Integral points on congruent number curves

Michael Bennett (with S. Dahmen, M. Mignotte and S. Siksek)

University of British Columbia

Budapest : July, 2013

A Goal.....

Given an elliptic curve $E/\mathbb{Q}$, understand the set $E(\mathbb{Z})$; i.e bound the number and size of the integral points on a given model of E. This number, via Siegel's Theorem is always finite, but it can be difficult to quantify such a statement.

A less ambitious goal.....

Understand $E_D(\mathbb{Z})$ in a family of twists of a given curve E. Here, there are a number of conjectures of Lang and of Abramovich and Pacelli which predict that this set, for many choices of E, is absolutely bounded.

An even less ambitious goal

Understand $E_N(\mathbb{Z})$ for my favourite family of twists of a given curve E, say

$$E_N \ : \ y^2 = x^3 - N^2 x.$$

These are known as *congruent number* curves. Recall that a positive integer N is a *congruent number* if there exists a right triangle with rational sides and area N. It is a classical result that N is congruent precisely when the elliptic curve E_N has infinitely many rational points.

My goal

Understand $E_N(\mathbb{Z})$ for

$$E_N \ : \ y^2 = x^3 - N^2 x,$$

where we will restrict N so that E_N has as little bad reduction as possible. Specifically, we will consider only $N = 2^a p^b$.

More precisely

In what follows, we will address the question of whether curves of the shape E_N possess *integral* points of infinite order, provided we know they have rational points with this property. We will concentrate on the case where $N = 2^a p^b$ for a and b nonzero integers and p an odd prime. Since E_N is rationally isomorphic to $E_{m^2 N}$ for each nonzero integer m, and since both E_1 and E_2 have rank 0 over $\mathbb{Q}$, we may suppose, without loss of generality, that b is odd.

A second excuse

Draziotis and Poulakis (2005) present an algorithm for computing $E_N(\mathbb{Z})$, when $N = 2^a p^b$, for a, b and p fixed, using Wildanger's algorithm to solve unit equations of the shape $u + \sqrt{2}v = 1$ in the field $\mathbb{Q}(\sqrt{2}, \sqrt{p})$. They illustrate this by showing that

$$E_6(\mathbb{Z}) = (0,0), (\pm 6, 0), (-3, \pm 9), (-2, \pm 8),$$

$$(12, \pm 36, (18, \pm 72), (294, \pm 5040).$$

This computation first finds (via Magma) the 72 solutions to the given unit equation.

A third excuse

This question leads (perhaps unexpectedly) to the use of Frey curves, including $\mathbb{Q}$-curves, as pioneered by Darmon, Ellenberg and Skinner, and Frey curves connected to Hilbert modular forms.

Primitive Solutions

From now on, we will fix p to be an odd prime number, and a and b to be nonnegative integers. We are interested in describing the integer solutions (x, y), with $y > 0$, say, to the Diophantine equation.

$$y^2 = x(x + 2^a p^b)(x - 2^a p^b). \tag{1}$$

A solution (x, y) (with $y > 0$) to (1) is called *primitive* if both

$$\min\{\nu_2(x), a\} \leq 1 \text{ and } \min\{\nu_p(x), b\} \leq 1.$$

Clearly it is enough to determine all primitive integer solutions. These correspond to the S-integral points on E_p and E_{2p}, where $S = \{2, p, \infty\}$.

An aside

A general (and vague!) philosophical assertion is that, while it is difficult to find uniform bounds on $E(\mathbb{Z})$ for E ranging over a family of cubic models, it is often much easier (and indeed classical) to do so for certain quartic models. For example, the equation

$$X^4 - DY^2 = 1$$

has at most a single solution in positive integers X, Y, provided $D \neq 1785$ (Cohn, Ljunggren). Cubic models with full rational 2-torsion are, in some sense, closest to quartic in that it is very simple to describe the rational maps between them.

Back to our regular programming

Recall that we were studying solutions to

$$y^2 = x^3 - N^2 x, \quad N = 2^a p^b.$$

Here are some primes p and values a where we have solutions; in each case $b = 1$.

p	a	x	p	a	x	p	a	x
3	1	−3	3	3	25	7	3	−7
3	1	−2	5	0	−4	7	4	−63
3	1	12	5	0	45	11	1	2178
3	1	18	5	2	25	17	5	833
3	1	294	7	1	112	17	7	16337
29	0	284229	41	6	42025			

Some families of solutions

$$p = r^4 + s^4, \ a = 1,$$

$$p = r^4 + 6r^2s^2 + s^4, \ a = 0,$$

$$p = r^4 + 12r^2s^2 + 4s^4, \ a = 1,$$

$$\left(2^{a-1}\right)^2 - ps^2 = -1, \ a \text{ odd},$$

$$p^2 - 2s^2 = -1, \ a = 0,$$

$$p^2r^4 - 2s^2 = 1, \ p \equiv 1 \text{ mod } 8, \ \ a = 1,$$

$$ps^2 = 2^{2(a-2)} + 3 \cdot 2^{a-1} + 1, \ a \geq 3,$$

and

$$p^2 \pm 6p + 1 = 8s^2, \ a = 1.$$

The punchline

Theorem (B, 2013) : The primitive integers solutions to the equation

$$y^2 = x^3 - N^2 x, \;\; N = 2^a p^b$$

in nonzero integers (x, y), nonnegative integers a, b and prime p correspond to those in the previous table and families.

Corollary : If $N = 2^a p^b$ where $p \equiv \pm 3 \bmod 8$ is prime, $p \neq 3, 5, 11, 29$, then

$$E_N(\mathbb{Z}) = \{(0,0), (\pm N, 0)\}.$$

Note

According to Monsky, we have that $p \equiv 5, 7 \bmod 8$ are congruent, while the same is true for $2p$, when $p \equiv 3, 7 \bmod 8$.

This follows from Heegner and mock-Heegner point analysis.

More results

Corollary 2 : Let p be an odd prime and $S = \{2, p, \infty\}$. Then the number of S-integral points on E_p is at most 9, while the number of S-integral points on E_{2p} is at most 19.

These bounds are sharp for $p = 5$ and $p = 17$, respectively.

Back to the families

For primes of the shape

$$p = r^4 + s^4,$$

we expect that

$$\sum_{\substack{p \leq N \\ p = t^4 + s^4}} \log p \sim \frac{\Gamma\left(5/4\right)^2}{\sqrt{\pi}} \, C \, N^{1/2},$$

where

$$C = \prod_{p \equiv 1 \mod 8} \left(1 - \frac{3}{p}\right) \prod_{p \equiv 3,5,7 \mod 8} \left(1 + \frac{1}{p}\right).$$

Similarly

we believe that

$$\sum_{\substack{p \leq N \\ p = r^4 + 12 r^2 s^2 + 4 s^4}} \log p \sim \frac{\Gamma\left(5/4\right)^2}{\sqrt{\pi}} \, C \, N^{1/2}$$

and

$$\sum_{\substack{p \leq N \\ p = r^4 + 6 r^2 s^2 + s^4}} \log p \sim \frac{\Gamma\left(5/4\right)^2}{\sqrt{2\pi}} \, C \, N^{1/2}.$$

The remaining families

If there exist odd a and s such that

$$\left(2^{a-1}\right)^2 - ps^2 = -1,$$

likely $p \in \{17, 257, 65537\}$. If we can find r and s with

$$p^2r^4 - 2s^2 = 1,\ p \equiv 1 \text{ mod } 8,$$

we suspect that $p \in \{17, 577, 665857\}$.

The remaining families

The remaining families of primes p corresponding to the equations

$$p^2 - 2s^2 = -1, \ a = 0,$$

$$ps^2 = 2^{2(a-2)} + 3 \cdot 2^{a-1} + 1, \ a \geq 3,$$

and

$$p^2 \pm 6p + 1 = 8s^2, \ a = 1,$$

are each, in all likelihood, infinite.

Counts

10^4	10^6	10^8	10^{10}	10^{12}	10^{14}	10^{16}
13	89	611	4915	40590	341872	2966902
8	64	453	3481	28525	242469	2097454
15	92	640	4949	40698	342349	2965304
2	3	3	3	3	3	3
3	3	4	4	5	5	5
2	3	3	3	3	3	3
6	7	10	10	11	11	11
6	7	8	8	8	9	9

One case

Recall yet again that we are considering

$$y^2 = x(x + 2^a p^b)(x - 2^a p^b),$$

where $x = 2^\alpha p^\beta x_1$ with $\gcd(x_1, 2p) = 1$, and where

$$\min\{a, \alpha\} \le 1 \text{ and } \min\{b, \beta\} \le 1.$$

If we consider the case $a = \alpha = 0, b > \beta$, then $\beta = 0$ and so

$$y_1^2 = x_1(x_1 - p^b)(x_1 + p^b),$$

for $y_1 \in Z$. If $x_1 < 0$, then we are led to

$$x_1 = -c^2,\ x_1 - p^b = -2d^2 \text{ and } x_1 + p^b = 2e^2,$$

for positive coprime integers c, d and e.

And so....

Adding the second and third equations, we find that $c^2 + e^2 = d^2$ and hence that there exist coprime positive integers f and g such that

$$c = f^2 - g^2, \; d = f^2 + g^2 \; \text{ and } \; e = 2fg.$$

Thus

$$f^4 + 6f^2g^2 + g^4 = p^b.$$

Conversely, such a solution implies one to

$$y_1^2 = x_1(x_1 - p^b)(x_1 + p^b),$$

with $x_1 = -(f^2 - g^2)^2$.
This equation, in fact, has no solutions with $b > 1$. To see this, note that

$$c^4 + (2de)^2 = p^{2b}.$$

Generally

We had the equations

$$r^4 + s^4 = p^b, \quad r^4 + 6r^2s^2 + s^4 = p^b$$

and

$$r^4 + 12r^2s^2 + 4s^4 = p^b.$$

The second of these implies that

$$A^4 + B^2 = p^{2b},$$

upon setting $A = r^2 - s^2, B = 4rs(r^2 + s^2)$, while the third becomes

$$A^4 + 2B^2 = p^{2b},$$

with $A = r^2 - 2s^2, B = 4rs(r^2 + 2s^2)$.

$\mathbb{Q}$-curves

To a solution to $A^4 + B^2 = C^q$, we associate the curve

$$E_1 : y^2 = x^3 + 2(1+i)Ax^2 + (B + iA^2)x,$$

while, given a solution to $A^4 + 2B^2 = C^q$, we consider

$$E_2 : y^2 = x^3 + 2\sqrt{-2}Ax^2 - (A^2 + \sqrt{-2}B)x.$$

Relevant facts

These "correspond" to weight 2, level N_i cuspidal newforms, where $N_1 = 256$ and $N_2 = 64$. Since all such forms have CM, we can, following Ellenberg (and after much work), conclude that $q < 211$ (here, q is prime). The small cases were subsequently finished in joint work with Ellenberg and Ng (IJNT 2010).

The last case.

One possibility we encounter when we consider the equation

$$y^2 = x(x + 2^a p^b)(x - 2^a p^b),$$

is that $a = 1$ and

$$x = 2c^2, \; x \pm 2p^b = 4d^2 \text{ and } x \mp 2p^b = 8e^2.$$

The last case.

One possibility we encounter when we consider the equation

$$y^2 = x(x + 2^a p^b)(x - 2^a p^b),$$

is that $a = 1$ and

$$x = 2c^2, \; x \pm 2p^b = 4d^2 \text{ and } x \mp 2p^b = 8e^2.$$

This implies that

$$p^{2b} \pm 6p^b + 1 = 8d^2.$$

The equation $x^{2n} + 6x^n + 1 = 8y^2$

We can rewrite this as

$$(x^n + 3)^2 - 8 = 8y^2,$$

whereby $4 \mid x^n + 3$ and

$$y^2 - 2\left(\frac{x^n+3}{4}\right)^2 = -1.$$

Hence

$$y + \left(\frac{x^n+3}{4}\right)\sqrt{2} = \pm\epsilon^k, \tag{2}$$

where k is odd and $\epsilon = 1 + \sqrt{2}$.

The equation $x^{2n} + 6x^n + 1 = 8y^2$

On the other hand, we can also rewrite this equation as

$$\left(\frac{x^n + 1}{2} \right)^2 - 2y^2 = -x^n$$

and so

$$\left(\frac{x^n + 1}{2} \right) + y\sqrt{2} = \epsilon^\ell \alpha^n, \tag{3}$$

where $\text{Norm}(\alpha) = (-1)^{\ell+1} x$.

We thus have

$$y + \left(\frac{x^n + 3}{4}\right)\sqrt{2} = \pm\epsilon^k$$

and

$$\left(\frac{x^n + 1}{2}\right) + y\sqrt{2} = \epsilon^\ell \alpha^n,$$

whence

$$\pm\, \epsilon^k \sqrt{2} - \epsilon^\ell \alpha^n = 1. \tag{4}$$

Linear forms in logarithms

Note that from

$$y+\left(\frac{x^n+3}{4}\right)\sqrt{2}=\pm\epsilon^k,$$

we have

$$\frac{|x^n+3|}{4}=\frac{\epsilon^k+\epsilon^{-k}}{2\sqrt{2}},$$

whence it follows that

$$\frac{|x|^n}{\sqrt{2}\,\epsilon^k}-1$$

is small, whereby the same is true of the linear form

$$\Lambda=n\log|x|-\log\sqrt{2}-k\log\epsilon.$$

Linear forms in logarithms (continued)

Lower bounds for linear forms in (three) complex logarithms thus implies, with care, an upper bound upon n (of the shape $n < 10^8$ or so).

Linear forms in logarithms (continued)

Lower bounds for linear forms in (three) complex logarithms thus implies, with care, an upper bound upon n (of the shape $n < 10^8$ or so).

It follows that our original equation

$$x^{2n} + 6x^n + 1 = 8y^2$$

has at most finitely many solutions in integers x, y and $n \geq 2$.

Handling the remaining cases

We associate to our solution (x, y, n) to

$$\pm\epsilon^k\sqrt{2} - \epsilon^\ell\alpha^n = 1$$

the Frey curve,

$$E_{s,k} \ : \ Y^2 = X(X+1)(X + s \cdot \epsilon^k\sqrt{2})$$

where the choice of sign $s = \pm 1$. By an easy application of Tate's algorithm we find that the curve $E_{s,k}$ has minimal discriminant

$$\Delta_{\min} = 32\epsilon^{2(k+\ell)}\alpha^{2n}$$

and conductor

$$\mathfrak{N} = (\sqrt{2})^9 \cdot \prod_{\mathfrak{p}|\alpha} \mathfrak{p}.$$

A little bit about representations

Let $E = E_{s,k}$ be our Frey curve, defined over the totally real field $K = \mathbb{Q}(\sqrt{2})$. Write $G_K = \mathsf{Gal}(\overline{K}/K)$ and $\overline{\rho}_{E,n}$ for the representation

$$\overline{\rho}_{E,n} \ : \ G_K \to \mathsf{Aut}(E[n]) \cong \mathsf{GL}_2(\mathbb{F}_n).$$

A little bit about representations

Let $E = E_{s,k}$ be our Frey curve, defined over the totally real field $K = \mathbb{Q}(\sqrt{2})$. Write $G_K = \mathrm{Gal}(\overline{K}/K)$ and $\overline{\rho}_{E,n}$ for the representation

$$\overline{\rho}_{E,n} \; : \; G_K \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{F}_n).$$

Via an argument of Freitas, we may show that $\overline{\rho}_{E,n}$ is absolutely irreducible for $n \geq 5$.

A little bit about representations

Let $E = E_{s,k}$ be our Frey curve, defined over the totally real field $K = \mathbb{Q}(\sqrt{2})$. Write $G_K = \mathsf{Gal}(\overline{K}/K)$ and $\overline{\rho}_{E,n}$ for the representation

$$\overline{\rho}_{E,n} \; : \; G_K \to \mathsf{Aut}(E[n]) \cong \mathsf{GL}_2(\mathbb{F}_n).$$

Via an argument of Freitas, we may show that $\overline{\rho}_{E,n}$ is absolutely irreducible for $n \geq 5$.

From the fact that 3 is inert in K and $E = E_{s,k}$ has good reduction at $3 \cdot \mathbb{Z}[\sqrt{2}]$, we know that E is modular.

More about representations

Applying standard level-lowering techniques of Fujiwara, Jarvis and Rajaei, we find that $\overline{\rho}_{E,n} \sim \overline{\rho}_{f,\mathfrak{n}}$ for some Hilbert newform over K of level $\mathfrak{M} = (\sqrt{2})^9$ and prime ideal $\mathfrak{n} \mid n$. Using MAGMA we find that the space of Hilbert newforms of level $\mathfrak{M}$ is 8-dimensional, and in fact decomposes into 8 rational eigenforms.

More on these eigenforms

Through a small search we found 8 elliptic curves over K of conductor $\mathfrak{M}$. By computing their traces at small prime ideals, we checked that they are in fact pairwise non-isogenous. It is not too hard to show that these elliptic curves are also modular. Hence they must correspond to the 8 Hilbert newforms of level $\mathfrak{M}$. Thus $\overline{\rho}_{E,n} \sim \overline{\rho}_{F_i,n}$ where $F_1, \ldots, F_8$ are the 8 elliptic curves.

These curves are

$$F_1 \ : \ Y^2 = X^3 + \sqrt{2}X^2 + (\sqrt{2}-1)X,$$
$$F_2 \ : \ Y^2 = X^3 + (-\sqrt{2}+3)X^2 + (-\sqrt{2}+2)X,$$
$$F_3 \ : \ Y^2 = X^3 + (2\sqrt{2}-1)X^2 + (-\sqrt{2}+2)X,$$
$$F_4 \ : \ Y^2 = X^3 + (\sqrt{2}-2)X^2 + (-\sqrt{2}+1)X,$$
$$F_5 \ : \ Y^2 = X^3 + (-\sqrt{2}+1)X^2 - \sqrt{2}X,$$
$$F_6 \ : \ Y^2 = X^3 + (\sqrt{2}-1)X^2 - \sqrt{2}X,$$
$$F_7 \ : \ Y^2 = X^3 + (\sqrt{2}+3)X^2 + (\sqrt{2}+2)X,$$
$$F_8 \ : \ Y^2 = X^3 - \sqrt{2}X^2 + (-\sqrt{2}-1)X.$$

What we have

Let $E = E_{s,k}$ and let F be one of the eight elliptic curves $F_1, \ldots, F_8$. Suppose $\overline{\rho}_{E,n} \sim \overline{\rho}_{F,n}$. Let $\mathfrak{q} \nmid 2$ be a prime ideal of K.

(i) If $\mathfrak{q} \nmid (s\epsilon^k\sqrt{2} - 1)$ then $a_{\mathfrak{q}}(E) \equiv a_{\mathfrak{q}}(F) \pmod{n}$.

(ii) If $\mathfrak{q} \mid (s\epsilon^k\sqrt{2} - 1)$ then $\mathrm{Norm}(\mathfrak{q}) + 1 \equiv \pm a_{\mathfrak{q}}(F) \pmod{n}$.

Note that $E_{s,k}$ has good reduction at $\mathfrak{q}$ in case (i), and multiplicative reduction in case (ii).

A local sieve

tells us that the $s = \pm 1$ sign in

$$\pm\epsilon^k\sqrt{2} - \epsilon^\ell\alpha^n = 1$$

is in fact $+1$. Moreover, either $k \equiv -1 \pmod{9240}$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{F_2,n}$ or $k \equiv 1 \pmod{9240}$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{F_7,n}$.

A local sieve

tells us that the $s = \pm 1$ sign in

$$\pm \epsilon^k \sqrt{2} - \epsilon^\ell \alpha^n = 1$$

is in fact $+1$. Moreover, either $k \equiv -1 \pmod{9240}$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{F_2,n}$ or $k \equiv 1 \pmod{9240}$ and $\overline{\rho}_{E,p} \sim \overline{\rho}_{F_7,n}$.

Note in fact that F_2 is isomorphic to $E_{1,-1}$ and F_7 is isomorphic to $E_{1,1}$, where

$$F_2 \ : \ Y^2 = X^3 + (-\sqrt{2}+3)X^2 + (-\sqrt{2}+2)X,$$
$$F_7 \ : \ Y^2 = X^3 + (\sqrt{2}+3)X^2 + (\sqrt{2}+2)X.$$

Further sieving

tell us that in

$$\epsilon^k\sqrt{2} - \epsilon^\ell\alpha^n = 1$$

we necessarily have $k \equiv \ell \equiv 1 \pmod{n}$.

Further sieving

tell us that in

$$\epsilon^k \sqrt{2} - \epsilon^\ell \alpha^n = 1$$

we necessarily have $k \equiv \ell \equiv 1 \pmod{n}$.

This observation enables us to reduce the above equation to a Thue equation of the shape

$$X^n - \sqrt{2}\, Y^n = 1 - \sqrt{2}.$$

Further sieving

tell us that in

$$\epsilon^k \sqrt{2} - \epsilon^\ell \alpha^n = 1$$

we necessarily have $k \equiv \ell \equiv 1 \pmod{n}$.

This observation enables us to reduce the above equation to a Thue equation of the shape

$$X^n - \sqrt{2}\, Y^n = 1 - \sqrt{2}.$$

Applying lower bounds for linear forms in two logarithms then lets us conclude that $n < 1000$.

Yet more sieving

tells us that in

$$\epsilon^k\sqrt{2} - \epsilon^\ell \alpha^n = 1$$

we have $k \equiv 1 \pmod{M}$ for $M > e^{10000}$.

Yet more sieving

tells us that in

$$\epsilon^k\sqrt{2} - \epsilon^\ell \alpha^n = 1$$

we have $k \equiv 1 \pmod{M}$ for $M > e^{10000}$.

This provides a lower bound of the shape $X > e^{e^{10000}}$ for $X \neq 1$ in

$$X^n - \sqrt{2}\,Y^n = 1 - \sqrt{2},$$

which, after much work, leads to the desired contradiction.