Canadian Mathematical Society
Conference Proceedings
Volume 15, 1995

On the number of solutions to the generalized Fermat equation

ANDREW GRANVILLE

ABSTRACT. We discuss the maximum number of distinct non-trivial solutions that a generalized Fermat equation $Ax^n + By^n = Cz^n$ might possibly have. The *abc*-conjecture implies that it can never have more than two solutions once $n > n_0$ (independent of A, B, C); and that it has no solutions for fixed A, B, C once $n > n_{A,B,C}$. On the other hand for *any* set of pairwise coprime integers $p_1, p_2, \dots, p_k$, no matter how large, we will construct non-zero integers A, B, C such that there are distinct non-trivial solutions to $Ax_i^{p_i} + By_i^{p_i} = Cz_i^{p_i}$ for $i = 1, 2, \dots, k$. We also show that $n_0 > 4$. In the final section we review some recent relevant results, consider generalizing these questions to all curves, and also briefly discuss the challenge of modifying the Frey–Ribet application of the Taniyama-Shimura-Weil Conjecture to Fermat's Last Theorem, to attack the generalized Fermat equation.

In about 1637 Fermat made the assertion, popularly known today as *Fermat's Last Theorem*[1], that there are no non-trivial integer solutions $x, y, z, p \geq 3$ to the equation $x^p + y^p = z^p$. In this paper we are interested in the number of non-trivial coprime integer solutions x, y, z, with $p \geq 4$, to the more general Fermat equation

$$Ax^p + By^p = Cz^p, \tag{1}$$

where A, B, C are given non-zero integers with $\gcd(A, B, C) = 1$. We note here that this is equivalent to counting rational points on the curve

$$\mathcal{C}_{\alpha,\beta,p} : \alpha u^p + \beta v^p = 1.$$

1991 *Mathematics Subject Classification.* Primary 11D41.
Key words and phrases. Fermat equation, abc-conjecture, Diophantine Equations.
The author is a Presidential Faculty Fellow and an Alfred P. Sloan Research Fellow. He is supported in part by a grant from the National Science Foundation.

[1]'Last' as in last to be proved!

This equivalence may be seen by 'de-homogenizing' (1) with the transformation $\alpha = A/C, \beta = B/C, u = x/z$ and $v = y/z$, and 'homogenizing' $\mathcal{C}_{\alpha,\beta,p}$ by multiplying points on this curve through by an appropriate common denominator.

We missed out the exponents $p = 2$ and 3 in our formulation of this problem for the same reason that Fermat missed out $p = 2$ in his problem. That is that, for these p, there are usually *infinitely* many solutions to (1) if there is one. Indeed if $p = 2$ then we consider the line of rational slope t that goes through the given point on the curve $\mathcal{C}_{\alpha,\beta,2}$, and find that for all but tangent lines, this line intersects the curve at a second rational point. From infinitely many rational t we thus get infinitely many rational points. If $p = 3$ we take the tangent at the given point on the curve $\mathcal{C}_{\alpha,\beta,3}$, and find that this line intersects the curve at a second rational point. We then repeat this process and if it continues indefinitely without returning to the same point, then we have an infinite sequence of rational points. Explicit formulae for doubling points on such curves were written down by Desboves [9]; with these we proved (see section 6a of [6]) that this proposed algorithm for finding infinitely many rational points fails[2] only if the initial point has one co-ordinate 0 or ∞, or is $(\pm 1, \pm 1)$. These ideas were all known in Fermat's time.

There are choices of A, B, C, p for which there are some solutions in (1). For example, $(3, 1, 2)$ is a solution to $x^5 + 13y^5 = 8z^5$. In fact, for any p it is easy to determine infinitely many triples A, B, C for which there are at least two solutions to (1): first select any two triples of pairwise coprime integers (x_i, y_i, z_i), $i = 1, 2$, and then determine A, B and C by solving for these three variables in the two linear equations which arise when we substitute the x, y and z values into (1).

So the question arises, can we choose $A, B, C, p \geq 4$ for which there are infinitely many solutions to (1) ? A brief computer search will quickly persuade you that it is difficult to find examples that give you more than a handful of solutions in (1). In fact the answer to the question is 'no'. It is a consequence of Faltings' celebrated theorem [10], long known as '*Mordell's conjecture*', that there are only finitely many solutions to (1) for any choice of $A, B, C, p \geq 4$. How many, you might ask, is 'finitely many' ? And, indeed, this is a very difficult question. Faltings' original proof was completely 'ineffective', in that it bounded neither the size nor quantity of solutions. However the recent, very different, proofs by Vojta [18] and Bombieri [2] allow one, in principle, to put an upper bound on the number of solutions. In practice though, major technical complications arise when one tries to write down a simply stated bound; all that is clear is that this bound will be a very fast growing function of A, B, C and p.

Still nagging questions remain:

- Is it true that there will be no solutions to (1) once p is sufficiently large, no matter what the choice of A, B, C ?

If so, then what about the number of solutions for smaller p:

[2]That is, we have hit upon a 'torsion point' of $\mathcal{C}_{\alpha,\beta,3}$

- Is it true that there is an absolute bound on the number of solutions to (1) no matter what the values of fixed $A, B, C, p \geq 4$?

Even more

- Is it true that there is an absolute bound on the number of solutions to (1) no matter what the values of A, B, C, as p varies ?

In recent years, mathematicians have turned to the *abc*-conjecture to help understand a dizzying array of Diophantine problems, including Fermat-type problems:

THE *abc*-CONJECTURE. *For any $\varepsilon > 0$ there exists a constant $\kappa_\varepsilon > 0$ such that if*

$$a + b = c$$

where a, b, c are coprime positive integers, then

$$a, b, c < \kappa_\varepsilon \left(\prod_{p|abc} p \right)^{1+\varepsilon}.$$

One can give simple heuristic counting arguments that support this conjecture. Also, it is easy to prove the following analogue in $\mathbb{C}[t]$ (due to R. C. Mason):

If $a + b = c$ in $\mathbb{C}[t]$, where polynomials a, b, c have no common roots, then the degrees of a, b and c are less than the total number of distinct roots of abc.

We can apply the *abc*-conjecture to solutions of (1). First we must divide through by any common factors of Ax^p, By^p, Cz^p. Since x, y, z are pairwise coprime, any common prime power factor must divide at least two of A, B and C. Thus our common factor is $\leqq (ABC)^{1/2}$. Therefore, by the *abc*-conjecture,

$$Ax^p, By^p, Cz^p \leqq (ABC)^{1/2} \kappa_\varepsilon (ABCxyz)^{1+\varepsilon}$$

and so, multiplying all three inequalities together gives, after some re-arranging,

$$|ABC| \gg_\varepsilon |xyz|^{\frac{2(p-3)}{7} - \varepsilon}.$$

Taking $\varepsilon = 1/7$ this implies that, for $p \geq 4$,

$$p \log |xyz| \ll \log |ABC|,$$

where the implied constant is absolute. Evidently this cannot hold once $p \gg \log |ABC|$, if $|xyz| > 1$. Thus we we are able to answer the first of our questions above: For any choice of A, B, C we expect that, like Fermat's Last Theorem, there are no solutions to (1) once p is sufficiently large (except what we now classify as further 'trivial' solutions, those with $|xyz| = 1$). Based on this justification we state

CONJECTURE 1. *For any given non-zero integers A, B, C there are no non-trivial solutions to* (1) *once p is sufficiently large (that is, if $p > p_{A,B,C}$, where $p_{A,B,C}$ is a constant that depends on A, B, C).*

To study our second question we follow a remarkable technique initiated by Desboves, subsequently re-discovered by Chowla and many others. In 1879 Desboves [8] observed that if, for any given integers A, B, C we have three distinct[3] solutions (x_i, y_i, z_i), $i = 1, 2, 3$, in pairwise coprime, non-zero integers to the generalized Fermat equation (1), then this gives rise to an integer solution (r, s, t, u, v, w) of the system of Diophantine conditions

$$\text{(2)} \qquad \begin{cases} r^p + s^p + t^p = u^p + v^p + w^p \\ \qquad rst = uvw \neq 0 \\ \text{with } \gcd(r, s, t, u, v, w) = 1, \\ \text{where } \{r^p, s^p, t^p\} \cap \{u^p, v^p, w^p\} = \emptyset. \end{cases}$$

Moreover each such solution to (2) gives rise to such a triplet of solutions to (1). The main idea in the proof of the first assertion is to note that the three solutions to (1) give rise to a solution to the matrix equation

$$\begin{pmatrix} x_1^p & y_1^p & z_1^p \\ x_2^p & y_2^p & z_2^p \\ x_3^p & y_3^p & z_3^p \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix};$$

and so the determinant of this matrix is zero. Thus

$$\text{(3)} \qquad \sum_{i=1}^{3} (x_i y_{i+1} z_{i+2})^p = \sum_{j=1}^{3} (x_j y_{j+2} z_{j+1})^p$$

(where the indices are taken mod 3) which is a solution to the two equations in (2); though it is not yet guaranteed that either of the last two conditions in (2) hold. Indeed to force $\gcd(r, s, t, u, v, w) = 1$ we shall need a little sleight-of-hand:

Suppose that all the terms in (3) have a common prime factor q, and that q divides x_1. If q does not divide x_2 then, since q divides $x_2 y_1 z_3$ and $x_2 y_3 z_1$, we have q divides $y_1 z_3$ and $z_1 y_3$. However x_1 is coprime to y_1 and z_1 so that q divides both y_3 and z_3 which contradicts the fact that they are coprime. Thus q must divide x_2 and similarly x_3. But then one can change A to Aq^p and divide each x_i through by q. Proceeding in this way (and with the y_j's and z_k's) we force the terms in (3) to be coprime.

The final condition in (2) is contravened precisely for triplets of solutions to (1) in which two of those solutions are not distinct. For example, if $r^p = u^p$ then $(x_1 y_2 z_3)^p = (x_2 y_1 z_3)^p$; and since $(x_1, y_1) = (x_2, y_2) = 1$ we must have $x_1^p = \pm x_2^p$, $y_1^p = \pm y_2^p$ and so $z_1^p = \pm z_2^p$ (where all of these '$\pm$' are the same).

[3] (x_1, y_1, z_1) is *not* to be considered distinct from (x_2, y_2, z_2) if $(x_1^p, y_1^p, z_1^p) = \pm(x_2^p, y_2^p, z_2^p)$.

To go from a solution of (2) to three solutions of (1) with an appropriate choice of A, B, C we select, in order,

$$x_1 = (r,u),\ \ y_3 = (r/x_1, v),\ \ z_2 = r/x_1y_3,\ \ x_2 = (s, v/y_3),\ \ y_1 = (s/x_2, w/z_2),$$
$$z_3 = s/x_2y_1,\ \ y_2 = u/x_1z_3,\ \ z_1 = v/x_2y_3,\ \ x_3 = w/y_1z_2,$$
$$A = (y_1z_2)^p - (y_2z_1)^p,\quad B = (z_1x_2)^p - (z_2x_1)^p,\quad C = (x_2y_1)^p - (x_1y_2)^p\ .$$

Note that each of A, B, C are non-zero else the final condition in (2) is not satisfied.

Desboves' idea is best viewed in a geometric context. What we have shown is that triples of points on $\mathcal{C}_{\alpha,\beta,p}$, no matter what the values α and β, are parametrized by points on the $\mathbf{P}^6$-variety

$$\{v^p + w^p + x^p - y^p - z^p = 1, \qquad vw = xyz\}.$$

Note that this variety is independent of α and β (or, equivalently, of A, B and C). Thus, to study our second question above, we need to ask about rational points on this variety; or equivalently solutions to the system of equations (2).

For this question we have no counterpart of Faltings' Theorem, no significant results at all. On the other hand, it does make sense to generalize the *abc*-conjecture to multi-term equations. In fact Brownawell and Masser [4], and Voloch [19] gave such a result for solutions to $x_1 + x_2 + \cdots + x_n = 0$ with each x_i in $\mathbb{C}[t]$; and various heuristic arguments imply that the following should hold:

THE GENERALIZED *abc*-CONJECTURE. *For any integer $n \geq 3$, there exist constants $c_n > 0$ and E_n such that if*

$$x_1 + x_2 + \cdots + x_n = 0 \qquad \textit{with} \quad \gcd(x_1, x_2, \ldots, x_n) = 1,$$

and no proper subsum vanishes, then

$$|x_1|, \ldots, |x_n| \leqq c_n \left(\prod_{p | x_1 \cdots x_n} p \right)^{E_n}.$$

We wish to use this to consider the system of equations in (2). Mueller [14] used the Brownawell-Masser/Voloch result to show that, in $\mathbb{C}[t]$, (2) has no solutions once $p \geq 31$, whence (1) can *never* have three distinct solutions in $\mathbb{C}[t]$, where $A, B, C \in \mathbb{C}[t]$.

Suppose that we have an integer solution to (2). Note that $|rst| = |uvw| > 1$, else we would have a contradiction to either the second or fourth condition in (2). Now, if no proper subsum of $r^p + s^p + t^p - u^p - v^p - w^p$ vanishes, then we may apply the generalized *abc*-conjecture directly to (2) with $n = 6$, to get that

$$|r|^p, |s|^p, |t|^p, |u|^p, |v|^p, |w|^p < c_6 \left(\prod_{\substack{q \text{ prime} \\ q | rst}} q \right)^{E_6} \leqq c_6 |rst|^{E_6}.$$

Multiplying the first three inequalities together we obtain $|rst|^p < c_6^3|rst|^{3E_6}$ which cannot hold if p is sufficiently large, since $|rst| \geq 2$. Now if some proper subsum of $r^p + s^p + t^p - u^p - v^p - w^p$ indeed vanishes then, given the last condition of (2), we easily determine a solution, in coprime integers, to either $x^p + y^p = z^p$ or to $t^p + x^p + y^p = z^p$ with no vanishing subsums. We then apply the generalized *abc*-conjecture with $n = 3$ or 4, respectively, and deduce a contradiction for sufficiently large p (it is easy to show that at least one of the integers involved has absolute value > 1). Therefore if p is sufficiently large then (1) cannot have more than two solutions, no matter what the values of A, B, C. We thus make the following

CONJECTURE 2. *If p is sufficiently large then there are at most two solutions to* (1) *for any non-zero integers A, B, C (that is, if $p > p_0$, where p_0 is an absolute constant, independent of A, B, C).*

As we remarked above, using elementary linear algebra it is easy to construct, for any given p, infinitely many examples of A, B, C for which there are two solutions to (1). Thus Conjecture 2 may be thought of as "best possible".

It seems plausible that rather more than Conjectures 1 and 2 might hold true. Indeed that there might exist a constant p_0, such that there are at most two solutions (x, y, z, p) to (1) with $p > p_0$ and x, y, z pairwise coprime, for any non-zero integers A, B, C. Plausible, yes, but correct, no! Indeed, the main purpose of this note is to show that this is quite untrue:

THEOREM 1. *For any set of pairwise coprime integers $p_1, p_2, \ldots, p_k$, there exist non-zero integers a, b, c such that there are solutions in pairwise coprime non-zero integers (x_i, y_i, z_i) to*

$$ax_i^{p_i} + by_i^{p_i} = cz_i^{p_i} \qquad \text{for } i = 1, 2, \ldots, k,$$

where the triples $\pm(x_i^{p_i}, y_i^{p_i}, z_i^{p_i})$ are all distinct.

PROOF. By induction on k. For $k = 2$ we can select (more-or-less) *any* such (x_i, y_i, z_i), $i = 1, 2$, and find a, b and c through elementary linear algebra. Indeed abc will be non-zero unless $(x_1^{p_1}, y_1^{p_1}, z_1^{p_1}) = (x_2^{p_2}, y_2^{p_2}, z_2^{p_2})$. (Note that we don't actually need to require p_1 and p_2 to be coprime, as in the hypothesis.)

So suppose that the result is true for k. It is an exercise in elementary number theory to show that there must exist non-zero integers $\lambda_1, \ldots, \lambda_k$ such that if

$$X = \sum_{i=1}^{k} \lambda_i x_i^{p_i}, \quad Y = \sum_{i=1}^{k} \lambda_i y_i^{p_i}, \quad Z = \sum_{i=1}^{k} \lambda_i z_i^{p_i},$$

then Xx_j, Yy_j, Zz_j are pairwise coprime for each j. Evidently

$$aX + bY = cZ.$$

By the Chinese remainder theorem we may select a positive integer n satisfying

$$\begin{aligned} & n \equiv 0 \qquad (\text{mod } \operatorname{lcm}[p_1, \dots, p_k]) \\ \text{and} \quad & n \equiv -1 \qquad (\text{mod } p_0). \end{aligned}$$

We multiply all equations $ax_i^{p_i} + by_i^{p_i} = cz_i^{p_i}$, as well as $aX + bY = cZ$, through by $X^n Y^n Z^n$ and let

$$A = aY^n Z^n, \quad B = bX^n Z^n, \quad C = cX^n Y^n.$$

Then

$$AX^{n+1} + BY^{n+1} = CZ^{n+1};$$

which is the same as

$$AX_0^{p_0} + BY_0^{p_0} = CZ_0^{p_0}$$

where

$$X_0 = X^{(n+1)/p_0}, \quad Y_0 = Y^{(n+1)/p_0}, \quad \text{and} \quad Z_0 = Z^{(n+1)/p_0}.$$

Similarly

$$AX_i^{p_i} + BY_i^{p_i} = CZ_i^{p_i}, \quad \text{for } i = 1, 2, \dots, k,$$

where

$$X_i = x_i X^{n/p_i}, \quad Y_i = y_i Y^{n/p_i}, \quad \text{and} \quad Z_i = z_i Z^{n/p_i}.$$

This gives $k+1$ solutions $AX_i^{p_i} + BY_i^{p_i} = CZ_i^{p_i}$, and the theorem is proved. □

It is important to observe that A, B and C are not pairwise coprime in our construction; this may be the cause of the downfall of our hitherto plausible assertion[4]. On the other hand, from the geometric perspective discussed above, one would not have expected any special difficulties to arise when A, B and C are not pairwise coprime.

It is of some interest to make a plausible guess as to the value of p_0 in Conjecture 2. We certainly believe, in analogy with what happens in $\mathbb{C}[t]$, that $p_0 \leq 30$. We will show that $p_0 \geq 4$ in $\mathbb{Z}[t]$, and thus in $\mathbb{Z}$:

THEOREM 2. *There are infinitely many distinct triples of pairwise coprime non-zero integers A, B, C such that (1) has three solutions with $p = 4$.*

PROOF. Stephane Vandemergel (see [13, D1]) observed that if $i^p + j^p = k^p + \ell^p$ then we get a solution $\{r, s, t, u, v, w\} = \{ik, jk, \ell^2, i\ell, j\ell, k^2\}$ to the first condition in (2). This leads to solutions $(x, y, z) = (i, \ell, k), (j, k, \ell), (1, 1, 1)$ in (1) with $A = \ell^p - k^p, B = j^p - \ell^p$ and $C = j^p - k^p$.

Unfortunately it is widely believed that there are no non-trivial solutions to $i^p + j^p = k^p + \ell^p$ once $p \geq 5$ (see [16] for the latest on that subject); and since our remarks in the first couple of paragraphs apply when $p \leq 3$, we need only consider the case $p = 4$: In 1772 Euler was the first person to find a non-trivial solution, namely $2219449^4 + 555617^4 = 1584749^4 + 2061283^4$. Six years later he

[4]However, do note that insisting that A, B and C are pairwise coprime is not the same trivial restriction when we vary over different values of p as when we fix our value of p

found the smallest solution, $158^4+59^4 = 133^4+134^4$. There are many parametric solutions to $i^4 + j^4 = k^4 + \ell^4$: we will work with

$$i = t^7 + t^5 - 2t^3 + 3t^2 + t, \quad j = t^6 - 3t^5 - 2t^4 + t^2 + 1,$$
$$k = t^7 + t^5 - 2t^3 - 3t^2 + t, \quad \ell = t^6 + 3t^5 - 2t^4 + t^2 + 1.$$

The resulting polynomials A, B, C (as above) all have common factor t^2+1 which we divide through by. The values of these polynomials are pairwise coprime[5] when $t = 510n$ for any positive integer n; and this then gives the triples needed to prove the theorem. □

With Theorem 1 we answered the third question asked above: No, there is no absolute bound on the number of solutions to (1), independent of A, B, C. However we *can* modify Desboves' idea to study when we have solutions to (1) with different exponents, but with A, B, C fixed. So suppose the exponents are p, q and r, and proceed as before to show that the matrix

$$\begin{pmatrix} x_1^p & y_1^p & z_1^p \\ x_2^q & y_2^q & z_2^q \\ x_3^r & y_3^r & z_3^r \end{pmatrix} \tag{4}$$

has determinant 0. From a null vector $(a, b, -c)^T$ of the transpose of this matrix we have three distinct solutions of the generalized Fermat equation

$$au^p + bv^q = cw^r \tag{5}$$

Theorem 2 of [3] asserts that, in $\mathbb{C}[t]$, if $p, q, r \geq 61$ then u and v must have a common root in at least one of these three solutions to (5). Thus if we have solutions to (1) with A, B, C fixed, but for exponents $p, q, r \geq 61$, then either x_1 and x_2 have a common root, or y_1 and y_2 do, or z_1 and z_2 do. Tracing carefully through the proof in [3], we expect that they will have a 'large' number of common roots. From analogous arguments using the generalized *abc*-conjecture, one can deduce that there exists a constant E such that

$$\prod_{w\in\{x,y,z\}} \gcd(w_1^p, w_2^q)\gcd(w_1^p, w_3^r)\gcd(w_2^q, w_3^r) \gg \prod_{w\in\{x,y,z\}} (w_1^{p-E} w_2^{q-E} w_3^{r-E})$$

in any three such solutions to (1) with A, B, C fixed, and each $\gcd(x_i, y_i, z_i) = 1$.

In general we expect that (5) should have no more than two solutions in coprime integers u, v, w when $1/p + 1/q + 1/r$ is sufficiently small (as is the case over $\mathbb{C}[t]$). In [6] we showed that (5) has only finitely many such solutions if $1/p + 1/q + 1/r < 1$.

[5]To see this, find A and B using Maple, then use the 'gcdex' routine to find polynomials $a, b \in \mathbb{Z}[t]$ such that $aA + bB \in \mathbb{Z}$. This integer only has prime divisors 2, 3, 5, 17 so that $\gcd(A(m), B(m))$ can only have prime factors from amongst these. But then $\gcd(A(m), B(m)) = 1$ when $2 \cdot 3 \cdot 5 \cdot 17$ divides m, since $A(0) = 1$. Finally since $C = A + B$ thus $A(m), B(m), C(m)$ are pairwise coprime.

We now prove that there are at least three such solutions to (5) for infinitely many different choices of a, b and c when $r = 2$ or 3, and p and q are chosen arbitrarily: To prove this we change both p and q to $n = pqr$ (only making the problem harder), and then select six pairwise coprime integers $u_1, u_2, u_3, v_1, v_2, v_3$, all > 1. Let $(A, B, -C)$ be a null vector of the matrix

$$\begin{pmatrix} u_1^n & u_2^n & u_3^n \\ v_1^n & v_2^n & v_3^n \end{pmatrix}.$$

with $ABC \neq 0$ (such null vectors exist since $u_1, u_2, u_3, v_1, v_2, v_3$ are pairwise coprime). Since we have at least two solutions to $Aw_1^r + Bw_2^r = Cw_3^r$ (namely $(u_1^{n/r}, u_2^{n/r}, u_3^{n/r})$ and $(v_1^{n/r}, v_2^{n/r}, v_3^{n/r})$), we know that there are infinitely many solutions (as discussed near the beginning of this article). Select any such triple of coprime integers (w_1, w_2, w_3); then

$$\begin{pmatrix} u_1^n & u_2^n & u_3^n \\ v_1^n & v_2^n & v_3^n \\ w_1^r & w_2^r & w_3^r \end{pmatrix}$$

has determinant 0, and thus any null vector $(a, b, -c)^T$, with $abc \neq 0$, of its transpose leads to a desired set of three solutions to (5) (as before, we are guaranteed that such vectors exist because $u_1, u_2, u_3, v_1, v_2, v_3$ were chosen to be pairwise coprime).

The arguments above can be shown to work in arbitrary number fields with an appropriate reformulation of the *abc*-conjecture (see [17]).

A few further remarks

Wiles [20] has recently proved a substantial part of the Taniyama-Shimura-Weil conjecture (see [12] for a reader-friendly review), which implies that Fermat's Last Theorem is true. This note is not the place to seriously discuss this result nor even this deduction (due to Frey, Serre and Ribet [15]). We note only that, from a purported counterexample to Fermat's Last Theorem, they are able to construct a weight 2 cusp form of level 2 (assuming the Taniyama-Shimura-Weil conjecture here and until the end); and thus deduce that the counterexample cannot exist since there are no such modular forms. Their argument can be modified to construct, from any non-trivial example in (1) with A, B and C fixed, a weight 2 cusp form whose level comes from a finite set of possibilities, determined by the prime factors of A, B and C. Since the possible cusp forms come from a finite set of finite dimensional vector spaces (some of which may be of dimension 0), there is hope of ruling out all of these possibilities, when there are no solutions to (1). However, a major difficulty arises when there *is* a non-trivial solution to (1) for some largish exponent p. It is not hard to create such an example using elementary linear algebra, but then we know that we genuinely *do* have a weight 2 cusp form of suitable level corresponding to a solution of (1). The important question then becomes: can we prove that such a modular form corresponds to only finitely many solutions to (1), even as p varies ? It may be

that the answer to this question lies very deep, but it may be that it is accessible to current techniques.

Conjecture 2 provides a *uniform* upper bound for the number of rational points on 'Fermat' curves $\mathcal{C}_{\alpha,\beta,p}$. It is, at first, surprising that such a tight bound should hold as we run through so many curves. Moreover similar techniques should work for other classes of plane curves with 'few' monomials in the equation describing them[6], the so-called 'fewnomials'. Thus it seems that we get bounds for the number of rational points on a curve depending on the degree and the number of non-zero coefficients in an appropriate 'model' of the curve, a view that doesn't entirely agree with the geometers' perspective that the genus should determine all (though it is not entirely incompatible):

Recently Caporoso, Harris and Mazur [5] proved that if it is true that the set of rational points on any given variety of general type is not Zariski dense[7] then, for any integer $g > 1$ there exists a constant κ_g such that any curve, defined over $\mathbb{Q}$, of genus g has no more than κ_g rational points. This is surprising since we usually expect that the larger the genus the fewer rational points on the curve whereas, in the extreme examples, this result implies that the higher the genus, the more rational points it can have. Abramovich [1] has shown that a similar bound holds for K-rational points, uniformly over all number fields K of degree ≤ 3 over $\mathbb{Q}$.[8] It is not clear how κ_g grows with g: there is no family of curves known that contradicts the possibility that $\kappa_g = O(g)$; and it is simple to construct examples with *at least* this many points (by linear algebra).

Finally, we mention a recent, beautiful, *unconditional*, uniform result of Debarre and Klassen (applying a result of Faltings [11]): If C is a smooth plane projective curve, defined over $\mathbb{Q}$, of degree $d \geq 8$, then there are only finitely many points on C, of degree $\leq d-1$ over $\mathbb{Q}$, except those that lie on the intersection of C with a rational line going through a rational point of C. In particular this applies to all equations (1) with $p \geq 8$. Combining this result with Wiles' Theorem [20] implies that if $p \geq 8$ then there are only finitely many points on $x^p + y^p = 1$, with $[\mathbb{Q}(x,y) : \mathbb{Q}] < p$, other than when x satisfies some equation $x^{p-1} + ((1+tx)^p - 1)/x = 0$ with t rational, and $y = 1 + tx$ (or $-(1+tx)$ if p is even). Klassen suggests that there may not be *any other* points on $x^p + y^p = 1$ of degree $< p$, and even that if $[\mathbb{Q}(x,y) : \mathbb{Q}] < p - 1$ then $x + y = 1$.[9].

ACKNOWLEDGMENTS: Thanks are due to Ken Ono for remarks made on this paper; and to the referee for a careful reading that uncovered too many careless minor errors in the first draft.

[6]Though the details of the proof can get somewhat complicated — see [3]

[7]As had been conjectured by Lang (see [17]).

[8]Presumably this will soon be extended to fields of arbitary degree over $\mathbb{Q}$.

[9]Note the example where x and y are the two primitive sixth roots of unity, and $(p, 6)$=1

REFERENCES

1. D. Abramovich, *Uniformité des points rationnels sur toutes les extensions quadratiques* (to appear).
2. E. Bombieri, *The Mordell Conjecture Revisited*, Annali Scuola Normale Sup. Pisa, Cl. Sci., S. IV **17** (1990), 615–640.
3. E. Bombieri and J. Mueller, *Trinomial equations in function fields* (to appear).
4. W. D. Brownawell and D. W. Masser, *Vanishing sums in function fields*, Math. Proc. Camb. Phil. Soc. **100** (1986), 427–434.
5. L. Caporaso, J. Harris and B. Mazur, *Uniformity of rational points* (to appear).
6. H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. (to appear).
7. O. Debarre and M. J. Klassen, *Points of low degree on smooth plane curves*, J. Reine Angew. Math. **446** (1994), 81–87.
8. A. Desboves, *Résolution en nombres entiers de* $ax^m + by^m = cz^n$, Nouv. Ann. Math., Sér. II **18** (1879), 481–489.
9. A. Desboves, *Résolution en nombres entiers et sous sa forme la plus générale, de l'équation cubique, homogène à trois inconnues*, Nouv. Ann. Math., Sér. III **5** (1886), 545–579.
10. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
11. G. Faltings, *Diophantine Approximation on Abelian Varieties*, Ann. of Math. (2) **133** (1991), 549–576.
12. F. Q. Gouvêa, *A marvelous proof*, Amer. Math. Monthly **101** (1994), 203–222.
13. R. K. Guy, *Unsolved Problems in Number Theory, 2nd ed.*, Springer-Verlag, New York, 1994.
14. J. Mueller, *The abc-inequality and the generalized Fermat equation in function fields*, Acta Arith. **64** (1993), 7–18.
15. K. Ribet, *On modular representations of* $Gal(\bar{Q}/Q)$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
16. C. M. Skinner and T. D. Wooley, *Sums of two kth powers*, J. Reine Angew. Math. (to appear).
17. P. Vojta, *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math. **1239** (1987), Springer-Verlag.
18. P. Vojta, *Siegel's Theorem in the compact case*, Ann. of Math. (2) **133** (1991), 509–548.
19. J. F. Voloch, *Diagonal equations over function fields*, Bol. Soc. Brasil. Mat. **16** (1985), 29–39.
20. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, (October 24th, 1994 preprint).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GEORGIA 30602, USA

E-mail address: andrew@math.uga.edu