Superelliptic equations via Frey curves

Mike Bennett

11 July 2016

Hilbert's 7th problem

What kind of number is $2^{\sqrt{2}}$?

Hilbert's 7th problem

What kind of number is $2^{\sqrt{2}}$?

More generally, if α and β are algebraic, what kind of number is α^β?

Hilbert's 7th problem

What kind of number is $2^{\sqrt{2}}$?

More generally, if α and β are algebraic, what kind of number is α^{β}?

Let's suppose that $\beta \notin \mathbb{Q}$ and $\alpha \neq 0, 1$.

The Gel'fond-Schneider Theorem

Theorem (Gel'fond-Schneider, 1934)

Let α and β be algebraic numbers in $\mathbb{C}$ with $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$. Then α^β is transcendental.

The Gel'fond-Schneider Theorem

Theorem (Gel'fond-Schneider, 1934)

Let α *and* β *be algebraic numbers in* $\mathbb{C}$ *with* $\alpha \neq 0, 1$ *and* $\beta \notin \mathbb{Q}$. *Then* α^β *is transcendental.*

Here, $\alpha^\beta = e^{\beta \log \alpha}$ for any determination of the logarithm.

The Gel'fond-Schneider Theorem

Theorem (Gel'fond-Schneider, 1934)

Let α and β be algebraic numbers in $\mathbb{C}$ with $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$. Then α^β is transcendental.

Here, $\alpha^\beta = e^{\beta \log \alpha}$ for any determination of the logarithm.

Corollary

Let α, β be algebraic numbers in $\mathbb{C}$ different from $0, 1$ such that $\log \alpha$ and $\log \beta$ are linearly independent over $\mathbb{Q}$. Then for all non-zero algebraic numbers γ, δ, we have

$$\gamma \log \alpha + \delta \log \beta \neq 0.$$

Baker's Theorem

Theorem (Baker, 1966)

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ *be algebraic numbers from* $\mathbb{C}$*, different from* $0, 1$*, such that* $\log \alpha_1, \log \alpha_2, \ldots, \log \alpha_m$ *are linearly independent over* $\mathbb{Q}$*. Then for every tuple* $(\beta_0, \beta_1, \ldots, \beta_m)$*, different from* $(0, 0, \ldots, 0)$*, we have that*

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m \neq 0.$$

Linear forms in logarithms : a special case

Theorem (Baker, 1975)

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ *be algebraic numbers from* $\mathbb{C}$*, different from* $0, 1$*, and let* $b_1, \ldots, b_m$ *be rational integers such that*

$$b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m \neq 0.$$

Then we have

$$|b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m| \geq (eB)^{-C},$$

where $B = \max\{|b_1|, \ldots, |b_m|\}$ *and* C *is an effectively computable constant depending only upon* m*, and upon* $\alpha_1, \ldots, \alpha_m$*.*

Applications of linear forms in logarithms

Applications of linear forms in logarithms

1. Class number problems

Applications of linear forms in logarithms

1. Class number problems
2. Effective Shafarevic

Applications of linear forms in logarithms

1. Class number problems
2. Effective Shafarevic
3. Catalan's Conjecture $x^n - y^m = 1$

Applications of linear forms in logarithms

1. Class number problems
2. Effective Shafarevic
3. Catalan's Conjecture $x^n - y^m = 1$
4. Primitive divisors in recurrence sequences

Applications of linear forms in logarithms

1. Class number problems
2. Effective Shafarevic
3. Catalan's Conjecture $x^n - y^m = 1$
4. Primitive divisors in recurrence sequences
5. Finiteness theorems for binary forms

Applications of linear forms in logarithms

1. Class number problems
2. Effective Shafarevic
3. Catalan's Conjecture $x^n - y^m = 1$
4. Primitive divisors in recurrence sequences
5. Finiteness theorems for binary forms
6. and lots and lots of results about Diophantine equations!

Superelliptic equations

A classic result of Siegel, from 1929, is that the set of K-integral points on a smooth algebraic curve of positive genus, defined over a number field K, is finite. As an application of this to Diophantine equations, Leveque showed that if $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree $k \geq 2$ with, say, no repeated roots, and $l \geq \max\{2, 5-k\}$ is an integer, then the *superelliptic* equation

$$f(x) = y^l$$

has at most finitely many solutions in integers x and y.

Superelliptic equations

Already in a 1925 letter from Siegel to Mordell (partly published in 1926 under the pseudonym X, Siegel had proved precisely this result in case $l = 2$ (and had remarked that his argument readily extends to all exponents $l \geq 2$). Via lower bounds for linear forms in logarithms, Schinzel and Tijdeman deduced that, in fact, the equation

$$f(x) = y^l$$

has at most finitely many solutions in integers x, y and *variable* $l \geq \max\{2, 5-k\}$ (where we count the solutions with $y^l = \pm 1, 0$ only once). This latter result has the additional advantage over Leveque's theorem in that it is effective (the finite set of values for x is effectively computable).

An example : $x^2 - 2 = y^p$

Via lower bounds for linear forms in logarithms, we can prove that if we have a solution to $x^2 - 2 = y^p$ with $|y| > 1$, then $41 \leq p < 1237$.

An example : $x^2 - 2 = y^p$

Via lower bounds for linear forms in logarithms, we can prove that if we have a solution to $x^2 - 2 = y^p$ with $|y| > 1$, then $41 \leq p < 1237$.

We also have bounds upon x and y for the remaining values of p.

An example : $x^2 - 2 = y^p$

Via lower bounds for linear forms in logarithms, we can prove that if we have a solution to $x^2 - 2 = y^p$ with $|y| > 1$, then $41 \leq p < 1237$.

We also have bounds upon x and y for the remaining values of p.

Of the order of $e^{e^{10000}}$.

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \; : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad t = 2.$

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \ : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad t = 2.$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{rad}(y), \qquad N_p = 128.$$

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \ : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad\qquad t = 2.$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{rad}(y), \qquad N_p = 128.$$

By Ribet, $E_{(x,y)} \sim_p F$ where F is one of

$$F_1 = 128A1, \quad F_2 = 128B1, \quad F_3 = 128C1, \quad F_4 = 128D1.$$

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime.}$$

Frey curve: $\quad E_{(x,y)} \; : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad t = 2.$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{rad}(y), \qquad N_p = 128.$$

By Ribet, $E_{(x,y)} \sim_p F$ where F is one of

$$F_1 = 128A1, \quad F_2 = 128B1, \quad F_3 = 128C1, \quad F_4 = 128D1.$$

Exercise: Show that $B_\ell(F_i) = 0$ for all ℓ and $i = 1, 2, 3, 4$.

Bounding the Exponent $x^2 - 2 = y^p$?

$$x^2 - 2 = y^p, \qquad p \geq 5 \text{ prime}.$$

$$\text{Frey curve:} \qquad E_{(x,y)} \ : \quad Y^2 = X^3 + 2xX^2 + 2X, \qquad\qquad t = 2.$$

$$\Delta_{\min} = 2^8 y^p, \qquad N = 2^7 \operatorname{rad}(y), \qquad N_p = 128.$$

By Ribet, $E_{(x,y)} \sim_p F$ where F is one of

$$F_1 = 128A1, \quad F_2 = 128B1, \quad F_3 = 128C1, \quad F_4 = 128D1.$$

Exercise: Show that $B_\ell(F_i) = 0$ for all ℓ and $i = 1, 2, 3, 4$.
No bound on p from the modular method. Note $E_{(-1,-1)} = F_1$ and $E_{(1,-1)} = F_3$.

Bounding the Exponent

$$B_\ell(f) \neq 0 \Longrightarrow p \text{ is bounded.}$$

Bounding the Exponent

$$B_\ell(f) \neq 0 \Longrightarrow p \text{ is bounded.}$$

We are guaranteed to succeed in two cases:

(a) **If f is irrational**, then $c_\ell \notin \mathbb{Q}$ for infinitely many of the coefficients ℓ, and so $B_\ell(f) \neq 0$.

Bounding the Exponent

$$B_\ell(f) \neq 0 \implies p \text{ is bounded.}$$

We are guaranteed to succeed in two cases:

(a) **If f is irrational**, then $c_\ell \notin \mathbb{Q}$ for infinitely many of the coefficients ℓ, and so $B_\ell(f) \neq 0$.

(b) Suppose

- f is rational,
- t is prime or $t = 4$,
- every elliptic curve F in the isogeny class corresponding to f we have $t \nmid \#F(\mathbb{Q})_{\mathrm{tors}}$.

Then there are infinitely many primes ℓ such that $B_\ell(f) \neq 0$.

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Easy exercise: Show there are no solutions with y odd.

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Easy exercise: Show there are no solutions with y odd.

- Hint: just like $x^2 + 1 = y^p$.

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Easy exercise: Show there are no solutions with y odd.

- Hint: just like $x^2 + 1 = y^p$.
- Don't bother doing the exercise!

Method of Kraus

$$x^2 + 7 = y^m, \qquad m \geq 3.$$

Easy exercise: Show there are no solutions with y odd.

- Hint: just like $x^2 + 1 = y^p$.
- Don't bother doing the exercise!

Plenty of solutions with y even.

m	x	y	m	x	y	m	x	y
3	± 1	2	3	± 181	32	4	± 3	± 2
5	± 5	2	5	± 181	8	7	± 11	2
15	± 181	2						

The Method of Kraus

$$x^2 + 7 = y^p, \qquad p \geq 11.$$

The Method of Kraus

$$x^2 + 7 = y^p, \qquad p \geq 11.$$

WLOG

$$x \equiv 1 \pmod 4 \qquad \text{and} \qquad y \text{ is even.}$$

The Method of Kraus

$$x^2 + 7 = y^p, \qquad p \geq 11.$$

WLOG

$$x \equiv 1 \pmod 4 \qquad \text{and} \qquad y \text{ is even.}$$

$$E_x : \qquad Y^2 = X^3 + xX^2 + \frac{(x^2+7)}{4} X$$

$$\Delta = \frac{-7y^p}{2^{12}}, \qquad N = 14 \prod_{\ell \mid y,\ \ell \nmid 14} \ell.$$

The Method of Kraus

$$x^2 + 7 = y^p, \qquad p \geq 11.$$

WLOG

$$x \equiv 1 \pmod 4 \qquad \text{and} \qquad y \text{ is even.}$$

$$E_x : \qquad Y^2 = X^3 + xX^2 + \frac{(x^2+7)}{4} X$$

$$\Delta = \frac{-7y^p}{2^{12}}, \qquad N = 14 \prod_{\ell \mid y,\ \ell \nmid 14} \ell.$$

$E_x \sim_p F$ where $F = 14A$. Note $E_{-11} = 14A4$.

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = -1.$

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = -1.$

So $\ell \nmid (x^2 + 7)$. Hence $\ell \nmid NN'$.

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = -1.$

So $\ell \nmid (x^2 + 7)$. Hence $\ell \nmid NN'$.

$$a_\ell(E_x) \equiv a_\ell(F) \pmod{p}.$$

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = -1.$

So $\ell \nmid (x^2 + 7)$. Hence $\ell \nmid NN'$.

$$a_\ell(E_x) \equiv a_\ell(F) \pmod{p}.$$

Let

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

Fix $p \geq 11$. We choose ℓ satisfying certain conditions so that we obtain a contradiction.

- **Condition 1:** $\ell \nmid 14, \qquad \left(\frac{-7}{\ell}\right) = -1.$

So $\ell \nmid (x^2 + 7)$. Hence $\ell \nmid NN'$.

$$a_\ell(E_x) \equiv a_\ell(F) \pmod{p}.$$

Let

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

So $x \equiv \alpha \pmod{\ell}$ for some $\alpha \in T(\ell, p)$.
Let

$$R(\ell, p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

Also $x \equiv \beta \pmod{\ell}$ for some $\beta \in R(\ell, p)$.

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell, p) \cap R(\ell, p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell, p) \cap R(\ell, p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

$$R(\ell, p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell, p) \cap R(\ell, p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

$$R(\ell, p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

Note $T(\ell, p) \neq \emptyset$. e.g. $\overline{-11} \in T(\ell, p)$.

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell, p) \cap R(\ell, p) = \emptyset$ then $x^2 + 7 = y^p$ has no solutions.

$$T(\ell, p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

$$R(\ell, p) = \{\beta \in \mathbb{F}_\ell : \beta^2 + 7 \in (\mathbb{F}_\ell^\times)^p\}.$$

Note $T(\ell, p) \neq \emptyset$. e.g. $\overline{-11} \in T(\ell, p)$.
If $p \nmid (\ell - 1)$ then

$$(\mathbb{F}_\ell^\times)^p = \mathbb{F}_\ell^\times \implies R(\ell, p) = \mathbb{F}_\ell \implies T(\ell, p) \cap R(\ell, p) \neq \emptyset.$$

The Method of Kraus

Lemma

If ℓ satisfies Condition 1 and $T(\ell,p) \cap R(\ell,p) = \emptyset$ then $x^2+7=y^p$ has no solutions.

$$T(\ell,p) = \{\alpha \in \mathbb{F}_\ell : a_\ell(E_\alpha) \equiv a_\ell(F) \pmod{p}\}.$$

$$R(\ell,p) = \{\beta \in \mathbb{F}_\ell : \beta^2+7 \in (\mathbb{F}_\ell^\times)^p\}.$$

Note $T(\ell,p) \neq \emptyset$. e.g. $\overline{-11} \in T(\ell,p)$.
If $p \nmid (\ell-1)$ then

$$(\mathbb{F}_\ell^\times)^p = \mathbb{F}_\ell^\times \implies R(\ell,p) = \mathbb{F}_\ell \implies T(\ell,p) \cap R(\ell,p) \neq \emptyset.$$

However, if $p \mid (\ell-1)$, then

$$\#(\mathbb{F}_\ell^\times)^p = \frac{\ell-1}{p} \implies \text{good chance that } T(\ell,p) = R(\ell,p).$$

An example : $x^2 + 7 = y^{37}$

So we have $p = 37$. Let's look for prime $\ell \equiv 1 \mod 37$.

An example : $x^2 + 7 = y^{37}$

So we have $p = 37$. Let's look for prime $\ell \equiv 1 \mod 37$.

The smallest is $\ell = 149$.

An example : $x^2 + 7 = y^{37}$

So we have $p = 37$. Let's look for prime $\ell \equiv 1 \mod 37$.

The smallest is $\ell = 149$.

But $\left(\frac{-7}{149}\right) = 1$. No problem, let's try anyway.

An example : $x^2 + 7 = y^{37}$

So we have $p = 37$. Let's look for prime $\ell \equiv 1 \mod 37$.

The smallest is $\ell = 149$.

But $\left(\frac{-7}{149}\right) = 1$. No problem, let's try anyway.

Suppose first that $149 \mid y$. Then we have

$$-18 = a_{149}(F) \equiv \pm(149 + 1) \equiv \pm 2 \mod 37,$$

a contradiction. So we may suppose that 149 does not divide y.

An example : $x^2 + 7 = y^{37}$

Our

$$T(149, 37) = \{\alpha \in \mathbb{F}_{149} : a_{149}(E_\alpha) \equiv a_{149}(F) = -18 \pmod{37}\}.$$

An example : $x^2 + 7 = y^{37}$

Our

$$T(149, 37) = \{\alpha \in \mathbb{F}_{149} : a_{149}(E_\alpha) \equiv a_{149}(F) = -18 \pmod{37}\}.$$

We compute to see that

$$T(149, 37) = \{7, 11, 23, 31, 32, 56, 62, 65, 84, 87, 93, 117, 118, 126, 138, 142\}.$$

An example : $x^2 + 7 = y^{37}$

Our

$$T(149, 37) = \{\alpha \in \mathbb{F}_{149} : a_{149}(E_\alpha) \equiv a_{149}(F) = -18 \pmod{37}\}.$$

We compute to see that

$$T(149, 37) = \{7, 11, 23, 31, 32, 56, 62, 65, 84, 87, 93, 117, 118, 126, 138, 142\}.$$

But, $y^{37} \equiv \pm 1, \pm 44 \mod 149$, so that

$$R(149, 37) = \{\beta \in \mathbb{F}_{149} : \beta^2 + 7 \in (\mathbb{F}_{149}^\times)^{37}\} = \{21, 22, 127, 128\}.$$

An example : $x^2 + 7 = y^{37}$

Our

$$T(149, 37) = \{\alpha \in \mathbb{F}_{149} : a_{149}(E_\alpha) \equiv a_{149}(F) = -18 \pmod{37}\}.$$

We compute to see that

$$T(149, 37) = \{7, 11, 23, 31, 32, 56, 62, 65, 84, 87, 93, 117, 118, 126, 138, 142\}.$$

But, $y^{37} \equiv \pm 1, \pm 44 \mod 149$, so that

$$R(149, 37) = \{\beta \in \mathbb{F}_{149} : \beta^2 + 7 \in (\mathbb{F}_{149}^\times)^{37}\} = \{21, 22, 127, 128\}.$$

Thus $T(149, 37) \cap R(149, 37) = \emptyset$ and so $x^2 + 7 = y^{37}$ has no solutions.

Proposition

There are no solutions to $x^2 + 7 = y^p$ with $11 \leq p \leq 10^8$.

Proof.

By computer. For each p find $\ell \equiv 1 \pmod{p}$ satisfying condition 1, so that $T(\ell, p) \cap R(\ell, p) = \emptyset$. $\square$

Theorem

The only solutions to $x^2 + 7 = y^m$, with $m \geq 3$ are

m	x	y	m	x	y	m	x	y
3	± 1	2	3	± 181	32	4	± 3	± 2
5	± 5	2	5	± 181	8	7	± 11	2
15	± 181	2						

Proof.

Linear forms in logs tell us $p \leq 10^8$. For small m reduce to Thue equations and solve by computer algebra. $\square$