ACTA ARITHMETICA
LXXXVI.3 (1998)

Some diophantine equations of the form $x^n + y^n = z^m$

by

Bjorn Poonen (Berkeley, Calif.)

1. Introduction. Let m and n be positive integers. A solution $(x, y, z) \in \mathbb{Z}^3$ to the equation $x^n + y^n = z^m$ will be called *primitive* if $\gcd(x, y, z) = 1$. A solution (x, y, z) will be called *trivial* if xyz is in $\{-1, 0, 1\}$. The purpose of this paper is to complete the proof of the following two theorems.

Theorem 1. *The equation $x^n + y^n = z^2$ has no nontrivial primitive solutions for $n \geq 4$.*

Theorem 2. *Assume the Shimura–Taniyama conjecture. Then the equation $x^n + y^n = z^3$ has no nontrivial primitive solutions for $n \geq 3$.*

We say "complete" because Darmon and Merel [DM] have proved both theorems ([1]) for prime $n \geq 7$, by applying the Shimura–Taniyama conjecture to Frey curves. (The Frey curves arising in their proof for Theorem 1 have semistable reduction at 3 and 5, and the Shimura–Taniyama conjecture for such elliptic curves had already been settled by Diamond's extension of the results of Wiles, Taylor–Wiles, etc.)

Since the truth of either theorem for a given n implies its truth for any multiple of n, we are left with only the cases $n = 4, 5, 6, 9$ in Theorem 1 and $n = 3, 4, 5$ in Theorem 2. The cases $n = 4$ and $n = 6$ in Theorem 1 are due to Fermat and Euler, respectively. The cases $n = 3$ and $n = 4$ in Theorem 2 are due to Euler and Lucas, respectively. (See [DM] for references and more historical details.) Therefore the only equations remaining to be treated are

$$x^9 + y^9 = z^2, \quad x^5 + y^5 = z^2, \quad x^5 + y^5 = z^3.$$

1991 *Mathematics Subject Classification*: Primary 11D41; Secondary 11G05, 11G30.
Key words and phrases: generalized Fermat equation, diophantine equations, descent.
This research was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship while the author was at Princeton University.

([1]) They prove a third theorem as well, that $x^n + y^n = 2z^n$ has no nontrivial primitive solutions once $n \geq 3$. The small exponent cases of this equation had already been solved by Dénes [De, Satz 9].

We have listed these in order of increasing difficulty, which is also the order in which we will tackle them.

For the most part, the method we use is the standard 2-descent for elliptic curves. But for the last equation, we will use the explicit descent recently developed by Schaefer for curves of the form $y^p = f(x)$, to find the rank of a certain 3-dimensional Jacobian. (See also [PS] for a further generalization of this method.) Once that is done, we will need to find the Mordell–Weil group of a 2-dimensional quotient A, without having an equation for a curve of which A is the Jacobian ([2]). Although the theory behind these techniques is certainly not new, carrying them out in a practical amount of time will require some tricks (see the final paragraph, for example) and use of GP-PARI ([3]). We hope and expect that these methods will be useful not only for solving other generalized Fermat equations, but also for explicitly determining rational solutions to other diophantine equations.

REMARK. The equations $x^n + y^n = z^2$ for $n \leq 3$, and $x^n + y^n = z^3$ for $n \leq 2$ each have infinitely many nontrivial primitive solutions. See [Be] for a general procedure for parameterizing the solutions of such equations.

2. The equation $x^9+y^9 = z^2$. Suppose (x, y, z) is a nontrivial primitive solution to $x^9 + y^9 = z^2$. Then the factors $x^3 + y^3$ and $x^6 - x^3y^3 + y^6$ of the left hand side are nonzero. If a prime p divides both of them, p also divides $3x^6$ and $3y^6$, but $\gcd(x, y) = 1$, so p can only be 3. Thus from unique factorization we obtain

$$\varepsilon v^2 = x^6 - x^3y^3 + y^6 \tag{1}$$

where $\varepsilon = \pm 1$ or ± 3, and $v \in \mathbb{Z}$. Then $(U, V) = (x/y, v/y^3)$ is a rational point on the genus 2 curve

$$\varepsilon V^2 = U^6 - U^3 + 1. \tag{2}$$

Since the right hand side is positive for $U \in \mathbb{R}$, ε must be 1 or 3.

The curve (42) admits two involutions other than the hyperelliptic one: $(U, V) \mapsto (1/U, V/U^3)$ and $(U, V) \mapsto (1/U, -V/U^3)$. The corresponding quotients are elliptic curves birational to

$$\varepsilon Y^2 = X^3 - 21X + 37 \tag{3}$$

and

$$\varepsilon Y^2 = X^3 - 9X + 9, \tag{4}$$

respectively.

([2]) Actually we will prove only $\#A(\mathbb{Q}) \leq 2$, which will suffice for our purposes.

([3]) In fact, it is not even clear from the beginning that the methods will succeed; we will need certain Mordell–Weil ranks to be zero, or at least not too large.

For $\varepsilon = 1$, (43) is curve $324A1$ in Cremona's tables [Cr], and has rank 0 and torsion subgroup of order 3. Hence when $\varepsilon = 1$, the curve (41) has at most six rational points. On the other hand, it is easy to list six points: those with $U = 0$, $U = 1$, and $U = \infty$. Therefore these are all. They give rise only to trivial solutions (x, y, z).

Similarly for $\varepsilon = 3$, (44) is curve $324A2$ in [Cr], which has rank 0 (it is isogenous to curve $324A1$) and trivial torsion subgroup. Hence when $\varepsilon = 3$, the curve (41) has at most two rational points. We can list two: those with $U = -1$. But again, these give rise only to trivial solutions (x, y, z).

3. The equation $x^5 + y^5 = z^2$. Suppose that (x, y, z) is a nontrivial primitive solution to $x^5+y^5 = z^2$. As in Section 2, using unique factorization in $\mathbb{Z}$, we have

$$\begin{cases} x + y = \varepsilon w_1^2, \\ x^4 - x^3y + x^2y^2 - xy^3 + y^4 = \varepsilon w_2^2, \end{cases}$$

where $\varepsilon = \pm 1$ or ± 5 and $\gcd(w_1, w_2) = 1$. Looking at the second equation over $\mathbb{R}$ rules out the cases $\varepsilon = -1$ or -5. If $\varepsilon = 5$, then we obtain a rational point with X-coordinate x/y on the genus 1 curve

$$5Y^2 = X^4 - X^3 + X^2 - X + 1. \tag{5}$$

This curve has a rational point $(-1, 1)$, so it is an elliptic curve, and in fact it is birational to the curve $200D1$ in [Cr]. Its Mordell–Weil rank is 0, and its torsion subgroup has order 2, so the only points on (45) are those with $X = -1$. Therefore from now on, we may assume that $\varepsilon = 1$.

Let ζ be a primitive 5th root of unity, and let $\mathcal{O} = \mathbb{Z}[\zeta]$. We may factor $x^5 + y^5$ over $\mathbb{Q}(\zeta)$ into $x + \zeta y$ and $x^4 - \zeta x^3y + \zeta^2x^2y^2 - \zeta^3xy^3 + \zeta^4y^4$. If a prime π in this number field divides both factors, then as before it must divide 5; i.e., it must be the prime $1-\zeta$. The class number of $\mathbb{Q}(\zeta)$ is 1, and its unit group modulo squares is generated by -1 and $\tau := (1 + \sqrt{5})/2$, so that

$$\begin{cases} x + \zeta y = \delta v_1^2, \\ x^4 - \zeta x^3y + \zeta^2x^2y^2 - \zeta^3xy^3 + \zeta^4y^4 = \delta v_2^2, \end{cases}$$

where $v_1, v_2 \in \mathcal{O}$ and $\delta = \pm\tau^i(1 - \zeta)^j$ for some $i, j \in \{0, 1\}$. If $j = 1$, then $x+\zeta y$ is divisible by $1-\zeta$, and then so is $x+y = (x+\zeta y)+y(1-\zeta)$. But $x+y$ is an integer, so this means that 5 divides $x+y$. Also $x^4-x^3y+x^2y^2-xy^3+y^4$ equals $5x^4$ modulo $x + y$, so $x^4 - x^3y + x^2y^2 - xy^3 + y^4$ is divisible by 5, contradicting $\varepsilon = 1$. Thus $j = 0$. Now, working in $\mathcal{O}/4\mathcal{O}$, and checking all $x, y \in \{0, 1, 2, 3\}$ such that $\gcd(x, y, 2) = 1$ and such that $x + y$ is a square modulo 4, we find that $x + \zeta y$ can equal δ times a square in $\mathcal{O}$ modulo 4 for $\delta = \pm\tau^i$ only if $\delta = 1$.

Thus we find a $\mathbb{Q}(\zeta)$-rational point P with X-coordinate $x/(\zeta y)$ on the elliptic curve

$$E: \quad Y^2 = X^4 - X^3 + X^2 - X + 1. \tag{6}$$

(We choose $(0,1)$ as origin on E.) Its minimal Weierstrass model is

$$Y^2 = (X+2)(X^2 - X - 1). \tag{7}$$

Let us compute the group $E(\mathbb{Q}(\zeta))$. Let $K = \mathbb{Q}(\sqrt{5})$, $\beta = -(5+\sqrt{5})/2$. Since $\mathbb{Q}(\zeta) = K(\sqrt{\beta})$, the rank of $E(\mathbb{Q}(\zeta))$ is the sum of the ranks of $E(K)$ and $E_\beta(K)$, where E_β denotes the β-twist of E. In turn, the rank of $E(K)$ is the sum of the ranks of $E(\mathbb{Q})$ and $E_5(\mathbb{Q})$ where E_5 is the 5-twist of E. These last two curves are $200B1$ and $200D1$ in [Cr], and they have ranks 1 and 0, respectively. The point $(-1,1)$ on (47) is a generator modulo torsion.

We now compute the rank of $E_\beta(K)$. Factoring the right hand side of (47) over K, we find that E_β has a model

$$E_\beta: \quad Y^2 = X(X-1)(X+\tau) \tag{8}$$

over K. Let ∞_1 and ∞_2 denote the real places of K for which $\sqrt{5}$ is positive and negative, respectively. Let $S = \{\infty_1, \infty_2, 2\}$. Note that E_β has good reduction outside S. Let $(K^\times/K^{\times 2})_S$ denote the subgroup of $K^\times/K^{\times 2}$ represented by elements α such that $\mathrm{ord}_v(\alpha)$ is even for all $v \notin S$. In our case, -1, τ, and 2 represent a basis for $(K^\times/K^{\times 2})_S$. Then we have the usual 2-descent homomorphism

$$\begin{aligned} \phi : E_\beta(K)/2E_\beta(K) &\to (K^\times/K^{\times 2})_S \times (K^\times/K^{\times 2})_S, \\ (X,Y) &\mapsto (X, X-1). \end{aligned} \tag{9}$$

One must use a special formula for some of the 2-torsion points: ϕ maps the identity on E_β to $(1,1)$, the point $(0,0)$ to $(-\tau,-1)$, and the point $(1,0)$ to $(1,1)$. In particular, the point $(1,0)$ is a double in $E_\beta(K)$: in fact, it is the double of the 4-torsion point $(1+\tau, 1+2\tau)$, which is mapped by ϕ to $(1,\tau)$.

Let $\mathbb{R}_i$ denote the completion of K at ∞_i. Since E_β has all its 2-torsion defined over $\mathbb{R}_i$, the $\mathbb{F}_2$-dimension of $E_\beta(\mathbb{R}_i)/2E_\beta(\mathbb{R}_i)$ is 1, and any point on the real component not containing the origin will be a generator. For $\mathbb{R}_1$, $-\tau < 0$, so we may take any point with X-coordinate between $-\tau$ and 0 as generator. The image of the local descent homomorphism

$$E_\beta(\mathbb{R}_1)/2E_\beta(\mathbb{R}_1) \to \mathbb{R}_1^\times/\mathbb{R}_1^{\times 2} \times \mathbb{R}_1^\times/\mathbb{R}_1^{\times 2} \tag{10}$$

is hence generated by $(-1,-1)$. Similarly, for $\mathbb{R}_2$, $0 < -\tau < 1$, so we may take a point with X-coordinate between 0 and $-\tau$, and the image of

$$E_\beta(\mathbb{R}_2)/2E_\beta(\mathbb{R}_2) \to \mathbb{R}_2^\times/\mathbb{R}_2^{\times 2} \times \mathbb{R}_2^\times/\mathbb{R}_2^{\times 2} \tag{11}$$

is generated by $(1,-1)$.

Let K_2 denote the completion of K at the (inert) prime 2. If $(X, Y) \in E_\beta(K_2)$ and the 2-adic valuation of X is nonnegative, then at most one of X, $X-1$, $X+\tau$ can be divisible by 2, so the valuations of X and $X-1$ must be even in order for $X(X-1)(X+\tau)$ to be a square. Similarly if the 2-adic valuation of X is negative, then it equals the 2-adic valuations of $X-1$ and $X+\tau$, and all three must be even. Thus the image of

$$E_\beta(K_2)/2E_\beta(K_2) \to K_2^\times/K_2^{\times 2} \times K_2^\times/K_2^{\times 2} \tag{12}$$

is contained in the subgroup on the right with even 2-adic valuation in each component.

The only elements of $(K^\times/K^{\times 2})_S \times (K^\times/K^{\times 2})_S$ that can map into the local images of (410), (411), and (412) are $(1,1)$, $(1,\tau)$, $(-\tau,-1)$, and $(-\tau,-\tau)$. Thus the 2-Selmer group of E_β over K is at most 2-dimensional over $\mathbb{F}_2$. On the other hand, all the 2-torsion of E_β is defined over K, so the torsion subgroup of $E_\beta(K)$ already surjects onto this 2-dimensional group. Hence $E_\beta(K)$ has rank 0.

The rank of $E(\mathbb{Q}(\zeta))$ is then $1+0+0=1$, and the group $E(\mathbb{Q})$ modulo torsion must be of 2-power index in $E(\mathbb{Q}(\zeta))$ modulo torsion. We check that neither $(-1,1)$ nor its translate $(3,-5)$ by the nontrivial torsion point in $E(\mathbb{Q})$ are doubles in $E(\mathbb{Q}(\zeta))$. Hence $(-1,1)$ is a generator of $E(\mathbb{Q}(\zeta))$ modulo torsion.

We next calculate the torsion subgroup of $E(\mathbb{Q}(\zeta))$. Note that E is isomorphic to E_β over $\mathbb{Q}(\zeta)$, and we already know that E_β has at least 8 torsion points over $\mathbb{Q}(\zeta)$ (all the 2-torsion, and a 4-torsion point). On the other hand, the reduction of E at a degree 1 prime of $\mathbb{Q}(\zeta)$ above 11 is an elliptic curve over $\mathbb{F}_{11}$ with 16 points, and the reduction at a prime above 41 has 40 points, so the torsion subgroup of $E(\mathbb{Q}(\zeta))$ has order exactly 8.

Let σ denote the nontrivial automorphism in $\mathrm{Gal}(\mathbb{Q}(\zeta)/K)$, which in particular takes ζ to ζ^{-1}. Since the generator of the free part of $E(\mathbb{Q}(\zeta))$ and all the 2-torsion are defined over K, the entire group $E(\mathbb{Q}(\zeta))$ is mapped by $\sigma-1$ into a $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$-stable group of order at most 2 (in fact, exactly 2). The only such nontrivial group is generated by the 2-torsion point in $E(\mathbb{Q})$. In particular, $P^\sigma - P$ is either trivial or this 2-torsion point. Translation by this 2-torsion point in the original model (46) is given by the map

$$(X, Y) \mapsto (1/X, -Y/X^2),$$

as can be seen from the fact that this map is an involution defined over $\mathbb{Q}$ without a fixed point. Since P has X-coordinate $x/(\zeta y)$, we find that $x/(\zeta^{-1}y) = x/(\zeta y)$ or $x/(\zeta^{-1}y) = (\zeta y)/x$. Each possibility gives rise only to trivial solutions to our original equation.

4. The equation $x^5 + y^5 = z^3$. Suppose that (x, y, z) is a nontrivial primitive solution to $x^5 + y^5 = z^3$. If a prime p divides both factors $x + y$

and $x^4 - x^3y + x^2y^2 - xy^3 + y^4$ of the left hand side, it also divides $5x^4$ and $5y^4$, but $\gcd(x, y) = 1$, so $p = 5$. Hence, by unique factorization, we find

$$x + y = mv^3 \tag{13}$$

where $m \in \{1, 5, 5^2\}$ and $v \in \mathbb{Z}$. Multiplying by $x^5 + y^5 = z^3$ and dividing by y^6, we find a point $(U, V) = (x/y, vz/y^2)$ on the genus 3 curve

$$C_m : \quad (U + 1)(U^5 + 1) = mV^3$$

(depending on m). This curve has an involution $(U, V) \mapsto (1/U, V/U^2)$, and the quotient is the elliptic curve

$$E_m : \quad Y^2 = X^3 + 2000m^2.$$

The quotient map, which is determined up to sign by decreeing that $(U, V) = (-1, 0)$ will map to the point at infinity, is

$$\begin{aligned} &\psi : C_m \to E_m, \\ &(U, V) \mapsto \left(\frac{20mV}{(U + 1)^2}, \frac{-100m(U^2 + 1)}{(U + 1)^2} \right). \end{aligned} \tag{14}$$

(The Weierstrass model for E_m and the formula for the quotient map were found with help from Mark van Hoeij's Maple package `IntBasis`, but of course they could easily be computed by hand as well.)

The elliptic curve E_5 is curve $675E1$ in [Cr], which has trivial Mordell–Weil group. It follows that the only rational point on C_5 is $(U, V) = (-1, 0)$. Unfortunately, the elliptic curves E_1 and E_{25} (which are curves $675A1$ and $225A1$, respectively, in [Cr]) have rank 1, so additional work will be required to handle the cases $m = 1$ and $m = 25$.

As in Section 3, let ζ denote a primitive 5th root of unity, let $\mathcal{O} = \mathbb{Z}[\zeta]$, let $\tau = -(\zeta^2 + \zeta^3) = (1 + \sqrt{5})/2$, and let $K = \mathbb{Q}(\sqrt{5})$. Also let $\beta = -(5 + \sqrt{5})/2$, so that $\mathbb{Q}(\zeta) = K(\sqrt{\beta})$, and let σ be the nontrivial automorphism in $\mathrm{Gal}(\mathbb{Q}(\zeta)/K)$. If a prime π of $\mathbb{Q}(\zeta)$ divides both $x + \zeta y$ and $x^4 - \zeta x^3y + \zeta^2x^2y^2 - \zeta^3xy^3 + \zeta^4y^4$, then it also divides $5x^4$ and $5\zeta^4y^4$, but $\gcd(x, y) = 1$, so π can only be the prime $1 - \zeta$ above 5. Since the class number of $\mathbb{Q}(\zeta)$ is 1, we must have $x + \zeta y = \varepsilon(1 - \zeta)^k u^3$ for some $\varepsilon \in \mathcal{O}^\times$, $u \in \mathbb{Q}(\zeta)^\times$, and $k \in \{0, 1, 2\}$. The unit group $\mathcal{O}^\times$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ with the free part generated by τ, so all roots of unity are cubes, and $1 - \zeta$ is equivalent to 5 modulo cubes, and we obtain

$$x + \zeta y = 5^i \tau^j w^3 \tag{15}$$

for some $w \in \mathbb{Q}(\zeta)^\times$ and $i, j \in \{0, 1, 2\}$. By taking norms of (415) and comparing with $x^5 + y^5 = z^3$, we find that $5^{4i}m$ must be a cube, where m is as in (413). In particular, we need only consider the cases $i = 0$ (i.e., $m = 1$) and $i = 1$ (i.e., $m = 25$).

We now eliminate the possibility $j = 2$ by local considerations. Since $x, y \in \mathbb{Z}$, the element w must be integral away from the prime $1 - \zeta$. The left hand side of (415) modulo 2 is either a cube (if x or y is even) or $1 + \zeta$ (if x and y are both odd), which is τ times a cube (modulo 2), so we see that $j = 0$ or $j = 1$.

Multiplying (415) by $x^5 + y^5 = z^3$ and dividing by $(\zeta y)^6$, we find a $\mathbb{Q}(\zeta)$-rational point $S := (U, V) = \left(\frac{x}{\zeta y}, \frac{wz}{\zeta^2 y^2}\right)$ on

$$C_\eta : \quad (U + 1)(U^5 + 1) = \eta V^3,$$

with $\eta = 5^i \tau^j$. This point maps down to a $\mathbb{Q}(\zeta)$-rational point P on the elliptic curve

$$E_\eta : \quad Y^2 = X^3 + 2000\eta^2.$$

Then $P^\sigma + P$ is a K-rational point on E_η, and $P^\sigma - P$ corresponds to a K-rational point on the β-twist, E_η^β. Our hope (which, as it turns out, will not be fully realized) is that for each η, one of these elliptic curves will have rank 0 over K.

First suppose $i = j = 0$, so $\eta = 1$. We know already that $E_1(K)$ has positive rank (since even $E_1(\mathbb{Q})$ has positive rank), so we now compute the Mordell–Weil rank of

$$E_1^\beta : \quad Y^2 = X^3 + 2000\beta^3$$

over K using 2-descent. This time, however, there are no K-rational 2-torsion points, so we will follow the more general descent outlined in [Ca]. Let $f(T) = T^3 + 2000\beta^3$, and let $L = K[T]/(f(T))$, which is a number field. Let S be a set of places of K including the (inert) prime 2, the infinite places, and the places of bad reduction for E_1^β. Let $(L^\times/L^{\times 2})_S$ denote the subgroup of $L^\times/L^{\times 2}$ represented by elements l of $L^\times$ such that the extension $L(\sqrt{l})$ of L is unramified outside places of L above those in S. Also let $L_\pi = L \otimes_K K_\pi$ for each completion K_π of K. Then there is an injective homomorphism

$$E_1^\beta(K)/2E_1^\beta(K) \hookrightarrow \ker(L^\times/L^{\times 2} \xrightarrow{\text{Norm}} K^\times/K^{\times 2})$$

whose image is also contained in the subgroup of elements of $(L^\times/L^{\times 2})_S$ which map down in $L_\pi^\times/L_\pi^{\times 2}$ into the images of the corresponding local injective homomorphisms

$$E_1^\beta(K_\pi)/2E_1^\beta(K_\pi) \hookrightarrow \ker(L_\pi^\times/L_\pi^{\times 2} \xrightarrow{\text{Norm}} K_\pi^\times/K_\pi^{\times 2}) \tag{16}$$

for each $\pi \in S$. In fact, these conditions characterize a subgroup isomorphic to the 2-Selmer group of E_1^β over K.

In our case, L has class number 1, and $S = \{\infty_1, \infty_2, 2, 3, \sqrt{5}\}$, so the group $(L^\times/L^{\times 2})_S$ has as basis a generator for the roots of unity in L, generators of the unit group of L modulo torsion, and generators of the primes of L above the finite primes in S. (Of course, we are free to change these

generators by squares.) The primes 2 and 3 of K totally ramify in L, while the prime $\sqrt{5}$ is unramified and splits into two primes, π_5 and π_5', of degrees 1 and 2, respectively. Hence we obtain the following basis for $(L^\times/L^{\times 2})_S$:

$$(L^\times/L^{\times 2})_S = \langle -1, u_1, u_2, u_3, 2, 3, \sqrt{5}, \pi_5' \rangle.$$

(Here u_1, u_2, and u_3 are the three generators for the unit group modulo torsion given by PARI.) By calculating the norms of these eight elements, we find

$$\ker((L^\times/L^{\times 2})_S \xrightarrow{\text{Norm}} K^\times/K^{\times 2}) = \langle -u_2, -u_3, -u_1\pi_5' \rangle. \tag{17}$$

The 2-torsion subgroup of $E_1^\beta(K_2)$ is trivial. Since multiplication-by-2 is an injective endomorphism on the compact group $E_1^\beta(K_2)$ which locally multiplies Haar measure by $2^{[K:\mathbb{Q}]}$, the $\mathbb{F}_2$-dimension of $E_1^\beta(K_2)/2E_1^\beta(K_2)$ is 2. Since $f(1)$ and $f(\tau^2)$ are units in K_2 congruent to 1 and τ^6 modulo 8, they are squares in K_2, and hence there are points Q and R in $E_1^\beta(K_2)$ with X-coordinates 1 and τ^2, respectively. With help from PARI's function `zideallog`, we check that the images of Q and R under (416) are $\mathbb{F}_2$-independent, so Q and R are generators of $E_1^\beta(K_2)/2E_1^\beta(K_2)$. The only nontrivial element in the subgroup (417) which maps in $L_2^\times/L_2^{\times 2}$ into the image of $E_1^\beta(K_2)/2E_1^\beta(K_2)$ is u_2u_3. It turns out that the local information from the places 3, ∞_1, and ∞_2 does not rule out u_2u_3 as a potential image of a point in $E_1^\beta(K)$, but this is irrelevant, since the information at $\sqrt{5}$ will rule it out, as we now explain.

The $\mathbb{F}_2$-dimension of $E_1^\beta(K_{\sqrt{5}})/2E_1^\beta(K_{\sqrt{5}})$ equals that of the 2-torsion subgroup defined over $K_{\sqrt{5}}$ (since multiplication-by-2 is now locally Haar measure preserving), and this is 1. There exists a point in $E_1^\beta(K_{\sqrt{5}})$ with X-coordinate $-10\sqrt{5}$ and it generates $E_1^\beta(K_{\sqrt{5}})/2E_1^\beta(K_{\sqrt{5}})$ since its image in $L_{\sqrt{5}}^\times/L_{\sqrt{5}}^{\times 2}$ has an odd valuation in the component corresponding to the degree 2 prime π_5'. On the other hand, the unit u_2u_3 has trivial valuation in this component, but is also not a square in $L_{\sqrt{5}}$, so it does not map into the image of (416) for $\pi = \sqrt{5}$. Thus the 2-Selmer group of E_1^β over K is trivial. Hence $E_1^\beta(K)$ is of rank 0. The reduction at the prime $4+\sqrt{5}$ above 11 has 12 points, and the reduction at the prime $1+2\sqrt{5}$ above 19 has 13 points, so in fact $E_1^\beta(K)$ is trivial. Thus the point $P \in E_1(\mathbb{Q}(\zeta))$ coming from our solution to $x^5+y^5=z^3$ must equal P^σ, and the point $S \in C_1(\mathbb{Q}(\zeta))$ must equal S^σ or its image under the involution. Looking at the U-coordinates, we obtain

$$\frac{x}{\zeta y} = \frac{x}{\zeta^{-1}y} \quad \text{or} \quad \frac{x}{\zeta y} = \left(\frac{x}{\zeta^{-1}y}\right)^{-1},$$

and these equations give rise only to trivial solutions. This completes the proof for the case $i = j = 0$.

Next suppose that $i = 0$ and $j = 1$, so $\eta = \tau$. The elliptic curve $E_\tau^\beta(K)$ has positive rank. (In fact, the point $(50 + 10\sqrt{5}, 250 + 50\sqrt{5})$ has infinite order, and the rank is exactly 1.) Luckily, though, $E_\tau(K)$ is of rank 0, as we now prove. We will use the model

$$E' : \quad Y^2 = X^3 + 16\tau^2$$

for E_τ (we have divided the constant term by the sixth power of $\sqrt{5}$), since then we see that S need only include 2, 3, and the infinite places. Redefine L as $K[T]/(T^3 + 16\tau^2)$, which is again a number field. The class number of L is 1, and

$$(L^\times/L^{\times 2})_S = \langle -1, u_1, u_2, u_3, 2, 3\rangle$$

where u_1, u_2, u_3 are generators for the unit group modulo torsion. Intersecting with the kernel of the norm reduces this to $\langle u_2, u_3\rangle$. Again $E'(K_2)/2E'(K_2)$ is generated by points with X-coordinates 1 and τ^2, but this time their images in $L_2^\times/L_2^{\times 2}$ together with those of u_2 and u_3 are already independent, so the 2-Selmer group of E' over K is trivial, and $E'(K)$ has rank 0. The reduction at $\sqrt{5}$ has 6 points, and the absolute ramification index of $\sqrt{5}$ is less than $5 - 1$, so $\#E'(K)$ divides 6. All nonzero 2-torsion points of E' are defined over extensions of K which are ramified above 2, so $\#E'(K)$ divides 3. In fact, the order is exactly 3: $E'(K) = \{O, (0, 4\tau), (0, -4\tau)\}$.

The point P on E_τ coming from the solution to $x^5 + y^5 = z^3$ has Y-coordinate

$$\frac{-100\tau(x^2 + \zeta^2 y^2)}{(x + \zeta y)^2}.$$

The corresponding point P' on the model E' has Y-coordinate

$$\frac{(-10 + 2\sqrt{5})(r^2 + \zeta^2)}{(r + \zeta)^2},$$

where $r = x/y \in \mathbb{Q}$. (We have simply divided by $5^{3/2}$.) We know that $P' + P'^\sigma$ is either the identity or a point with X-coordinate 0. If the sum is the identity, then P' and P'^σ have opposite Y-coordinates:

$$\frac{(-10 + 2\sqrt{5})(r^2 + \zeta^2)}{(r + \zeta)^2} = -\frac{(-10 + 2\sqrt{5})(r^2 + \zeta^{-2})}{(r + \zeta^{-1})^2}.$$

The solutions to this equation in r are $-\zeta^2$, $-\zeta^3$, $-\tau$, and $1 - \tau$, none of which are rational. By computing the sum of two generic points (x_0, y_0) and (x_1, y_1) on E', setting the numerator of the resulting X-coordinate equal to 0, combining with the equations $y_i^2 = x_i^3 + 16\tau^2$, and eliminating x_0 and x_1, we find a polynomial in y_0 and y_1 that vanishes whenever the sum of the two points has X-coordinate 0 or ∞. It is

$$g(y_0, y_1) := y_0^2 y_1^2 - (24 + 8\sqrt{5})(y_0^2 + y_1^2) - (192 + 64\sqrt{5})y_0 y_1 + (8064 + 3456\sqrt{5}).$$

The equation

$$g\left(\frac{(-10+2\sqrt{5})(r^2+\zeta^2)}{(r+\zeta)^2}, \frac{(-10+2\sqrt{5})(r^2+\zeta^{-2})}{(r+\zeta^{-1})^2}\right) = 0$$

has no rational solutions r. (In fact, there are not even any solutions in $\mathbb{Q}(\zeta)$.) Thus we have completed the proof for the case $i = 0$, $j = 1$.

The only remaining cases are those where $i = 1$. For the subcase $j = 0$, we find that $E_\eta(K)$ is trivial. But for the last subcase where $j = 1$, both $E_\eta(K)$ and $E_\eta^\beta(K)$ have rank 1, so the methods we have been using so far fail to resolve this last case ([4]). Nor do direct local considerations rule this subcase out. Therefore we try a different approach, one which, as it turns out, will rule out the entire case $i = 1$ at once.

Recall that $i = 1$ corresponds to $m = 25$, and that we could not immediately list all rational points on the genus 3 curve

$$C_{25}: \quad (U+1)(U^5+1) = 25V^3$$

by looking at its quotient

$$E_{25}: \quad Y^2 = X^3 + 2000 \cdot 25^2$$

because $E_{25}(\mathbb{Q})$ had rank 1. On the other hand, the Jacobian J of C_{25} has (at least) one other abelian variety as a factor, and we can hope to show that this other piece has Mordell–Weil rank 0. Define A to be the cokernel of the map $E_{25} \to J$ of Picard varieties induced by $C_{25} \to E_{25}$, so that A is a 2-dimensional abelian variety over $\mathbb{Q}$.

Since we do not have an explicit equation for a genus 2 curve whose Jacobian is isogenous to A, we will prove that $A(\mathbb{Q})$ has rank 0 by proving that $J(\mathbb{Q})$ has rank 1. In order to do this, we will need the 3-descent described in [Sc]. First note that C_{25} is isomorphic to the nonsingular plane quartic

$$C: \quad Y^3 = X^4 + 50X^3 + 1250X^2 + 15625X + 78125$$

via the map

$$(U, V) \to \left(-\frac{25}{U+1}, \frac{125V}{(U+1)^2}\right).$$

To do the descent we will need to work over the field $F = \mathbb{Q}(\zeta_3)$, where ζ_3 denotes a primitive cube root of unity. By identifying ζ_3 with the automorphism $(X, Y) \to (X, \zeta_3 Y)$ of C, we obtain an action of $\mathbb{Z}[\zeta_3]$ on J. Let ϕ denote the endomorphism $1 - \zeta_3$ of J, which is defined over F. Let

$$f(T) = T^4 + 50T^3 + 1250T^2 + 15625T + 78125$$

and let $L = F[T]/(f(T))$, which is isomorphic to the 15th cyclotomic field. Also let $L_\pi = L \otimes_F F_\pi$ for each completion F_π of F. The set $S = \{\sqrt{-3}, 5, \infty\}$

([4]) We omit the computations of these ranks since they will not be needed.

of places of F contains all places of bad reduction, all infinite places, and all places above 3. (The last is needed since we are doing a 3-descent.) We define $(L^\times/L^{\times 3})_S$ in the obvious way, as the subgroup of $L^\times/L^{\times 3}$ represented by elements l such that $L(\sqrt[3]{l})$ is unramified over L at places lying above places outside S. Then we have an injection

$$J(F)/\phi J(F) \hookrightarrow \ker(L^\times/L^{\times 3} \xrightarrow{\text{Norm}} F^\times/F^{\times 3})$$

and the image is contained in both $(L^\times/L^{\times 3})_S$ and in the subgroup mapping into the images of the local injections

$$J(F_\pi)/\phi J(F_\pi) \hookrightarrow \ker(L_\pi^\times/L_\pi^{\times 3} \xrightarrow{\text{Norm}} F_\pi^\times/F_\pi^{\times 3})$$

for each $\pi \in S$. These restrictions define a subgroup of $(L^\times/L^{\times 3})_S$ isomorphic to the ϕ-Selmer group of J over F. (See [Sc] for details.)

In our case, L has class number 1, and we have the following $\mathbb{F}_3$-basis for $(L^\times/L^{\times 3})_S$:

$$(L^\times/L^{\times 3})_S = \langle \zeta_3, u_1, u_2, u_3, \sqrt{-3}, 5\rangle,$$

where u_1, u_2, u_3 are generators for the unit group of $L = \mathbb{Q}(\zeta_{15})$ modulo torsion given by PARI. The subgroup H killed by the norm map from L to F is

$$H := \langle u_1, \zeta_3 u_2, \zeta_3^2 u_3\rangle.$$

Let ∞ denote the (rational) point at infinity on C. The group $J[\phi]$ of ϕ-torsion points is generated as an $\mathbb{F}_3$-vector space by the divisor classes $[W - \infty]$ where W is an affine point on C with $Y = 0$, and the only relation is that the sum of all four of these is zero. The action of Galois on these is the same as the action of Galois on the primitive 5th roots of unity. In particular, there are no nontrivial ϕ-torsion points defined over $F_{\sqrt{-3}}$. Since ϕ locally multiplies Haar measure on the compact group $J(F_{\sqrt{-3}})$ by $3^{\dim J} = 3^3$, we see that the $\mathbb{F}_3$-dimension of $J(F_{\sqrt{-3}})/\phi J(F_{\sqrt{-3}})$ is 3. Since $f(3) \equiv f(8) \equiv -1 \pmod 9$, there exist points $G_3, G_8 \in C(F_{\sqrt{-3}})$ with X-coordinates 3 and 8, respectively. Also, $f(4+\sqrt{2}) \equiv 1 \pmod 9$, so there exists a point $G_{4+\sqrt{2}}$ on C defined over the quadratic unramified extension of $F_{\sqrt{-3}}$. Let $G_{4-\sqrt{2}}$ denote the Galois conjugate of $G_{4+\sqrt{2}}$. Then we obtain the following three points in $J(F_{\sqrt{-3}})$:

$$\begin{aligned} D_1 &= [G_3 - \infty], \\ D_2 &= [G_8 - \infty], \\ D_3 &= [G_{4+\sqrt{2}} + G_{4-\sqrt{2}} - 2\infty]. \end{aligned}$$

These form an $\mathbb{F}_3$-basis, since their images in $L_{\sqrt{-3}}^\times/L_{\sqrt{-3}}^{\times 3}$ are independent. The only elements of H that map down in $L_{\sqrt{-3}}^\times/L_{\sqrt{-3}}^{\times 3}$ into the image of $J(F_{\sqrt{-3}})$ are the powers of u_1, which maps to the image of $D_1 + D_2$. Thus

the $\mathbb{F}_3$-dimension of the ϕ-Selmer group of J over F is at most 1, and hence the $\mathbb{Z}[\zeta_3]$-rank of $J(F)$ is at most 1. On the other hand, the automorphism ζ_3 on C descends to E_{25}, so the $\mathbb{Z}[\zeta_3]$-action on J preserves the subgroup E_{25}, and the $\mathbb{Z}[\zeta_3]$-rank of $E(F)$ must be positive, since the $\mathbb{Z}$-rank of $E(\mathbb{Q})$ is. Thus the $\mathbb{Z}[\zeta_3]$-rank of $A(F)$ is 0, and so is the $\mathbb{Z}$-rank of $A(\mathbb{Q})$.

Now that we know that $A(\mathbb{Q})$ is torsion, we find its order by looking at reductions. Since J is isogenous over $\mathbb{Q}$ to $E_{25} \times A$,

$$\#J(\mathbb{F}_p) = \#E_{25}(\mathbb{F}_p) \cdot \#A(\mathbb{F}_p)$$

for any prime p of good reduction for J. The order of $J(\mathbb{F}_p)$ is expressible in terms of $C(\mathbb{F}_p)$, $C(\mathbb{F}_{p^2})$, and $C(\mathbb{F}_{p^3})$, which we can compute by brute force, trying all values $x \in \mathbb{F}_{p^i}$ and counting the cube roots of $f(x)$ in that field. In fact, if $p \equiv 2 \pmod 3$, every element of $\mathbb{F}_p$ or of $\mathbb{F}_{p^3}$ is a cube, so it suffices to check whether $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(f(x))$ is a cube in $\mathbb{F}_p$ for each $x \in \mathbb{F}_{p^2}$. In this way, we find that $\#J(\mathbb{F}_{11}) = 2^3 \cdot 3^3 \cdot 7$ and $\#J(\mathbb{F}_{17}) = 2^3 \cdot 3^2 \cdot 79$. Since $j(E_{25}) = 0$, we have $\#E_{25}(\mathbb{F}_p) = p + 1$ for $p \equiv 2 \pmod 3$. Hence $\#A(\mathbb{F}_{11}) = 2 \cdot 3^2 \cdot 7$ and $\#A(\mathbb{F}_{17}) = 2^2 \cdot 79$, from which we deduce that $\#A(\mathbb{Q})$ divides 2.

If P is a rational point on C, then the point in $J(\mathbb{Q})$ represented by $2(P - \infty)$ maps to 0 in $A(\mathbb{Q})$, so it is the image of some point $Q \in E_{25}(\overline{\mathbb{Q}})$ under $E_{25} \to J$. By definition, this image of Q is the point on J represented by the divisor class of $R_1 + R_2 - 2\infty$, where R_1 and R_2 are the preimages of Q under $C \to E_{25}$. Thus $R_1 + R_2 - 2P$ is the divisor of a function f on C. If $P = R_1 = R_2$, then P is fixed by the involution on C, and the only such rational point is ∞, which corresponds to $(U, V) = (-1, 0)$ on the model C_{25}, and we are done, since this gives rise to only a trivial solution of $x^5 + y^5 = z^3$. Otherwise, f defines a nonconstant map from C to $\mathbb{P}^1$ of degree at most 2. This is a contradiction, because a nonsingular plane quartic curve is neither hyperelliptic nor rational.

Acknowledgements. I thank Henri Darmon and Loïc Merel for sharing these problems with me. I thank also Ed Schaefer, for some comments on a draft of this paper.

References

[Be] F. Beukers, *The Diophantine equation $Ax^p + By^q = Cz^r$*, Duke Math. J. 91 (1998), no. 1, 61–88.

[Ca] J. W. S. Cassels, *The Mordell–Weil group of curves of genus* 2, in: Arithmetic and Geometry, Vol. I, Progr. Math. 35, Birkhäuser, Boston, Mass., 1983, 27–60.

[Cr] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1992.

[DM] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. 490 (1997), 81–100.

[De] P. Dénes, *Über die Diophantische Gleichung* $x^l + y^l = cz^l$, Acta Math. 88 (1952), 241–251.

[PS] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. 488 (1997), 141–188.

[Sc] E. F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. 310 (1998), 447–471.

Department of Mathematics
University of California
Berkeley, California 94720-3840
U.S.A.
E-mail: poonen@math.berkeley.edu

Received on 4.3.1997 (3143)