a contradiction.

General strategy

1. Construction of the curve: To a putative non-trivial primitive solution (a, b, c) of $x^2 + dy^6 = z^p$ we associate the following curve defined over $K := \mathbb{Q}(\sqrt{-d})$

$$E_{a,b}/K : y^2 + 6b\sqrt{-d}xy - 4d(a + b^3\sqrt{-d})y = x^3,$$

$$\Delta(E_{(a,b)}) = -2^8 3^3 d^4 c^p (a + b^3\sqrt{-d})^2.$$

   If $\mathfrak{q}|q$ is a prime ideal in $\mathcal{O}_K$ such that $q \nmid 6d$, then $E_{(a,b)}$ has multiplicative reduction at $\mathfrak{q}$ and $p|v_{\mathfrak{q}}(\Delta(E_{(a,b)}))$.

2. Modularity of the curve: $E_{(a,b)}$ turns out to be a $\mathbb{Q}$-curve defined over $\mathbb{Q}(\sqrt{-d}, \sqrt{-2})$. Then by a result of Ribet, there exists a character χ such that $\rho_{E,p} \otimes \chi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Q}_p)$ extends to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and hence it is modular.

General strategy

Pacetti and Villagra construted a character χ unramified outside 2 such that $\rho_{E,p} \otimes \chi$ extends to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then there exists a cuspidal form $g \in S_2(\Gamma_0(N_{d,a,b}), \varepsilon)$ such that $\rho_{E_{a,b},p} \equiv \rho_{g,K,p} \otimes \chi^{-1} \pmod{p}$.

3. Lower the level: There exists a bound N_d such that if $p > N_d$ then $\rho_{E,p}$ has absolutely irreducible residual image. Then applying Ribet lowering the level result, there exists $g \in S_2(n_d, \varepsilon)$ with $n_d | N_{d,a,b}$ such that $f \equiv g \pmod{p}$.
4. Discard the possible modular forms: We need to discard the forms in $S_2(n_d, \varepsilon)$
   - Mazur's trick
   - Symplectic Method

Mazur's Trick

Let $g \in S_2(\Gamma_0(n_d), \varepsilon)$ and $\ell \neq p$ such that ℓ does not ramify in $K = \mathbb{Q}(\sqrt{-d})$. Let $\mathfrak{l}|\ell$ and

$$B(\ell, g) = \begin{cases} \mathcal{N}\left(a_\ell(E_{(a,b)})\chi(\ell) - a_\ell(g)\right) & \text{if } \ell \nmid c \text{ and } \ell \text{ splits in } K, \\ \mathcal{N}\left(a_\ell(g) - a_\ell(E_{(a,b)})\chi(\ell) - 2\ell\varepsilon(\ell)\right) & \text{if } \ell \nmid c \text{ and } \ell \text{ is inert } K, \\ \mathcal{N}\left(\varepsilon^{-1}(\ell)(\ell+1)^2 - a_\ell(g)^2\right) & \text{if } \ell | c. \end{cases}$$

Then $p|B(\ell, g)$. Therefore if

$$p > \gcd_{(a,b)\in\mathbb{F}_\ell^2} B(\ell, g)$$

we can discard g.

Obstacles:

- It might happen that $B(\ell, g) = 0$.
- If N is big ($N > 10^6$), then it is inefficient to calculate $a_\ell(g)$.

$x^2 + 13y^6 = z^p$

In the case $d = 13$, we arrive, after lowering the level, that the spaces to analyze are

$$S_2(\Gamma_0(2^4 \cdot 3 \cdot 13^2, \varepsilon) \text{ and } S_2(\Gamma_0(2^4 \cdot 3^3 \cdot 13^2, \varepsilon).$$

- The space $S_2(\Gamma_0(2^4 \cdot 3 \cdot 13^2, \varepsilon)$ has 29 conjugacy classes of newforms, 7 of them with complex multiplication. For $p > 1527$ we can discard the CM modular forms. To discard the non-CM modular forms we apply the Mazur's trick and we can discard them for $p > 13$.

```
DiscardPlace(13,eps,Chi,new,1,5,40);
Cannot discard the form with parameter: 1
{ 0 }

DiscardPlace(13,eps,Chi,new,6,5,40);
{ 2, 13 }
```

$x^2 + 13y^6 = z^p$

- The space $S_2(\Gamma_0(2^4 \cdot 3^3 \cdot 13^2, \varepsilon)$ has 68 conjugacy classes of newforms, 14 of them with complex multiplication. For $p > 1527$ we can discard the CM modular forms. To discard the non-CM modular forms we apply the Mazur's trick and we can discard them for $p > 29$.

Theorem

Let $p > 1627$ be a prime number. Then there are no non-trivial primitive solutions of the equation

$$x^2 + 13y^6 = z^p$$

Symplectic Method

Let p be prime, $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ such that $E[p] \cong E'[p]$ (as Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-modules) and $\phi : E[p] \to E'[p]$ an isomorphism. Then there exists $d(\phi) \in \mathbb{F}_p^\times$ such that:

$$e_{E',p}(\phi(P), \phi(Q)) = e_{E,p}(P, Q)^{d(\phi)} \quad \text{for all } P, Q \in E[p]$$

We say that ϕ is a **symplectic isomorphism** if $\left(\frac{d(\phi)}{p}\right) = 1$ and an **anti-symplectic isomorphism** if $\left(\frac{d(\phi)}{p}\right) = -1$.
We say that (E, E', p) is of **symplectic type** or **anti-symplectic type** if all the Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-modules isomorphisms between $E[p]$ and $E'[p]$ are symplectic or antisymplectic isomorphism respectively.

Symplectic Method

Given a triple (E, E', p), How can we determine its symplectic type?

Theorem

(Krauss-Freitas) Let $\ell \neq p$ be primes with $p \geq 3$. Let E and E' be elliptic curves over $\mathbb{Q}_\ell$ with multiplicative reduction. Suppose that $E[p] \simeq E'[p]$ as Gal$(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$-modules. Assume further that $p \nmid v_\ell(\Delta(E))$. Then $p \nmid v_\ell(\Delta(E'))$. Furthermore, $E[p]$ and $E'[p]$ are symplectic isomorphic $\Leftrightarrow \left(\frac{v_\ell(\Delta(E))/v_\ell(\Delta(E'))}{p}\right) = 1$.
Moreover, $E[p]$ and $E'[p]$ are not both symplectically and anti-symplectically isomorphic.

Case $d = 11$

$$x^2 + 11y^6 = z^p$$

We need to discard the spaces $S_2(\Gamma_0(2^2 \cdot 3^2 \cdot 11^2))$ and $S_2(\Gamma_0(2^2 \cdot 3^3 \cdot 11^2))$.

- For the space $S_2(\Gamma_0(2^2 \cdot 3^3 \cdot 11^2))$, which correspond to solutions (a, b, c) such that $3|ab$, we are able to discard all modular forms using Mazur's Trick.
- For the space $S_2(\Gamma_0(2^2 \cdot 3^2 \cdot 11^2))$ we are able to discard all modular forms using Mazur's Trick but f_{15} and f_{20}. The last one we are able to discard it using a ramification argument.

$$f_{15} \rightsquigarrow A_{f_{15}} = E_{15} \times E_{15}$$

where $E_{15}/\mathbb{Q}(\sqrt{-11})$ is given by:

$$E_{15} : y^2 = x^3 + \frac{1+\sqrt{-11}}{2}x^2 + \frac{1907\sqrt{-11}-1615}{2}x - 19479\sqrt{-11} - 31012$$

This curve has discriminant $\Delta(E_{15}) = 3^9 \cdot (\sqrt{-11})^8 \cdot 2^{20}$.

Remark

Assuming that f_{15} is the modular form associated it to $E_{a,b}$, we obtain that $E_{A,B}[p] \cong E_{15}[p]$, as Gal$(\overline{K}/K)$-modules.

Discarding f_{15}

- We apply the symplectic theorem with $\ell = 11$, $\mathfrak{p}_{11} = (\sqrt{-11})$, $K = \mathbb{Q}(\sqrt{-11})_{\mathfrak{p}_{11}}$, to the curves $E_{A,B}$ and we obtain that they are symplectically isomorphic since $v_{\mathfrak{p}_{11}}(\Delta_{E_{A,B}}) = v_{\mathfrak{p}_{11}}(\Delta_{E_{15}}) = 8$.
- We look now at $\ell = 3$, $\mathfrak{p}_3 = <\frac{1-\sqrt{-11}}{2}>$ and $K = \mathbb{Q}(\sqrt{-11})_{\mathfrak{p}_3}$. Note that $\mathbb{Q}(\sqrt{-11})_{\mathfrak{p}_3} \cong \mathbb{Q}_3$, then we can use the rational version of the symplectic theorem. Then, since $v_{\mathfrak{p}_3}(\Delta_{E_{A,B}}) = 3p - 9$ and $v_{\mathfrak{p}_3}(\Delta_{E_{15}}) = 9$, we obtain that they are symplectically isomorphic if and only if $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$

Conclusion

Theorem

The equation $x^2 + 11y^6 = z^p$ has no non-trivial primitive solution if $p > 409$ and either one of the following conditions is satisfied:

- Either x or y is divisible by 3,
- The prime $p \equiv 3 \pmod{4}$.

Case $d = 2$

Theorem

(Pacetti - Villagra) Let $p > 257$ be a prime number. Then there are no non-trivial primitive solutions of the equation

$$x^2 + 2y^6 = z^p.$$

Question: Can we lower this bound?

In order to use Ribet's lowering the level result we need to prove that $\bar{\rho}_{E,p}$ is irreducible.

Proposition

$\bar{\rho}_{E,p}$ is irreducible for $p \geq 5$.

Then using the Ribet's theorem we need to analyze the spaces $S_2(\Gamma_0(2^8 \cdot 3^2))$ and $S_2(\Gamma_0(2^8 \cdot 3^3))$. Using Mazur's trick we are able to discard all non-CM forms for $p > 3$.

Case $d = 2$

Question: How can we eliminate the CM-forms?

If $f \in S_2(\Gamma_0(2^8 \cdot 3^2))$ is a CM-form, then f comes from the trivial solution, i.e. $A_f \cong E_{(\pm 1,0,1)}$, which is a curve that has CM by $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

$$\mathbb{P}\mathrm{Im}(\rho_{E_\pm,p}) \subset \text{Normalizer of a Cartan Subgroup}$$

- If $p \equiv 1 \pmod 3$,
  $\mathrm{Im}(\rho_{E_\pm,p}) \subset$ Normalizer of a split Cartan subgroup
- If $p \equiv 2 \pmod 3$,
  $\mathrm{Im}(\rho_{E_\pm,p}) \subset$ Normalizer of a non-split Cartan subgroup

Proposition

If $p \geq 5$ then the projective image of $\rho_{E_{(a,b)},p}$ is not contained in the normalizer of a split Cartan subgroup of $\mathbb{P}\,\mathrm{GL}_2(\mathbb{F}_p)$.

Case $d = 2$

Proposition

Let $p \geq 5$ be a prime and suppose there exist either

- a p-new form in $S_2(\Gamma_0(3p^2))$ with $w_p f = f$ and $w_3 f = -f$; or
- a p-newform in $S_2(\Gamma_0(p^2))$ with $w_p f = f$

such that $L(f \otimes \chi_{-8}, 1) \neq 0$, where χ_{-8} is the Dirichlet character associated to $\mathbb{Q}(\sqrt{-2})$. Then the mod p projective image of the Galois representation attached to a non-trivial solution of $A^2 + 2B^6 = C^p$ does not have image contained in the normalizer of a non-split Cartan Subgroup.

However, for $p = 5$ this does not work.

Thank you

References i

[1], [2], [3], [4], [5], [6]

M. A. Bennett and I. Chen.
Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$.
Algebra Number Theory, 6(4):707–730, 2012.

N. Freitas and A. Kraus.
On the symplectic type of isomorphims of the p-torsion of elliptic curves, 2016.

F. Golfieri, A. Pacetti, and L. V. Torcomian.
On the equation $x^2 + dy^6 = z^p$ for square-free $1 \leq d \leq 20$, 2021.

A. Koutsianas.
On the generalized fermat equation $a^2 + 3b^6 = c^n$.
Bulletin of the Hellenic Mathematical Society, 64:56–68, 2020.

References ii

A. Pacetti and L. Villagra Torcomian.
$\mathbb{Q}$-curves, hecke characters and some diophantine equations, 2020.

K. A. Ribet.
Abelian varieties over $\mathbb{Q}$ and modular forms.
In Modular curves and abelian varieties, volume 224 of Progr. Math., pages 241–261. Birkhäuser, Basel, 2004.