The Diophantine Equation $x^2 + 7 = y^m$

John Cremona

University of Nottingham, UK

26 May, 2003

The problem

Find all integer solutions to the following equation:

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

(Joint work with **Samir Siksek***, to appear in Acta Arithmetica (2003).)*

Plan of the talk

- Known solutions and previous results
- Summary of our results
- Eliminating small m
- Eliminating very large m
- Eliminating individual prime m using a Frey curve and level lowering
- The algorithm
- The computation and results

Known solutions

$$x^2 + 7 = y^m$$

$$\begin{array}{rll} m = 3 & x = 1 & y^m = 8 = 2^3 \\ m = 3, 5, 15 & x = 181 & y^m = 32768 = 32^3 = 8^5 = 2^{15} \\ m = 4 & x = 3 & y^m = 16 = 2^4 \\ m = 5 & x = 5 & y^m = 32 = 2^5 \\ m = 7 & x = 11 & y^m = 128 = 2^7 \end{array}$$

Conjecture [J.H.E.Cohn, 1993]: there are no more solutions.

Previous results

- The only solution with m even is clearly $3^2 + 7 = 4^2 = 2^4$
- [Cohn 1993] no solutions with y odd
- [Cohn 1993] no more solutions with $m = 3$

So from now on we assume that $\gcd(6, m) = 1$ and y is even.

In a 1998 paper (J. Number Th.), Lesage showed

- for $m = 5, 7$ there are no more solutions;
- for m prime, $11 \le m \le 5000$, there are no solutions;
- for $m > 6.6 \cdot 10^{15}$ there are no solutions

Main result

Theorem (SS, JEC). *$x^2 + 7 = y^p$ has no solutions for p prime, $11 \leq p \leq 10^8$.*

We treat each prime p independently, and have an algorithm to eliminate each p quickly (but there are a lot of p...).

Moreover, Lesage's upper bound implies:

Corollary. *If $x^2 + 7 = y^m$ with $x \in \mathbb{Z} \setminus \{1, 3, 5, 11, 181\}$, then m is prime and $10^8 < m < 6.6 \cdot 10^{15}$.*

Eliminating small m

For $m = 3, 5, 7$ we use classical techniques to reduce to Thue equations.

Set $\rho = (1 + \sqrt{-7})/2$. Using unique factorization in $\mathbb{Z}[\rho]$ we easily obtain

$$\frac{1}{2}(x - 1) + \rho = \rho^{m-2}(u + v\rho)^m$$

with $u, v \in \mathbb{Z}$. For $m = 3$, this gives

$$u^3 + 3u^2v - 3uv^2 - 3v^3 = 1$$

whose only solutions (using Kant or Magma) are $(u, v) = (1, 0), (-2, 3)$. The cases $m = 5, 7$ are similar; the Thue equations to be solved have degree m.

Eliminating very large m

A 1976 theorem of Schinzel and Tijdeman implies the existence of an effectively computable constant C such that for all solutions to the equation $x^2 + 7 = y^m$ with $m > 1$ and $|y| > 1$ we have $m < C$.

Finding an explicit value for C involves estimating linear forms in three complex logarithms. Using this method, Lesage obtained the upper bound $m < 6.6 \cdot 10^{15}$.

Eliminating individual primes m

Let $p > 7$ be a prime. To show that the equation has no solutions with $m = p$, we use a variant of the Frey curve $+$ level-lowering method, following quite closely a similar use of the method by Kraus. A recent paper by Bennett and Skinner shows how to handle many trinomial equations using this strategy.

The method is similar to that used in proving FLT, except that the level-lowering does not take one down to level 2, where there are no weight two cuspforms, but to level 14, where there is one. So we need to use the arithmetic of the unique (up to isogeny) curve of conductor 14.

The elliptic curves

From now on, p denotes a prime ≥ 11, and x, y are integers satisfying $x^2 + 7 = y^p$, and (w.l.o.g.) $x \equiv 1 \pmod 4$, y even.

- The Frey curve:

$$E_{x,y} : \qquad Y^2 = X^3 + xX^2 + \frac{y^p}{4}X$$

has minimal discriminant $\Delta = -7y^{2p}2^{-12}$
and conductor $N = \prod_{l|14y} l$.

- The base curve of conductor 14:

$$E(= 14A1) : \qquad Y^2 + XY + Y = X^3 + 4X - 6$$

The Galois representations

Let ρ_p^E and $\rho_p^{x,y}$ denote the mod-p Galois representations associated to the curves E and $E_{x,y}$ respectively.

Let $a_l(E)$ and $a_l(E_{x,y})$ denote the Trace of Frobenius of E (resp. $E_{x,y}$) at the prime l.

Lemma. *1.* $\rho_p^E \cong \rho_p^{x,y}$*;*

2. $a_l(E_{x,y}) \equiv a_l(E) \pmod{p}$ *for all primes* $l \nmid N$*;*

3. $a_l(E_{x,y}).a_l(E) \equiv l+1 \pmod{p}$ *for all primes* $l \mid y, l \neq 2, 7$*.*

Proof of the lemma

- $E_{x,y}$ is semistable, and by Wiles et al., $E_{x,y}$ is modular.
- Since $p \geq 11$, by Mazur the representation $\rho_p^{x,y}$ is surjective (onto $\mathrm{GL}(2,p)$).
- Ribet's level-lowering theorem now implies that $\rho_p^{x,y}$ is isomorphic to some ρ_f attached to a new weight 2 cuspform f at level 14.
- Since $\dim(S_2(\Gamma_0(14))) = 1$ there is only one such f, and $\rho_f = \rho_p^E$ as defined above.
- This gives (1), from which (2) follows, as does (3) (cf. Kraus-Oesterlé 1992).

Kraus's method

Choose a prime $q = np + 1$. Then y^p is either 0 or an nth root of unity in $\mathbb{F}_q$.

List all $x \in \mathbb{F}_q$ such that $x^2 + 7$ is 0 or an nth root of unity.

Compute $a_q(E_{x,y})$ and compare with $a_q(E)$ for each x in the list. If the conclusions of the Lemma fail, reject x.

If all x have been eliminated, our equation has no solutions with exponent p.

Otherwise, try a new prime $q \equiv 1 \pmod{p}$.

The algorithm

Theorem. *Let E be as above and $p \geq 11$. Suppose that there exists $n \geq 2$ such that all of the following hold:*

- $q = np + 1$ *is prime;*
- *either* $a_q(E)^2 \not\equiv 4 \pmod{p}$ *or* $\left(\frac{-7}{q}\right) = -1$;
- *for all* $z \in \mathbb{F}_q$ *such that* $z^n = 1$ *and* $\left(\frac{z-7}{q}\right) \neq -1$, *we have*

$$a_q(z)^2 \not\equiv a_q(E)^2 \pmod{p}.$$

Then $x^2 + 7 = y^p$ *has no solutions.*

The algorithm (continued)

Here, $a_q(z)$ is the Trace of Frobenius of the curve (over $\mathbb{F}_q$)

$$E_z : \qquad Y^2 = X^3 + xX^2 + \frac{z}{4}X$$

where $x^2 \equiv z - 7 \pmod{q}$, so that $E_z \equiv E_{x,y} \pmod{q}$ where $y^p \equiv z \equiv x^2 + 7$.

The computation and results

A simple Pari/GP program was written to implement the search for a suitable q, for each p, satisfying the conditions of the preceding Theorem.

In about 4 days all $p < 10^8$ were eliminated. We also covered the ranges $10^k < p < 10^k + 1000$ for $8 \leq k \leq 20$.

The largest value of n required was $n = 284$, for $p = 73342163$.

N.B. Lesage's program, based on his method, took "une douzaine de jours" for $p < 5000$, and 4 hours for $p < 1000$. By comparison, our method takes 6.13s and 1.26s for these ranges. Even for primes up to 10^{15}, each prime only takes between 0.1s and 2s – but there are too many to cover all the range up to $6.6 \cdot 10^{15}$.

Conclusion

It seems very likely that Cohn's conjecture is true, and we are tantalizingly close to settling it.

It seems most likely that an improvement in the results on lower bounds for linear forms in three logarithms will be required – which we are happy to leave to others!