January 23rd 1994.

# On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$

Henri Darmon[1] and Andrew Granville[2]

**Abstract:** We investigate integer solutions of the *superelliptic equation*

(1) $$z^m = F(x,y),$$

where $F$ is a homogenous polynomial with integer coefficients, and of the *generalized Fermat equation*

(2) $$Ax^p + By^q = Cz^r,$$

where $A, B$ and $C$ are non-zero integers. Call an integer solution $(x,y,z)$ to such an equation *proper* if $\gcd(x,y,z) = 1$. Using Faltings' Theorem, we shall show that, other than in certain exceptional circumstances, these equations have only finitely many proper solutions.

We examine (1) using a descent technique of Kummer, which allows us to obtain, from any infinite set of proper solutions to (1), infinitely many rational points on a curve of (usually) high genus, thus contradicting Faltings' Theorem (for example, this works if $F(t,1) = 0$ has three simple roots and $m \geq 4$).

We study (2) via a descent method which uses unramified coverings of $\mathbf{P}_1 - \{0,1,\infty\}$ of *signature* $(p,q,r)$. ¿From infinitely many proper solutions to (2) we obtain infinitely many rational points on some curve of (usually) high genus in some number field, thus contradicting Faltings' Theorem if $1/p + 1/q + 1/r < 1$.

We then collect together a variety of results for (2) when $1/p + 1/q + 1/r \geq 1$. In particular we consider 'local-global' principles for proper solutions, and consider solutions in function fields.

## Introduction.

Faltings' extraordinary 1983 Theorem (née *Mordell's Conjecture* [V2]) states that there are only finitely many rational points on any irreducible algebraic curve of genus $> 1$ in any number field. Two important immediate consequences are:

**Theorem.** *There are only finitely many pairs of rational numbers $x, y$ for which $f(x,y) = 0$, if the curve so represented has genus $> 1$.*

**Theorem.** *If $p \geq 4$ and $A, B$ and $C$ are non-zero integers, then there are only finitely many triples of coprime integers $x, y, z$ for which $Ax^p + By^p = Cz^p$.*

[1] Supported by an NSERC post-doctoral fellowship and by NSF grant DMS-8703372

[2] An Alfred P. Sloan Research Fellow. Also supported, in part, by an NSF grant.

Here we shall see that, following various arithmetic descents, one can also apply his result to rational points on certain interesting surfaces.

(Vojta [Vo1] and Bombieri [Bo] have now given effective versions of Faltings' Theorem. In principle, we can thus give an explicit upper bound to the number of solutions in each equation below, instead of just writing 'finitely many'.)

**The superelliptic equation.**

In 1929, Siegel [Si] showed that a polynomial equation $f(x, y) = 0$ can have infinitely many *integral* solutions in some algebraic number field $K$, only if a component of the curve represented has genus 0. In 1964, LeVeque [Le] applied Siegel's ideas to prove that the equation

$$y^m = f(x) \tag*{(1)$^*$}$$

has infinitely many integral solutions in some number field $K$, if and only if $f(X)$ either takes the form $c(X-a)^e g(X)^m$ or the form $f(X) = c(X^2 - aX + b)^{m/2} g(X)^m$. In all other cases one can obtain explicit upper bounds on solutions of (1)*, using Baker's method (see [ST]).

By using a descent technique of Kummer, we can apply Faltings' Theorem to the *superelliptic equation* (1), much as LeVeque applied Siegel's Theorem to (1)*:

**Theorem 1.** *Let $F(X, Y)$ be a homogenous polynomial with algebraic coefficients and suppose that there exists a number field $K$ in which*

$$z^m = F(x, y) \tag{1}$$

*has infinitely many $K$–integral solutions with the ideal $(x, y) = 1$, and the ratios $x/y$ distinct. Then $F(X, Y) = cf(X, Y)^m$ times one of the following forms:*
*(i)* $(X - \alpha Y)^a (X - \beta Y)^b$;
*(ii)* $g(X, Y)^{m/2}$, *where $g(X, Y)$ has at most 4 distinct roots;*
*(iii)* $g(X, Y)^{m/3}$, *where $g(X, Y)$ has at most 3 distinct roots;*
*(iv)* $(X - \alpha Y)^{m/2} g(X, Y)^{m/4}$, *where $g(X, Y)$ has at most 2 distinct roots;*
*(v)* $(X - \alpha Y)^a g(X, Y)^{m/2}$, *where $g(X, Y)$ has at most 2 distinct roots;*
*(vi)* $(X - \alpha Y)^{m/2} (X - \beta Y)^{am/3} (X - \gamma Y)^{bm/5}$;
*(vii)* $(X - \alpha Y)^{m/2} (X - \beta Y)^{am/3} (X - \gamma Y)^{bm/12}$, *where $(b, 12) > 1$;*
*where $a$ and $b$ are non-negative integers, $c$ is a constant, $f(X, Y)$ and $g(X, Y)$ are homogenous polynomials, and exponents ${}^{im/j}$ are always integers. Moreover, for each such $F$ and $m$, there are number fields $K$ in which (1) has infinitely many distinct, coprime $K$-integral solutions.*

This result answers the last of the five questions posed by Mordell[3] in his famous paper [Mo1] (the others having been resolved by Siegel [Si] and Faltings [F1]).

As an immediate consequence of Theorem 1 we see that there are only finitely many distinct, coprime $K$-integral solutions to (1) when $F(X,Y)$ has $k(\geq 3)$ distinct simple roots and $m \geq \max\{2, 7-k\}$. There are many other interesting consequences, for instance:

**Corollary 1.** *Fix integers $m \geq 2$ and $k \geq 3$ with $m+k \geq 6$. There are only finitely many $k$-term arithmetic progressions of coprime positive integers, whose product is the $m$th power of an integer.*

We shall discuss this further in section 2. Also

**Corollary 2.** *If $F(x,y)$ has three distinct factors then, in any number field $K$, there are only finitely many pairs $(x,y)$ of coprime $K$-integers with $x/y$ distinct, such that $F(x,y)$ is a unit of $K$.*

To see this, choose $m \equiv 1 \pmod d$ large enough so that we are not in any exceptional case of Theorem 1. If $\xi = F(x,y)$ is a unit of $K$ then $F(x\xi^{(m-1)/d}, y\xi^{(m-1)/d}) = \xi^m$, and by Theorem 1 there can be only finitely many such solutions to this equation. This may be proved more directly via transcendental methods.

**The generalized Fermat equation.**

The last theorem of Fermat that remained to be re-proven, stated that there are no non-zero integer solutions to

$$x^p + y^p = z^p$$

when $p \geq 3$. (This corresponds to the case $p = q = r \geq 3$ and $A = B = C = 1$ of the *generalized Fermat equation*

$$Ax^p + By^q = Cz^r, \tag{2}$$

where $A, B$ and $C$ are non-zero integers.) Fortunately, Fermat never wrote down his proof, and many beautiful branches of number theory grew out of attempts to re-discover it. In the last few years, there have been a number of spectacular advances in the theory of Fermat's equation, culminating in Wiles' announcement of the proof on June 23rd, 1993.

As we discussed above, Faltings' Theorem immediately implies that there are only finitely many triples of coprime integers $x, y, z$ for which $x^p + y^p = z^p$. One might hope to also apply Faltings' Theorem directly to (2), since this is a curve in an appropriate *weighted* projective space. However this curve often has genus 0 (for instance, if $p, q$ and $r$

[3] Actually Mordell conjectured finitely many *rational* solutions in his last three questions, where he surely meant *integral*.

are pairwise coprime), so that finiteness statements for proper solutions must be reached through a less direct approach.

It has often been conjectured that (2) has only finitely many proper solutions if $1/p + 1/q + 1/r < 1$. This is easily proved to be true in function fields, and it follows for integers from the *'abc'–conjecture*. We will use Faltings' theorem to show:

**Theorem 2.** *If* $1/p + 1/q + 1/r < 1$, *then the generalized Fermat equation*

$$Ax^p + By^q = Cz^r, \tag{2}$$

*has only finitely many proper solutions.*

Catalan conjectured in 1844 that $3^2 - 2^3 = 1$ are the only powers of positive integers that differ by 1. Tijdeman proved this for sufficiently large powers ($> \exp\exp\exp\exp(730)$: Langevin, 1976). One can unify and generalize the Fermat and Catalan Conjectures in

**The Fermat-Catalan Conjecture.** *There are only finitely many triples of coprime positive integer powers* $x^p, y^q, z^r$ *(with integers* $p, q, r > 1$*), giving rise to solutions of the equation*

$$x^p + y^q = z^r \text{ with } \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1. \tag{2$'$}$$

This conjecture may be deduced from the *abc*-conjecture (see section 5b). There are five 'small' solutions $(x, y, z)$ to the above equation:[4]

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2.$$

Beukers and Zagier have surprisingly found five larger solutions:

$$17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7,$$

$$43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

Given Theorem 2, it is natural to ask what happens in (2) when $1/p + 1/q + 1/r \geq 1$: In the cases where $1/p + 1/q + 1/r = 1$, the proper solutions correspond to rational points on certain curves of genus one. It is easily demonstrated that, for each such $p, q, r$, there exist values of $A, B, C$ such that the equation has infinitely many proper solutions; and some such examples are given in section 6. There also exist values of $A, B, C$ such that the equation has no proper solutions (which can be proved by showing that there are no

[4] Blair Kelly III, Reese Scott and Benne De Weger all found these examples independently.

proper solutions modulo some prime); though, for any $A, B, C$, there are number fields which contain infinitely many proper solutions.
In the cases where $1/p + 1/q + 1/r > 1$, the proper solutions correspond to rational points on certain curves of genus zero. However, even when the curve has infinitely many rational points, they may not correspond to proper solutions of the equation. So is there an easy way to determine whether such an equation has infinitely many proper solutions?

In the case of conics ($p = q = r = 2$), Legendre proved the *local-global principle* in 1798; and using this we can easily determine whether (2) has any proper solutions. However, in section 8 we shall see that there are no proper solutions for

$$x^2 + 29y^2 = 3z^3,$$

despite the fact that there are proper solutions everywhere locally, as well as a rational parametrization of solutions. We prove this using what we call a 'class group obstruction', which may be the only obstruction to a local-global principle in (2) when $1/p+1/q+1/r > 1$; and we study this carefully for a family of equations of the form $x^2 + By^2 = Cz^r$.

It has long been known that there is no general local-global principle for (2) when $1/p + 1/q + 1/r = 1$: Indeed, Lind and Selmer gave the examples

$$u^4 - 17v^4 = 2w^2, \quad \text{and} \quad 3x^3 + 4y^3 = 5z^3,$$

respectively, of equations which are everywhere locally solvable but nonetheless have no non-trivial integer solutions. This obstruction is described by the appropriate *Tate–Shafarevič group*; which may be determined by an algorithm that is only known to work if the Birch-Swinnerton Dyer Conjectures are true.

There are no local obstructions or class group obstructions to *any* equation

$$Ax^2 + By^3 = Cz^5, \tag{3}$$

if $A, B$ and $C$ are pairwise coprime. So are there are always infinitely many proper solutions? If so, is there a parametric solution to (3) with $x, y$ and $z$ coprime polynomials in $A, B$ and $C$?

### Application of modular curves.

The driving principle behind the proof of theorem 2 is a descent method based on coverings of signature $(p, q, r)$ (see section 3 for the definition). Sometimes, these coverings can be realized as coverings of modular curves. A lot more is known about the Diophantine properties of modular curves than about the properties of Fermat curves, thanks largely to the fundamental work of Mazur. Hence one can hope that descent using modular coverings yields new insights into such equations. The basic example for this is the covering $X(2p) \longrightarrow X(2)$ which is of signature $(p,p,p)$, ramified over the three cusps of $X(2)$, and forms the basis for Frey's attack on Fermat's Last theorem. Thanks to the deep work of Ribet and Wiles, this approach has finally lead to the proof of Fermat's Last theorem, and there is a strong incentive for seeing whether other modular coverings of signature $(p,q,r)$ will yield similar insights into the corresponding generalized Fermat equation[5]. In section 7 we will give a classification of the coverings of signature $(p,q,r)$ obtained from modular curves, and state some Diophantine applications.

Table of Contents

*Acknowledgements*: Our work here was inspired by ideas in the papers of Elkies [E2], and of Powell and Ribenboim [PR] which we are pleased to acknowledge. We would like to thank Enrico Bombieri for many interesting discussions, and Fernando Rodriguez–Villegas for getting us together. Thanks are also due to Sybilla Beckmann, Bryan Birch, Nigel Boston, Mo Hendon, Joe Silverman, Roy Smith and Rob

[5] As also noted by Wiles in his Cambridge lectures.

Tijdeman for helpful conversations, and Frits Beukers, Blair Kelly III, Reese Scott, Benne de Weger and Don Zagier for some useful computations.

## 1. Remarks and observations.

There are many remarks to be made about what has been written above. For instance, why the restrictions on pairs $x, y$ in the statement of Theorem 1? What if $A, B, C$ are not pairwise coprime in Theorem 2? Rather than weigh down the main body of the paper with these remarks, we discuss them here.

### 1a. Proper and Improper solutions.

The study of integer solutions to homogenous polynomials in three variables, 'projectivizes' naturally to the study of rational points on curves, by simply de-homogenizing the equation. However the study of integer solutions to non-homogenous polynomials in three variables does not so naturally 'projectivize', because there are often parametric families of solutions with common factors, that are of little interest from a number theoretic viewpoint. As an example, look at the integer solutions to $x^3 + y^3 = z^4$. It is easy to find a solution for any fixed ratio $x/y$: if we want $x/y = a/b$ then simply take $z = a^3 + b^3$, $x = az$ and $y = bz$. This is not too interesting. However if we do not allow $x, y$ and $z$ to have a large common factor, then we can rule out the above parametric family of solutions (and others), and show that there are only finitely many solutions.

In general we will define a *proper* solution to an equation (1) or (2) in some given number field $K$, to be a set of integer solutions $(x, y, z)$ with the value of $x/y$ fixed, and $(x, y)$ dividing some given, fixed ideal of $K$.

Notice that in this definition we consider a proper solution to be a *set* of integer solutions $(x, y, z)$ with the value of $x/y$ fixed. This is because one can obtain infinitely many solutions of (1) of the form $x\xi^m, y\xi^m, z\xi^{\deg F}$, and of (2) of the form $x\xi^{qr}, y\xi^{rp}, z\xi^{pq}$, as $\xi$ runs over the units of $K$, given some initial solution $x, y, z$. Thus a proper solution is really an equivalence class of solutions under a trivial action of the unit group of the field.

Even when we work with a homogenous equation like the Fermat equation it is not always possible to 'divide out' a common factor $(x, y)$ as we might when dealing with rational integer solutions: for instance, if the ideal $(x, y)$ is irreducible and non-principal[6]. However, in this case let $I$ and $J$ be the ideals of smallest norm from the ideal class, and inverse ideal class of $G = (x, y)$, respectively. Multiply each of $x, y, z$ through by the

[6] Even Kummer made this mistake, which Weil calls an 'unaccountable lapse' in Kummer's "Collected Works".

generator of the principal ideal $IJ$, so that now $(x,y)=GIJ$. Since $GJ$ is principal we may divide through by the generator of that ideal, but then $(x,y)=I$, one of a finite set of ideals. Thus it makes sense to restrict solutions in (1) and (2) by insisting that $(x,y)$ can only divide some fixed ideal of the field.

It is not entirely clear how to describe proper solutions, as opposed to improper solutions, in the language of arithmetic geometry. It may be that one should be able to describe the improper solutions as belonging to some easily described family of subvarieties. Alternately improper solutions lead to locally trivial solutions; and thus we are only considering solutions that are everywhere locally non-trivial.

If the degree of $F$ is coprime with $m$ then we can always construct a parametric improper solution of (1): since there exist positive integers $r$ and $s$ with $mr-\deg(F)s=1$, we may take $x=aF(a,b)^s,\ y=bF(a,b)^s,\ z=F(a,b)^r$. More generally if $g=$gcd(deg$(F),m$)$=mr-\deg(F)s$, then we can obtain a solution of (2) from a solution of $F(a,b)=c^g$ by taking $x=ac^s,\ y=bc^s$ and $z=c^r$.

Equation (2) may be similarly approached, and indeed its generalization to arbitrary diagonal equations (see [By]): The solutions to a diagonal equation $a_1X_1^{e_1}+...+a_nX_n^{e_n}=0$ may be obtained from the solutions of $a_1Y_1^{g_1}+...+a_nY_n^{g_n}=0$, where each $g_j=\gcd(e_j,L_j)$ and $L_j=\text{lcm}[e_i,\ 1\le i\le n,\ i\ne j]$. (If $g_j=e_js_j-L_jr_j$ then we may take $X_i=Y_i^{s_i}\prod_{j\ne i}Y_j^{r_jL_j/e_j}$.)

## 1b. What happens when $A,B$ and $C$ are not pairwise coprime?

Evidently any common factor of all three of $A,B$ and $C$ in (2) may be divided out, so we may assume that $(A,B,C)=1$. But what if $A,B$ and $C$ are not pairwise coprime?

If prime $\ell$ divides $A$ and $B$, but not $C$ then, in any solution of (2), $\ell$ divides $Cz^r$ and so $z$. Thus $Cz^r=C\ell^rz'^r$ and so we can rewrite $C\ell^r$ as $C$, and $z'$ as $z$. But then $\ell$ divides each of $A,B$ and $C$ and so we remove the common power of $\ell$ dividing them. If $\ell$ now divides only one of $A,B$ and $C$ then there are no further such trivial manipulations, but if $\ell$ divides two of $A,B$ and $C$ then we are forced to repeat this process. Sometimes this will go on *ad infinitum*, such as for the equation $x^3+2y^3=4z^3$. In general it is easily decided whether this difficulty can be resolved:

**Proposition.** *Suppose that $\alpha,\beta$ and $\gamma$ are the exact powers of $\ell$ that divide $A,B$ and $C$, respectively. If there is an integer solution to (2) then either $(p,q)$ divides $\alpha-\beta$, or $(q,r)$ divides $\beta-\gamma$, or $(r,p)$ divides $\gamma-\alpha$.*

*Proof:* Let $a,b,c$ and $d$ be the exact powers of $\ell$ dividing $x,y,z$ and $(Ax^p,By^q,Cz^r)$, respectively. Evidently $d$ must be equal to at least two of $\alpha+ap,\ \beta+bq,\ \gamma+cr$. From the Euclidean algorithm we know that there exist integers $a$ and $b$ such that $ap-bq=\beta-\alpha$ if and only if $(p,q)$ divides $\alpha-\beta$; the result follows from examining all three pairs in this way.

## 2. Finitely many proper solutions of the superelliptic equation.

The proof of Theorem 1 is a (technical) generalization of the proof of Corollary 1 given in the next subsection. The idea is to 'factor' the left-hand side of (1) into ideals in the field $K$ (which may be enlarged to contain the splitting field extension for $F$), so that these ideals are $m$th powers of ideals, times ideals from some fixed, finite set. We then multiply these ideals through by ideals from some other fixed, finite set to get principal ideals. Equating the generators of the ideals, modulo the unit group, we get a set of linear equations in $X$ and $Y$. Taking linear combinations to eliminate $X$ and $Y$, we have now 'descended' to a new variety to which we may be able to apply Faltings' Theorem. If not, we descend again and again, until we can.

### 2a. Kummer's descent and the proof of Corollary 1.

In 1975 Erdős and Selfridge [ES], proved the beautiful result that the product of two or more consecutive integers can never be a perfect power. We conjecture that the product of three or more consecutive integers of an arithmetic progression $a \pmod q$ with $(a,q)=1$ can never be a perfect power except in the two cases parametrized below. This is well beyond the reach of our methods here, though we prove Corollary 1 above, and note the following cases already considered in the literature:

If the product of a three term arithmetic progression is a square (the case $k=3,\ m=2$), then we are led to the systems of equations, $a=\lambda x^2, a+d=y^2, a+2d=\lambda z^2$ with $\lambda=1$ or 2, so that $x^2+z^2=(2/\lambda)y^2$. This leads to the parametric solutions $(t^2-2tu-u^2)^2,\ (t^2+u^2)^2,\ (t^2+2tu-u^2)^2$ and $2(t^2-u^2)^2,\ (t^2+u^2)^2,\ 8t^2u^2$ where, in each case, $(t,u)=1$ and $t+u$ odd (for $\lambda=1$ and 2, respectively).

Euler proved, in 1780, that there are only trivial four term arithmetic progressions whose product is a square, ruling out the case $k=4, m=2$. In 1782 he showed that there are only trivial integer solutions to $x^3+y^3=2z^3$, which implies that there are no three term arithmetic progressions whose product is a cube, ruling out the case $m=k=3$.

Now fix integers $k\geq 3$ and $m\geq 2$, with $m+k\geq 7$, so that $2/k+1/m<1$. We will assume that there exist infinitely many $k$-term arithmetic progressions of coprime integers, whose products are all $m$th powers of integers. In other words, that there are infinitely many pairs of positive integers $a$ and $d$ for which

$$(a+d)(a+2d)\dots(a+kd)=z^m \quad \text{with } (a,d)=1. \tag{2.1}$$

For any $i \neq j$ we have that

$(a+id, a+jd)$ divides $((a+id)-(a+jd), j(a+id)-i(a+jd)) = (i-j)(d,a) = (i-j)$.

Therefore, for each $i$, we have

$$a + id = \lambda_i z_i^m, \quad \text{for} \quad i = 1, 2, \dots k,$$

for some integers $z_i$, where each $\lambda_i$ is a factor of $\left(\prod_{p \leq k-1} p\right)^{m-1}$. ¿From elementary linear algebra we know that we can eliminate $a$ and $d$ from any three such equations; explicitly taking $i = 1, 2$ and $j$ above we get

$$\lambda_j z_j^m = j\lambda_2 z_2^m - (j-1)\lambda_1 z_1^m, \quad \text{for} \quad j = 3, 4, \dots k. \tag{2.2}$$

If $m \geq 4$ then any single such equation has only finitely many proper solutions, by Faltings' Theorem; and as there are only finitely many choices for the $\lambda_i$, this gives finitely many proper solutions to (2.1).

More generally, the collection of equations (2.2) defines a non-singular curve $C$, as the complete intersection of hypersurfaces in $\mathbf{P}^{k-1}$. By considering the natural projection from $C$ onto the Fermat curve in $\mathbf{P}^2$ defined by the single equation (2.2) with $j = 3$, we may use the Riemann-Hurwitz formula to deduce that $C$ has genus $g$ given by

$$\begin{aligned} 2g - 2 &= m^{k-3}\left(2\binom{m-1}{2} - 2\right) + (k-3)m^2(m^{k-3} - m^{k-4}) \\ &= km^{k-1}\left(1 - \frac{2}{k} - \frac{1}{m}\right) > 0; \end{aligned}$$

since the degree of the covering map is $m^{k-3}$, and the only ramification points are where $z_j = 0$ for some $j \geq 4$ (and it is easy to show that $z_i = z_j = 0$ is impossible). Thus $C$ has genus $> 1$, and so has only finitely many rational points, by Faltings' Theorem. Therefore (2.1) has only finitely many proper integer solutions.

Suppose that, in equation (1),

$$F(X,Y) = a_0 Y^{r_0} \prod_{i=1}^{n} (X - \alpha_i Y)^{r_i},$$

where the $\alpha_i$'s are distinct complex numbers, and the $r_i$ are non-negative integers; we enlarge $K$, if necessary, to contain the $\alpha_i$. Let $S$ denote the multiset of integers $s > 1$, each counted as often as there are values of $i$ for which $m/(m, r_i) = s$. Theorem 1 is implied by

**Theorem** $1'$**.** *Suppose that there are infinitely many proper $K$–integral solutions to (1), in some number field $K$. Then either (i) $|S| \leq 2$; or (ii) $S \subseteq \{2,2,2,2\}$; or (iii) $S = \{3,3,3\}$ ; or (iv) $S = \{2,4,4\}$ ; or (v) $S = \{2,2,n\}$ for some integer $n$; or (vi) $S = \{2,3,5\}$; or (vii) $S = \{2,3,3\}$ or $\{2,3,4\}$ or $\{2,3,6\}$.*

Re-writing (1) as the ideal equation

$$(y)^{r_0} \prod_{i=1}^{n} (a_0 x - \beta_i y)^{r_i} = (a_0)^{d-1-r_0} (z)^m$$

with $\beta_i = a_0 \alpha_i$, we proceed in the familiar, analogous way to above: All ideals of the form $(y, a_0 x - \beta_i y)$ and $(a_0 x - \beta_i y, a_0 x - \beta_j y)$ (with $i \neq j$), divide the ideals $J$ and $(\beta_i - \beta_j)J$, respectively (where $J$ is that fixed ideal which is divisible by $(a_0 x, y)$ for any proper solution of (1)). Therefore, by the unique factorization theorem for ideals, we have

$$\begin{aligned} (a_0 x - \beta_i y)^{r_i} &= \sigma_i \theta_i^m, \quad \text{for each } i, \ 1 \leq i \leq n, \\ (y)^{r_0} &= \sigma_0 \theta_0^m, \end{aligned}$$

for some ideals $\theta_i$ of $K$ and some set of ideal divisors $\sigma_i$ of $(J')^{m-1}$, where

$$J' := J \left( \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j) \right).$$

We may factor both sides of each of the above equations in terms of their prime ideal divisors. If the exact power to which the prime ideal $\mathbf{p}$ divides $(a_0 x - \beta_i y)$ or $(y)$ is $e$, and $\mathbf{p}$ does not divide $\sigma_i$, then $er_i$ must be divisible by $m$, and thus $e$ is a multiple of $m/(m, r_i) = s_i$. Therefore, since all prime divisors $\mathbf{p}$ of $\sigma_i$ divide $J'$, we can re-write the above equations as

$$\begin{aligned} (a_0 x - \beta_i y) &= \tau_i \theta_i^{s_i}, \quad \text{for each } i, \ 1 \leq i \leq n, \\ (y) &= \tau_0 \theta_0^{s_0}, \end{aligned} \tag{2.3}$$

where each $\tau_i$ divides $(J')^{s_i - 1}$.

Let $\bar{\theta}_i$ and $\bar{\tau}_i$ be those ideals with smallest norm, in the inverse ideal classes of $\theta_i$ and $\tau_i$ in $K$, respectively. Both $\bar{\theta}_i \theta_i = (z_i)$ and $\bar{\tau}_i \tau_i = (\omega_i)$ are principal ideals, by definition. Moreover $\tau_i \theta_i^{s_i}$ is principal by (2.3), and thus so is $\bar{\tau}_i \bar{\theta}_i^{s_i} = (\lambda_i)$, say. Let $\lambda$ be a fixed integer of the field divisible by all of the $\lambda_i$. Multiplying (2.3) through by $\lambda$ we get

$$\begin{aligned} (a_0(\lambda x) - \beta_i(\lambda y)) &= ((\lambda/\lambda_i) \omega_i z_i^{s_i}), \quad \text{for each } i, \ 1 \leq i \leq n, \\ (\lambda y) &= ((\lambda/\lambda_0) \omega_0 z_0^{s_0}). \end{aligned}$$

In each of these ideal equations, the ideals involved are all principal, and so the integers generating the two sides must differ by a unit. Dirichlet's unit theorem tells us that the unit group $U$ of $K$ is finitely generated, and so $U/U^{s_i}$ is finite; that is, for each $i$, the ratio of the generators of the two sides of the $i$th equation above, a unit, may be written as $u_i {v_i}^{s_i}$, where $u_i$ is a unit from a fixed, finite set of representatives of $U/U^{s_i}$, and $v_i$ is some other unit. Replacing $v_i z_i$ in the equations above by $z_i$, as well as $\lambda x$ by $x$ and $\lambda y$ by $y$, we get

$$(a_0 x - \beta_i y) = u_i(\lambda/\lambda_i)\omega_i z_i^{s_i}, \quad \text{for each } i,\ 1 \le i \le n,$$
$$y = u_0(\lambda/\lambda_0)\omega_0 z_0^{s_0}.$$

Let $\rho_i = \lambda u_i \omega_i/\lambda_i$ for each $i$, and let $L$ be the field $K$ extended by $(\rho_i)^{1/s_i},\ i = 0, 1, \ldots, n$, a finite extension.

Since $J'$ has only finitely many prime ideal divisors, there are finitely many choices for the $\tau_i$, and thus for the $\omega_i$. Since the *class group* of $K$ is finite, there can only be finitely many choices for the $\bar{\theta}_i$, and thus for the $\lambda_i$, and so for $\lambda$: let $\mu$ be an integer divisible by all of the possible $\lambda$. Therefore there are only finitely many possible choices for the $\rho_i$ and so for the fields $L$: let $M$ be the compositum of all possible such fields $L$. We now replace $(\rho_i)^{1/s_i} z_i$ by $z_i$ in the equations above, to deduce:

*There exists a number field $M$ in which there are infinitely many proper $M$-integral solutions $x, y, z_0, z_1, \ldots, z_n$ to the system of equations*

$$a_0 x - \beta_i y = z_i^{s_i}, \quad \text{for each } i,\ 1 \le i \le n, \qquad (2.4)$$
$$y = z_0^{s_0}.$$

Taking the appropriate linear combination of any three given equations in (2.4), we can eliminate $x$ and $y$. Explicitly, if $1 \le i < j < k \le n$ then

$$(\beta_j - \beta_k) z_i^{s_i} + (\beta_k - \beta_i) z_j^{s_j} + (\beta_i - \beta_j) z_k^{s_k} = 0 \qquad (2.5)$$
$$\text{and, if } r_0 \ge 1 \text{ then } z_i^{s_i} - z_j^{s_j} + (\beta_i - \beta_j) z_0^{s_0} = 0$$

Note that we obtain a proper solution here, since the $(z_i^{s_i}, z_j^{s_j})$ all divide the fixed ideal $(\lambda)J$; and the $z_i^{s_i}/z_j^{s_j}$ are all distinct for if $z_i^{s_i}/z_j^{s_j} = (z_i')^{s_i}/(z_j')^{s_j}$ then $\frac{a_0 x - \beta_i y}{a_0 x' - \beta_i y'} = \frac{a_0 x - \beta_j y}{a_0 x' - \beta_j y'}$, and so $(\beta_i - \beta_j)(x/y - x'/y') = 0$, contradicting the hypothesis.

Notice that if $F$ has $n$ simple roots then all of the corresponding $s_j = m$. Therefore, descending as we did above for (2.1), we see that (2.5) describes a curve of genus $> 1$ if $2/n + 1/m < 1$, and so we have proved:

**Proposition 2a.** *If $F(x, y)$ has $n$ simple roots, where $2/n + 1/m < 1$, then there are only finitely proper solutions to (1) in any given number field.*

## 2b. Iterating descent and the proof of Theorem 1.

The descent just described is entirely explicit; that is, we can compute precisely what variety we will descend to. On the other hand, the descent described in section 3 invokes the Riemann Existence Theorem at a crucial stage, and thus is not, *a priori*, so explicit. For this reason we will proceed as far as we can in the proof of Theorem $1'$ using only the concrete methods of the previous subsection; which turn out to be sufficient unless the elements of the set $S$ are pairwise coprime.

Indeed, if the elements of $S$ are pairwise coprime, and are not case (i) or (vi) of Theorem $1'$, then there must be three elements $p, q, r \in S$ with $1/p + 1/q + 1/r < 1$. Therefore we can apply Theorem 2 to (2.5), and deduce that there are only finitely many proper solutions to (1).

Now suppose that there are infinitely many proper solutions to (1) in some number field. We need only consider those sets $S$ in which some pair of elements have a common factor: say $pa, pb \in S$ where $p \geq 2$ and $a \geq b \geq 1$ are coprime. To avoid case (i)[7] we may assume that $S$ contains a third element $q \geq 2$.

The equations (2.5) imply that there are infinitely many proper solutions of some equation of the form $Ax^p + By^p = Cz^q$ in an appropriate number field. So, applying proposition 2a to this new equation, we deduce that $2/p + 1/q \geq 1$. Thus $p = 2, 3$ or 4 since $q \geq 2$.

Now suppose $S$ contains a fourth element, call it $r$, with $q \geq r \geq 2$. Applying the descent procedure of section 2a, we obtain infinitely many proper solutions to simultaneous equations of the form

$$c_1 x^p + c_2 y^p = c_3 z^q \quad \text{and} \quad c_1' x^p + c_2' y^p = c_3' w^r.$$

Applying the descent procedure of section 2a to the first equation here, we see from (2.4) that $x^a$ and $y^b$ can both be written as certain linear combinations of $u^q$ and $v^q$, where $u$ and $v$ are integers of some fixed number field. Substituting these linear combinations into the second equation above, we see that $Cw^r$ can be written as the value of a binary homogenous form in $u$ and $v$ of degree $pq$. It is straightforward to check that this binary form can only have simple roots, and so, by proposition 2a, we have $2/pq + 1/r \geq 1$. This implies that $pq \leq 4$, since $r \geq 2$. On the other hand, $pq \geq 4$ since $p, q \geq 2$, and so we deduce that $p = q = 2$ and $r = 2$.

We have thus proved that if $\{pa, pb, q, r\}$ is a subset of $S$ then $p = q = r = 2$. But then $\{2, 2, 2a, 2b\}$ is a subset of $S$ and, applying the same analysis to this new ordering of the set, we get that $2a = 2b = 2$. Therefore if $S$ has four or more elements, then they must all be 2s. If so then we multiply together the linear equations (2.4) that arise from each $s_i = 2$, giving a form with $|S|$ simple roots whose value is a square. Proposition 2a implies that we must be in case (ii).

[7] For the rest of this section, 'case' refers to the case number of Theorem 1'.

Henceforth we may assume that $S = \{pa, pb, q\}$, where $2/p + 1/q \geq 1$ and $p = 2, 3$ or 4, with $q \geq 2,\ a \geq b \geq 1$ and $(a, b) = 1$. If $a = 1$ then $b = 1$, and we must be in one of the cases (iii), (iv), (v), or the first example in (vii). So assume that $a \geq 2$.

¿From (2.5) we obtain a single equation of the form $Ax^{ap} + By^{bp} = Cz^q$. We could apply Theorem 2 to this equation, but instead prefer to continue with the explicit descents of section 2a: ¿From (2.4) this equation now leads to $p$ equations of the form

$$\alpha_i x^a + \beta_i y^b = z_i^q, \quad i = 1, 2, \ldots, p. \tag{2.6}$$

Eliminating the $y^b$ term from the first two such equations, we obtain an equation of the form $x^a = \gamma_1 z_1^q + \gamma_2 z_2^q$; we deduce that $2/q + 1/a \geq 1$ by proposition 2a, and so $q \leq 4$.

If $(p, q) > 1$ then we may re-order $S$ so that $ap$ is the third element, and thus, by the same reasoning as above, $ap \leq 4$. However, since $a, p \geq 2$, this implies that $a = p = 2,\ b = 1$ and $q = 2$ or 4, and so we have case (iv) or (v). So we may assume now that $(p, q) = 1$ which, with all the above, leaves only the possibilities $p = 2, q = 3$, and $p = 3, q = 2$.

If $q = 3, p = 2$ then $a = 2$ or 3. This leads to the second two examples in (vii), and $S = \{6, 4, 3\}$ which was already ruled out, taking 4 as the third element.

If $p = 3, q = 2$ then we can eliminate $x^a$ and $y^b$ from the three equations in (2.6) to get a conic in variables $z_1, z_2, z_3$. As is well known, the integral points on this may be parametrized by a homogenous quadratic form in new variables $u$ and $v$, say. Solving for $x^a$ in (2.6), we now get that $x^a$ is equal to the value of a homogenous form in $u$ and $v$, of degree 4. It is easy to check that the roots of this form must be simple, and so, by proposition 2a, $a \leq 2$, leading to the third example in (vii).

## 3. Finitely many proper solutions of the generalized Fermat equation.

It has often been conjectured that

$$Ax^p + By^q = Cz^r \tag{2}$$

has only finitely many proper solutions if $1/p+1/q+1/r < 1$. One reason for this is that the whole Fermat-Catalan conjecture follows from the *'abc'–conjecture* (see [Ti2] and section 5b). Another reason is that the analogous result in function fields is easily proved (see section 5a). A simple heuristic argument is that there are presumably $N^{1/p+1/q+1/r+o(1)}$ integer triples $(x, y, z)$ for which $-N \leq Ax^p + By^q - Cz^r \leq N$; and so if the values of $Ax^p + By^q - Cz^r$ are reasonably well-distributed on $(-N, N)$, then we should expect that 0 is so represented only finitely often if $1/p + 1/q + 1/r < 1$.

Let $S_{p,q,r}$ denote the surface in affine 3-space $\mathbf{A}^3$ defined by (2). When $p = q = r$ the proper solutions are in an obvious two-to-one correspondence with the rational points on a smooth projective curve in $\mathbf{P}^2$. The genus of this *Fermat curve* is $\binom{p-1}{2}$, which is $> 1$ when $p > 3$; and Faltings' Theorem then implies that such a projective curve has only finitely many rational points.

Define the *characteristic* of the generalized Fermat equation (2) to be

$$\chi(p,q,r) := \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1.$$

Fix an embedding of $\bar{\mathbf{Q}} \subset \mathbf{C}$. Given a curve $X$, defined over $\bar{\mathbf{Q}}$, we will consider absolutely irreducible algebraic covering maps $\pi : X \longrightarrow \mathbf{P}_1$, defined over $\bar{\mathbf{Q}}$. Such a covering map $\pi$ is *Galois* if the group of fiber-preserving automorphisms of $X$ has order exactly $d = \deg \pi$.

Moreover, if $\pi$ is unramified over $\mathbf{P}_1 - \{0, 1, \infty\}$, and the ramification indices of the points over $0, 1$ and $\infty$ are $p, q$ and $r$, respectively, then we say that '$\pi$ has *signature* $(p, q, r)$' .

Using the Riemann Existence Theorem, one can show that for all positive integers $p, q, r > 1$, such a map exists[8]. From the Riemann-Hurwitz formula we can compute the genus of $X$ using this covering map:

$$2g - 2 = d(2 \cdot 0 - 2) + \left(d - \frac{d}{p}\right) + \left(d - \frac{d}{q}\right) + \left(d - \frac{d}{r}\right) = -d\chi(p,q,r).$$

Thus $g < 1, g = 1, g > 1$ according to whether $\chi(p,q,r) > 0, \chi(p,q,r) = 0, \chi(p,q,r) < 0$. Since $g$ and $d$ are non-negative integers we have proved:

**Proposition 3a.** *For any positive integers $p, q, r > 1$, there exists a Galois covering $\pi : X \longrightarrow \mathbf{P}_1$ of signature $(p, q, r)$. Let $d$ be its degree, and let $g$ be the genus of $X$.*

*If $\chi(p,q,r) > 0$, then $g = 0$ and $d = 2/\chi(p,q,r)$.*

*If $\chi(p,q,r) = 0$, then $g = 1$.*

*If $\chi(p,q,r) < 0$, then $g > 1$.*

Let $\pi : X \longrightarrow \mathbf{P}_1$ be such a covering map of signature $(p, q, r)$. Since it is defined over $\bar{\mathbf{Q}}$, it can be defined in some finite extension $K$ of $\mathbf{Q}$. By enlarging $K$ if necessary, we can ensure that the automorphisms of $\mathrm{Gal}(X/\mathbf{P}_1)$ are also defined over $K$.

Given a point $t \in \mathbf{P}_1(K) - \{0, 1, \infty\}$, define $\pi^{-1}(t)$ to be the set of points $P \in X(\bar{\mathbf{Q}})$ for which $\pi(P) = t$; by definition this is a set of cardinality $d$. Define $L_t$ to be the field extension of $K$ generated by the elements of $\pi^{-1}(t)$. Evidently $L_t$ is a Galois extension of $K$ with degree at most $d$.

[8] See Theorem 6.3 on page 58 of [Se1] together with the discussion at the end of section 6.3

Define $V$ to be the finite set of places in $K$ for which the covering $\pi : X \longrightarrow \mathbf{P}_1$ has bad reduction.

For a given place $v$ of $K$, let $e_v$ be a fixed uniformizing element for $v$. Then, for any $t \in \mathbf{P}_1(K) - \{0, 1, \infty\} = K^* - 1$, we have $t = e_v^{\mathrm{ord}_v(t)} u$, where $u$ is a $v$-unit and $\mathrm{ord}_v(t)$ is a fixed integer, independent of the choice of $e_v$. Define the arithmetic intersection numbers

$$\begin{aligned}(t \cdot 0)_v &:= \max(\mathrm{ord}_v(t), 0),\\ (t \cdot 1)_v &:= \max(\mathrm{ord}_v(t-1), 0),\\ (t \cdot \infty)_v &:= \max(\mathrm{ord}_v(1/t), 0).\end{aligned}$$

The following result of Beckmann [Be] describes the ramification in $L_t$.

**Lemma 3b.** *(Beckmann). Suppose that we are given a point $t \in \mathbf{P}_1(K) - \{0, 1, \infty\}$, and a place $v$ of $K$, which is not in the set $V$ (defined above). If*

$$(t \cdot 0)_v \equiv 0 \pmod p, \quad (t \cdot 1)_v \equiv 0 \pmod q, \text{ and } (t \cdot \infty)_v \equiv 0 \pmod r, \tag{3.1}$$

*then $L_t$ is unramified at $v$.*

¿From here we can proceed to the proof of Theorem 2: Let $(x, y, z)$ be a proper solution to the generalized Fermat equation

$$Ax^p + By^q = Cz^r, \tag{2}$$

and take $t = Ax^p/Cz^r$. The congruences in (3.1) are evidently satisfied if $v$ does not divide $A, B$ or $C$ and so, by Lemma 3b, $L_t$ is unramified at any $v \notin V_{ABC}$ (the union of $V$ and the places dividing $ABC$).

Minkowski's Theorem asserts that there are only finitely many fields with bounded degree and ramification; and we have seen that each $L_t$ has degree $\leq d$, and all of its ramification is inside $V_{ABC}$. Therefore there are only finitely many distinct fields $L_t$, with $t = Ax^p/Cz^r$ arising from proper solutions $x, y, z$ of (2), and so the compositum $L$, of all such fields $L_t$, must be a finite extension of $\mathbf{Q}$.

Since the genus of $X$ is $> 1$ and $L$ is a number field, Faltings' Theorem implies that $X(L)$ is finite. Therefore there are only finitely many proper solutions $x, y, z$ to (2), as $X(L)$ contains all $d$ points of $\pi^{-1}(Ax^p/By^q)$ for each such solution.

It is easy to see that this proof extends to proper solutions in arbitrary number fields. Actually the proof here is similar to that of the weak Mordell-Weil theorem: the role of the isogeny of an elliptic curve is played here by coverings of $\mathbf{P}_1 - \{0, 1, \infty\}$ of signature $(p, q, r)$, and Minkowski's theorem is used in much the same way (see [Weil's thesis]).

Theorem 2 may be deduced directly from the *abc*-conjecture. In fact, unramified coverings of $\mathbf{P}_1 - \{0, 1, \infty\}$ also play a key role in Elkies' result [E2] that the *abc*-conjecture implies Mordell's conjecture.

It is sometimes possible to be more explicit about the curve $X$ and the covering map $\pi$, as we shall see in the next few sections.

## 4. Explicit coverings of (2) when $1/p + 1/q + 1/r < 1$.

The curve $X$ (of the proof in section 3) can be realized as the quotient of the upper half plane by the action of a Fuchsian group $\Gamma$; that is, a discrete subgroup of $\mathbf{PSL_2}(\mathbf{R})$ with finite covolume. Actually $X$ is quite special among all curves of its genus, since it has many automorphisms. One can sometimes show that these automorphisms uniquely determine $X$ over $\mathbf{C}$, and hence the curve $X$ may be defined over $\mathbf{Q}$ using the descent criterion of Weil. Examples, in which even the Galois action of $\Gamma$ is defined over $\mathbf{Q}$, can be constructed using the rigidity method ([Se1]).

Those finite groups $G$ which occur as Galois groups of such coverings are said to be 'of signature $(p, q, r)$'. Evidently such groups have generators $\alpha, \beta, \gamma$ for which

$$\alpha^p = \beta^q = \gamma^r = \alpha\beta\gamma = 1.$$

Because of the connection to the Fermat equation, it is natural to start with coverings of signature $(p, p, p)$, where $p$ is an odd prime. Although we are far from a satisfying classification of coverings of signature $(p, p, p)$, we discuss the construction of a few examples in the next two subsections, which lead to the approaches of Kummer and Frey [Fr] for tackling Fermat's Last Theorem. In the third subsection we look to exploit Frey's method to construct coverings of other signatures.

### 4a. Solvable coverings of signature $(p, p, p)$.

Let $\pi : X \longrightarrow \mathbf{P}_1$ be a covering of signature $(p, p, p)$ with solvable Galois group $G$. Let $G^{'} = [G, G]$ be the derived group of $G$, and let $G^{ab} := G/G^{'}$ be the maximal abelian quotient of $G$. In fact, $\pi$ is an unramified covering of a quotient of the $p$th Fermat curve:

**Proposition.** *The group $G^{ab}$ is isomorphic either to $\mathbf{Z}/p\mathbf{Z}$ or $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. The quotient curve $F = X/G^{'}$ is isomorphic (over $\bar{\mathbf{Q}}$) to a quotient of the pth Fermat curve. The map $X \longrightarrow F$ is unramified.*

We may construct an example as follows: Let

$$L = \mathbf{Q}\left(T^{1/p}, \left(\frac{T^{1/p} - \zeta_p^i}{T^{1/p} - 1}\right)^{1/p} \quad \text{for } 1 \le i \le p-1\right)$$

be an extension of $\mathbf{Q}(T)$, where $\zeta_p$ is a primitive $p$th root of unity. The inclusion $\mathbf{Q}(T) \subset L$ corresponds to a covering map $\pi : X \longrightarrow \mathbf{P}_1$ of signature $(p,p,p)$ with Galois group

$$G = (\mathbf{Z}/p\mathbf{Z})^{p-1} \times \mathbf{Z}/p\mathbf{Z},$$

where the action of $\mathbf{Z}/p\mathbf{Z}$ on $(\mathbf{Z}/p\mathbf{Z})^{p-1}$ in the semi-direct product is by the regular representation, minus the trivial representation (i.e., the space of functions on $\mathbf{Z}/p\mathbf{Z}$ whose integral over the group is zero). Note that the action of $G$ is defined over $\mathbf{Q}(\zeta_p)$. The group $G^{ab}$ is isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$, and $X$ is isomorphic to an unramified covering of the $p$th Fermat curve with Galois group $(\mathbf{Z}/p\mathbf{Z})^{p-2}$. If $a^p + b^p = c^p$ is a non-trivial solution of the Fermat equation, then setting $t = a^p/b^p$, one finds that $L_t$ is the Galois closure of $\mathbf{Q}(\zeta_p, (a - \zeta_p c)^{1/p})$ over $\mathbf{Q}$. A crude analysis shows that $L_t/\mathbf{Q}(\zeta_p)$ is unramified outside the prime $(1 - \zeta_p)$ above $p$. It is possible to replace $X$ by a curve which is isomorphic to $X$ over $\bar{\mathbf{Q}}$, for which $L_t/\mathbf{Q}(\zeta_p)$ is unramified *everywhere*, and non-trivial, so deriving a contradiction when $p$ does not divide the class number of $\mathbf{Q}(\zeta_p)$. This explains Kummer's approach to Fermat's Last Theorem from a more geometric perspective.

### 4b. Modular coverings of signature $(p,p,p)$.

Let $X(N)$ be the modular curve classifying elliptic curves with full level $N$ structure. The curve $X(2)$ of level 2 is isomorphic to $\mathbf{P}_1$, and has three cusps: let $t$ be a function on $X(2)$ such that $t = 0, 1, \infty$ at these cusps. The natural projection

$$X(2p) \longrightarrow X(2)$$

is then a covering of signature $(p,p,p)$ ramified over $t = 0, 1, \infty$. Its Galois group $\mathbf{PSL}_2(\mathbf{F}_p)$ is a non-abelian simple group, which is somewhat different from the solvable coverings above. If $a^p + b^p = c^p$ is a non-trivial solution of the Fermat equation, then setting $t = a^p/b^p$, one finds that $t$ corresponds (via the moduli interpretation of $X(2)$) to the elliptic curve

$$Y^2 = X(X - a^p)(X + b^p),$$

(or its twist over $\mathbf{Q}(i)$). The field $L_t$ is then that field generated by the points of order $p$ of this curve; and so we recover Frey's strategy for tackling Fermat's Last Theorem.

### 4c. Modular coverings of signature $(p,q,r)$.

Wiles' proof of Fermat's Last theorem, uses Frey's approach via modular coverings, described above. Serre has noted that this is easily generalized to many equations of the form $x^p + y^p = cz^p$. Here we look to see for what equations (2) we may construct analogous modular coverings:

**Proposition.** *The only coverings of signature $(p,q,r)$, that arise as pullbacks of the covering $X(p) \longrightarrow X(1)$, are for signatures*
*$(2,3,p)$: The identity covering $X(1) \longrightarrow X(1)$;*
*$(3,3,p)$: The Kummer covering of degree two ramified over $j = 1728$ and $j = \infty$;*
*$(2,p,p)$: The covering $X_0(2) \longrightarrow X(1)$;*
*$(3,p,p)$: The Kummer covering of degree two ramified over $j = 0$ and $j = 1728$;*
*$(3,p,p)$: The covering $X_0(3) \longrightarrow X(1)$;*
*$(p,p,p)$: The covering $X(2) \longrightarrow X(1)$.*

Using these modular coverings for signatures $(2,p,p)$ and $(3,p,p)$, we proved, in [Da]:

**Proposition.** *Let $p > 13$ be prime. If the Taniyama-Weil conjecture is true, then*
*(i) The equation $x^p + y^p = z^2$ has no non-trivial proper solutions when $p \equiv 1 \pmod 4$.*
*(ii) The equation $x^p + y^p = z^3$ has no non-trivial proper solutions when $p \equiv 1 \pmod 3$.*

## 5. The generalized Fermat equation in function fields, and the *abc*-conjecture.

In most Diophantine questions it is much easier to prove good results in function fields (here we restrict ourselves to $\mathbf{C}[t]$): In section 5a below we show that (2) has no proper $\mathbf{C}[t]$-solutions when $1/p + 1/q + 1/r \leq 1$. On the other hand, in section 7, we will exhibit proper $\mathbf{C}[t]$-solutions of (2) for each choice of $p, q, r$ with $1/p + 1/q + 1/r > 1$ (all of this was first proved by Welmin [We] in 1904).

The proof of this result stems from an application of the *abc*-conjecture for $\mathbf{C}[t]$, which is easily proved. Its analogue for number fields is one of the most extraordinary conjectures of recent years; and implies many interesting things about the Generalized Fermat equation (which we discuss in sections 5b and 9).

It is typical, in the theory of curves of genus 0 and 1, that if one finds a rational point, then it can be used to derive infinitely many other such points through some geometric process (except for 'torsion points'). However, it is not clear that new points derived on the curves corresponding to (2) will necessarily lead to new proper solutions of (2). In section 5c we discuss a method of deriving new proper solutions by finding points on appropriate curves over $\mathbf{C}[t]$.

### 5a. Proper solutions in function fields.

Liouville (1879) was the first to realize that equations like (2), in $\mathbf{C}[t]$, can be attacked using elementary calculus. Relatively recently Mason [Ma] recognized that such methods can be applied to prove a very general type of result, the so-called '*abc*-conjecture'. A sharp version of Mason's result, which has appeared by now in many places, is

**Proposition 5a.** *Suppose that $a, b, c \in$ $\mathbf{C}[t]$ satisfy the equation $a + b = c$, where $a, b$ and $c$ are not all constants, and do not have any common roots. Then the degrees of $a, b$ and $c$ are less than the number of distinct roots of $a(t)b(t)c(t) = 0$.*

*Proof:* Define $w(t) = \prod_{abc(\delta)=0}(t-\delta)$. Since $a + b = c$ and thus $a' + b' = c'$, we have

$$\begin{aligned} aw(\log(a/c))' + bw(\log(b/c))' &= w(a(\log a)' + b(\log b)' - (a+b)(\log c)') \\ &= w(a' + b' - c') = 0, \end{aligned}$$

Therefore $a$ divides $bw(\log(b/c))'$, and so $a$ divides $w(\log(b/c))'$ since $a$ and $b$ have no common root. Evidently $w(\log(b/c))' \neq 0$ else $b$ and $c$ would have the same roots, which by hypothesis is impossible unless $b$ and $c$ are both constants, but then $a, b$ and $c$ would all be constants, contradicting the hypothesis. Therefore the degree of $a$ is at most the degree of $w(\log(b/c))'$. However if $b/c = \prod_{bc(\delta)=0}(t-\delta)^{e_\delta}$ then $(\log(b/c))' = \sum_{bc(\delta)=0} e_\delta/(t-\delta)$, so that $w(\log(b/c))'$ is evidently an element of $\mathbf{C}[t]$ of lower degree than $w$. This gives the result for $a$, and the result for $b$ and $c$ is proved analogously.

Applying this to a solution of (2) proves a strong version of our 'Fermat-Catalan' conjecture for $\mathbf{C}[t]$: Take $a = Ax^p, b = By^q, c = Cz^r$, to get $p\deg(x)$, $q\deg(y)$, $r\deg(z) < \deg(xyz)$ and so $1/p + 1/q + 1/r > 1$.

The proposition above (and even the proof) may be generalized to $n$-term summands (see [Ma], [BM] and [Vl]): From Theorem B of [BM] we know that if $y_1, y_2, \ldots y_n$ are non-constant polynomials, without (pairwise) common roots, whose sum vanishes, then $\frac{1}{n-2}\deg(y_j)$ is less than the number of distinct roots of $y_1 y_2 \ldots y_n$, for each $j$. Proceeding as above we then deduce:

**Proposition 5b.** *If $p_1, p_2, \ldots, p_n$ are positive integers with $1/p_1 + 1/p_2 + \ldots 1/p_n \leq 1/(n-2)$, then there do not exist non-constant polynomials $x_1, x_2, \ldots x_n$, without (pairwise) common roots, such that $x_1^{p_1} + x_2^{p_2} + \ldots + x_n^{p_n} = 0$.*

## 5b. The *abc*-conjecture for integers, and some consequences.

Proposition 5a, and particularly its formulation, have led to an analogous '*abc*–conjecture' for the rational integers (due to Oesterlé and Masser):

**The *abc*-conjecture.** *For any fixed $\varepsilon > 0$ there exists a constant $\kappa_\varepsilon > 0$ such that if $a + b = c$ in coprime positive integers then*

$$c \leq \kappa_\varepsilon \, G(a,b,c)^{1+\varepsilon}, \qquad \text{where} \quad G(a,b,c) = \prod_{p \text{ divides } abc} p.$$

Fix $\varepsilon = 1/83$, and suppose that we are given a proper solution to $(2)'$ in which all terms are positive. Then

$$G(x^p, y^q, z^r) \le xyz \le |x^p|^{1/p}|y^q|^{1/q}|z^r|^{1/r} \le |z^r|^{1/p+1/q+1/r} \le |z^r|^{41/42},$$

since $1/p + 1/q + 1/r \le 41/42$. Therefore, by the *abc*-conjecture we have $z^r \le \kappa_{1/83}^{83}$, and thus the solutions of $(2)'$ are all bounded. This implies the 'Fermat-Catalan' conjecture; and indeed this argument may be extended to include all equations (2) where the prime divisors of $ABC$ come from some fixed finite set (see [Ti2]).

In [E2] Elkies succeeded in applying the *abc*–conjecture (suitably formulated over arbitrary number fields) to any curve of genus $> 1$ and deduced Faltings' Theorem. His subtle proof inspired some of our work here, particularly Theorem 2.

The following generalization of the *abc*–conjecture has been proposed for equations with $n$ summands; implying a result analogous to Proposition 5b:

**The generalized *abc*-conjecture.** *For every integer $n \ge 3$ there is a constant $T(n)$ such that for every $T > T(n)$, there exists a constant $\kappa_T > 0$, such that if $x_1 + x_2 + \ldots + x_n = 0$ in coprime integers $x_1, x_2, \ldots, x_n$, and no subsum vanishes, then*

$$\max_j\ |x_j| \le \kappa_T \left( \prod_{p | x_1 x_2 \ldots x_n} p \right)^T$$

### 5c. Generating new proper integer solutions when $1/p + 1/q + 1/r \ge 1$.

Given integers $p, q, r$ we wish to find $f(t), g(t), h(t) \in \mathbf{Z}[t] \setminus \mathbf{Z}$, without common roots, for which

$$tf(t)^p + (1-t)g(t)^q = h(t)^r, \tag{5.1}$$

and the degrees of $f(t)^p$, $g(t)^q$ and $h(t)^r$ are equal (to $d$, say). Applying Proposition 5a to any such solution, we determine that $d+1 < d/p+d/q+d/r+2$, and so $1/p+1/q+1/r \ge 1$.

Now if we find a solution to (5.1), let

$$F(u, v) = v^{d/p} F(u/v),\ G(u, v) = v^{d/q} G(u/v),\ \text{and } H(u, v) = v^{d/r} H(u/v).$$

Then, given any solution $x, y, z$ to (2), we derive another one:

$$X = xF(u, v),\ Y = yG(u, v),\ Z = zH(u, v), \tag{5.2}$$

where $u = Ax^p$ and $v = Cz^r$.

If $x, y, z$ had been a proper solution to (2), so that $(u, v) = 1$, then $k = (AX^p, BY^q) = (uF(u,v)^p, vG(u,v)^q)$ which divides $K = (u, G(0,1)^q)(F(1,0)^p, v)\text{Resultant}(f, g)$. Thus $k$ is easily determined from the congruence classes of $u$ and $v \pmod K$. We may thus divide out an appropriate integer from each of $X, Y$ and $Z$ to get a proper solution, provided $k$ is a $[p, q, r]$th power.

We measure the 'size' of a solution of (2) by the magnitude $|x^p y^q z^r|$. Thus our new proper solution is larger than our old proper solution unless $|X^p/k||Y^q/k||Z^r/k| \le |x^p y^q z^r|$, that is $|F^p/k||G^q/k||H^r/k| \le 1$. Since each term here is an integer, this implies that either one of them is zero, or else they are all equal in absolute value. Thus either $f(u/v)g(u/v)h(u/v) = 0$, or $f(u/v)^p = g(u/v)^q = h(u/v)^r$ using (5.1) (here we do not allow $u = v$ or $u = 0$ since they would both imply $xyz = 0$).

### 5d. Number fields in which there are infinitely many solutions.

In section 7 we will give values of $a, b, c$ for which $ax^p + by^q = cz^r$ has a parametric solution, for each choice of $p, q, r > 1$ with $1/p + 1/q + 1/r > 1$. Now $ax^p$ is a $p$th power in $\mathbf{Q}(a^{1/p}, b^{1/q}, c^{1/r})$ (similarly $by^q$ and $cz^r$), so we have a parametric solution, in this field, to $x^p + y^q = z^r$. Then, given any choice of coprime $A, B, C$, we can certainly choose the parameters in an appropriate number field so that $A$ divides $x^p$, $B$ divides $y^q$ and $C$ divides $z^r$. This thus leads to a number field in which there are infinitely many solutions of (2).

In the last subsection we described a technique that allowed us, given one proper solution to (2), to generate infinitely many (except in a few easily found cases), provided one has an appropriate solution to (5.1). In section 7 an appropriate solution will be found whenever $1/p + 1/q + 1/r = 1$. Thus given algebraic numbers $x, y$, chosen so that $C$ divides $ax^p + by^q$, we can find $z$ from (2), and then get infinitely many solutions to (2) by the method of (5.1). If our original choice of $x, y$ lies in the torsion of the method of section 5c, then we may replace $x$ by any number $\equiv x \pmod c$ (and similarly $y$ by any number $\equiv y \pmod c$) and it is easily shown to work for some such choice.

For any $F(X, Y)$ and $m$ satisfying the cases (i)–(vii) of Theorem 1, we claim that there are number fields $K$ in which (1) has infinitely many proper $K$-integral solutions. To see this start by taking $K$ to be a field which contains $c^{1/m}$ as well as the roots of $F(t, 1) = 0$. Then we shall try to select $X$ and $Y$ so that each of the factors in cases (i)–(vii) is itself an $m$th power.

In (i) we can determine $X$ and $Y$ directly from the two linear equations $X - \alpha Y = u^m$, $X - \beta Y = v^m$, where $u$ and $v$ are selected to be coprime with each other and $\beta - \alpha$, but with $v - u$ divisible by $\beta - \alpha$.

In each of the cases (iii)–(vii) we get three linear equations in $X$ and $Y$, which we can assume are each equal to a constant times an appropriate power of a new variable. Eliminating $X$ and $Y$ by taking the appropriate linear combination of the three linear equations, we get to an equation of the form (2), with $1/p+1/q+1/r \geq 1$. Just above we saw how to find number fields in which there are infinitely many proper solutions to such equations.

The only case not yet answered arises from case (ii) of Theorem 1, defining an equation (2) with $m = 2$ and $F$ quartic. Select $x$ and $y$ to be large coprime integers and $z = \sqrt{F(x,y)}$; by the appropriate modification of the Lutz-Nagell Theorem, we see that these can certainly be chosen to get a non-torsion point on the corresponding curve. Taking multiples of this point we get an infinite sequence of solutions to $z^2 = F(x,y)$ in the same field. As in section 1a we may replace $x$ and $y$ by appropriate multiples, to force $(x,y)$ to belong to a certain finite set of ideals; and thus find proper solutions (we leave it to the reader to show that these must be distinct).

## 6. The generalized Fermat equation when $1/p + 1/q + 1/r = 1$.

In each of these cases the proper solutions to (2) correspond to rational points on certain curves of genus one. The coverings $X$ are well-known, and are to be found in the classical treatment of curves with complex multiplication: in fact, it has long been known that the equations $x^p + y^q = z^r$ with $xyz \neq 0$ and $1/p+1/q+1/r = 1$, have only one proper solution, namely $3^2 + 1 = 2^3$. Our discussion here is little more than a reformulation of the descent arguments of Euler and Fermat, from their studies of the Fermat equation for exponents 3 and 4.

In looking for appropriate solutions to (5.1), we note that we may look for suitable $\mathbf{Q}[t]$-points on the genus one curve $E_t : \ tf(t)^p + (1-t)g(t)^q = 1$ (taking $r = 3, 6$ and 4 below, respectively); which we will be able to find by taking multiples of the point $(1,1)$. Thus, except in a few special cases, any one proper solution to (2) gives rise to infinitely many.

### 6a. $Ax^3 + By^3 = Cz^3$: The Fermat cubic.

The elliptic curve $E : v^3 = u^3 - 1$ has $j$-invariant 0 and complex multiplication by $\mathbf{Q}(\sqrt{-3})$. It has no non-trivial rational points, as was proved by Euler in 1753 (though an incomplete proof was proposed by Alkhodjandi as early as 972). In fact the proper solutions to the equation

$$Ax^3 + By^3 + Cz^3 = 0$$

correspond to rational points on a certain curve of genus 1, which is a principal homogeneous space for $E$.

In 1886, Desboves [De2] gave explicit expressions for deriving new proper solutions from old ones (essentially doubling the point on the associated curve). In fact these identities correspond to doubling the point $(1, 1)$ on $E_t$ getting

$$t(t-2)^3 + (1-t)(1+t)^3 = (1-2t)^3.$$

Thus if we begin with a solution $(x, y, z)$ of $Ax^3+By^3 = Cz^3$ then we have another solution to $AX^3 + BY^3 = CZ^3$ given by

$$X = x(u-2v), \quad Y = y(u+v), \quad Z = z(v-2u)$$

where $u = Ax^3$ and $v = Cz^3$ (and $k = (3, u+v)^3$). All cases where this fails to give a larger proper solution correspond to the point $(\pm 1, \pm 1, \pm 1)$ on $x^3 + y^3 = 2z^3$.

### 6b. $Ax^2 + By^3 = Cz^6$: Another Fermat cubic.

The elliptic curve $E : v^2 = u^3 - 1$ also has $j$-invariant 0. The map $\pi : E \mapsto \mathbf{P}_1$ defined by $\pi(u, v) = u^3 = t$ has degree 6 and signature $(3, 2, 6)$. The points $t = y^3/z^6$ in $\mathbf{P}_1(\mathbf{Q})$ derived from proper solutions of $x^2 = y^3 - z^6$ are in a natural $1-1$ correspondance with the points $(u, v) = (y/z^2, x/z^3)$ in $E(\mathbf{Q})$. Euler showed that $E(\mathbf{Q})$ has rank 0, and hence $x^2 = y^3 - z^6$ has no non-trivial proper solutions. One can similarly look at rational points on twists of the curve $E$, when considering $Ax^2 = -By^3 + Cz^6$.

In fact Bachet showed that, other than $3^2 - 2^3 = 1$ there are no non-trivial proper solutions to $x^2 - y^3 = z^6$.

Quintupling the point $(1, 1)$ on $E_t$ we get

$$t(t^{12} + 4680t^{11} - 936090t^{10} + 10983600t^9 - 151723125t^8 - 508608720t^7 + 3545695620t^6 - 12131026560t^5 + 27834222375t^4 - 37307158200t^3 + 27119434230t^2 - 10331213040t +1937102445)^2 + (1-t)(t^8 - 2088t^7 + 64908t^6 + 21384t^5 + 1917270t^4 - 5616216t^3 +7007148t^2 - 4251528t + 531441)^3 = (5t^4 + 360t^3 - 1350t^2 + 729)^6.$$

A straightforward computation gives that $k$ is always the sixth power of an integer dividing $2^8 3^6$. All cases where this fails to give a larger proper solution correspond to the points $(\pm 1, 1, \pm 1)$ on $4y^3 - 3x^2 = z^6$, and $(\pm 3, 2, \pm 1)$ on $x^2 - y^3 = z^6$.

### 6c. $Ax^4 + By^4 = Cz^2$: The curve with invariant $j = 1728$.

Fermat's only published account of his *method of descent* was his proof, in around 1636, that there are no non-trivial proper solutions to $x^4 + y^4 = z^2$, thus establishing his Last Theorem for exponent 4. In 1678 Leibniz showed that $x^4 - y^4 = z^2$ has no non-trivial proper solutions.

The elliptic curve $E : v^2 = u^3 - u$ has $j$-invariant 1728 and complex multiplication by $\mathbf{Q}(\sqrt{-1})$. The map $\pi : E \mapsto \mathbf{P}_1$ defined by $\pi(u, v) = u^2 = t$ has degree 4 and signature $(4, 2, 4)$. The points $t = x^4/y^4$ in $\mathbf{P}_1(\mathbf{Q})$ derived from proper solutions of $x^4 - y^4 = z^2$ are in a natural $1 - 1$ correspondance with the points $(u, v) = (x^2/y^2, xz/y^3)$ in $E(\mathbf{Q})$; and one can easily show that $E(\mathbf{Q})$ has rank 0.

Tripling the point $(1, 1)$ on $E_t$ we get

$$t(t^2 + 6t - 3)^4 + (1 - t)(t^4 - 28t^3 + 6t^2 - 28t + 1)^2 = (3t^2 - 6t - 1)^4.$$

A straightforward computation gives that $k$ is always the fourth power of an integer dividing 8. All cases where this fails to give a larger proper solution correspond to the point $(1, 1, 1)$ on $x^4 + y^4 = 2z^2$.

## 7. The generalized Fermat equation when $1/p + 1/q + 1/r > 1$.

In each of these cases the proper solutions to (2) correspond to rational points on certain curves of genus zero. Sometimes we can write down equations for Galois coverings of signature $(p, q, r)$, which may allow us to exhibit infinitely many proper solutions to (2): To each such $(p, q, r)$ we will associate a certain (explicit) finite subgroup $\Gamma$ of $\mathbf{PGL}_2$, corresponding to the symmetries of a regular solid. The covering $\pi$ is then given by the quotient map $\pi : \mathbf{P}_1 \longrightarrow \mathbf{P}_1/\Gamma$; and we may write down equations for $\pi$ over $\mathbf{Q}$, even though the action of $\Gamma$ may not be defined over $\mathbf{Q}$. Rational points on these coverings will then lead to infinitely many proper solutions to (2).

It is easy to show that there are infinitely many proper solutions of every equation $x^p + y^q = z^r$ with $1/p + 1/q + 1/r > 1$. If two of the exponents are 2 then the solutions are easy to parametrize; small examples in the other cases include:

$$11^3 + 37^3 = 228^2, \quad 143^3 + 433^2 = 42^4, \quad 3^4 + 46^2 = 13^3 \quad \text{and} \quad 10^2 + 3^5 = 7^3.$$

### 7a. $Ax^2 + By^2 = Cz^r$: Dihedral coverings.

The dihedral group $\Gamma = D_{2r} = \langle \sigma, \tau : \ \sigma^r = \tau^2 = (\sigma\tau)^2 = 1 \rangle$ of order $2r$, acts on $t \in X = \mathbf{P}_1$ by the actions $\sigma(t) = \zeta_r t$ and $\tau(t) = 1/t$, where $\zeta_r$ is a primitive $r$th root of unity. The function $(t^r + t^{-r})/4$ generates the field of invariants of $\Gamma$, and so

$$\pi_{2,2,r} : X \longrightarrow \mathbf{P}_1 \quad \text{defined by} \quad \pi_{2,2,r}(t) = (t^r + t^{-r})^2/4$$

is a covering map of signature $(2, 2, r)$ with Galois group $\Gamma$. One can recover the parametric solution $(t^r + 1)^2 - (t^r - 1)^2 = 4t^r$ from $\pi$.

Parametric solutions to $x^2+y^2=z^r$ may be obtained by defining polynomials $x$ and $y$ from the formula $x(u,v)+iy(u,v)=(u+iv)^r$, with $z=u^2+v^2$. Parametric solutions to $x^2+y^2=z^r$ may be obtained by taking $(u^r+2^{r-2}v^r)^2-(u^r-2^{r-2}v^r)^2=(2uv)^r$. In each case we get proper solutions whenever $v$ is even and $(u,v)=1$.

To obtain a solution to (5.1), define polynomials $f$ and $h$ by $h-\sqrt{t}f=(1-\sqrt{t})(1-\sqrt{t}(1-t))^{2r}$ so that $tf^2+(1-t)(1-t(1-t)^2)^{2r}=h^2$. With some work we find that, in all cases, $k=1$ and our new proper solution is larger than our old one.

### 7b. $Ax^3+By^3=Cz^2$: Tetrahedral coverings.

The group of rotations, $\Gamma$, which preserve a regular tetrahedron, is isomorphic to the alternating group on four letters. The covering map

$$\pi_1 : X' \longrightarrow \mathbf{P}_1 \quad \text{defined by} \quad \pi_1(t)=-(t-1)^3(t-9)/64t$$

has signature $(3,2,3)$ and degree 4, since $1-\pi_1(t)=(t^2-6t-3)^2/64t$. Let $X$ be the Galois closure of $X'$ over $\mathbf{P}_1$. Since the covering map $\pi_2 : X \longrightarrow X'$ must be cyclic of degree 3, and ramified at both 0 and $9\in X'$, we may define it by $\pi_2(u)=9/(1-u^3)$. The composition covering map $\pi_{2,3,3}=\pi_1\circ\pi_2 : X \longrightarrow \mathbf{P}_1$ is then given by

$$\pi_{2,3,3}(u)=\frac{(u^3+8)^3u^3}{64(u^3-1)^3} \quad \text{so that} \quad 1-\pi_{2,3,3}(u)=\frac{-(u^6-20u^3-8)^2}{64(u^3-1)^3}\ .$$

The general solution to $x^3+y^3=z^2$ splits into two parametrizations:
$x=a(a^3-8b^3)/t^2,\ y=4b(a^3+b^3)/t^2,\ z=(a^6+20a^3b^3-8b^6)/t^3$,
where $(a,b)=1$, $a$ is odd and $t=(3,a+b)$ (due to Euler, 1756); and
$x=(a^4+6a^2b^2-3b^4)/t^2,\ y=(3b^4+6a^2b^2-a^4)/t^2,\ z=6ab(a^4+3b^4)/t^3$,
where $(a,b)=1$, 3 doesn't divide $a$, and $t=(2,a+1,b+1)$ (due to Hoppe, 1859).

One obtains infinitely many proper solutions of $x^3+y^3=Cz^2$ by taking $ab=Ct^2$ even, with $(a,b)=1$ and 3 not dividing $a$, in Euler's identity
$(6ab+a^2-3b^2)^3+(6ab-a^2+3b^2)^3=ab\{6(a^2+3b^2)\}^2$.
Moreover Gerardin (1911) gave a formula to obtain a new solution from a given one:
$(a^3+4b^3)^3-(3a^2b)^3=(a^3+b^3)(a^3-8b^3)^2$.

A solution to (5.1) is given by

$$t(-7-42t+t^2)^3+(1-t)(1+109t-109t^2-t^3)^2=(1-42t-7t^2)^3.$$

The prime divisors of $k$ can only be 2 and 3; but $k$ is not necessarily a sixth power; so proper solutions do not necessarily lead to new proper solutions of the same equation.

### 7c. $Ax^2+By^3=Cz^4$: Octahedral coverings.

The group of rotations, $\Gamma$, which preserve a regular octahedron (or *cube*), is isomorphic to the permutation group on four letters. A map $\pi_{2,3,4} : \mathbf{P}_1 \longrightarrow \mathbf{P}_1$ of signature $(2,3,4)$ can be obtained by considering the projection $\mathbf{P}_1 \longrightarrow \mathbf{P}_1/\Gamma$, so that $\pi_{2,3,4}$ has degree $|\Gamma| = 24$. However we may obtain an equation for $\pi_{2,3,4}$ without explicitly finding the $\Gamma$-invariants or even writing down the action of $\Gamma$, by observing that one can take $\pi_{2,3,4} = \phi \cdot \pi_{2,3,3}$, where $\phi : \mathbf{P}_1 \longrightarrow \mathbf{P}_1$ is a map of degree 2 for which

$$\phi(1) = \infty, \quad \phi(0) = \phi(\infty) = 0, \quad \text{and} \quad \phi \text{ is ramified over } 1.$$

The only function $\phi$ with these properties is $\phi(t) = -4t/(t-1)^2$, so that

$$\pi_{2,3,4}(u) = \frac{-2^8(u(u^3-1)(u^3+8))^3}{(u^6-20u^3-8)^4} \quad \text{and} \quad 1-\pi_{2,3,4}(u) = \frac{((u^6+8)(u^6+88u^3-8))^2}{(u^6-20u^3-8)^4} \quad .$$

We have a parametric solution to $x^2 + y^3 = z^4$ by taking $A = a^4,\ B = b^4$ and $C = 4A - 3B$ in
$C^2(16A^2 + 408AB + 9B^2)^2 + \left(144AB - C^2\right)^3 = AB(24A + 18B)^4$.
This leads to a proper solution if $b$ is odd, 3 does not divide $a$, and $(a,b) = 1$. We have a parametric solution to $x^2 + y^4 = z^3$ by taking $P = p^2,\ Q = q^2$ in
$16PQ(P-3Q)^2(P^2+6PQ+81Q^2)^2(3P^2+2PQ+3Q^2)^2+(3Q+P)^4(P^2-18PQ+9Q^2)^4 = (P^2-2PQ+9Q^2)^3(P^2+30PQ+9Q^2)^3$.
This leads to a proper solution if $p+q$ is odd, 3 does not divide $p$, and $(p,q) = 1$. There is an easy parametric solution to $108x^4 + y^3 = z^2$ gotten by taking $U = u^4,\ V = v^4$ in
$108UV(U+V)^4 + (U^2 - 14UV + V^2)^3 = (U^3 + 33U^2V - 33UV^2 - V^3)^2$.
This leads to a proper solution if $uv$ is even and $(u,v) = 1$.

### 7d. $Ax^2 + By^3 = Cz^5$: Klein's Icosahedron.

We follow [Hi] (p. 657) in describing Klein's beautiful analysis of $x^2 + y^3 = z^5$: The group of rotations, $\Gamma$, which preserve a regular icosahedron, is isomorphic to the alternating group on five letters. A map $\pi_{2,3,5} : \mathbf{P}_1 \longrightarrow \mathbf{P}_1$ of signature $(2,3,5)$ can be obtained by considering the projection $\mathbf{P}_1 \longrightarrow \mathbf{P}_1/\Gamma$, with $\Gamma$ thought of as a subgroup of $\mathbf{PGL}_2$. The ramification points of order $2, 3$ and $5$ occur, respectively, as the edge midpoints, face centers, and vertex points, of the icosahedron.

The zeroes of $z(u,v) = uv(u^{10} + 11u^5v^5 - v^{10})$ in $\mathbf{P}_1(\mathbf{C})$ lie at $u/v = 0,\ \infty$ and $\left(\frac{-1\pm\sqrt{5}}{2}\right)e^{2i\pi j/5}$, corresponding to the twelve vertices of the icosahedron under stereographic projection onto the Riemann sphere. The homogeneous polynomials

$$x(u,v) = (\nabla z \times \nabla y)\cdot \vec{k} \qquad \text{and} \qquad y(u,v) = \frac{1}{121}\det(\text{Hessian}(z(u,v))),$$

are invariant under the action of the icosahedral group (where $\nabla$ denotes the gradient of a function in the $(u,v)$-plane, and $\vec{k}$ is the unit vector normal to the $(u,v)$-plane and oriented in the standard positive direction). They satisfy the icosahedral relation $x(u,v)^2+y(u,v)^3=1728z(u,v)^5$ leading to Klein's identity,

$$\begin{aligned}&(a^6+522a^5b-10005a^4b^2-10005a^2b^4-522ab^5+b^6)^2\\&\quad-(a^4-228a^3b+494a^2b^2+228ab^3+b^4)^3=1728ab(a^2+11ab-b^2)^5.\end{aligned}$$

This gives proper solutions to $x^2+y^3=Cz^5$, if we take $ab=144Ct^5$, with $\gcd(a,b)=1$ and $a\not\equiv 2b \pmod 5$.

The factor $1728=12^3$ which appears above is familiar to amateurs of modular forms (it is the constant term in the modular function $j$). Klein observed that this is no accident, since our icosahedral covering can be realized as the covering of modular curves $X(5)\longrightarrow X(1)$, where $X(1)$ is the $j$-line.

## 8. The 'class group' obstruction to a 'local-global' principle.

If 3 does not divide $ab$ then $z=(a^2+29b^2)/3,\ x=az,\ y=bz$ is a solution to

$$x^2+29y^2=3z^3. \tag{8.1}$$

Taking $a=b=1$ gives $x=y=z=10$; taking $a=2,b=1$ gives $x=22,\ y=z=11$. For every prime $p$ at least one of these two solutions has no more than one of $x,y,z$ divisible by $p$; that is there exist 'proper local solutions' to (8.1) for every prime $p$. So are there any proper solutions 'globally' ?

Suppose that we are given a proper solution to (8.1). Factor (8.1) as an ideal equation:

$$(x+\sqrt{-29}y)(x-\sqrt{-29}y)=(3)(z)^3.$$

$G=(x+\sqrt{-29}y,x-\sqrt{-29}y)$ divides $(2x,2\sqrt{-29}y,3z^3)=(2,z)$, which equals 1; since if $z$ were even then $x$ and $y$ must both be odd, and so (8.1) would give $1+29\equiv 0 \pmod 8$, which is false. Thus $G=1$ and so (choosing the sign of $y$ appropriately),

$$(x+\sqrt{-29}y)=(3,1+\sqrt{-29})\zeta_+^3 \text{ and } (x-\sqrt{-29}y)=(3,1-\sqrt{-29})\zeta_-^3,$$

where $\zeta_+\zeta_-=(z)$. This implies that the ideal classes which $(3,1\pm\sqrt{-29})$ belong to, must both be cubes inside the class group $C$ of $\mathbf{Q}(\sqrt{-29})$. However this is false since they both are generators of $C$, which has order 6. Therefore (8.1) has no proper solutions, indicating that the 'local-global' principle fails.

It is not too hard to generalize this argument to get 'if and only if' conditions for the existence of proper solutions to (2); especially for carefully chosen values of $A,B,C$ and $r$. We prove

**Proposition.** *Suppose $r \geq 2$, and $b$ and $c$ are coprime positive integers with $b \equiv 1 \pmod 4$ and squarefree, and $c$ odd.*
*i) There are proper integer solutions to $x^2 + by^2 = cz^r$ if and only if there exist coprime ideals $J_+, J_-$ in $\mathbf{Q}(\sqrt{-b})$ with $J_+J_- = (c)$, whose ideal classes are $r$th powers inside the class group of $\mathbf{Q}(\sqrt{-b})$.*
*ii) There are proper local solutions to $x^2 + by^2 = cz^r$ at every prime $p$ if and only if the Legendre symbol $(-b/p) = 1$ for every prime $p$ dividing $c$; and, when $r$ is even we have $(c/p) = 1$ for every prime $p$ dividing $b$, as well as $c \equiv 1 \pmod 4$.*

*Proof:* Given proper integer solutions to $x^2+by^2 = cz^r$, the proof of i) is entirely analogous to the case worked out above. In the other direction, if the ideal class of $J_+$ is an $r$th power we may select an integral ideal $\zeta_+$ for which $J_+\zeta_+^r$ is principal, $= (x + \sqrt{-b}y)$ say. Then $(x^2 + by^2) = (cz^r)$ where $(z)$ =Norm$(\zeta_+)$, and the result follows.

In (ii) it is evident that all of the conditions are necessary. We must show how to find a proper local solution at prime $p$ given these conditions: It is well known that if prime $p$ does not divide $2bc$ then there is a solution in $p$-adic units $x, y$ to $x^2 + by^2 = c$ and so we can take $(x, y, 1)$. It is also well known that if prime $p$ is odd and $(-b/p) = 1$ then there is a $p$-adic unit $x$ such that $x^2 = -b$, and so we take $(x, 1, 0)$. Similarly if $(c/p) = 1$ then there is a $p$-adic unit $x$ such that $x^2 = c$, and so we take $(x, 0, 1)$. If $r$ is odd and $p$ does not divide $c$ then we may take $(c^{(r+1)/2}, 0, c)$. Finally if $r$ is even and $c \equiv 5 \pmod 8$ then there is a $p$-adic unit $x$ such that $x^2 = c - 4b$, so we take $(x, 2, 1)$.

The conditions for proper integer solutions, given above, depend on the value of $(r, h)$ where $h$ is the class number of $\mathbf{Q}(\sqrt{-b})$. On the other hand the conditions for proper local solutions everywhere, given above, depend only on the parity of $r$. The local-global principle for conics tells us that these are the same for $r = 2$; but it is evident that the conditions are not going to co-incide if $(r, h) \geq 3$.

The techniques used here may be generalized to study when the value of an arbitrary binary quadratic form is equal to a given constant times the $r$th power of an integer. The techniques can also be modified to find obstructions to a local-global principle for equations $x^2 + by^4 = cz^3$; and probably to $x^3 + by^3 = cz^2$. On the other hand there are never any local obstructions for equations $Ax^2 + By^3 = Cz^5$ which have $A, B, C$ pairwise coprime: If $p$ does not divide $AB$ or $AC$ or $BC$, then we can take $(AB^2, -AB, 0)$ or $(A^2C^3, 0, AC)$ or $(0, B^3C^2, B^2C)$, respectively. Could it be that such equations always have proper integer solutions ?

## 9. Conjectures on generalized Fermat equations.

### 9a. How many proper solutions can (2) have if $1/p + 1/q + 1/r < 1$ ?

It is evident that any equation of the form

$$(y_1^q z_2^r - y_2^q z_1^r)\ x^p \ + \ (z_1^r x_2^p - z_2^r x_1^p)\ y^q \ = \ (x_2^p y_1^q - x_1^p y_2^q)\ z^r$$

has the two solutions $(x_i, y_i, z_i)$. If there are three solutions to an equation (2) then we may eliminate $A, B$ and $C$ using linear algebra to deduce that

$$x_1^p y_2^q z_3^r + x_2^p y_3^q z_1^r + x_3^p y_1^q z_2^r = x_1^p y_3^q z_2^r + x_2^p y_1^q z_3^r + x_3^p y_2^q z_1^r.$$

If $1/p + 1/q + 1/r$ is sufficiently small then the generalization of the *abc*-conjecture (see section 5b) implies that this has only finitely many solutions. Thus there are only finitely many triples of coprime integers $A, B, C$ for which (2) has more than two proper solutions. (Bombieri and Mueller [BU] proved such a result unconditionally in $\mathbf{C}[t]$, since [BM] provides the necessary generalization of the *abc*-conjecture).

If $n = p = q = r$, then it is easy to determine $A, B, C$ from the equation above. In fact Desboves [De1] proved that the set of coprime integers $A, B, C$ together with three given distinct solutions to $Ax^n + By^n = Cz^n$, is in $1-1$ correspondance with the set of coprime integer solutions to

$$r^n + s^n + t^n = u^n + v^n + w^n \qquad \text{with} \qquad rst = uvw.$$

Applying a suitable generalized *abc*-conjecture to this we immediately deduce: There exists a number $n_0$ such that *If* $n \geq n_0$ *then there are at most two proper solutions to* $Ax^n + By^n = Cz^n$ *for any given non-zero integers* $A, B, C$. Moreover there exist infinitely many triples $A, B, C$ for which there do exist two proper solutions.

### 9b. Diagonal equations with four or more terms.

The generalized *abc*-conjecture implies that

$$a_1 x_1^{p_1} + a_2 x_2^{p_2} + \ldots + a_n x_n^{p_n} = 0$$

has only finitely many *proper* $K$-integral solutions, in every number field $K$, if $\sum_j 1/p_j$ is sufficiently small. Here are a few interesting examples of known solutions to such equations: i) Ryley proved that every integer can be written as the sum of three rational cubes[9]. For example, Mahler noted that $2 = (1 + 6t^3)^3 + (1 - 6t^3)^3 - (6t^2)^3$. Ramanujan gave a parametric solution for $x^3 + y^3 + z^3 = t^3$:

$$(3a^2 + 5ab - 5b^2)^3 + (4a^2 - 4ab + 6b^2)^3 + (5a^2 - 5ab - 3b^2)^3 = (6a^2 - 4ab + 4b^2)^3.$$

[9] which appeared in *The Ladies' Diary* (1825), 35.

Examples include $3^3 + 4^3 + 5^3 = 6^3$, and Hardy's taxi-cab number $1^3 + 12^3 = 9^3 + 10^3$.
ii) Taking $u = (x_n - y_n)/2$, $v = y_n$, where $\left(\frac{x_n+y_n\sqrt{-3}}{2}\right) = \left(\frac{5+\sqrt{-3}}{2}\right)^n$, in Diophantos's identity

$$(9.1) \qquad u^4 + v^4 + (u+v)^4 = 2(u^2 + uv + v^2)^2,$$

gives proper solutions to $a^4 + b^4 + c^4 = 2d^n$; specifically,

$$(9.2) \qquad \left(\frac{x_n + y_n}{2}\right)^4 + \left(\frac{x_n - y_n}{2}\right)^4 + y_n^4 = 2 \times 7^{2n}.$$

iii) Euler gave the first parametric solution to $x^4 + y^4 = a^4 + b^4$, in polynomials of degree seven; an example is $59^4 + 158^4 = 133^4 + 134^4$. By a sophisticated analysis of Demanjenko's pencil of genus one curves on the surface $t^4 + u^4 + v^4 = 1$, Elkies [E1] showed that there are infinitely many triples of coprime fourth powers of integers whose sum is a fourth power[10], the smallest of which is

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

iv) In 1966 Lander and Parkin's gave the first counterexample to Euler's conjecture,

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

In 1952 Swinnerton-Dyer had shown how to give a parametric solution to $a^5 + b^5 + c^5 = x^5 + y^5 + z^5$; a small example is $49^5 + 75^5 + 107^5 = 39^5 + 92^5 + 100^5$.
iv) In 1976 Brudno gave a parametric solution to $a^6 + b^6 + c^6 = x^6 + y^6 + z^6$ of degree 4; a small example is $3^6 + 19^6 + 22^6 = 10^6 + 15^6 + 23^6$.

We do know of various examples of

$$(4) \qquad Ax^j + By^k + Cz^\ell = Dw^m,$$

with infinitely many proper solutions and $1/j + 1/k + 1/\ell + 1/m$ small:
a) (9.2) is an example of an equation (4) having infinitely many proper solutions, with $1/j + 1/k + 1/\ell + 1/m$ arbitrarily close to 3/4. We can also get this by taking $u = x^p$ and $v = y^q$ in (9.1).
b) In section 6 we saw how to choose $A, B, C$, for any given $1/p + 1/q + 1/r = 1$, so that there are infinitely many proper solutions to (2). Substituting $u = Ax^p$ and $v = By^q$ of

[10] radically contradicting Euler's Conjecture that, for any $n \geq 3$, the sum of $n-1$ distinct $n$th powers of positive integers cannot be an $n$th power.

(2) into Diophantos's identity (9.1), we obtain infinitely many proper solutions of some equation (4) with exponents $(4p, 4q, 4r, 2)$, so that $1/j + 1/k + 1/\ell + 1/m = 3/4$.

c) By taking $t = 2z^n$ in the identity $(t+1)^3 - (t-1)^3 = 6t^2 + 2$, we get infinitely many proper solutions to $x^3 + y^3 = 24z^{2n} + 2w^m$; here $1/j + 1/k + 1/\ell + 1/m$ is arbitrarily close to 2/3.

d) If we allow *improper* solutions, that is where pairs of the monomials in (4) have large common factors, then one can get $1/j + 1/k + 1/\ell + 1/m$ arbitrarily close to 1/2 from the identity $x^{2n} + 2(xy)^n + y^{2n} = (x^n + y^n)^2$.

## References

[Be] Beckmann, S., *On extensions of number fields obtained by specializing branched coverings*, Jour. für die reine und ang. Math. **419** (1991), 27–53.

[Bo] Bombieri, E., *The Mordell Conjecture Revisited*, Annali Scuola Normale Sup. Pisa, Cl. Sci., S. IV, **17** (1990), 615–640.

[BU] Bombieri, E., and Mueller, J., *The Generalized Fermat Equation in Function Fields*, J. Number Theory, **39** (1991), 339–350.

[BM] Brownawell, W.D., and Masser, D.W., *Vanishing sums in function fields*, Math. Proc. Camb. Phil. Soc., **100** (1986), 427–434.

[Da] Darmon, H., *The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$*, Int. Math. Res. Notices, **10** (1993), 263–274.

[De1] Desboves, A., , Nouv. Ann. Math., Sér II, **18** (1879), 481–489.

[De2] Desboves, A., *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.

[Di] Dickson, L.E., *History of the Theory of Numbers* in 3 volumes, (Chelsea, New York, 1971).

[E1] Elkies, N.D., *On $A^4 + B^4 + C^4 = D^4$*, Math. Comp. **51** (1988), 825–835.

[E2] Elkies, N.D., *'abc' implies Mordell*, Int. Math. Res. Notices, **7** (1991), 99–109.

[ES] Erdős, P. and Selfridge, J.L., *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292–301.

[F1] Faltings, G., *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math., **73** (1983), 349–366.

[F2] Faltings, G., *Diophantine Approximation on Abelian Varieties*, Annals of Math., **133** (1991), 549–576.

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

[Hi] Hirzebruch, *The Icosahedron*, Sackler Lecture, Tel Aviv, (1981); Collected Works, 656–661.

[Le] LeVeque, W. J., *On the equation $y^m = f(x)$*, Acta Arith., **9** (1964), 209–219.

[Ma] Mason, R. C., *Diophantine Equations over Function Fields*, L.M.S. Lecture Notes No. 96, Cambridge, 1984.

[Mo1] Mordell, L. J., *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Camb. Phil. Soc., **21** (1922), 179–192.

[Mo2] Mordell, L. J., *Diophantine Equations*, Academic Press, London, 1969.

[PR] Powell, B. J. and Ribenboim, P. R., *Note on a paper of M. Filaseta regarding Fermat's Last Theorem*, Ann. Univ. Turku, **187** (1985), 1–22.

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

[Se 1] Serre, J.-P., *Topics in Galois Theory*, Research Notes in Math, Vol. 1, (Jones and Bartlett, Boston, 1992).

[Se 2] Serre, J.-P., *Sur les représentations modulaires de degré* 2 *de Gal*($\bar{\mathbf{Q}}/\mathbf{Q}$), Duke Math. J. **54** (1987), 179–230.

[Si] Siegel, C. L., *Über einige Anwendungen Diophantischer Approximationen*, Abh. preuss. Akad. Wiss. 1929, No 1.

[ST] Shorey, T. N. and Tijdeman, R., *Exponential Diophantine Equations*, Cambridge Tracts No. 87, Cambridge, 1986.

[Ti1] Tijdeman, R., *On the equation of Catalan*, Acta Arith. **29** (1976), 197–209.

[Ti2] Tijdeman, R., *Diophantine Equations and Diophantine Approximations*, Number Theory and Applications (ed. R.A. Mollin), (Kluwer, NATO ASI series, Ser.C, vol. 265), 1989, 215–244.

[V1] Vojta, P., *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math. No. 1239, Springer–Verlag, 1987.

[V2] Vojta, P., *Arithmetic and Hyperbolic Geometry*, Vol. I., I.C.M. proceedings 1990 (Springer-Verlag), 757–765.

[V3] Vojta, P., *Siegel's Theorem in the compact case*, Annals of Math., **133** (1991), 509–548.

[Vl] Voloch, J.F., *Diagonal equations over function fields*, Bol. Soc. Brasil. Mat., **16** (1985), 29–39.

[W] Welmin, W.P., Mat. Sbornik (Math. Soc. Moscow), **24** (1903–4), 633–661.

Henri Darmon, Dept. of Math., Princeton U., Princeton, NJ 08540, USA.
(darmon@math.Princeton.EDU)

Andrew Granville, Dept. of Math., U. of Georgia, Athens, Ga 30602, USA.
(andrew@sophie.math.uga.edu)