A Multiply Exponential Diophantine Spree

Samir Siksek

Joint work with Y. Bugeaud & M. Mignotte } Strasbourg

Theme To combine two approaches to Diophantine equations

1. Baker's Theory for bounding exponents and variables.
2. Modular Approach (initiated by Frey), used in Wiles' proof of Fermat's Last Theorem.

Theorem The only perfect powers in the Fibonacci sequence are 0, 1, 8, 144.

Theorem The only solutions to $x^2+7=y^m$ are

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

Focus On $q_1^u x^p - q_2^v y^p = 1$

q_1, q_2 fixed primes

p, x, y, u, v unknowns

$p \geq 7$ is prime & $0 < u, v < p$

New Bounds for Linear Forms in 3 Logs

By Mignotte $\Longrightarrow$ $p \lesssim 10^9$ for reasonable q_1, q_2

(special refined case of Baker's Theory)

Apply Modular Approach Associate solution to a 'Frey elliptic curve' with

$$\Delta = A \cdot B^p$$

discriminant

has fixed prime divisors

depends on solution

Ribet's Thm $\Longrightarrow$ modulo technical conditions

Galois rep. on p-torsion arises from a newform of 'small' level

$$q_1^u x^p - q_2^v y^p = 1$$

Let $\psi = q_2^v y^p$

$\therefore \quad \psi + 1 = q_1^u x^p$

Frey curve $F_\psi : Y^2 = X(X+\psi)(X+\psi+1)$

$$\Delta = 16\psi^2(\psi+1)^2$$

$$= \underbrace{16 q_1^{2u} q_2^{2v}}_{\text{has fixed prime divisors}} (x^2 y^2)^p$$

Galois representation on $F_\psi[p]$ arises from a newform f of level

$$N_p = 2^? q_1 q_2$$

[e.g. if q_1, q_2 are odd $N_p = 2q_1q_2$]

Fact If f is irrational, we get good bounds on p.

Assume f is rational

$\therefore$ f corresponds to elliptic curve F.

$$q_1^u x^p - q_2^v y^p = 1 \qquad \psi = q_2^v y^p$$

$$F_\psi : \quad Y^2 = X(X+\psi)(X+\psi+1)$$

F elliptic curve

Upshot for any prime $\ell \nmid 2 q_1 q_2$

(i) if $\psi \not\equiv 0, -1 \pmod{\ell}$ then

$$a_\ell(F_\psi) \equiv a_\ell(F) \pmod{p}$$

(ii) if $\psi \equiv 0, -1 \pmod{\ell}$ then

$$\pm(\ell+1) \equiv a_\ell(F) \pmod{p}$$

Defn $$B_\ell = \left((\ell+1)^2 - a_\ell(F)^2\right) \prod_{\phi \in \mathbb{F}_\ell \setminus \{0,-1\}} \left(a_\ell(F_\phi) - a_\ell(F)\right)$$

Theorem $p \mid B_\ell$.

This gives a bound on p if $B_\ell \neq 0$.

<u>Heuristic</u> Probability that $B_\ell \neq 0$ is roughly

$$\left(1 - \frac{1}{\sqrt{\ell}}\right)^{\ell} \approx e^{-\sqrt{\ell}} \longrightarrow 0 \quad \text{as } \ell \to \infty.$$

[Note $-2\sqrt{\ell} \leq a_\ell(F_\phi),\ a_\ell(F) \leq 2\sqrt{\ell}$]

Bad News!

<u>Second Frey Curve</u> $G_\psi : \ Y^2 = X(X^2 + 2X - \psi)$

$$\Delta = 64\psi^2(\psi+1) = 64\, q_2^{2\nu} q_1^4 (xy^2)^p$$

Apply level-lowering $\Longrightarrow$ newform g of level $2^? q_1 q_2$

Suppose g is rational, corresponding to elliptic curve G.

Get same congruences as before with G instead of F.

Defn $$B_\ell = \gcd\left((\ell+1)^2 - a_\ell(F)^2,\ (\ell+1)^2 - a_\ell(G)^2\right) \times \prod_{\phi \in \mathbb{F}_\ell \setminus \{0,-1\}} \gcd\left(a_\ell(F_\phi) - a_\ell(F),\ a_\ell(G_\phi) - a_\ell(G)\right)$$

Theorem $p \mid B_\ell$.

Heuristic Probability that $B_\ell \neq 0$ is roughly $\left(1 - \frac{1}{\ell}\right)^\ell \longrightarrow e^{-1}$ as $\ell \to \infty$.

Third Frey Curve $H_\psi : Y^2 + 3XY - \psi Y = X^3$

Probability that $B_\ell \neq 0$ is roughly $\left(1 - \frac{1}{\ell\sqrt{\ell}}\right)^\ell \approx e^{-1/\sqrt{\ell}} \longrightarrow 1$ as $\ell \to \infty$.

Theorem If $3 \leq q_1 < q_2 \leq 31$ are primes then the equation

$$q_1^u x^p - q_2^v y^p = 1 \qquad u, v \geq 0,\ xy \neq 0,\ p \geq 7 \text{ prime}$$

has no solutions.

Proof Sketch List the possible triples of newforms (f, g, h) obtained by applying level-lowering to (F_ψ, G_ψ, H_ψ). For a few $\ell \nmid 6q_1q_2$ compute $B_\ell(f, g, h)$.

If gcd of $B_\ell(f,g,h)$ is divisible only by primes $p \leq 5$ then we have a contradiction. $\square$

More Difficult $5^u x^p - 2^r y^p = 1$ $0 < u < p$, $xy \neq 0$, $p \geq 7$ prime

(has solution $5 \times 1^p - 4 \times 1^p = 1$)

F_ψ, G_ψ Frey curves as above.

N_f, N_g levels after level-lowering

	N_f	N_g
~~y even, or $r=0$ or $r \geq 6$~~	~~5, 10~~	~~5, 10~~
~~y odd & $r=5$~~	~~10~~	~~40~~
~~y odd & $r=4$~~	~~5~~	~~40~~
~~y odd & $r=3$~~	~~10~~	~~160~~
$y \equiv 1\ (4)$ & $r=2$	40	20
~~$y \equiv 3\ (4)$ & $r=2$~~	~~40~~	~~40~~
~~y odd & $r=1$~~	~~$2^5 \times 5$~~	~~$2^7 \times 5$~~

impossible

Look at y odd, $r=3$.

f has level $40 \Rightarrow f = 40A1$

g has level $160 \Rightarrow$

$g = g_1$ or g_2 or g_3

$g_1 = 160A1$, $g_2 = 160B1$,

$g_3 = q + 2\sqrt{2}\, q^3 + q^5 - 2\sqrt{2}\, q^7 + \cdots$

$B_3(f, g_1) = 0$, $B_7(f, g_1) = 24$, ...

$B_3(f, g_2) = 4$, ...

$B_3(f, g_3) = 48$, ...

$\therefore$ No solutions. $(p \geq 7)$

For $y \equiv 1 \ (4)$, $r = 2$

$f = 40A1$, $g = 20A1$

$B_3(f,g) = B_7(f,g) = B_{11}(f,g) = \cdots = 0$

Why? Because we have solution

$x = 1$, $y = 1$, p arbitrary

$u = 1$, $r = 2$ (i.e. $5 - 4 = 1$)

Reduced to $r=2$

i.e. $5^u x^p - 4y^p = 1 \qquad (0<u<p)$

$F_\psi : \; Y^2 = X(X+\psi)(X+\psi+1)$

$F = 40A1 \qquad \begin{pmatrix} \psi = 4y^p \\ \psi+1 = 5x^p \end{pmatrix}$

If $\ell \neq 2,5$ is prime, then

(i) $\psi \not\equiv 0, -1 \pmod{\ell} \Longrightarrow a_\ell(F_\psi) \equiv a_\ell(F) \pmod{p}$

(ii) $\psi \equiv 0, -1 \pmod{\ell} \Longrightarrow \pm(\ell+1) \equiv a_\ell(F) \pmod{p}$

Fix $p \geq 7$. Want to show that $u=1$.

Find a prime ℓ satisfying (a), (b), (c), (d):

(a) $\ell = np+1$

(b) $p \nmid \left((\ell+1)^2 - a_\ell(F)^2\right)$

$\therefore \quad \psi \not\equiv 0, -1 \pmod{\ell}$

$\therefore \quad \ell \nmid x, y$

But $\psi \pmod{\ell} \equiv 4y^p \pmod{\ell}$

$\in 4(\mathbb{F}_\ell^*)^p = \{\bar{4}, \phi_1, \dots, \phi_{n-1}\}$

(c) $a_\ell(F_{\phi_i}) \not\equiv a_\ell(F) \pmod p$ for $i = 1, \dots, n-1$.

But $a_\ell(F_\psi) \equiv a_\ell(F) \pmod p$

$\therefore \quad \psi \equiv 4 \pmod \ell$

$\therefore \quad 5^u x^p \equiv \psi + 1 \equiv 5 \pmod \ell$

$\therefore \quad 5^{nu} \equiv 5^n \pmod \ell$

(Recall $\ell \nmid x$ & $\ell - 1 = np$)

$\therefore \quad 5^{n(u-1)} \equiv 1 \pmod \ell$

(d) $5^n \not\equiv 1 \pmod \ell$

$\therefore \quad p \mid (u-1)$

But $0 < u < p$

$\therefore \quad u = 1$.

Lemma $u = 1$ for $7 \leq p \leq 10^8$

Reduced to $5x^p - 4y^p = 1$.

Bennett's Theorem If A, B, n integers $AB \neq 0$, $n \geq 3$ then $Ax^n - By^n = 1$ has at most 1 solution.

Lemma If $7 \leq p \leq 10^8$ then $(x,y) = (1,1)$.

But

Mignotte: If $5^u x^p - 2^r y^p = 1$ & $(x,y) \neq (1,1)$ then $p \leq 4.9 \times 10^7$.

Theorem Suppose $3 \leq q < 100$ is prime. Then the only solutions to

$$q^u x^n - 2^r y^n = \pm 1 \qquad \begin{matrix} n \geq 3, & xy \neq 0 \\ u, r \geq 0 & \end{matrix}$$

are

$$1 - 2 = -1, \quad 3 - 2 = 1, \quad 3 - 4 = -1,$$

$$9 - 8 = 1, \quad 5 - 4 = 1, \quad 7 - 8 = -1,$$

$$17 - 16 = 1, \quad 31 - 32 = -1,$$

$$5 \times 2^4 - 3^4 = -1, \quad 19 \times 3^3 - 8^3 = 1,$$

$$17 \times 7^3 - 18^3 = -1, \quad 37 \times 3^3 - 10^3 = -1,$$

$$43 \times 2^3 - 7^3 = 1, \quad 53 - 2 \times 3^3 = -1.$$

Almost Solved

$$5^u x^p - 2^r 3^s y^p = 1$$

Challange Show that the only solutions to

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

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