It's As Easy As *abc*

Andrew Granville and Thomas J. Tucker

Introduction

Fermat's Last Theorem

In this age in which mathematicians are supposed to bring their research into the classroom, even at the most elementary level, it is rare that we can turn the tables and use our elementary teaching to help in our research. However, in giving a proof of Fermat's Last Theorem, it turns out that we can use tools from calculus and linear algebra only. This may strike some readers as unlikely, but bear with us for a few moments as we give our proof.

Fermat claimed that there are no solutions to

$$x^p + y^p = z^p \tag{1}$$

for $p \geq 3$, with x, y, and z all nonzero. If we assume that there are solutions to (1), then we can assume that x, y, and z have no common factor, else we can divide out by that factor. Our first step will be to differentiate (1) to get

$$px^{p-1}x' + py^{p-1}y' = pz^{p-1}z',$$

and after dividing out the common factor p, this leaves us with

$$x^{p-1}x' + y^{p-1}y' = z^{p-1}z'. \tag{2}$$

We now have two linear equations (1) and (2) (thinking of x^{p-1}, y^{p-1}, and z^{p-1} as our variables), which suggests using linear algebra to eliminate a variable: Multiply (1) by y' and (2) by y, and subtract to get

$$x^{p-1}(xy' - yx') = z^{p-1}(zy' - yz').$$

Therefore x^{p-1} divides $z^{p-1}(zy' - yz')$, but since x and z have no common factors, this implies that

$$x^{p-1} \text{ divides } zy' - yz'. \tag{3}$$

This is a little surprising, for if $zy' - yz'$ is nonzero, then a high power of x divides $zy' - yz'$, something that does not seem consistent with (1).

We want to be a little more precise. Since we differentiated, we evidently never were working with integers x, y, z, but rather with polynomials. Thus if $zy' - yz' = 0$, then $(y/z)' = 0$, and so y is a constant multiple of z, contradicting our statement that y and z have no common factor. Therefore (3) implies that

$$\begin{aligned}(p-1)\ \text{degree}(x) &\leq \text{degree}(zy' - yz')\\ &\leq \text{degree}(y) + \text{degree}(z) - 1,\end{aligned}$$

since $\text{degree}(y') = \text{degree}(y) - 1$ and $\text{degree}(z') = \text{degree}(z) - 1$. Adding degree($x$) to both sides gives

$$p\ \text{degree}(x) < \text{degree}(x) + \text{degree}(y) + \text{degree}(z). \tag{4}$$

The right side of (4) is symmetric in x, y, and z. The left side is a function of x simply because of the order in which we chose to do things above. We

Andrew Granville is a Canadian Research Chair of mathematics at the Université de Montréal. His email address is `andrew@dms.umontreal.ca`.

Thomas J. Tucker is currently a visiting assistant professor at the City University of New York Graduate Center. His email address is `ttucker@math.uga.edu`.

This article is based on the first named author's AMS-MAA invited lecture at the Orlando annual meeting in January 1996.

could just as easily have derived the same statement with y or z in place of x on the left side of (4), so that

$$p \text{ degree}(y) < \text{ degree}(x) + \text{ degree}(y) + \text{ degree}(z)$$

and

$$p \text{ degree}(z) < \text{ degree}(x) + \text{ degree}(y) + \text{ degree}(z).$$

Adding these last three equations together and then dividing out by $\text{degree}(x) + \text{degree}(y) + \text{degree}(z)$ implies

$$p < 3,$$

and so Fermat's Last Theorem is proved!

Well, not quite, but what we have proved (and so simply) is still of great interest:

Proposition 1. There are no genuine polynomial solutions $x(t), y(t), z(t) \in \mathbb{C}[t]$ to $x(t)^p + y(t)^p = z(t)^p$ with $p \geq 3$. By "genuine" we mean that the triple $(x(t), y(t), z(t))$ is not a polynomial multiple of a solution of (1) in $\mathbb{C}$.

That Fermat's Last Theorem is easy to prove for polynomials is an old result, going back certainly as far as Liouville (1851), although his proof, which goes through integration, is much more involved than that given here. The proof we have presented above is certainly some years old; for instance, a variant can be found in standard textbooks of fifty years ago. After reading through it, one sees that this argument is easily generalizable to other Diophantine problems, though it is not obvious what would be the ultimate generalization.

Mason's Generalization

It takes a certain genius to generalize to something far simpler than the original. But what could possibly be more simply stated, yet more general, than Fermat's Last Theorem? It was Richard C. Mason (1983) who gave us that insight:

Look for solutions to

$$a + b = c. \tag{5}$$

We will just follow through the proof above and see where it leads: Start by assuming, with no loss of generality, that a, b, and c are all nonzero polynomials without common factors (else all three share the common factor and we can divide it out). Then we differentiate to get

$$a' + b' = c'.$$

Next we need to do linear algebra. It is not quite so obvious how to proceed analogously, but what we do learn in a linear algebra course is to put our coefficients in a matrix, and solutions follow if the determinant is nonzero. This suggests defining

$$\Delta(t) := \begin{vmatrix} a(t) & b(t) \\ a'(t) & b'(t) \end{vmatrix}.$$

Then if we add the first column to the second, we get

$$\Delta(t) = \begin{vmatrix} a(t) & c(t) \\ a'(t) & c'(t) \end{vmatrix},$$

and similarly

$$\Delta(t) = \begin{vmatrix} c(t) & b(t) \\ c'(t) & b'(t) \end{vmatrix}$$

by adding the second column to the first, a beautiful symmetry.

We note that $\Delta(t) \neq 0$, else $ab' - a'b = 0$, so b is a scalar multiple of a (with the same argument as above), contradicting the hypothesis.

To find the appropriate analogy to (3), we interpret that as stating that the factors of x (as well as of y and z) divide our determinant to a high power. So now suppose that α is a root of $a(t)$ and that $(t-\alpha)^e$ is the highest power of $(t-\alpha)$ which divides $a(t)$. Evidently $(t-\alpha)^{e-1}$ is the highest power of $(t-\alpha)$ which divides $a'(t)$, and thus it is the highest power of $(t-\alpha)$ which divides $\Delta(t) = a(t)b'(t) - a'(t)b(t)$ (since α is not a root of $b(t)$). Therefore $(t-\alpha)^e$ divides $\Delta(t)(t-\alpha)$. Multiplying all such $(t-\alpha)^e$ together, we obtain

$$a(t) \text{ divides } \Delta(t) \prod_{a(\alpha)=0} (t-\alpha).$$

In fact, $a(t)$ appears on the left side of this equation only because we studied the linear factors of a; analogous statements for $b(t)$ and $c(t)$ are also true, and since $a(t)$, $b(t)$, $c(t)$ have no common roots, we can combine those statements to read

$$a(t)b(t)c(t) \quad \text{divides} \quad \Delta(t) \prod_{(abc)(\alpha)=0} (t-\alpha). \tag{6}$$

The next step is to take the degrees of both sides and see what that gives. Using the three different representations of Δ above, we have

$$\text{degree}(\Delta) \leq \begin{cases} \text{degree}(a) + \text{ degree}(b) - 1, \\ \text{degree}(a) + \text{ degree}(c) - 1, \\ \text{degree}(c) + \text{ degree}(b) - 1. \end{cases}$$

The degree of $\prod_{(abc)(\alpha)=0}(t-\alpha)$ is precisely the total number of distinct roots of $a(t)b(t)c(t)$. Inserting all this into (6) we find that

$$\max\{\text{degree}(a),\ \text{degree}(b),\ \text{degree}(c)\} < \#\{\alpha \in \mathbb{C} :\ (abc)(\alpha) = 0\}.$$

Put another way, this result can be read as:

Proposition 2. If $a(t), b(t), c(t) \in \mathbb{C}[t]$ do not have any common roots and provide a genuine polynomial solution to $a(t) + b(t) = c(t)$, then the maximum of the degrees of $a(t), b(t), c(t)$ is less than the number of distinct roots of $a(t)b(t)c(t) = 0$.

This is a "best possible" result in the sense that we can find infinitely many examples where there is exactly one more zero of $a(t)b(t)c(t) = 0$ than the largest of the degrees: for example, the familiar identity

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

or the rather less interesting

$$t^n + 1 = (t^n + 1).$$

Classifying such polynomial identities leads us naturally to the study of a special class of rational functions, as we shall see next.

Silverman's Proof

Silverman provided a more sophisticated route to Proposition 2, via the theory of covering maps, an approach that will turn out to be very useful. Consider rational functions

$$\pi : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\};$$

that is, $\pi(t) = f(t)/g(t)$ for some polynomials f and g. The Riemann-Hurwitz formula is a key result about rational maps; in this case it tells us that

$$\text{(7)} \quad 2 \ \mathrm{degree}(\pi) = 2 + \sum_{z \in \mathbb{C} \cup \{\infty\}} \left\{ \mathrm{degree}(\pi) - \#\pi^{-1}(z) \right\}.$$

Here $\mathrm{degree}(\pi) = \max\{\mathrm{degree}(f),\ \mathrm{degree}(g)\}$, and $\pi^{-1}(z)$ is the set of $x \in \mathbb{C} \cup \{\infty\}$ for which $\pi(x) = z$. This is the set of roots of $f(x) - zg(x) = 0$, and so there are at most $\mathrm{degree}(\pi)$ elements of $\pi^{-1}(z)$, and usually exactly that number. If not, then $f(x) - zg(x) = 0$ must have a double root, so that $f'(x) - zg'(x) = 0$.

From a solution to (5) we set $\pi(t) := a(t)/c(t)$. Since every term on the right side of (7) is nonnegative, we get a lower bound if we consider just the sum over a subset of $\mathbb{C} \cup \{\infty\}$. We select our subset to be $\{0, 1, \infty\}$. Note that if $\pi(\infty) \neq 0$, then $\pi(t) = 0$ if and only if $a(t) = 0$, so $\pi^{-1}(0)$ is the set of distinct roots of a. Similarly, if $\pi(\infty) \neq 1$, then $\pi^{-1}(1)$ is the set of distinct roots of b; and if $\pi(\infty) \neq \infty$, then $\pi^{-1}(\infty)$ is the set of distinct roots of c. Since ∞ can belong to at most one of the sets $\pi^{-1}(0), \pi^{-1}(1), \pi^{-1}(\infty)$, we deduce, by putting all this information into (7), that

$$\text{(8)} \quad \mathrm{degree}(\pi) \le \#\{\text{distinct roots of } abc\} - 1,$$

which is equivalent to Proposition 2.

We get equality in (8) if and only if the subsum we considered in (7) actually includes all of the nonzero terms; that is, $\pi^{-1}(z) = \mathrm{degree}(\pi)$ for every $z \notin \{0, 1, \infty\}$. Maps with this property are called *Belyĭ maps* after G. V. Belyĭ, who first identified their central importance. He showed, amongst other things, that for any finite subset S of $\overline{\mathbb{Q}}$ there is a map $\pi : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ for which $\pi(S) \subseteq \{0, 1, \infty\}$, and $\pi^{-1}(z) = \mathrm{degree}(\pi)$ for every $z \notin \{0, 1, \infty\}$. We can reinterpret this in terms of polynomials as follows.

Proposition 3. For any $f(t) \in \mathbb{Z}[t]$ there exist $a(t), b(t), c(t) \in \mathbb{Z}[t]$ which do not have any common roots and provide a genuine polynomial solution to $a(t) + b(t) = c(t)$ for which $f(t)$ divides $a(t)b(t)c(t)$, and such that the maximum of the degrees of $a(t), b(t), c(t)$ is exactly one less than the number of distinct roots of $a(t)b(t)c(t) = 0$.

Thus we can use Belyĭ maps to construct many "best possible examples" in Proposition 2. As we shall see later, this elegant construction is central to several important results.

An Analogy for Integers?

Many results for Diophantine equations in integers are analogous to results for Diophantine equations in polynomials. Given Mason's wonderfully simple inequality for polynomial solutions to $a + b = c$ (namely Proposition 2), one cannot help but wonder whether there is a similar result for integers (and evidently, if there is, it should imply a direct proof of Fermat's Last Theorem!).

Usually primes are considered to be the appropriate analogy to irreducible factors of polynomials, so one might guess that the analogy to Proposition 1 would be something like:

If $a + b = c$ in coprime integers a, b, c, then the total number of prime factors of a (or b or c) counting multiplicities is less than the total number of distinct prime factors of abc.

When one checks out this conjecture, one quickly finds counterexamples, like $1 + 1 = 2$ or $1 + 3 = 4$ or $1 + 7 = 8$; and the more one looks, the worse the counterexamples get.[1]

That was too easy! Maybe if we modify the conjecture a bit, it will stand up to testing better. It has long been established in analytic number theory that primes, when counted, are best counted with the weight $\log p$ attached. Thus perhaps the appropriate measure for an integer $a = \prod_p p^{e_p}$, analogous to the degree of the polynomial $a(t)$, is not $\sum_p e_p$, but rather $\sum_p e_p \log p$, which equals $\log a$. Then we replace the total number of distinct factors of $a(t)b(t)c(t)$ by $\sum_{p|abc} \log p$, where the sum is over the distinct prime factors p of abc. Taking exponentials of both sides, we get the aesthetically pleasing conjecture:

If $a + b = c$ in coprime integers a, b, c, then

$$\text{(9)} \qquad \max\{a, b, c\} \le \prod_{\substack{p \text{ prime} \\ p|abc}} p.$$

[1] *In fact, if $2^n - 1$ is prime, the above statement implies $n < 1 + 1$!*

Unfortunately, one quickly finds counterexamples: $1+8=9$, then $5+27=32$, $1+48=49$, $1+63=64$, $1+80=81$, $32+49=81\ldots$, though in all of these examples the ratio of the two sides never gets too large. Indeed, when $1 \le a,b,c \le 1000$, the largest ratio we encounter is $9/2$, in the example $1+2^9 = 3^3 \times 19$. This suggests that maybe if we multiply the right side of (9) by a suitably large constant (perhaps 5), we could have a valid inequality. Unfortunately, even this is false, for if $a=1$ and $c = 2^{p(p-1)}$ for some large prime p, then $b = 2^{p(p-1)} - 1$ is divisible by p^2, so that the right side of (9) is $\le 2b/p$, which means that inequality (9) cannot hold with only very minor modifications.

It has become frustrating trying to make a precise conjecture, even though numerical investigation does indicate that we are getting closer to something that is valid. At this point we resort to the mathematician's trick (to be used only when one knows one is close but is unable to formulate things precisely): Fudge things a little by throwing in an ε.

Oesterlé and Masser's abc-conjecture. For any given $\varepsilon > 0$ there exists a constant κ_ε such that if a, b, and c are coprime positive integers for which

$$a+b=c,$$

then

$$c \le \kappa_\varepsilon \left(\prod_{\substack{p \text{ prime} \\ p \mid abc}} p \right)^{1+\varepsilon} .$$

Is This Good for Anything?

One of our goals in formulating this analogy to Mason's Theorem was that we should be able to deduce Fermat's Last Theorem over the integers. We should check that this is the case. If

$$x^n + y^n = z^n$$

in coprime positive integers x, y, z, then take

$$a = x^n, \; b = y^n, \; \text{ and } c = z^n$$

in the abc-conjecture. We have no way of determining the product of the primes dividing $x^n y^n z^n$ precisely, but we do know that these are exactly the primes dividing xyz, and so their product must be $\le xyz$. Moreover, since x and y are positive, they are both less than z, so $xyz < z^3$. The abc-conjecture therefore gives

$$z^n \le \kappa_\varepsilon \left(z^3\right)^{1+\varepsilon},$$

for any given $\varepsilon > 0$. Taking $\varepsilon = 1/6$ and $n \ge 4$, so that $n - 3(1+\varepsilon) \ge n/8$, we deduce from the abc-conjecture that

$$z^n \le \kappa_{1/6}^8.$$

We have thus proved that in any solution of (1) with $n \ge 4$, the numbers x^n, y^n, and z^n are all less than some absolute bound, and so there are no more than finitely many such solutions (and Euler had shown that there are no solutions to (1) with $n = 3$).

If we had an explicit version of the abc-conjecture (that is, with the values of κ_ε given), then we could give an explicit bound on all solutions to the Fermat equation and compute up to that bound to finally determine whether there are any solutions. It would not be the most elegant proof of Fermat's Last Theorem imaginable, but it would achieve our goal.

It has been suggested that the abc-conjecture might be valid with $\varepsilon = \kappa_\varepsilon = 1$, so that

$$c \le \left(\prod_{\substack{p \text{ prime} \\ p \mid abc}} p \right)^{2} .$$

If so, then Fermat's Last Theorem for $n \ge 6$ follows immediately, and the cases $n = 3, 4, 5$ have been known for almost two hundred years (see [Ri]).

It is appealing to look for other Diophantine questions to which we can directly apply the abc-conjecture. Obviously it is directly applicable to the Fermat equation with arbitrary coefficients,

$$Ax^n + By^n = Cz^n$$

for fixed integers A, B, C, as well as to the Catalan equation

$$x^p - y^q = 1 \quad \text{with } p,q \ge 2.$$

We leave it as an exercise for the reader to apply the abc-conjecture to the more general trinomial equation

$$Ax^p + By^q = Cz^r. \tag{10}$$

We really would like to generalize the Fermat equation not only to other trinomial equations but in fact to equations with arbitrarily many terms. Equations in one variable are not of much Diophantine interest, but the rational solutions to equations in two variables,[2] that is, rational points on curves, have been very much in the center of number theory research.

In 1930 Mordell [Mo] wrote one of the greatest papers in the history of mathematics, a paper which we shall be discussing for two reasons.[3] At the

[2] *The novice might note that rational solutions to equations in two variables are equivalent to integer solutions to equations in three variables where every monomial has the same total degree, as may be seen by multiplying through by denominators.*

[3] *Mordell notes in his "Reminiscences of an octogenarian" that this paper was rejected as uninteresting by the first journal it was submitted to!*

very end of the paper, Mordell asked five questions which were instrumental in motivating much of the important research in Diophantine arithmetic in the twentieth century. The most important and difficult of these questions was answered by Faltings in 1983 by inventing some of the deepest and most powerful ideas in the history of mathematics. In the next section we will try to give some idea of what Faltings' Theorem is about.

The *abc*-conjecture and the *Number Theory "Hall of Fame"*

Faltings' Theorem née Mordell's Conjecture (Fields Medal 1986)

Gerd Faltings

Let $f(x, y) \in \mathbb{Z}[x, y]$ be a polynomial in two variables with integer coefficients. We are interested in finding rational numbers u and v for which $f(u, v) = 0$. Sometimes it is very easy to do so: for example, if $f(x, y) = x + y - 1$, then we can take $u = 1/2 + t$ and $v = 1/2 - t$ for any rational number t, and all rational solutions are of this form. Another example, not so easy but very well known, is $f(x, y) = x^2 + y^2 - 1$, which has solutions $u = 2t/(1 + t^2)$ and $v = (1 - t^2)/(1 + t^2)$ for every rational t. These are both examples of equations in which infinitely many rational solutions may be obtained in a parametrized form (that is, as a rational function of the variable t).

A second class of examples in which we can have infinitely many rational solutions is given by "cubic curves". As an example consider the taxicab curve,[4]

$$x^3 + y^3 = 1729.$$

Ramanujan's two solutions are $12^3 + 1^3 = 10^3 + 9^3 = 1729$; one can easily check that these are the only solutions in integers. However, it is not hard to find infinitely many solutions in rationals. In fact, given any solution (u, v), one can find another simply by taking

$$U = u(u^3 - 3458)/(1729 - 2u^3)$$

and

$$V = v(u^3 + 1729)/(1729 - 2u^3).$$

Starting with $(12, 1)$ we then get further solutions

$$(20760/1727, -3457/1727),$$

$$(18402633089285064 0/15522982448334911,$$
$$61717391872243199/15522982448334911),$$

and the next solution is pointless to write down, since each ordinate has seventy digits! Our main concern is that we have observed, for a certain class of curves, that one can obtain further solutions as a function of previous solutions and thus get infinitely many solutions (and, since the ordinates grow so fast, one can prove that they could not possibly come from a parametrized form).

Thus we know of two ways that an equation $f(x, y) = 0$ can have infinitely many rational solutions. In fact, Faltings' Theorem tells us that these are the only two ways that an equation like this can have infinitely many rational solutions; in other words, there are only finitely many "sporadic" solutions. Indeed, if we put to one side all solutions of $f(x, y) = 0$ that come from the two methods above, we are left with finitely many solutions. It is even conceivable that the number of rational points left over is bounded by a function of the degree of f. This extraordinary theorem has many wonderful consequences. For example, for any given $p \geq 4$ there are only finitely many positive coprime integer solutions to (1). Similarly, there are only finitely many positive coprime integer solutions to (10) when that is predicted by the *abc*-conjecture. So, for instance,

$$(11) \qquad x^4 + y^4 = 17z^4 \quad \text{and} \quad x^2 + y^3 = z^7$$

each have only finitely many coprime integer solutions.

One important failing of Faltings' Theorem is that it gives no upper bound on the size of the solutions and thus no "algorithm" for finding them all, even though we know there are only finitely many (it took new methods to prove that we know all solutions to the two equations in (11)).

In 1991 Elkies showed that using an explicit version of the *abc*-conjecture (that is, with a value assigned to κ_ε for each ϵ), one can deduce an explicit version of Faltings' Theorem. The proof revolves around a careful study of Belyĭ maps (in particular the ideas involved in Proposition 3).

Moret-Bailly, building on ideas of Szpiro, went a step further. He showed that if one could get *good* upper bounds for the size of the coordinates of the rational points on[5] $y^2 = x^5 - x$ in any number field,[6] then the *abc*-conjecture follows. ("Good" bounds in this case are bounds that depend

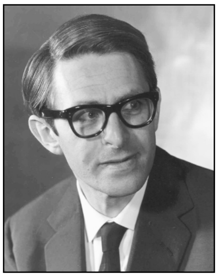
[4] *When Ramanujan lay ill from pneumonia in an English hospital, he was visited by G. H. Hardy, his friend and coauthor. Struggling for conversation, Hardy remarked that the number 1729 on the taxicab in which he had ridden from the train station to the hospital was extremely dull. Ramanujan contradicted him, noting that it is the smallest number which is the sum of two cubes in two different ways. However, Ramanujan did miss the other notable fact that it is the third smallest Carmichael number!*

[5] *Or, for the initiated, on any other algebraic curve of genus* > 1.

[6] *That is, a finite field extension of* $\mathbb{Q}$.

explicitly on the discriminant of the number field over which the points are rational.) Therefore, in a certain sense, this problem and the *abc*-conjecture are equivalent.

Roth's Theorem (Fields Medal 1958)



Klaus Roth

Let α be a real algebraic irrational number of degree d. A simple pigeonhole principle argument gives infinitely many rational numbers m/n for which $|\alpha - m/n| < 1/n^2$. On the other hand, substituting m/n into the minimum polynomial for α shows that there exists a constant $c_\alpha > 0$ such that $|\alpha - m/n| > c_\alpha/n^d$.

A famous question of number theory was whether this lower bound could be improved, and Roth (1955) gave the "best possible" such result: For any fixed $\epsilon > 0$ there exists a constant $c_{\alpha,\epsilon} > 0$ such that

$$\left|\alpha - \frac{m}{n}\right| \geq \frac{c_{\alpha,\epsilon}}{n^{2+\epsilon}}.$$

Suppose that $F(x,y) \in \mathbb{Z}[x,y]$ is a binary homogenous form without repeated factors.[7] Using Roth's Theorem we then have, for any coprime integers m and n,

$$\begin{aligned} |F(m,n)| &\gg_F n^{\deg(F)} \prod_{\alpha:\ F(\alpha,1)=0} \left|\alpha - \frac{m}{n}\right| \\ &\gg_{F,\epsilon} n^{\deg(F)-2-\epsilon}. \end{aligned} \tag{12}$$

(The meaning of "$A \gg_F B$" may be unfamiliar to many readers. This simply means that there exists a constant $c_F > 0$, depending only on F, such that we have "$A \geq c_F B$"; similarly, "$A \gg_{F,\epsilon} B$" means that there is an analogous inequality with a constant $c_{F,\epsilon} > 0$ depending only on F and ϵ. This notation saves a lot of writing in analytic number theory.) We leave it to the reader to verify that this statement is actually equivalent to Roth's Theorem.

The *abc*-conjecture implies something that is somewhat stronger than Roth's Theorem: For any coprime integers m and n,

$$\prod_{p|F(m,n)} p \gg_{F,\epsilon} (\max\{|m|,|n|\})^{\deg(F)-2-\epsilon}. \tag{13}$$

Note that $|F(m,n)| \geq \prod_{p|F(m,n)} p$ (if $F(m,n) \neq 0$), so Roth's Theorem (in the form (12)) follows immediately. Notice also that by taking $F(x,y) = xy(x+y)$ we recover the original *abc*-conjecture. Thus this conjecture is *equivalent* to the *abc*-conjecture, although it appears far stronger.

One can sketch a proof that (13) follows from the *abc*-conjecture as follows: Let $f(t) = F(t,1)$ and apply Proposition 3. Let $f(t)g(t)$ be the product of the distinct linear factors dividing $a(t)b(t)c(t)$ (where $a(t)$, $b(t)$, and $c(t)$ are as in Proposition 3), and homogenize by taking $t = m/n$ to get an equation $A(m,n) + B(m,n) = C(m,n)$. We may assume without loss of generality that $A(m,n)$, $B(m,n)$, and $C(m,n)$ are all positive, if necessary by rearranging them, and notice that the $\gcd(A,B)$ divides the resultant of $a(t)$ and $b(t)$, so is bounded. Now apply the *abc*-conjecture to this equation, bounding the product of the primes dividing ABC by $|G(m,n)|$ times the product of the primes dividing $F(m,n)$. Notice that the number of linear factors of FG is at most one more[8] than the number of roots of fg, that is, $\leq d+2$, where d is the maximum of the degrees of a, b, and c by Proposition 3. The result follows from combining these observations with the fact that $\max\{A(m,n), B(m,n), C(m,n)\} \gg \max\{|m|,|n|\})^d$.

Baker's Theorem (Fields Medal 1970)

Alan Baker

In 1929 Siegel showed that for any given $f(x,y) \in \mathbb{Z}[x,y]$ all but finitely many of the integer pairs u and v for which $f(u,v) = 0$ are given by parametrizations. Although it is easy, in practice, to find all of the parametric solutions, Siegel was unable to provide a way to bound those finitely many other integer points (just as Faltings' Theorem does not provide a way to bound the rational points u and v with $f(u,v) = 0$). In 1968 Baker made an extraordinary breakthrough in "*linear forms in logarithms*" which allowed, in many interesting cases, such bounds on the size of integer points. However, his theorem can be stated only in a technical form!

Let $p_1, \ldots, p_n$ be prime numbers. We write $L = \log|\log(p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})|$, where the a_i are integers.

By the pigeonhole principle we can show that, for any integer $A > 1$, there exist integers $a_1, a_2, \ldots, a_k$ with each $|a_i| \leq A$ such that $L \leq -(k-1)\log A + \log\log(p_1 p_2 \ldots p_k)$. Baker's Theorem (as improved in a recent paper with Wüstholz) gives the lower bound

$$L \geq -(16k)^{2(k+2)}(\log A)\prod_{i=1}^{k} \log p_i.$$

This result seems likely to be far from "best possible". Moreover, the *abc*-conjecture gives

[7] *In other words, if F has degree d, then $F(t,1)$ is a polynomial of degree $\geq d-1$, without repeated roots, and $F(x,y) = y^d F(x/y,1)$.*

[8] *The "one more" because there could be a factor n here corresponding in the abc equation to one of a, b, or c having lower degree than the other two.*

$$L \gg -(\log A)\sum_{i=1}^{k}\log p_i,$$

a remarkable improvement and close to best possible, given the upper bound mentioned above. Moreover, this lower bound on L implies a modified version of the abc-conjecture, so these two questions are, in a certain sense, equivalent.

We should note that techniques from this area have been used to attack the abc-conjecture. In 1991 Stewart and Yu proved that if $a+b=c$ in positive coprime integers, then

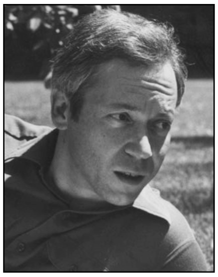
$$c \ll \exp\left(O\left(\left(\prod_{p|abc} p\right)^{2/3}\right)\right).$$

Remove one "exp" and we would be there! This is unfortunately typical of results using these techniques: as beautiful as the results are, they fall short of our goal; still, better some result than nothing.

Motivated by applications to estimates for linear forms in logarithms, Baker recently came up with the following interesting explicit version of the abc-conjecture:

$$c \ll N \sum_{\substack{n\le N\\ p|n \implies p|N}} 1 \quad \text{where } N = \prod_{p|abc} p.$$

Bombieri's Theorem (Fields Medal 1974)



Enrico Bombieri

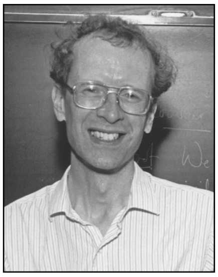
Let χ be a Dirichlet character[9] (mod q). The Generalized Riemann Hypothesis states that if $L(s,\chi)=0$, then either s is a negative integer (a "trivial zero") or $\mathrm{Re}(s)=1/2$. There seems to be little prospect of proving this statement or anything too similar. However, many of the consequences of the Generalized Riemann Hypothesis follow from the assertion that if $L(s,\chi)=0$, then $\mathrm{Re}(s)$ is not *too* big, or that there are not too many s with $L(s,\chi)=0$, and $\mathrm{Re}(s)$ "large". One version of Bombieri's famous result (1965) may be paraphrased as

The zeros of $L(s,\chi)$ *are sparse "far away"*
from $\mathrm{Re}(s)=1/2$,
for "almost all[10]*"* χ (mod q).

By 1930 it had been shown, for a sufficiently small constant $c>0$, that if $L(s,\chi)=0$ with $\mathrm{Re}(s)>1-c/\log q$, then s is real, χ is a quadratic real character, and there is at most one such value of q between Q and Q^2 for any sufficiently large Q. Such zeros are known as "Siegel zeros".[11]

In 1995 Granville and Stark proved, assuming the abc-conjecture, that $L(s,\chi)$ has no Siegel zeros for all χ (mod q) with $q\equiv 3$ (mod 4).

Wiles' Theorem (IMU Plaque 1998)



Andrew Wiles

Wiles did not prove Fermat's Last Theorem directly. Instead, he attacked a famous old conjecture about elliptic curves called the "Taniyama conjecture"[12] and proved enough of it to deduce Fermat. Recently others have completed the proof of Taniyama's conjecture. We can give here only a brief, somewhat inadequate, description of the conjecture.

Above we saw how the curve $x^2+y^2=1$ could be parametrized by $x=2t/(1+t^2)$ and $y=(1-t^2)/(1+t^2)$ where $t\in\mathbb{C}$. There are many other types of parametrizations possible: for example, we saw how to find infinitely many points on the curve $C: x^3+y^3=1729$ by using a map that sends a point on C to a "larger" point on C, in other words, a map $\phi: C\to C$ that is a rational function in the co-ordinates of the point.[13] One can generalize by saying that a curve C "parametrizes" a curve X if there is such a map $\phi: C\to X$ that is a rational function in the coordinates of the point on C.

Taniyama's conjecture (now a theorem) states that *every* cubic curve can be parametrized by a "modular" curve: The modular curves $\{X_0(N)\}_{N=1,2,3,\ldots}$ are a very special set of curves that come up naturally in a somewhat different context. For use in $a+b=c$ equations we look at the elliptic curve

$$E:\ y^2=x(x-a)(x+b);$$

we now know that this can be parametrized by the curve $X_0(N)$, where

$$N=N_E \text{ is approximately } \prod_{p|abc} p.$$

[9] *A homomorphism* $(\mathbb{Z}/q\mathbb{Z})^*\to\mathbb{C}$.

[10] *That is, 100%.*

[11] *An unfortunate reward for Siegel after much remarkable work showing how unlikely they are to exist!*

[12] *The vague statement of the conjecture that we give is close to the original statement of Taniyama. This was subsequently made more precise by Shimura, who proved that it was true in infinitely many examples. Arguably this conjecture only became as widely known as it deserved because of the works and influence of Weil, and thus this conjecture has confusingly been credited to various subsets of these three names!*

[13] *Moreover,* ϕ *had degree four, explaining the explosion in the size of the numbers involved.*

(Here "approximately" means that the ratio of the two sides is a rational with small numerator and denominator.)

There may be many parametrizations $\phi : X_0(N_E) \to E$. Let ϕ_E be one of the ones of smallest degree. A fantastic theorem of Weil shows that all such ϕ can be written as the composition of ϕ_E with some other maps (which are automorphisms). Thus it is of interest to find ϕ_E, or at least to determine its degree. It turns out that

$$\deg(\phi_E) = cN_E^{1+o(1)}.$$

(By "$o(1)$" we mean some number that $\to 0$ as $N \to \infty$.) Put like this, one sees that the *abc*-conjecture is *equivalent* to the conjecture

$$\deg(\phi_E) \ll N_E^{2+o(1)}.$$

The result of Stewart and Yu mentioned above tells us that, unconditionally,

$$\deg(\phi_E) \ll \exp\left(N_E^{2/3+o(1)}\right).$$

The *abc*-conjecture: The Future

We have seen that the *abc*-conjecture is equivalent to extensions of several of the most important theorems in number theory: Roth's Theorem, Faltings' Theorem, Baker's Theorem, and Wiles' Theorem.[14] Resolving the *abc*-conjecture would therefore have an extraordinary impact on our understanding of number theory. Proving it or disproving it would be amazing. The least desirable state of affairs would be to find out that the *abc*-conjecture is undecidable, and thus so are these extensions of so many of the important questions in the subject!

We are in the process of writing a book explaining in detail how the *abc*-conjecture relates to all of these problems and thus trying to map out possible future directions of several important themes in number theory. We shall include sketches of the proofs of Roth's and Faltings' Theorems, since, when approached from an appropriate direction, these indicate the slightly different philosophy of arithmetic first proposed by Vojta [Vo], which we develop from the perspective of Belyĭ maps. Our intent is to keep the style of this article in much of the book.

References

[Ba] A. Baker, *Transcendental Number Theory*, Cambridge University Press, London and New York, 1975.

[Be] G. V. Belyĭ, On the Galois extensions of the maximal cyclotomic field (Russian), *Izv. Akad. Nauk SSSR* **43** (1979), 267–76.

[Bo] E. Bombieri, Le grand crible dans la théorie analytique des nombres, *Astérisque* **18** (1987).

[El] N. Elkies, *ABC* implies Mordell, *Int. Math. Res. Not.* **7** (1991), 99–109; *Duke Math. J.* **64** (1991).

[Fa] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–66.

[La] M. Langevin, *Imbrications entre le théorème de Mason, la descente de Belyĭ et les différentes formes de la conjecture* (*abc*), J. Théor. Nombres Bordeaux, **11** (1999), 91–109.

[Ma] R. C. Mason, *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Ser. 96, Cambridge Univ. Press, Cambridge, 1984.

[Mo] L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, *Proc. Cambridge Philos. Soc.* **21** (1922), 179–92.

[Md] ____ , Reminiscences of an octogenarian mathematician, *Amer. Math. Monthly* **78** (1971), 952–61.

[Ri] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York and Heidelberg, 1979.

[Ro] K. F. Roth, Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 1–20.

[Se] J. P. Serre, *Lectures on the Mordell–Weil Theorem*, Viewig, Braunschweig, 1990.

[Vo] P. Vojta, *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math., vol. 1239, Springer, New York, 1987.

[Wi] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* **141** (1995), 443–551.

Note: Photograph of Klaus Roth courtesy of the London Mathematical Society, with permission from the Royal Society. Photograph of Enrico Bombieri by H. Landshoff, used with permission of the IAS.

[14] *One audience member pointed out that number theorists thus won several Fields Medals in striving for the same result!*