The Lebesgue–Nagell–Ramanujan Equation

Samir Siksek — University of Warwick

— joint work with J. Cremona (Nottingham)

— joint work with Y. Bugeaud, M. Mignotte } Strasbourg

LNR equation

$$x^2 + D = y^n \qquad x, y \in \mathbb{Z}, \; n \geq 3$$

History I

Fermat, Euler (1770) } $x^2 + 2 = y^3 \Rightarrow x = \pm 5, \; y = 3$

Ramanujan 1913 proposed, Nagell 1948 solved } $x^2 + 7 = 2^n$

$$\Downarrow$$

$x = \pm 1, \pm 3, \pm 5, \pm 11, \pm 181$

Fixed n, Arbitrary y

Example $x^2+2=y^3$

Factor over $\mathbb{Z}[\sqrt{-2}]$ (PID)

$$\Rightarrow \underbrace{(x+\sqrt{-2})(x-\sqrt{-2})}_{\text{coprime}} = y^3$$

$$\Rightarrow x+\sqrt{-2} = (u+v\sqrt{-2})^3$$

$$= (u^3-6uv^2)+(3u^2v-2v^3)\sqrt{-2}$$

$$\Rightarrow 1 = v(3u^2-2v^2) \quad \left(\text{coeff of } \sqrt{-2}\right)$$

$$\Rightarrow v=\pm 1,\ u=\pm 1$$

$$\Rightarrow x=\pm 5,\ y=3.$$

Example $x^2+25=y^3$

(i) $x+5i = (u+iv)^3$

$$\Rightarrow 3u^2v-v^3=5 \quad (\text{coeff of } i)$$

$$\Rightarrow v=\pm 1, \pm 5$$

$\Rightarrow$ no solutions

(ii) $x+5i = (10+5i)(u+iv)^3$

$$\Rightarrow 5u^3+30u^2v-15uv^2-10v^3=5$$

$\Longrightarrow \; u^3 + 6u^2v - 3uv^2 - 2v^3 = 1$

Thue equation
can be solved by MAGMA

$\Longrightarrow \; u = 1, \quad v = 0 \quad \Rightarrow \; x = 10, \quad y = 5$

(iii) $x + 5i = (-10 + 5i)(u + iv)^3$

$\Rightarrow \; x = -10, \quad y = 5$

Summary $\quad x^2 + D = y^n \qquad n$ fixed

- factor LHS
- get finitely many Thue eqns
- solve using MAGMA

(algorithm of Bilu & Hanrot).

(practical for $n \lesssim 20$)

History II (n arbitrary)

Lebesgue 1850 $\quad x^2 + 1 = y^n \quad n \geq 3$

Nagell 1923 $\quad x^2 + 3 = y^n$

$x^2 + 5 = y^n$

⋮

hundreds of people

John Cohn 1993 completed the soln of $x^2+D=y^n$ for $1 \le D \le 100$ except

$D = 7, 15, 18, 23, 25, 31, 39, 45, 47, 60, 63, 71, 72, 79, 87, 92, 99, 100.$

19 bad values of D

How to Deal with Good Values of D?

For good D, write $D = D_1^2 D_2$

D_2 square-free.

Suppose $n = p$ prime. Then

$$(x + D_1\sqrt{-D_2})(x - D_1\sqrt{-D_2}) = y^p$$

$$\Rightarrow x + D_1\sqrt{-D_2} = (u + v\sqrt{-D_2})^p$$

for $p \ge C$

$$\Rightarrow v \mid D_1 \quad \text{etc.}$$

For bad D

$$x + D_1\sqrt{-D_2} = \underbrace{(a + b\sqrt{-D_2})}_{\neq 1}(u + v\sqrt{-D_2})^p$$

Cremona & Siksek 2002:

Apply the proof of Fermat's Last Theorem

to $x^2 + D = y^p$ (because of variable exponent)

Proof Sketch of FLT (Wiles)

Suppose $a, b, c \in \mathbb{Z}$ are coprime, $abc \neq 0$

$a^p + b^p + c^p = 0$, $p \geq 5$ prime.

Associate to this the 'Frey elliptic curve'

$$E: \; Y^2 = X(X - a^p)(X + b^p)$$

Wiles: E is modular.

Ribet's Theorem $\Longrightarrow$ Galois representation on $E[p]$ arises from a cusp form at level 2.

But, there are no cusp forms at level 2. Contradiction. $\square$

Return to $x^2+7=y^p$ $\quad p \geq 11$ ⑥

Frey elliptic curve

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

Wiles $\Longrightarrow$ E_x is modular

Ribet's Theorem $\Longrightarrow$ Galois representation on $E_x[p]$ arises from a <u>cusp form</u> at level 14.

Cusp form at level 14 corresponds to

$$E : Y^2 + XY + Y = X^3 + 4X - 6 .$$

[diverged from proof of FLT]

'..... arises from ...' means:

$\forall$ primes $\ell \neq 2, 7$

(i) if $\ell \nmid y$ then

$$(\# E_x \bmod \ell) \equiv (\# E \bmod \ell) \mod p$$

(ii) if $\ell \mid y$ then

$$(\# E \bmod \ell) \equiv 0 \quad \text{or} \quad 2\ell + 2 \mod p .$$

Fix $p \geq 11$. We want to get a contradiction [adapting ideas of Kraus].

Choose a prime ℓ such that

- $\ell = mp+1$
- $(\#E \bmod \ell) \not\equiv 0,\ 2\ell+2 \bmod p$.

By (ii) $\ell \nmid y$. Hence

$$(\#E_x \bmod \ell) \equiv (\#E \bmod \ell) \bmod p$$

$$\Longrightarrow \quad x \equiv x_1, x_2, \dots, x_r \bmod \ell.$$

But $\quad x^2+7 = y^p$

$$\Longrightarrow (x^2+7)^m = y^{mp}$$
$$= y^{\ell-1} \qquad (\ell = mp+1)$$
$$\equiv 1 \quad \bmod \ell$$

If $(x_i^2+7)^m \not\equiv 1 \bmod \ell \quad i = 1, \dots, r$

then contradiction.

Get a <u>criterion</u> for non-existence of solutions for any particular value of p.

Theorem (Cremona & Siksek 2002)

The equation $x^2+7=y^p$ (p prime) does not have solutions for

$$11 \leq p \leq 10^8.$$

[Computation took 4 days]

History II $x^2+7=y^p$

Baker's theory $\Longrightarrow$ bounds for p

Baker & Wüstholz 1993 $\Longrightarrow$ $p \leq 6.6 \times 10^{15}$

Matveev 1999 $\Longrightarrow$ $p \leq 6.81 \times 10^{12}$

Mignotte 2003 $\Longrightarrow$ $p \leq 1.11 \times 10^{9}$

Bugeaud, Mignotte & Siksek

Lemma Suppose $p \geq 11$. Then

$$y \geq (\sqrt{p} - 1)^2$$

(Modular lower bound for y)

Proof Let $\ell \mid y$. Then

$$(\#E \bmod \ell) \equiv 0 \text{ or } 2\ell+2 \bmod p.$$

Case 1 $(\# E \bmod \ell) \equiv 0 \bmod p.$

Hasse-Weil

$$\ell+1-2\sqrt{\ell} \leq (\# E \bmod \ell) \leq \ell+1+2\sqrt{\ell}$$

Then
$$p \leq (\# E \bmod \ell)$$
$$\leq \ell+1+2\sqrt{\ell} = (\sqrt{\ell}+1)^2$$

$$\therefore \quad \ell \geq (\sqrt{p}-1)^2.$$

But $\ell | y \qquad \therefore \; y \geq (\sqrt{p}-1)^2.$

Case 2 Similar. $\square$

Suppose $p \geq 11$. Then $p \geq 10^8$.

$$\therefore \quad y \geq (\sqrt{10^8}-1)^2 = 9999^2$$

i.e. y is big. Baker's theory now works better. Get

$$p \leq 1.81 \times 10^8$$

Re-run the program upto this new bound.

Theorem The only solutions to

$$x^2 + 7 = y^n \qquad n \geq 3$$

are

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

Also solved $x^2 + D = y^n$ for $1 \leq D \leq 100$.

Role of MAGMA

- Reducing to Thue eqns and solving for small n

- Computing cusp forms at levels predicted by Ribet's Theorem

- Computing elliptic curves corresponding to rational cusp forms

} Modular forms package Stein + Elliptic curve database Cremona

Theorem Bugeaud, Mignotte & Siksek

Let $\{F_n\}$ be the Fibonacci sequence:

$F_0 = 0, F_1 = F_2 = 1, \quad F_{n+2} = F_{n+1} + F_n$.

The only perfect powers in the Fib. sequence are

$F_0 = 0, F_1 = F_2 = 1, \quad F_6 = 8, \quad F_{12} = 144$.

Proved again using modularity + Baker's theory — but much, much deeper.

Theorem BMS

The only solutions to

$$7^u x^n - 2^r 3^s y^n = \pm 1 \qquad \begin{array}{l} n \geq 3 \\ u, r, s > 0 \end{array}$$

are

$$7 \times 1^n - 2 \times 3 \times 1^n = 1$$
$$7^2 \times 1^n - 2^4 \times 3 \times 1^n = 1$$
$$7 \times 5^4 - 2 \times 3^7 \times 1^4 = 1.$$

Proved using
- multi-Frey curves
- Baker's theory
- Deep theorems of M. Bennett.

Challange Show that the only solns to $x^2 - 2 = y^p$ are

$$(\pm 1)^2 - 2 = (-1)^p$$

[Current method fails for

$$x^2 - (a^2 \pm 1) = y^p$$

but seems to work for

$$x^2 - D = y^p$$

if $D \neq a^2 \pm 1$.]

Papers

1. Siksek & Cremona
   "On the Diophantine equation $x^2+7=y^m$"
   Acta Arithmetica 109.2 (2003)

2. Bugeaud, Mignotte & Siksek
   "Classical & Modular Approaches to Diophantine Equations I: Fibonacci and Lucas Perfect Powers",
   Annals of Math. (to appear).

3. Bugeaud, Mignotte & Siksek
   "Classical & Modular Approaches to Diophantine Equations II: The Lebesgue–Nagell Equations" Compositio Math. (to appear).

4. Bugeaud, Mignotte & Siksek
   "A Multi-Frey Approach to Some Multi-Parameter Families of Diophantine Equations"