IJMMS 2003:71, 4473–4500
PII. S0161171203210668
http://ijmms.hindawi.com

ON A FEW DIOPHANTINE EQUATIONS, IN PARTICULAR, FERMAT'S LAST THEOREM

C. LEVESQUE

Received 20 October 2002

This is a survey on Diophantine equations, with the purpose being to give the flavour of some known results on the subject and to describe a few open problems. We will come across Fermat's last theorem and its proof by Andrew Wiles using the modularity of elliptic curves, and we will exhibit other Diophantine equations which were solved *à la* Wiles. We will exhibit many families of Thue equations, for which Baker's linear forms in logarithms and the knowledge of the unit groups of certain families of number fields prove useful for finding all the integral solutions. One of the most difficult conjecture in number theory, namely, the *ABC conjecture*, will also be described. We will conclude by explaining in elementary terms the notion of modularity of an elliptic curve.

2000 Mathematics Subject Classification: 11-02, 11-06.

1. Introduction. On June 23, 1993, at the Isaac Newton Institute of Cambridge (England), Professor Andrew Wiles (Princeton University) made a striking announcement. He had found a proof of Fermat's last theorem.

Fermat's last theorem. *Let n be an integer greater than or equal to* 3. *Then there are no nonzero integers A, B, C such that*

$$A^n + B^n = C^n. \tag{1.1}$$

The mathematical community became very excited and the news spread all over the world in a matter of days. For more than 350 years, many mathematicians and a greater number of amateurs had tried without success to obtain a proof of this conjecture. Already in 1918, Paul Wolfskehl poured some oil on the fire by promising a 100 000 German marks reward to whoever provides the first proof of this theorem. The mark devaluation almost annihilated the value of the prize, but did not decrease the interest of specialists in this question and similar problems.

In this survey article, we offer you an excursion over centuries into this fantastic world of Diophantine equations. Though we will not deal with the equations considered by Mordell and by Shorey and Tijdeman in their classical books [31, 39], we plan to make you more familiar with other Diophantine equations. You will encounter some equations which have integral solutions,

sometimes a finite number, sometimes an infinite number; you will also see some equations which have no solution at all, and you will come across some equations about which the only thing we know is that we know nothing about them. We will say a few words about the Fermat equation and in Section 9, you will get the flavour of Wiles' proof. We will exhibit other Diophantine equations which were solved *à la* Wiles, namely, by using some modular elliptic curves. You will also see that Baker's linear forms in logarithms and the knowledge of the unit groups of some families of number fields proved useful in solving some families of the so-called Thue equations. By the way, the delights of the *ABC conjecture* may make your mouth water: the assumption of this conjecture provides a short proof of Fermat's last theorem (for all n but a finite number). In Section 10, we will dare to open a parenthesis on the modularity notion of an elliptic curve, but we will rush to close it in order to avoid getting involved in technicalities.

2. Diophantus and Fermat. The Greek mathematician Diophantus (born in 325) got interested in finding solutions of a given equation belonging to the set $\mathbb{Q}$ of rational numbers. However, under modern terminology, solving a *Diophantine equation* is looking for integral solutions, that is, for solutions belonging to the set $\mathbb{Z}$ of integers.

On the one hand, you may agree with the fact that the equation

$$X + Y = Z \tag{2.1}$$

is easy to solve, but there are still open problems concerning this equation (as will be seen in Section 6). On the other hand, the situation often gets complicated if powers X^n, where n is an integer greater than or equal to 2, come into play. Some solutions may be easily exhibited; for instance, a solution of the Diophantine equation

$$X^3 + Y^2 = Z^2 \tag{2.2}$$

is $X = 2$, $Y = 1$, and $Z = 3$, while another is $X = 3$, $Y = 3$, and $Z = 6$. Some Diophantine equations may happen to have no integral solution at all, like the equation $X^2 - 2Y^2 = 0$.

The so-called Fermat-Pell equation

$$X^2 - DY^2 = 1 \tag{2.3}$$

has been around for many centuries, and the continued fraction expansion of $\sqrt{D}$ leads to its solution. This equation goes back to Archimedes (with the cattle problem) and was studied by the Indian mathematician Brahmagupta around 1630 and by the English mathematician William Brouncker around 1650.

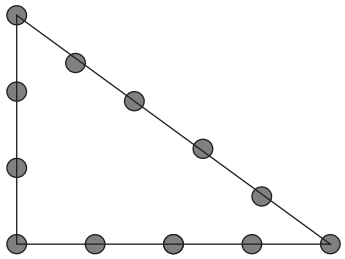

FIGURE 3.1

Pierre de Fermat (1601–1665) had a copy of the Latin translation (made by Bachet) of Diophantus book Arithmetica. Quite often, Fermat used to write personal notes in the margin of this book, and a Latin annotation of him (once translated) reads

> *"It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers, and in general, a power (except a square) as a sum of two powers with the same exponent. I possess a truly wonderful proof of this result, that this margin is too narrow to contain."*

This is equivalent to stating that the equations $X^3+Y^3=Z^3$, $X^4+Y^4=Z^4$, $X^5+Y^5=Z^5$, and so on, have no solutions in positive integral integers.

3. Pythagoras. Stating his theorem, Fermat assumed $n \geq 3$, precisely because for $n=2$, the Diophantine equation $X^2+Y^2=Z^2$ has integral solutions. As a matter of fact (see Figure 3.1), all the solutions of the equation

$$X^2+Y^2=Z^2 \tag{3.1}$$

are given by $X=kU^2-kV^2$, $Y=2kUV$, and $Z=kU^2+kV^2$, in which one substitutes any integer for k, U, and V. Indeed, we come across a very old result.

PYTHAGORAS' THEOREM. *Suppose that in a given rectangle triangle, the length of the base is a, the height b, and the diagonal c. Then*

$$a^2+b^2=c^2. \tag{3.2}$$

The proof appears as Proposition XLVII of the first book of *Euclid's Elements* [36, page 38]. A modern proof of this theorem is to let $c=d$ in the statement of a result called the *parallelogram law* (easy to prove with some use of the scalar product).

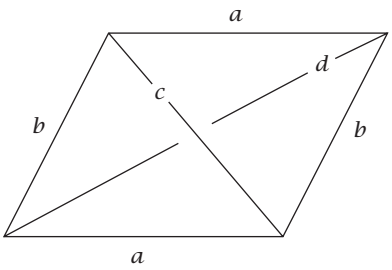

FIGURE 3.2

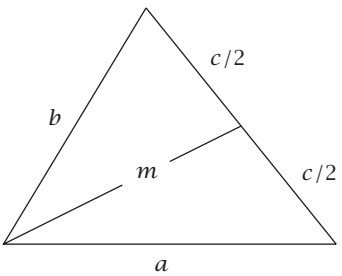

FIGURE 3.3

PARALLELOGRAM LAW. Let a and b be the two sides of a parallelogram, and let c and d be the two diagonals (as in Figure 3.2). Then

$$2a^2 + 2b^2 = c^2 + d^2. \tag{3.3}$$

The parallelogram law immediately leads to the median formula.

MEDIAN FORMULA. Let a, b, and c be the sides of a triangle and let m be the median (as in Figure 3.3). Then

$$2a^2 + 2b^2 = 4m^2 + c^2. \tag{3.4}$$

For the proof, expand this triangle into a parallelogram (see Figures 3.3 and 3.4). One finds in Proposition XLVIII of *Euclid's Elements* [36, page 39] the proof of the following result.

CONVERSE OF PYTHAGORAS' THEOREM. *If $a^2 + b^2 = c^2$, then the triangle of sides a, b, and c is rectangle with c as the hypotenuse.*

Thanks to the median formula, one can supply a short proof. Let $a^2 + b^2 = c^2$; then $2m^2 + (1/2)c^2 = c^2$, that is, $c = 2m$. Hence, the two diagonals of Figure 3.4 are equal, and the parallelogram is a rectangle, that is, is made of two rectangle triangles.

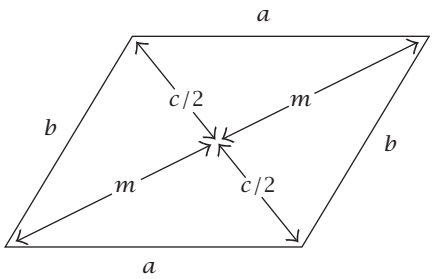

FIGURE 3.4

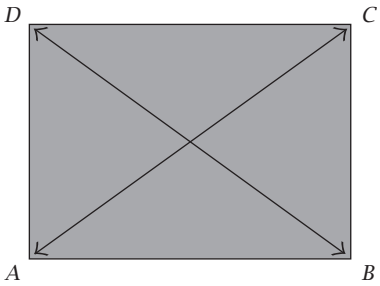

FIGURE 3.5

Babylonians applied the converse of Pythagoras' theorem to build an angle of 90 degrees. Indeed, they used ropes having knots at intervals of the same length and used them as in Figure 3.1. They were sure to obtain a right angle of 90 degrees between the horizontal line and the vertical line.

Nowadays, when it comes to fixing the wooden rectangle (wooden rail) on the foundations of a building to be built (see Figure 3.5), where the length between A and D is equal to the length between B and C, and where the length between A and B is equal to the length between C and D, home builders make sure that the length between A and C is equal to the length between B and D. Though they may not be aware of it, they "use" the parallelogram law (see Figure 3.2) and make sure that $c^2\ (= a^2 + b^2) = d^2$, and then use the converse of Pythagoras' theorem to conclude that the two glued triangles are rectangle triangles.

Thanks to Pythagoras (and to the converse of his theorem), we can solve a problem which became famous in San Francisco on July 28, 1993, during a public conference on Fermat.

PIZZA PROBLEM. The owner of a restaurant advertizes a small pizza at \$6, a medium size pizza at \$9, and a large pizza at \$15. Spending \$15, do you get a better deal by buying a large pizza, or by buying a small pizza and a medium size one? You may use only a pizza knife to make your decision.

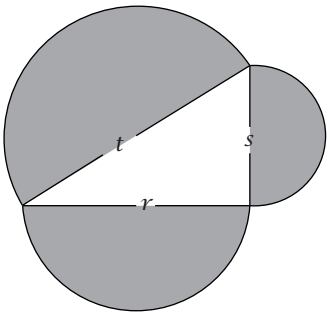

FIGURE 3.6

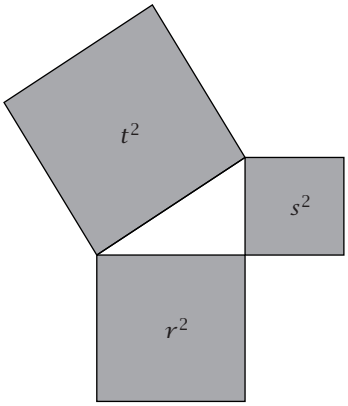

FIGURE 3.7

Just cut the three pizzas in two equal parts and place the three half pizzas of different sizes as to form a triangle. Three cases can occur.

CASE 3.1. If you get a rectangle triangle (Figures 3.6 and 3.7), your choice is as good as mine since

$$\frac{\pi}{8}r^2+\frac{\pi}{8}s^2=\frac{\pi}{8}t^2,\quad \text{that is, } r^2+s^2=t^2. \tag{3.5}$$

CASE 3.2. If the triangle is obtuse (Figure 3.8), your best deal is to take the large pizza since

$$\frac{\pi}{8}r^2+\frac{\pi}{8}s^2<\frac{\pi}{8}t^2,\quad \text{that is, } r^2+s^2<t^2. \tag{3.6}$$

With Figures 3.9 and 3.10, one sees that

$$r^2+s^2=r^2+u^2+v^2<(r+u)^2+v^2=t^2. \tag{3.7}$$

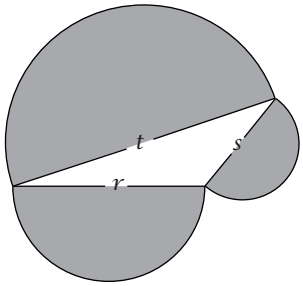

FIGURE 3.8

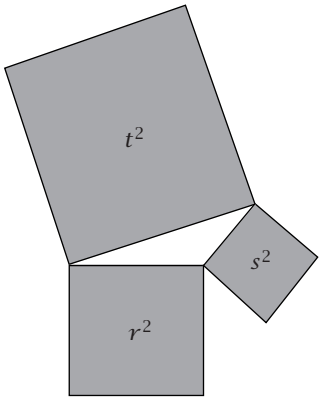

FIGURE 3.9

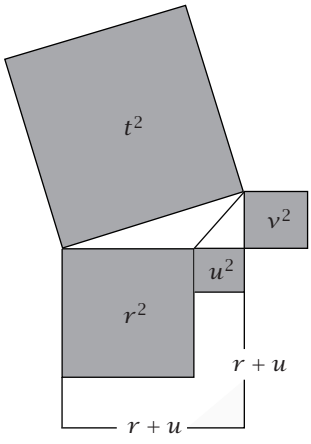

FIGURE 3.10

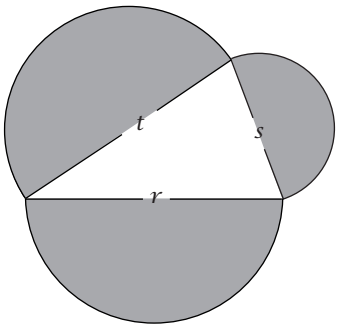

FIGURE 3.11

CASE 3.3. Finally, if the triangle is acute (Figure 3.11), it is better to order a small pizza and a medium size one since

$$\frac{\pi}{8}r^2+\frac{\pi}{8}s^2>\frac{\pi}{8}t^2,\quad \text{that is, } r^2+s^2>t^2. \tag{3.8}$$

Figures 3.12 and 3.13 show that

$$r^2+s^2=r^2+u^2+v^2>(r-u)^2+v^2=t^2. \tag{3.9}$$

4. Some Diophantine equations. Diophantine equations are often mysterious. Two very similar equations may have very different solution sets, and it may happen that one is difficult to deal with, and the other one is easy to study. We just saw that for $n\geq 3$, the equation $X^n+Y^n=Z^n$ has no nontrivial solution. Nevertheless, for all $n\geq 1$, the equation

$$X^n+Y^n=2Z^n \tag{4.1}$$

possesses the positive solution $X=Y=Z=1$. Are there more for $n\geq 3$? We will see later that the answer is no, though the proof is deep.

We explain why, for $n\geq 2$, the Diophantine equation

$$X^2+Y^2=Z^n \tag{4.2}$$

has an infinite number of (nontrivial) solutions, and that it is easy to find all of them. For all $n\geq 0$, let A_n and B_n be defined by

$$A_n+B_n i=(a+bi)^n, \tag{4.3}$$

where $i=\sqrt{-1}$ and where a and b are variables running through $\mathbb{Z}$. On the one hand, we have

$$(A_n+B_n i)\cdot(\overline{A_n+B_n i})=(A_n+B_n i)\cdot(A_n-B_n i)=A_n^2+B_n^2, \tag{4.4}$$

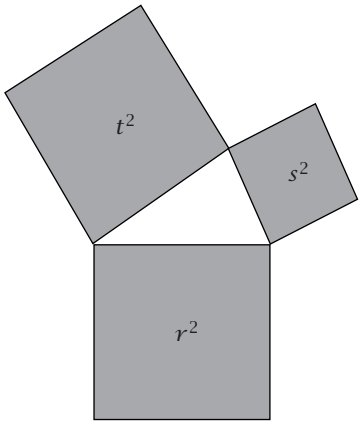

FIGURE 3.12

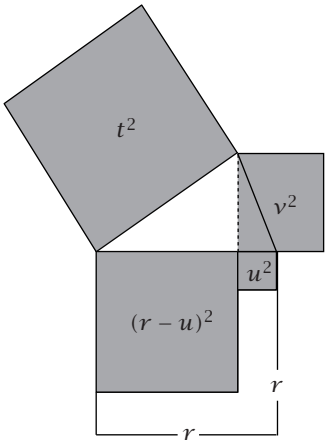

FIGURE 3.13

where $\overline{z}$ is the complex conjugate of z. On the other hand,

$$\begin{aligned}(A_n + B_n i)\cdot(\overline{A_n + B_n i}) &= (a+bi)^n \cdot \overline{(a+bi)^n} \\ &= (a+bi)^n \cdot (a-bi)^n \\ &= (a^2+b^2)^n.\end{aligned} \tag{4.5}$$

Hence $A_n^2 + B_n^2 = (a^2+b^2)^n$. Thus the equation $X^2 + Y^2 = Z^n$ has an infinite number of solutions given by $X = A_n$, $Y = B_n$, and $Z = a^2 + b^2$, where the

TABLE 4.1

n	A_n	B_n
0	1	0
1	a	b
2	a^2-b^2	$2ab$
3	a^3-3ab^2	$3a^2b-b^3$
4	$a^4-6a^2b^2+b^4$	$4a^3b-4ab^3$
5	$a^5-10a^3b^2+5ab^4$	$5a^4b-10a^2b^3+b^5$
6	$a^6-15a^4b^2+15a^2b^4-b^6$	$6a^5b-20a^3b^3+6ab^5$
7	$a^7-21a^5b^2+35a^3b^4-7ab^6$	$7a^6b-35a^4b^3+21a^2b^5-b^7$
8	$a^8-28a^6b^2+70a^4b^4-28a^2b^6+b^8$	$8a^7b-56a^5b^3+56a^3b^5-8ab^7$

binomial expansion of $(a+bi)^n$ gives

$$A_n=\sum_{s=0}^{[n/2]}(-1)^s\binom{n}{2s}a^{n-2s}b^{2s},\qquad B_n=\sum_{s=0}^{[(n-1)/2]}(-1)^s\binom{n}{2s+1}a^{n-1-2s}b^{2s+1}. \tag{4.6}$$

It turns out that all the solutions are of that form, and this is justified by the fact that the class number of the imaginary quadratic field $\mathbb{Q}(i)$ is 1. We write a few values of A_n and B_n in Table 4.1.

It is now easy to deduce that an infinite family of solutions of

$$X^2-Y^2=Z^n \tag{4.7}$$

is given by $X=R_n$, $Y=S_n$, and $Z=a^2-b^2$, where

$$R_n=\sum_{s=0}^{[n/2]}\binom{n}{2s}a^{n-2s}b^{2s},\qquad S_n=\sum_{s=0}^{[(n-1)/2]}\binom{n}{2s+1}a^{n-1-2s}b^{2s+1}. \tag{4.8}$$

According to Euler, the equation

$$W^3+X^3+Y^3=Z^3 \tag{4.9}$$

has an infinity of solutions; it suffices to consider

$$\begin{aligned} W&=-a^3+3a^2b-3ab^2+9b^3+1,\\ X&=a^3+3a^2b+3ab^2+9b^3-1,\\ Y&=a^4+6a^2b^2-a+9b^4-3b,\\ Z&=a^4+6a^2b^2-a+9b^4+3b, \end{aligned} \tag{4.10}$$

or

$$\begin{aligned} W &= 3a^2 + 5ab - 5b^2, \\ X &= 4a^2 - 4ab + 6b^2, \\ Y &= 5a^2 - 5ab - 3b^2, \\ Z &= 6a^2 - 4ab + 4b^2. \end{aligned} \tag{4.11}$$

Thanks to Elkies [12], we know that the Diophantine equation

$$W^4 + X^4 + Y^4 = Z^4 \tag{4.12}$$

also possesses an infinite number of solutions (with W, X, Y, and Z different from 0), with the smallest, according to R. Frye, being $W = 95800$, $X = 217519$, $Y = 414560$, and $Z = 422481$. We first deal with

$$W^4 + X^4 + \widetilde{Y}^2 = Z^4. \tag{4.13}$$

Elkies [12] exhibited an infinite family of solutions of the latter Diophantine equation:

$$\begin{aligned} W &= 2a^2 + 6a + 20, \\ X &= a^2 + 31, \\ \widetilde{Y} &= 4(2a^4 + 28a^2 - 75a + 80), \\ Z &= 3(a^2 + 11). \end{aligned} \tag{4.14}$$

Using a judiciously chosen elliptic curve, he next showed that there exist an infinite number of integers a (effectively computable) for which $\widetilde{Y}$ is a perfect square, thus giving rise to an infinity of solutions of the equation $W^4 + X^4 + Y^4 = Z^4$.

The equation

$$V^5 + W^5 + X^5 + Y^5 = Z^5 \tag{4.15}$$

possesses, for instance, the solution $V = 27$, $W = 84$, $X = 110$, $Y = 133$, and $Z = 144$, though we still do not know whether it possesses an infinite number of solutions.

Along the same lines, so far nobody could exhibit an integer n (with $n \geq 6$) and $n-1$ nonzero integers such that the sum of the nth powers of these $n-1$ integers is an nth power. The case where $n = 6$ reads

$$U^6 + V^6 + W^6 + X^6 + Y^6 = Z^6 \tag{4.16}$$

and no solution with $UVWXYZ \neq 0$ is known.

We conclude this section with three other open problems.

Problem 4.1. Does there exist a *perfect rectangular box* (Figure 4.1), that is, a rectangular box such that the lengths of the three sides and of the four diagonals are integers? In other words, we do not know whether or not there are positive integers a, b, c, d, e, f, and g such that

$$a^2+b^2=d^2, \qquad a^2+c^2=f^2, \qquad b^2+c^2=e^2, \qquad b^2+f^2=g^2. \tag{4.17}$$

If we do not require the interior diagonal to be integral, such a box exists: simply take $a=117$, $b=44$, $c=240$, $d=125$, $e=244$, and $f=267$.

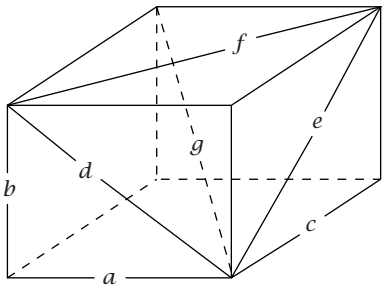

Figure 4.1

Problem 4.2. Does there exist a *perfect square* (Figure 4.2), that is, a square with sides of length A, having an interior point respectively at distances B, C, D, and E from the four corners such that A, B, C, D, and E are all positive integers?

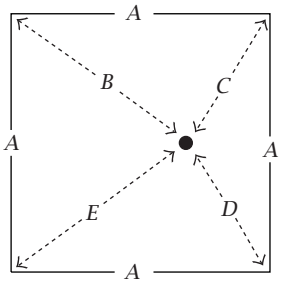

Figure 4.2

Problem 4.3. Does there exist a *perfect triangle* (Figure 4.3), that is, a triangle such that the sides A, B, and C, the medians D, E, and F, and the area are all positive integers?

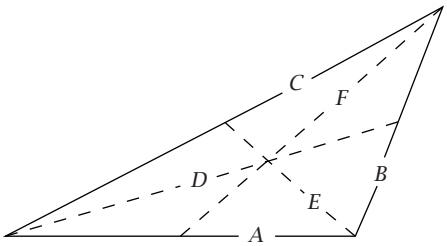

Figure 4.3

5. First attempts on $X^n + Y^n = Z^n$. Between 1640 and 1850, a few mathematicians, Fermat, Euler, Lejeune Dirichlet, Legendre, Lamé, and Lebesgue, successfully studied the equation

$$X^n + Y^n = Z^n \tag{5.1}$$

for $n = 3,4,5,6,7$. In 1857, Kummer settled Fermat's conjecture for all the exponents $n \leq 100$.

In 1983, a major breakthrough was made by Faltings [13] when he proved that for a fixed $n \geq 4$, the equation $X^n + Y^n = Z^n$ has only a finite number of solutions (with no common divisors). As a matter of fact, Faltings obtained in 1986 the Fields Medal for having proved the Mordell conjecture: *every smooth algebraic curve of genus $g \geq 2$ over any given algebraic number field K has a finite number of K-rational solutions*. If one views an algebraic curve $\mathcal{C}$ as a Riemann surface, the genus of $\mathcal{C}$ is the number of holes. Since for $n \geq 4$, the Fermat algebraic curve $X^n + Y^n = Z^n$ is of genus $(n-1)(n-2)/2$, the curve has only a finite number of positive integral solutions coprime to one another.

We know since 1993 that Fermat's last theorem is true for $n \leq 4000000$; this was established with the help of computers. Moreover, a result of K. Inkeri implies that if there exist integers $C \geq B \geq A \geq 1$ such that $A^n + B^n = C^n$, then $A > 4000000^{11999996}$. This last integer is so big that if we wanted to write it at full length, it would require more than 70 million digits, which would make it close to 100 kilometers long (with 6 digits per centimeter). However, Wiles wanted to prove Fermat's last theorem definitely without the help of a computer, and so he did!

6. A small detour: the *ABC* conjecture. As odd as this may look, there exists an open problem concerning the equality

$$A+B=C, \tag{6.1}$$

and it is called the *ABC* conjecture. This is one of the deepest conjectures in mathematics and it is far from being proved, though many experts think it is true. The *ABC* conjecture, formulated in 1985 by J. Oesterlé and D. W. Masser, provides an upper bound for $|C|$ in terms of the product of the prime divisors of *ABC*. More precisely, first choose a real number $\varepsilon > 0$ (e.g., $\varepsilon = 0.000001$). Next suppose that $A+B=C$, where A and B have no divisor in common. Then the *ABC* conjecture asserts the existence of a constant M (depending only on ε) such that

$$|C| \le MR^{1+\varepsilon}. \tag{6.2}$$

Assuming the *ABC* conjecture, one can give a short proof of the existence of a (noneffective) constant N such that Fermat's last theorem is true for all $n \ge N$. Here is how it goes. Choose and fix ε with, for instance, $0 < \varepsilon < 1/10$. Suppose next that there exist $n \ge 4$ and some integers $c > b > a > 0$, coprime to one another, such that $a^n + b^n = c^n$. Put $A = a^n$, $B = b^n$, and $C = c^n$. Then the *ABC* conjecture guarantees the existence of a constant M (depending only on ε) such that

$$a^n < b^n < c^n < M\left(\prod_{p|abc} p\right)^{1+\varepsilon}. \tag{6.3}$$

Hence

$$(abc)^n < M^3\left(\prod_{p|abc} p\right)^{3+3\varepsilon}, \tag{6.4}$$

from which we conclude that n is bounded.

NOTICE TO AMATEURS: Let $C > 0$. Denote by E what was C, that is, $A+B=E$; use the letter C for what was R, and take $\varepsilon = 1$. Then the conjecture states that $E \le MC^2$, and the relativity of this shaky conjecture will certainly scare physicists.

7. Some generalized Fermat equations. For a long time, it was conjectured that 8 and 9 are the only consecutive powers. Many mathematicians contributed numerous partial results till this so-called *Catalan conjecture* was officially proved by Mihăilescu (see [30] or [4]), thanks to a clever use of the arithmetic of cyclotomic fields. The result can be stated in the following terms.

Theorem 7.1. *The only positive solution of the Diophantine equation*

$$X^m + 1 = Y^n, \tag{7.1}$$

with $m, n \geq 2$, *is* $(X, Y, m, n) = (2, 3, 3, 2)$.

Using deep mathematics, namely, elliptic curves *à la* Wiles, Darmon and Merel [11] solved some variants of the Fermat equation. They proved that the Dénes conjecture is true: *for* $n \geq 3$, *the only positive solution of the Diophantine equation*

$$X^n + Y^n = 2Z^n, \tag{7.2}$$

with $XYZ \neq 0$ *and* $\gcd(X, Y, Z) = 1$, *is* $X = Y = Z = 1$. They also proved the following: *for* $n \geq 4$ *and for* $q \in \{2, 3\}$, *the Diophantine equation*

$$X^n + Y^n = Z^q \tag{7.3}$$

has no integral solution with $\gcd(X, Y, Z) = 1$ *and* $XYZ \neq 0$.

We justify their hypothesis $\gcd(X, Y, Z) = 1$. Assume that n is of the form $n = 6m + 5$ and that $a^n + b^n = C$; then

$$(aC)^n + (bC)^n = \left(C^{3m+3}\right)^2 = \left(C^{2m+2}\right)^3. \tag{7.4}$$

Darmon and Granville [9] and Beukers [3] obtained great results on the Diophantine equation

$$AX^p + BY^q = CZ^r, \tag{7.5}$$

where A, B, and C are nonzero integers. Attach to the last equation the invariant

$$w = \frac{1}{p} + \frac{1}{q} + \frac{1}{r}. \tag{7.6}$$

Using a big result of Faltings, Darmon and Granville [9] proved that when $w < 1$, there are only finitely many integral solutions with $\gcd(X, Y, Z) = 1$. If $w = 1$, that is, if $\{p, q, r\} = \{3, 3, 3\}, \{2, 4, 4\}, \{2, 3, 6\}$, it turns out that we are in front of an elliptic curve, and we know from Mordell that there exists only a finite number of integral solutions. When $w > 1$, the possible sets of exponents $\{p, q, r\}$ are $\{2, 3, 5\}$, $\{2, 3, 4\}$, $\{2, 3, 3\}$, and $\{2, 2, k\}$ with $k \geq 2$, and Beukers [3] proved that either there is no integral solution or there are infinitely many solutions in integers verifying $\gcd(X, Y, Z) = 1$.

If $A = B = C = 1$, then in the cases where $\{p, q, r\}$ is $\{2, 3, 3\}$ or $\{2, 3, 4\}$, D. Zagier was more explicit. He first showed (see [3, Appendix A]) that all integral solutions of

$$X^3 + Y^3 = Z^2 \tag{7.7}$$

are given by the following parametrizations:

$$\begin{aligned} X &= s^4 + 6s^2t^2 - 3t^4, \\ Y &= -s^4 + 6s^2t^2 + 3t^4, \\ Z &= 6st(s^4 + 3t^4); \end{aligned}$$

$$\begin{aligned} X &= s^4 + 8st^3, \\ Y &= -4s^3t + 4t^4, \\ Z &= s^6 - 20s^3t^3 - 8t^6; \end{aligned} \tag{7.8}$$

$$\begin{aligned} X &= \frac{s^4 + 6s^2t^2 - 3t^4}{4}, \\ Y &= \frac{-s^4 + 6s^2t^2 + 3t^4}{4}, \\ Z &= \frac{3st(s^4 + 3t^4)}{4}. \end{aligned}$$

D. Zagier also showed that all integral solutions of

$$X^4 + Y^2 = Z^3 \tag{7.9}$$

are given by the following parametrizations:

$$\begin{aligned} X &= 6st(3s^4 - 4t^4), \\ Y &= (3s^4 + 4t^4)(9s^8 - 408s^4t^4 + 16t^8), \\ Z &= 9s^8 + 168s^4t^4 + 16t^8; \end{aligned}$$

$$\begin{aligned} X &= 6st(s^4 - 12t^4), \\ Y &= (s^4 + 12t^4)(s^8 - 408s^4t^4 + 144t^8), \\ Z &= s^8 + 168s^4t^4 + 144t^8; \end{aligned}$$

$$\begin{aligned} X &= \frac{3st(s^4 - 3t^4)}{2}, \\ Y &= \frac{(s^4 + 3t^4)(s^8 - 102s^4t^4 + 9t^8)}{8}, \\ Z &= \frac{s^8 + 42s^4t^4 + 9t^8}{4}; \end{aligned} \tag{7.10}$$

$$\begin{aligned} X &= (s^2 + 3t^2)(s^4 - 18s^2t^2 + 9t^4), \\ Y &= 4st(s^2 - 3t^2)(s^4 + 6s^2t^2 + 81t^4)(3s^4 + 2s^2t^2 + 3t^4), \\ Z &= (s^4 - 2s^2t^2 + 9t^4)(s^4 + 30s^2t^2 + 9t^4). \end{aligned}$$

Finally, D. Zagier showed that all the integral solutions of

$$X^4 + Y^3 = Z^2 \tag{7.11}$$

are given by the following parametrizations:

$$\begin{aligned}
&X = 6st(s^4 + 12t^4),\\
&Y = s^8 - 168s^4t^4 + 144t^8,\\
&Z = (s^4 - 12t^4)(s^8 + 408s^4t^4 + 144t^8);
\end{aligned}$$

$$\begin{aligned}
&X = (s^2 - 3t^2)(s^4 + 18s^2t^2 + 9t^4),\\
&Y = -(s^4 + 2s^2t^2 + 9t^4)(s^4 - 30s^2t^2 + 9t^4),\\
&Z = 4st(s^2 + 3t^2)(s^4 - 6s^2t^2 + 81t^4)(3s^4 - 2s^2t^2 + 3t^4);
\end{aligned}$$

$$\begin{aligned}
&X = 6st(3s^4 + 4t^4),\\
&Y = 9s^8 - 168s^4t^4 + 16t^8,\\
&Z = (3s^4 - 4t^4)(9s^8 + 408s^4t^4 + 16t^8);
\end{aligned}$$

$$\begin{aligned}
&X = s^6 + 40s^3t^3 - 32t^6,\\
&Y = -8st(s^3 - 16t^3)(s^3 + 2t^3),\\
&Z = s^{12} - 176s^9t^3 - 5632s^3t^9 - 1024t^{12};
\end{aligned}$$

$$\begin{aligned}
&X = s^6 + 6s^5t - 15s^4t^2 + 20s^3t^3 + 15s^2t^4 + 30st^5 - 17t^6,\\
&Y = 2s^8 - 8ts^7 - 56t^3s^5 - 28t^4s^4 + 168t^5s^3 - 112t^6s^2 + 88t^7s + 42t^8,\\
&Z = -3s^{12} + 12s^{11}t - 66s^{10}t^2 - 44s^9t^3 + 99s^8t^4 + 792s^7t^5 - 924s^6t^6\\
&\quad + 2376s^5t^7 - 1485s^4t^8 - 1188s^3t^9 + 2046s^2t^{10} - 156st^{11} + 397t^{12};
\end{aligned}$$

$$\begin{aligned}
&X = -5s^6 + 6s^5t + 15s^4t^2 - 60s^3t^3 + 45s^2t^4 - 18st^5 + 9t^6,\\
&Y = 6s^8 - 56s^7t + 112s^6t^2 - 168s^5t^3 + 252s^4t^4 - 168s^3t^5 + 72st^7 - 18t^8,\\
&Z = -29s^{12} - 15s^{11}t - 726s^{10}t^2 + 2420s^9t^3 - 4059s^8t^4 + 3960s^7t^5 - 2772s^6t^6\\
&\quad + 2376s^5t^7 - 3267s^4t^8 + 3564s^3t^9 - 1782s^2t^{10} + 324st^{11} + 27t^{12}.
\end{aligned} \tag{7.12}$$

R. Tijdeman conjectured that for $p,q,r \geq 3$, the Diophantine equation

$$X^p + Y^q = Z^r \tag{7.13}$$

has no integral solution in integers coprime to one another with $XYZ \neq 0$. This has become Beal's conjecture (http://www.bealconjecture.com/) when Beal offered \$100 000 to the first author who provides a proof of the conjecture or a mere counterexample. If exactly one of the exponents p, q, and r takes the

TABLE 7.1

$X^p + Y^p = Z^r$
$1^p + 2^3 = 3^2$
$2^5 + 7^2 = 3^4$
$7^3 + 13^2 = 2^9$
$2^7 + 17^3 = 71^2$
$3^5 + 11^4 = 122^2$
$17^7 + 76271^3 = 21063928^2$
$1414^3 + 2213459^2 = 65^7$
$9262^3 + 15312283^2 = 113^7$
$43^8 + 96222^3 = 30042907^2$
$33^8 + 1549034^2 = 15613^3$

value 2, then there are 10 known solutions (see [9]). Moreover, H. Darmon conjectured that there are no other solutions than those found by B. Kelly III, R. Scott, B. De Weger, F. Beukers, and D. Zagier (see Table 7.1).

Bennett [1] proved a breathtaking theorem concerning the Diophantine equation

$$\left| AX^n - BY^n \right| = 1, \tag{7.14}$$

with $n \geq 3$, when A and B are nonzero fixed integers: *it has at most one integral solution in positive integers X and Y*. This is quite a powerful result, as can be seen in the following two examples.

(i) For a given m, fix an integer $B = s^m + 1$. Then an integral solution of $|X^m - BY^m| = 1$ is $(X, Y) = (s, 1)$ and (in positive integers) there is no other one.

(ii) Fix an integer $A \geq 1$. For $n \geq 3$, the only positive integral solution of $(A+1)X^n - AY^n = 1$ is $(X, Y) = (1, 1)$.

Bennett also contributed major results on *simultaneous Diophantine equations*. In particular, he proved the following [2]: *if $a, b \in \mathbb{N} \setminus \{0\}$ with $a \neq b$, then the simultaneous Diophantine equations*

$$X^2 - aZ^2 = 1, \qquad Y^2 - bZ^2 = 1 \tag{7.15}$$

have at most three integral positive solutions with $XYZ \neq 0$. As a matter of fact, Bennett, supported by some of his results, conjectured that there are at most two solutions.

8. On certain families of Thue equations. Consider an algebraic number field $K = \mathbb{Q}(\omega)$, where ω is a solution of an irreducible polynomial

$$f(X) = X^m + a_1 X^{m-1} + a_2 X^{m-2} + \cdots + a_{m-1} X + a_m \tag{8.1}$$

of degree m with r real roots and $2s$ complex roots: $m = r + 2s$. Inside the ring $\mathbb{O}_K$ of algebraic integers of K lives the unit group E_K, which, by Dirichlet theorem [37], is isomorphic to a finite group of roots of unity times $r+s-1$ copies of $\mathbb{Z}$:

$$E_K \simeq W \times \langle \varepsilon_1 \rangle \times \langle \varepsilon_2 \rangle \times \cdots \times \langle \varepsilon_{r+s-1} \rangle. \tag{8.2}$$

It is classical to call $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1}\}$ a *fundamental system of units* of $\mathbb{Q}(\omega)$.

For small values of m, some mathematicians exhibited a fundamental system of units $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r+s-1}\}$ of K (resp., a maximal independent system of units of K) and when the coefficient a_m of $f(X)$ is in $\{1, -1\}$, a natural problem is the following one: solve families of Thue equations naturally associated to $f(X)$; namely, exhibit the integral solutions of the Thue equation

$$F(X,Y) = X^m + a_1 X^{m-1} Y + \cdots + a_{m-1} X Y^{m-1} + a_m Y^m = c \tag{8.3}$$

with $c \in \{1, -1\}$. Most of the time, Baker's linear forms in logarithms are used and the knowledge of the unit group of $K = \mathbb{Q}(\omega)$ proves useful.

(**A**) For instance, Thomas [41] with the help of Mignotte [26] proved that, for all $n \geq 0$, the three solutions of the Diophantine equation

$$X^3 - (n-1)X^2 Y - (n+2)XY^2 - Y^3 = c, \tag{8.4}$$

with $c \in \{1, -1\}$, are $(c, 0)$, $(0, -c)$, and $(-c, c)$, except for $n \in \{0, 1, 3\}$, where the extra solutions (X, Y) are given by

$$(x,y) = \begin{cases} (5c,4c),\ (4c,-9c),\ (-9c,5c),\ (2c,-c),\ (-c,-c),\ (-c,2c) & \text{if } n=0, \\ (2c,c),\ (-3c,2c),\ (c,-3c) & \text{if } n=1, \\ (-7c,-2c),\ (-2c,9c),\ (9c,-7c) & \text{if } n=3. \end{cases} \tag{8.5}$$

(**B**) Mignotte and Tzanakis [27, 29] and, independently, Lee [20] proved that, for $n = 2$ and for all $n \geq 5$, the five solutions of the Diophantine equation

$$X^3 - nX^2 Y - (n+1)XY^2 - Y^3 = c, \tag{8.6}$$

with $c \in \{1, -1\}$, are $(c, 0)$, $(0, -c)$, $(c, -c)$, $(-c(n+1), -c)$, and $(c, -cn)$. For $n \in \{0, 1, 3, 4\}$, the solutions are $(c, 0)$, $(0, -c)$, $(c, -c)$, and $(-c(n+1), -c)$ and extra solutions are provided by

$$(x,y) = \begin{cases} (4c,3c), & \text{if } n=0 \\ (-5c,14c),\ (-2c,3c),\ (-c,2c),\ (c,-3c),\ (9c,-13c) & \text{if } n=3, \\ (c,\text{-}4c),\ (7c,-9c) & \text{if } n=4. \end{cases} \tag{8.7}$$

(**C**) Assuming $1 \le a < b$ and $r \in \{1,-1\}$, Thomas [42] proved that, for all $n \ge 2\times 10^6(a+2b)^{4.85(b-a)}$, the four solutions of the Diophantine equation

$$X(X-n^aY)(X-n^bY)+rY^3=c, \tag{8.8}$$

with $c \in \{1,-1\}$, are $(c,0)$, $(0,cr)$, (n^arc,rc), and (n^brc,rc).

(**D**) First, Ljunggren [25], and later, Tzanakis [44], with a different method, proved that the six solutions of

$$X^3-3XY^2-Y^3=1 \tag{8.9}$$

are $(1,0)$, $(0-1)$, $(-1,1)$, $(2,1)$, $(-3,2)$, and $(1,-3)$.

(**E**) Pethő with the help of Mignotte and Roth [28, 34] proved that, for all $n \in \mathbb{Z}$ such that $|n| \ge 5$, and for $|n| = 3$, the twelve solutions of the Diophantine equation

$$X^4-nX^3Y-X^2Y^2+nXY^3+Y^4=1 \tag{8.10}$$

are given by $(1,0)$, $(-1,0)$, $(0,1)$, $(0,-1)$, $(1,1)$, $(-1,-1)$, $(1,-1)$, $(-1,1)$, $(n,1)$, $(-n,-1)$, $(1,-n)$, and $(-1,n)$. For $|n| = 4$, in addition to the last twelve solutions, there are four more solutions given by

$$(x,y)=\begin{cases}(8,7),\ (-8,-7),\ (7,-8),\ (-7,8) & \text{if } n=4,\\ (8,-7),\ (-8,7),\ (7,8),\ (-7,-8) & \text{if } n=-4.\end{cases} \tag{8.11}$$

Moreover, the Diophantine equation $X^4-nX^3Y-X^2Y^2+nXY^3+Y^4=-1$ has no integral solution at all.

(**F**) In [34], Pethő also proved that, for $|n| \ge 9.9\times 10^{27}$ and for $1 \le |n| \le 100$, the four solutions of

$$X^4-nX^3Y-3X^2Y^2+nXY^3+Y^4=c, \tag{8.12}$$

with $c \in \{1,-1\}$, are given by

$$(x,y)=\begin{cases}(1,0),\ (-1,0),\ (0,1),\ (0,-1) & \text{if } c=1,\\ (1,1),\ (1,-1),\ (-1,1),\ (-1,-1) & \text{if } c=-1,\end{cases} \tag{8.13}$$

except for $n \in \{1,-1\}$ and $c=-1$, where there are four extra solutions given by $(2n,1)$, $(-2n,-1)$, $(1,-2n)$, and $(-1,2n)$.

(**G**) Lettl and Pethő [21] and Chen and Voutier [7] proved that, for $|n| \ge 1$, the four solutions of

$$X^4-nX^3Y-6X^2Y^2+nXY^3+Y^4=d, \tag{8.14}$$

with $d \in \{-4,-1,1,4\}$, are given by

$$(x,y)=\begin{cases}(1,0),\ (-1,0),\ (0,1),\ (0,-1) & \text{if } d=1,\\ (1,1),\ (-1,-1),\ (1,-1),\ (-1,1) & \text{if } d=-4,\end{cases} \tag{8.15}$$

except for $n \in \{-4,-1,1,4\}$, where there are four extra solutions given by

$$(x,y) = \begin{cases} (2,3),\ (-2,-3),\ (3,-2),\ (-3,2) & \text{if } n = 4 \text{ and } d = 1, \\ (3,2),\ (-3,-2),\ (2,-3),\ (-2,3) & \text{if } n = -4 \text{ and } d = 1, \\ (1,2),\ (-1,-2),\ (2,-1),\ (-2,1) & \text{if } n = 1 \text{ and } d = -1, \\ (2,1),\ (-2,-1),\ (1,-2),\ (-1,2) & \text{if } n = -1 \text{ and } d = -1, \\ (5,1),\ (-5,-1),\ (1,-5),\ (-1,5) & \text{if } n = 4 \text{ and } d = -4, \\ (1,5),\ (-1,-5),\ (5,-1),\ (-5,1) & \text{if } n = -4 \text{ and } d = -4, \\ (3,1),\ (-3,-1),\ (1,-3),\ (-1,3) & \text{if } n = 1 \text{ and } d = 4, \\ (1,3),\ (-1,-3),\ (3,-1),\ (-3,1) & \text{if } n = -1 \text{ and } d = 4. \end{cases} \tag{8.16}$$

(**H**) Pethő and Tichy [35] proved that, for $10^{2\times 10^{28}} < m+1 < n \le m(1+(\log m)^{-4})$, the integer solutions of

$$X(X-Y)(X-mY)(X-nY) - Y^4 = c, \tag{8.17}$$

with $c \in \{-1,1\}$, are

$$(x,y) = \begin{cases} (1,0),\ (-1,0) & \text{if } c = 1, \\ \begin{cases} (0,1),\ (0,-1),\ (1,1),\ (-1,-1), \\ (m,1),\ (-m,-1),\ (n,1),\ (-n,-1) \end{cases} & \text{if } c = -1. \end{cases} \tag{8.18}$$

When $n = m+1$, Heuberger, Pethő, and Tichy [19] previously proved that the integer solutions are the same as the ones given above.

(**I**) Wakabayashi [45] proved that, for $n \ge 8$, the integral solutions of

$$X^4 - n^2X^2Y^2 + Y^4 = f, \tag{8.19}$$

with $f \in \{1, -(n^2-2)\}$, are

$$(x,y) = \begin{cases} \begin{cases} (0,1),\ (0,-1),\ (1,0),\ (-1,0),\ (n,1),(n,-1),(-n,1), \\ (-n,-1),\ (1,n),\ (1,-n),\ (-1,n),\ (-1,-n) \end{cases} & \text{if } f = 1, \\ (1,1),\ (1,-1),\ (-1,1),\ (-1,-1) \quad \text{if } f = -(n^2-2). \end{cases} \tag{8.20}$$

For $1 \le |f| \le n^2-2$ with $f \notin \{1, -(n^2-2)\}$, there is no integral solution.

(**J**) Assuming n, $n+2$, and n^2+4 to be square-free, Togbé [43] proved that, for $1 \le n \le 5\times 10^6$ and $n \ge 1.191\times 10^{19}$, the four integral solutions of

$$X^4 - n^2X^3Y - (n^3+2n^2+4n+2)X^2Y^2 - n^2XY^3 + Y^4 = 1 \tag{8.21}$$

are $(1,0)$, $(-1,0)$, $(0,1)$, and $(0,-1)$.

(**K**) Heuberger [18] showed that, for $|n| > 3.6\times 10^{19}$, the integral solutions of

$$X(X^2-Y^2)(X^2-n^2Y^2)-Y^5=c, \tag{8.22}$$

with $c\in\{1,-1\}$, are $(c,0)$, $(0,-c)$, $(-c,-c)$, $(c,-c)$, $(n,-c)$, and $(-n,-c)$.

(**L**) In [14, 15], Gaál and Lettl proved that, for all $n\in\mathbb{Z}$, the two integral solutions of

$$\begin{aligned} &X^5+(n-1)^2X^4Y-(2n^3+4n+4)X^3Y^2\\ &\quad+(n^4+n^3+2n^2+4n-3)X^2Y^3+(n^3+n^2+5n+3)XY^4+Y^5=c, \end{aligned} \tag{8.23}$$

with $c\in\{1,-1\}$, are $(c,0)$ and $(0,c)$, except for $n\in\{0,-1\}$, where there are three extra solutions given by

$$(x,y)=\begin{cases}(c,-c),\ (-c,-c),\ (2c,-c) & \text{if } n=0,\\ (c,-c),\ (c,c),\ (-2c,c) & \text{if } n=-1.\end{cases} \tag{8.24}$$

(**M**) Levesque and Mignotte [24] proved that, for all $n\ge 10^{12}$, the three solutions of the Diophantine equation

$$X^5+2X^4Y+(n+3)X^3Y^2+(2n+3)X^2Y^3+(n+1)XY^4-Y^5=c, \tag{8.25}$$

with $c\in\{1,-1\}$, are $(c,0)$, $(0,-c)$, and $(c,-c)$.

(**N**) In [22, 23], using hypergeometric methods and Baker's linear forms in logarithms, Lettl, Pethő, and Voutier [22] proved that, for all $n\ge 89$, the six integer solutions of

$$\begin{aligned} X^6-2nX^5Y-(5n+15)X^4Y^2-20X^3Y^3\\ +5nX^2Y^4+(2n+6)XY^5+Y^6=c, \end{aligned} \tag{8.26}$$

with $c\in\{1,-27\}$, are

$$(x,y)=\begin{cases}(1,0),(-1,0),(0,1),(0,-1),(1,-1),(-1,1) & \text{if } c=1,\\ (1,1),(-1,-1),(2,-1),(-2,1),(1,-2),(-1,2) & \text{if } c=-27.\end{cases} \tag{8.27}$$

When $1\le|c|\le 27$ with $c\notin\{1,-27\}$, there is no integer solution.

9. Andrew Wiles. We come back to Fermat's last theorem and to the proof of Wiles. The main ingredient of the proof is the theory of elliptic curves. An elliptic curve E (see Figure 9.1) over the field $\mathbb{Q}$ of rational numbers can be characterized as the set of rational solutions (i.e., solutions in $\mathbb{Q}$) of an equation of the form

$$Y^2=X^3+aX^2+bX+c, \tag{9.1}$$

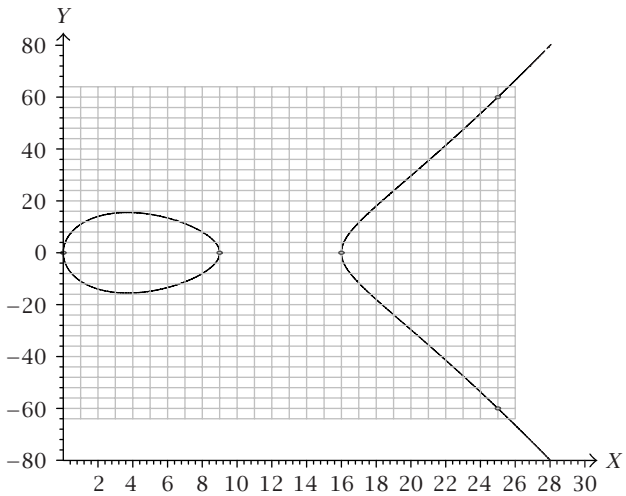

FIGURE 9.1 Elliptic curve $E: Y^2 = X(X-9)(X-16)$.

with $a, b, c \in \mathbb{Z}$. We mention, by the way, that according to Mordell [31], the number of integral solutions (x, y) of E is finite.

On the one hand, G. Frey showed in 1985 that if nonzero integers a, b, $c \geq 1$ happen to verify $a^n + b^n = c^n$, $n \geq 5$, then the elliptic curve

$$Y^2 = X(X - a^n)(X + b^n) \tag{9.2}$$

is *semistable*, that is, its conductor (to be defined in the next section) involves only prime integers raised to the power 1. On the other hand, K. A. Ribet proved a few years later that such an elliptic curve $Y^2 = X(X-a^n)(X+b^n)$ (built from a hypothetical solution a, b, and c of $A^n + B^n = C^n$ with $a, b, c \neq 0$) cannot be *modular*, that is, cannot be written in terms of certain functions dubbed as *modular functions*. In a *tour de force*, Andrew Wiles next proved the following remarkable result: *every semistable elliptic curve is modular.* If you reread this paragraph, you will see that Fermat's last theorem is proved by contradiction, with the help of this striking result of Wiles.

10. Modular elliptic curves. In this section, we give the flavour of the notions of *conductor*, *semistability*, and *modularity* of an elliptic curve E over $\mathbb{Q}$ which can be written in the affine plane as

$$E: Y^2 = X^3 + aX + b \quad \text{with } a, b \in \mathbb{Z}, \tag{10.1}$$

and whose *discriminant* is, by definition, $\Delta = -16(4a^3 + 27b^2) \neq 0$. If $p \nmid \Delta$, we say that E has *good reduction* at p. If $p|\Delta$ and if the elliptic curve E, viewed as a curve over $\mathbb{Z}/p\mathbb{Z}$, has a double point with two different tangents (resp., with

the same tangent), we say that E has *multiplicative* (resp., *additive*) *reduction* at p. The *conductor* N of E, a divisor of Δ, is by definition

$$N = \prod_{p|\Delta} p^{\delta_p} \tag{10.2}$$

with $\delta_p = 1$ if the reduction of E at p is multiplicative, $\delta_p = 2$ if the reduction of E at p for $p \geq 5$ is additive, and $\delta_p \geq 2$ if the reduction of E at p for $p \in \{2,3\}$ is additive. We say that E is *semistable* if the conductor N of E happens to be square-free.

Denote by $\mathcal{N}_p$ the number of solutions of the curve E modulo p, that is, $\mathcal{N}_p$ is the number of pairs $(x,y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ which are solutions of the equation of the curve, the equation being considered as a congruence modulo p. Since ∞ (which happens to be the identity element of the group of rational points of the curve) is also a solution, in practice, the number $\#E(\mathbb{Z}/p\mathbb{Z})$ of points of the curve E over $\mathbb{Z}/p\mathbb{Z}$ is $\mathcal{N}_p + 1$. The pieces of information obtained for all primes p generate the numbers

$$a_p = p - \mathcal{N}_p = p + 1 - \#E(\mathbb{Z}/p\mathbb{Z}). \tag{10.3}$$

These numbers are used to build the L-function associated to the curve E, denoted by $L(E,s)$, defined formally as the infinite product

$$\prod_{p|\Delta} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p\nmid\Delta} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}. \tag{10.4}$$

Here $L(E,s)$ is a function of the complex variable s and it is well known that the Dirichlet series

$$L(E,s) = \prod_{p|\Delta} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p\nmid\Delta} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \tag{10.5}$$

converges for $\Re s > 3/2$ (where $\Re s$ is the real part of s, with $\Im(s)$ being the imaginary part of s).

Let $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$ denote the *Poincaré upper half-plane*. Consider the group of matrices

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} : a,b,c,d \in \mathbb{Z},\ ad - Nbc = 1 \right\}. \tag{10.6}$$

By definition, the action of $\Gamma_0(N)$ on $\mathcal{H}$ is given by

$$\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}(z) = \frac{az+b}{Ncz+d}. \tag{10.7}$$

Two points z and w of $\mathcal{H}$ will be considered as equivalent modulo $\Gamma_0(N)$ (in symbols $w \sim z$) if there exists $M \in \Gamma_0(N)$ such that $Mw = z$. The quotient space

$\mathcal{H}/\sim$, classically written as $\mathcal{H}/\Gamma_0(N)$, can be compactified by adding a finite number of the so-called *cusps* to obtain a compact Riemann surface denoted by

$$X_0(N) = \mathcal{H}/\Gamma_0(N) \cup \{\text{cusps}\}. \tag{10.8}$$

A *modular form* $f(z)$ *of level* N (and of *weight* 2) is a function f of a complex variable defined on $\mathcal{H}$ with values in $\mathbb{C}$, holomorphic on $\mathcal{H} \cup \{\text{cusps}\}$, and verifying

$$f\left(\frac{az+b}{Ncz+d}\right) = (Ncz+d)^2 f(z), \quad \forall \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N). \tag{10.9}$$

In particular, $f(z+1) = f((z+1)/(0z+1)) = f(z)$, which implies that f has a Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}, \quad a_n \in \mathbb{C}, \tag{10.10}$$

so one associates with f the Dirichlet series $\sum_{n=1}^{\infty}(a_n/n^s)$.

The study of an L-series associated with an elliptic curve E is easier if we *know* that the L-series associated with E is an L-series attached as above to a modular form f. This is exactly what the Shimura-Taniyama conjecture predicts: *for every elliptic curve* E *over* $\mathbb{Q}$, *there exists a modular form* f *whose* L*-series associated to* f *is the same as the* L*-series associated to* E. As a matter of fact, the conjecture predicts more, and the reader is invited to look at [5, 8, 10, 16, 17, 32, 33, 38].

11. Epilogue. Starting from June 23, 1993, the members of the mathematical community intensively studied the proof of Wiles and realized that there was a gap. In a public e-mail dated December 6, 1994, Andrew Wiles himself confessed that the proof was not complete since an upper bound of the order of a so-called Selmer group was missing. With the help of his former Ph.D. student, Richard Taylor, Andrew Wiles overcame this difficulty by using other machinery.

One year later, the proof was complete. On October 11, 1994, a handful of mathematicians, including my colleague Henri Darmon (McGill University), received the long proof of Wiles together with a joint preprint of R. Taylor and A. Wiles. On October 25, 1994, about 20 mathematicians were officially sent this proof. Then fax machines and e-mails got into action, and we know the end of the story. Specialists agreed: this time, devil played no trick and Fermat may rest in peace. The proof appeared in [46]; the proof uses results of leaders in mathematics together with, for the final step, the results of a paper by Taylor and Wiles [40].

A few years later, Breuil et al. [6] proved along the lines of the programme of Wiles that indeed *every elliptic curve over* $\mathbb{Q}$ *is modular*. This result allowed mathematicians to unconditionally solve other Diophantine equations.

Acknowledgments. This survey article is the written expanded version of a plenary lecture given in French on November 7, 2001, during the conference *Second Colloque International d'Algèbre et de Théorie des Nombres* held in Fes, Morocco. The author wants to express all his gratitude to Professor M. Boulagouaz and Professor M. Charkani, organizers of the meeting, to Professor Stefaan Caenepeel for his support, and to Professor Saïd El Morchid for his help with the figures drawing. This work was supported by grants from NSERC (Canada) and FCAR (Québec).

References

[1] M. A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. reine angew. Math. **498** (1998), 173–199.

[2] ———, *Rational approximation to algebraic numbers of small height: the Diophantine equation* $|ax^n - by^n| = 1$, J. reine angew. Math. **535** (2001), 1–49.

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

[4] Yu. F. Bilu, *Catalan's conjecture (after Mihăilescu)*, Séminaire Bourbaki **55ème année** (2002-2003), Exposé 909, 1–25.

[5] N. Boston, *A Taylor-made plug for Wiles' proof*, College Math. J. **26** (1995), no. 2, 100–105.

[6] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[7] J. H. Chen and P. Voutier, *Complete solution of the Diophantine equation* $X^2 + 1 = dY^4$ *and a related family of quartic Thue equations*, J. Number Theory **62** (1997), no. 1, 71–99.

[8] D. A. Cox, *Introduction to Fermat's last theorem*, Amer. Math. Monthly **101** (1994), no. 1, 3–14.

[9] H. Darmon and A. Granville, *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), no. 6, 513–543.

[10] H. Darmon and C. Levesque, *Sommes infinies, équations diophantiennes et le dernier théorème de Fermat*, Gazette Sc. Math. Québec **18** (1996), no. 1, 3–26.

[11] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last theorem*, J. reine angew. Math. **490** (1997), 81–100.

[12] N. D. Elkies, *On* $A^4 + B^4 + C^4 = D^4$, Math. Comp. **51** (1988), no. 184, 825–835.

[13] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* [*Finiteness theorems for abelian varieties over number fields*], Invent. Math. **73** (1983), no. 3, 349–366 (German).

[14] I. Gaál and G. Lettl, *A parametric family of quintic Thue equations*, Math. Comp. **69** (2000), no. 230, 851–859.

[15] ———, *A parametric family of quintic Thue equations. II*, Monatsh. Math. **131** (2000), no. 1, 29–35.

[16] C. Goldstein, *Le théorème de Fermat*, La recherche **263** (1994), 268–275 (French).

[17] F. Q. Gouvêa, *A marvelous proof*, Amer. Math. Monthly **101** (1994), no. 3, 203–222.
[18] C. Heuberger, *On a family of quintic Thue equations*, J. Symbolic Comput. **26** (1998), no. 2, 173–185.
[19] C. Heuberger, A. Pethő, and R. F. Tichy, *Complete solution of parametrized Thue equations*, Acta Math. Inform. Univ. Ostraviensis **6** (1998), no. 1, 93–114.
[20] E. Lee, *Studies on diophantine equations*, Ph.D. thesis, Dept. Math., Cambridge University, Cambridge, 1992.
[21] G. Lettl and A. Pethő, *Complete solution of a family of quartic Thue equations*, Abh. Math. Sem. Univ. Hamburg **65** (1995), 365–383.
[22] G. Lettl, A. Pethő, and P. Voutier, *On the arithmetic of simplest sextic fields and related Thue equations*, Number Theory, Diophantine, Computational and Algebraic Aspects (Eger, 1996), Walter de Gruyter, Berlin, 1998.
[23] ———, *Simple families of Thue inequalities*, Trans. Amer. Math. Soc. **351** (1999), no. 5, 1871–1894.
[24] C. Levesque and M. Mignotte, *Sur une famille d'équations quintiques*, preliminary draft (French).
[25] W. Ljunggren, *Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante*, Acta Math. **75** (1943), 1–21 (German).
[26] M. Mignotte, *Verification of a conjecture of E. Thomas*, J. Number Theory **44** (1993), no. 2, 172–177.
[27] ———, *Pethő's cubics*, Publ. Math. Debrecen **56** (2000), no. 3-4, 481–505.
[28] M. Mignotte, A. Pethő, and R. Roth, *Complete solutions of a family of quartic Thue and index form equations*, Math. Comp. **65** (1996), no. 213, 341–354.
[29] M. Mignotte and N. Tzanakis, *On a family of cubics*, J. Number Theory **39** (1991), no. 1, 41–49.
[30] P. Mihăilescu, *Primary units and a proof of Catalan's conjecture*, submitted to Crelle Journal.
[31] L. J. Mordell, *Diophantine Equations*, Pure and Applied Mathematics, vol. 30, Academic Press, New York, 1969.
[32] M. R. Murty, *Fermat's last theorem: an outline*, Gazette Sc. Math. Québec **16** (1993), no. 1, 4–13.
[33] ———, *Reflections on Fermat's last theorem*, Elem. Math. **50** (1995), no. 1, 3–11.
[34] A. Pethő, *Complete solutions to families of quartic Thue equations*, Math. Comp. **57** (1991), no. 196, 777–798.
[35] A. Pethő and R. F. Tichy, *On two-parametric quartic families of Diophantine problems*, J. Symbolic Comput. **26** (1998), no. 2, 151–171.
[36] F. Peyrard, *Les oeuvres d'Euclide*, traduction d'un manuscrit grec publiée en 1819, Libraire Scientifique et Technique Albert Blanchard, Paris, 1966.
[37] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Universitext, Springer-Verlag, New York, 2001.
[38] K. Ribet and B. Hayes, *Fermat's last theorem and modern arithmetic*, Amer. Sci. **82** (1994), 144–156.
[39] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics, vol. 87, Cambridge University Press, Cambridge, 1986.
[40] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.
[41] E. Thomas, *Complete solutions to a family of cubic Diophantine equations*, J. Number Theory **34** (1990), no. 2, 235–250.

[42] ———, *Solutions to certain families of Thue equations*, J. Number Theory **43** (1993), no. 3, 319–369.
[43] A. Togbé, *On the solutions of a family of quartic Thue equations*, Math. Comp. **69** (2000), no. 230, 839–849.
[44] N. Tzanakis, *The Diophantine equation* $x^3 - 3xy^2 - y^3 = 1$ *and related equations*, J. Number Theory **18** (1984), no. 2, 192–205.
[45] I. Wakabayashi, *On a family of quartic Thue inequalities. I*, J. Number Theory **66** (1997), no. 1, 70–84.
[46] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

C. Levesque: Département de Mathématiques et de Statistique, Université Laval, Québec, Canada G1K 7P4
E-mail address: cl@mat.ulaval.ca