The equation $x^4 - y^4 = z^p$

Henri Darmon

September 9, 2007

Let p be an odd prime. We consider the equation

$$x^4 - y^4 = z^p, \qquad \gcd(x, y) = 1. \tag{1}$$

When $p = 2$, this equation was considered by Fermat, who used it to prove his celebrated "last theorem" for exponent 4.

In [Po], Powell proved that this equation has no integer solutions with $p \not| xyz$ (analogous to the "first case" of Fermat's Last theorem) and proved a similar (slightly weaker) result for the equation $x^4 + y^4 = z^p$.

Terai and Osada [TO] and Cao [Ca] have extended this analysis to the equations $x^4 + dy^4 = z^p$ and $cx^4 + dy^4 = z^p$ respectively, proving that there are no first case solutions under certain assumptions.

The methods used by these authors involve factoring the left hand side of the equations over the appropriate quadratic field, and are close in spirit to the descent ideas which form the basis of Kummer's work on Fermat's Last Theorem.

Recently, it has been observed that Fermat's equation can be tackled by different methods based on elliptic curves and the Galois representations attached to them. Following work of Frey [Fr] and Serre [Sr2], Ribet [Ri] showed that the celebrated conjecture of Shimura and Taniyama that every elliptic curve is modular implies Fermat's last theorem. Thanks to the revolutionary work of Wiles, the Shimura Taniyama conjecture, previously thought to be inaccessible, now seems within reach.

Our main result is:

Theorem I: *Suppose the Shimura-Taniyama conjecture is true, and let* $p \geq 11$ *be a prime. Then:*

1. *Equation (1) has no non-trivial solution if* $p = 1 \mod 4$.
2. *Equation (1) has no non-trivial solution with* z *even.*

Proof: Let $p \geq 11$ be prime, and let

$$a^4 - b^4 = c^p$$

be a solution to equation (1). If c is odd, assume without loss of generality that a is odd and b is even (otherwise, interchange a and b and replace c by $-c$). Factorizing the left hand side of $a^4 - b^4 = c^p$, the assumption $\gcd(a, b) = 1$ forces the three factors

$$a + b, \quad a - b, \quad a^2 + b^2$$

to be pth powers up to powers of 2. Hence, so are the integers

$$\begin{aligned} A = (a+b)^2 &= a^2 + 2ab + b^2, \\ B = (a-b)^2 &= a^2 - 2ab + b^2, \\ C &= a^2 + b^2, \end{aligned}$$

which also satisfy the equation

$$A + B - 2C = 0.$$

This equation gives three integers that are "almost" p-th powers and sum up to 0, and suggests considering the Frey curve

$$E : y^2 = x(x + A)(x - B).$$

Expanding the right hand side, the equation for E becomes:

$$y^2 = x^3 + 4abx^2 - (a^2 - b^2)^2 x.$$

The j-invariant and discriminant of E are:

$$j = 2^6 \frac{(a^2 + 3b^2)^3 (3a^2 + b^2)^3}{c^{2p}(a^2 - b^2)^2}, \quad \Delta = 2^6 c^{2p} (a^2 - b^2)^2.$$

The conductor N of E can be computed using Tate's Algorithm [Ta]; let N_l denote the conductor of E at l, so that $N = \prod N_l$. The calculation is divided into two cases:

1. $l \neq 2$: Then E has good or semistable reduction at l; the conductor $N_l = 1$ if l does not divide c, and $N_l = l$ if l divides c. In any case, $\mathrm{ord}_l(\Delta) \equiv 0 \pmod{p}$, since $a^2 - b^2$ is a pth power up to powers of 2.
2. $l = 2$: If 2 divides c, then E is semi-stable and $N_2 = 2$; if 2 does not divide c, then $N_2 = 2^5$.

Let $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}\,(E_p)$ be the Galois representation associated to the p-division points of E. By a result of Mazur [Mz], the representation ρ is irreducible. By using the Tate curve to analyze the local behaviour of ρ at the primes l of bad reduction for E ($l \neq 2, p$) one sees that ρ is unramified outside of 2 and p, and is finite at p (cf. [Sr2]). Hence, the conductor $N(\rho)$ is a power of 2 which satisfies:

$$N(\rho) = 2 \quad \text{if } 2|c,$$

$$N(\rho)|2^5 \quad \text{otherwise.}$$

Assuming the Shimura Taniyama conjecture, the elliptic curve E corresponds to a cusp form of weight 2 and level N. The "lowering the level" result of Ribet [Ri] shows that ρ corresponds to a cusp form of weight 2 and level $N(\rho)$ mod p. But:

1. If c is even, such a cusp form cannot exist, because there are no modular forms of weight 2 and level 2: the curve $X_0(2)$ has genus 0. This proves the second part of theorem I.

2. If c is odd, then ρ corresponds to a modular form of weight 2 and level dividing 32. There is a unique such form, of level 32, which corresponds to the elliptic curve $A = X_0(32)$, with complex multiplication by $\mathbf{Q}(i)$. By Chebotarev's density theorem, it follows that

$$E_p \simeq A_p \quad \text{as Galois modules.}$$

In particular, by the theory of complex multiplication, the Galois representation ρ maps to the normalizer of a Cartan subgroup of $\mathbf{GL}_2(\mathbf{F}_p)$, and the restriction of ρ to $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(i))$ has abelian image. Furthermore, when $p = 1$

(mod 4), then ρ maps to the normalizer of a split Cartan subgroup; hence E has a rational subgroup of order p defined over $\mathbf{Q}(i)$; moreover all of its points of order 2 are defined over $\mathbf{Q}(i)$. It follows from work of Mazur [Mz] and Kamienny [Ka] (cf. cor. 1.7 of [Da]) that the denominator of $j(E)$ is divisible only by 2 or 3. Hence $a^4 - b^4$ is a power of 3, and so is $a^2 + b^2$. This can occur only if $ab = 0$, i.e., (a, b, c) is a trivial solution. This proves the first statement in theorem I.

Remarks:
1. Observe that in the proof we could not rule out the existence of the curve E, and had to obtain a contradiction in a more indirect manner. There is a good reason for this: the curve $A = X_0(32)$ is precisely the curve that arises from the trivial solution $(1, 0, 1)$ to the equation $x^4 - y^4 = z^p$.
2. When $p = -1 \bmod 4$, the image of ρ is the normalizer of a non-split Cartan subgroup. This case seems more difficult to rule out using the "Eisenstein descent" methods of Mazur and Kamienny, although one also expects it cannot occur when p is large. More precisely, one expects that the image of the Galois representation coming from a non-CM elliptic curve should be the full $\mathbf{GL}_2(\mathbf{F}_p)$ when p is large enough ($p > 19$, perhaps?) A similar issue arises in [Da] in the study of the equations $x^p + y^p = z^2$ and $x^p + y^p = z^3$.
3. A natural question is to analyze the equation $x^4 + y^4 = z^p$ (or even more general variants such as $x^4 + cy^4 = z^p$). This equation is quite different from the previous one: $x^4 + y^4$ is irreducible over $\mathbf{Q}$ and only splits after adjoining primitive 8th roots of unity. A promising approach in this case is to consider the Galois representations arising from certain $\mathbf{Q}$-curves, that are defined over $\mathbf{Q}(i)$ and are 2-isogenous to their Galois conjugates. The methods used in that case are more involved and will be treated in a seperate paper.

References

[Ca] Cao, Zhen Fu, *The Diophantine equation* $cx^4 + dy^4 = z^p$, C.R. Math. Rep. Acad. Sci. Canada 14 (1992), no. 5, pp. 231-234.

[DG] Darmon, H., Granville, A., *On the equations* $Ax^p + By^q = Cz^r$ *and* $z^m = F(x, y)$, to appear.

[Da] Darmon, H. *The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$*, Intern. Math. Res. Not. no 10, 1993, pp. 263-273.

[Fr] Frey G., *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Saraviensis, **1** (1986), 1–40.

[Ka] Kamienny, S., *Points on Shimura curves over fields of even degree*, Math. Ann. 286, 731-734 (1990).

[Mz] Mazur, B., *Rational isogenies of prime degree*, inv. Math. 44, 129-162 (1978)

[Po] Powell, B. *Sur l'équation Diophantienne $x^4 \pm y^4 = z^p$*, Bull. Sc. Math., 107 (1983), 219-223.

[Ri] Ribet, K., *On modular representations of $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms*, Invent. Math. 100, 431-476 (1990).

[Sr1] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. 15, 259-331 (1972).

[Sr2] Serre, J.-P., *Sur les représentations modulaires de degré 2 de $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$*, Duke Math. J. Vol. 54, no. 1, 179-230 (1987).

[Ta] Tate, J., *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in Modular Functions of One Variable, SLN 476, pp. 33–52.

[TO] Terai, N. and Osada, H. *The Diophantine equation $x^4 + dy^4 = z^p$*, C.R. Math. Rep. Acad. Sci. Canada 14 (1992), No. 1, pp. 55-58.