Séminaire de philosophie et mathématiques

Paulo Ribenboim

Catalan's Conjecture

Séminaire de Philosophie et Mathématiques, 1994, fascicule 6
« Catalan's conjecture », , p. 1-11
<http://www.numdam.org/item?id=SPHM_1994___6_A1_0>

Catalan's Conjecture

PAULO RIBENBOIM

Lecture at the Seminar "Philosophie et Mathématique",
École Normale Supérieure, Paris.

November 28, 1994

Summary

§1. The Problem
§2. Relation with other Problems
§3. Special Cases
§4. Algebraic Methods
§5. Analytical Methods
§6. Conclusion

§1. The Problem

I shall consider sequences of integers and ask some questions. First, consider the sequence of all squares or cubes:

$$4, 8, 9, 16, 25, 27, 36, 49, 64, 81, 100, \ldots$$

It may be observed that 8 and 9 are consecutive numbers in this sequence. The first problem is:

Are there any other consecutive integers in the above sequence? How many pairs of consecutive integers? Finitely many? Infinitely many?

I may also consider the sequence of all proper powers, which includes also 5th powers, 7th powers, 11th powers, etc... (note that powers with even exponents are squares, powers with exponent multiplis of 3 are cubes...)

The same problem may be asked. Are there consecutive powers other than 8 and 9?

But for the sequence of all powers a new problem makes sense: Are there three consecutive integers which are proper powers?

Sinie powers grow very fast, lists of powers are necessarily very limited and, besides 8 and 9, no consecutive powers have ever been observed. This is an indication to keep in mind, but one should be careful before jumping to any conclusion.

Just think, for example, that up to 100, 10% of the numbers are squares, up to 10.000, 1% are squares, up to 1.000.000, 1 in 1000 are squares, and so on. Yet, Lagrange proved that despite the increasing scarcity of squares, every natural number is the sum of at most 4 squares. As, if the squares occupy strategic positions. Of course, ours is a different problem.

Similar problems may be asked with the following sequence. Let a, b be integers, $1 < a < b$ and consider the sequence of all powers of a or of b. For example, if $a = 2$, $b = 3$, it is the sequence.

$$4, 8, 9, 16, 27, 32, 64, 81, \ldots$$

How many pairs of consecutive integers may be found in such sequences?

Now, let E be a finite (nonempty) set of prime numbers and let $E^\times$ be the set of all natural numbers whose prime factors belong to E. How many pairs of consecutive integers belong to $E^\times$?

All the above problems may be easily expressed in terms of diophantine equations.

The first problem amounts to the solution in natural numbers of the equations

$$X^2 - Y^3 = 1\,, \qquad X^3 - Y^2 = 1$$

The problem concerning arbitrary powers is expressed by the exponential diophantine equation, in form unknowns.

$$X^U - Y^V = 1$$

to be solved in integers greater than 1.

If $1 < a < b$, the third problem is the same as the solution in integers greater than 1, of the equations

$$a^U - b^V = 1\,, \qquad b^V - a^U = 1\,.$$

Finally, the problem for the sequence $E^\times$, corresponds to the simple equation

$$X - Y = 1\,,$$

but the solutions have to belong to $E^\times$.

In 1844. Catalan conjectured that 8, 9 are the only consecutive integers which are powers.

Despite much progress —which I'll soon describe— Catalan's conjecture has yet to be proved.

§2. Relation with other problems

In the seminars of this series, it is more important to understand the nature of the problems, their place in the theory, rather than to enter into technical details.

Let P be a set of natural numbers; whenever convenient, it may be assumed that $0 \in P$.

I shall describe addition and subtraction problems.

Addition Problems

Let $P + P = \{p + p' \mid p, p' \in P\}$. If $n \geq 1$, let $nP = \{p_1 + p_2 + \cdots + p_n \mid \text{each } p_i \in P\}$. Let $\langle P \rangle = \bigcup_{n \geq 1} nP$.

One wishes to study the sets nP, $\langle P \rangle$ and compare them with the set $\mathbf{N}$ of all natural numbers or with some appropiate subset of $\mathbf{N}$.

For example, these are the usual questions:

Does there exist n such that $nP = \mathbf{N}$? Is $\langle P \rangle = \mathbf{N}$?

There are also the corresponding asymptotic questions. Does there exist k_0 such that

$$\{k \in \mathbb{N} \mid k \geq k_0\} \subseteq nP \quad \text{or} \quad \{k \in \mathbb{N} \mid k \geq k_0\} \subseteq \langle P\rangle .$$

In such situations, can one find k_0 effectively?

Subtraction Problems

Now the problem is to to identify the set $P - P$.

More precisely, if $n \in P - P$ to determine the set $\{(p, p') \in P \times P \mid n = p - p'\}$ or at least to find bounds for the number of elements of the set.

Again, in some cases, the answer is only known asymptotically and it may be quite difficult.

These ideas will now be illustrated

1) Prime numbers

Let P be the set of all prime numbers. More generally. if $k \geq 1$ let P_k be the set of all integers of the form $p_1^{e_1} \cdots p_n^{e_n}$ with $0 < e_1 + \cdots + e_n \leq k$ which are called k-almost primes.

Thus $P_1 = P$.

Addition problem: Goldbach problem.

The famous conjecture of Goldbach starts that

$$\{2n \mid n \geq 2\} \subset P + P ,$$

or equivalently,

$$\{n \mid n \geq 6\} = P + P + P .$$

In my book on prime numbers (quoted in the references), I described the main results obtained in the study of Goldbach's conjecture.

For example, Vinogradov proved:

$$\{n \mid n \text{ odd}, \ n > 3^{3^{15}}\} \subset P + P + P .$$

Schnirelmann showed that there exists S_0 such that

$$\{n \mid n \geq 4\} = \bigcup_{k=1}^{S_0} kP .$$

Riesel and Vaughan calculated that S_0 may be taken to be 19.

Allowing almost primes, I note the pioneering result of Brun:

$$\{n \mid n \geq 4\} = P_9 + P_9 .$$

The best result known today is due to Chen:

$$\{n \mid n \geq 4\} = P + P_2$$

Subtraction problems: Polignac's conjecture and twin primes conjecture

Polignac conjectured that every even number is the difference of two primes; in other words:

$$\{2k \mid k \geq 1\} \bigcup \{1\} = P - P.$$

This conjecture has never been proved.

The twin primes conjecture is the statement that there exist infinitely many primes p such that $p+2$ is also a prime. In other words, 2 may be represented in infinitely many ways in the form $2 = p' - p$, where p, p' are primes. This statement is also waiting for a proof.

For each $N > 1$, let $\pi_2(N)$ denote the number of primes $p \leq N$ such that $p+2$ is also prime. The following is a quantitive version of the twin primes conjecture:

$$\pi_2(N) \sim \frac{N}{(\log N)^2},$$

that is, the quotient of the two expressions has limit equal to 1 (as $N \to \infty$).

According to Brun, twin primes are scarce, sinie

$$\sum \frac{1}{p} = B < \infty$$

(sum extended for all primes p such that $p+2$ is also a prime). Note that $\sum \frac{1}{p} = \infty$ (sum for all primes).

2) Powers and powerful numbers

Let P be the set of all proper powers. Let Q be the set of all powerful numbers (that is numbers N such that if p divides N, then p^2 divides N).

It is immediate that $Q = \{a^2b^3 \mid a, b \geq 1\}$

Addition problems. The interesting problem concerning the set $P+P$ is the description of $(P+P) \cap P$; in others words, the study of the solutions of $X^l + Y^m = Z^n$ for fixed l, m, n or even arbitrary l, m, n. In particular, the study of the equation $X^n + Y^n = Z^n$ (Fermat's equation) has been going for over three centuries. The problem of Fermat has just been solved by A. Wiles (with the collaboration of R. Taylor):

If $n \geq 3$ and x, y, z are natural numbers such that $x^n + x^n = z^n$, then $xyz = 0$.

The situation is very different when $n = 2$. It has long been known that there exist infinitely many triples of pairwise relatively integers (x, y, z) such that $x^2 + y^2 = z^2$ (these are the Pythagorean triples).

A similar result has been recently obtained by Elkres: there exist infinitely many fourth powers which are sums of three fourth powers.

Another famous addition problem is due to Waring. Given $k \geq 2$ does there exist an integer $G(k) > 1$ such that every sufficiently large natural number is the sum of at most $G(k)$ kth powers? Similarly, does there exist an integer $g(k) > 1$ such that every natural number is the sum of at most $g(k)$ kth powers?

In this respect —as I have already mentioned— Lagrange proved that for squares, $g(2) = 4$, while Gauss showed that $G(2) = 4$.

Hilbert showed the existence of $g(k)$ for each $k \geq 2$. The problem became the exact calculation of $G(k)$ $g(k)$. Thus, Davenport showed that $g(4) = 19$. The complete solution for 4th powers was given recently by Balasubramanian, Dcshouillers and Dress: $G(4) = 16$. Explicitly, all sufficiently large integers are sums of 16 fourth powers; there exist infinitely many integers which are not sums of 15 fourth powers; all integers are sums of at most 19 fourth powers.

More results about Waring's problem are gathered in my book on prime numbers.

Concerning powerful numbers, I note that not every natural number is the sum of two powerful numbers. On the contrary

$$\lim_{N\to\infty} \frac{\#\{n \in Q+Q \mid n \leq N\}}{N} = 0\,.$$

However Heath-Brown has shown that every sufficiently large natural number is the sum of at most three powerful numbers.

Subtraction problems

This time I consider first the powerful numbers. The notation $1 \underset{\infty}{\in} Q - Q$ means that 1 is in infinitely many was the difference of powerful numbers; in other words there exists infinitely many pairs of consecutive powerful numbers. Indeed there are infinitely many pairs (x, y) such that $x^2 - 8y^2 = 1$, thus x^2, $8y^2$ are consecutive powerful numbers.

With similar notation, Mollin and McDaniel showed that $n \underset{\infty}{\in} Q - Q$, for every $n \geq 2$.

Concerning three consecutive powerful numbers. Erdös conjectured: there do not exist three consecutive powerful numbers.

Granville showed how to deduce from this conjecture the theorem of Adleman, Heath-Brown& Fouvry: there exist infinitely many primes p such that if x, y, z are natural numbers and $x^p + y^p = z^p$, then p divides xyz (first case of Fermat's last theorem). Despite the recent proof of Fermat's last theorem, the connection between this theorem and powerful numbers remains intriguing.

The corresponding question for powers amounts to Catalan's conjecture if: $1 = p' - p$ (with $p, p' \in P$) then $p' = 9$, $p = 8$.

Pillai conjectured: for every $k > 1$ there exist only finitely many pairs of powers (p, p') with $p, p' \in P$ and $k = p' - p$.

Pillai's conjecture may be expressed in terms of the sequence

$$z_1 < z_2 < z_3 < \cdots$$

of all powers. Namely

$$\lim_{i\to\infty}(z_{1+1} - z_i) = \infty\,.$$

At the appropriate moment, I shall deal with three consecutive powers.

§3. Special Cases

The first recorded result in connection with the problems of Catalan and analogues dates back to around 1320 and it is due to Levi ben Gerson (= Leo Hebraeus), a famous astronomer of his time. He proved that if powers of 2 and 3 are consecutive, then it must be 9-8 =1. Today this is no more than an easy exercise with congruences.

Euler proved that if $X^2 - Y^3 = \pm 1$ then it must be $9 - 8 = 1$. Here is the idea behind the proof that $X^2 - Y^3 = -1$ has no solution in integers $x, y > 0$. Indeed, if $x^2 - y^3 = -1$ then $y^3 = x^2 + 1 = (x+i)(x-i)$, where $i^2 = -1$. From the arithmetic of Gaussian integers (easy facts known to Euler), $x + i = \alpha(a+bi)^3$, where a, b are integers and $\alpha = \pm 1$ or $\pm i$. Then $x - i = \overline{\alpha}(a-bi)^3$ with $\overline{\alpha} = \pm 1$ or $\mp i$ (respectively). Then $2i = \alpha(a+bi)^3 - \overline{\alpha}(a-bi)^3$ and an easy calculation, shows that this is impossible. The fact to note is the appeal to Gaussian integers. This idea, duly modified, is found also in the study of other special cases. This is embodied in the following lemma preceded by an obvious remark. If $m, n \geq 2$ and $x^m - y^n = 1$, let p, q be primes, $m = pm'$, $n = qn'$, then $(x^{m'})^p - (y^{n'})^q = 1$. Thus to show that $X^m - Y^n = 1$ has no solution it suffices to consider the same equation, when the exponents are primes p, q.

Now if p, q are odd primes $x, y \neq 0$, $x^p - y^q = 1$, then $y^q = x^p - 1 = (x-1)\left(\frac{x^p-1}{x-1}\right)$.

Since $\gcd(x-1, \frac{x^p-1}{x-1}) = 1$ or p, two cases are possible:

$$\begin{cases} x - 1 = r^q \\ \frac{x^p-1}{x-1} = r'^q \end{cases}$$

with $\gcd(r, r') = 1$ and $rr' = y$, or

$$\begin{cases} x - 1 = p^{q-1}r^q \\ \frac{x^p-1}{x} = pr'^q \end{cases}$$

with $\gcd(r, r') = 1$ and $prr' = y$ (since p^2 does not divide $\frac{x^p-1}{x-1}$).

From $x^p = y^q + 1 = (y+1)\left(\frac{y^q-1}{y+1}\right)$, one obtains analogous expressions for $y+1$, $\frac{y^q+1}{y+1}$ in two cases.

There are also similar expressions derived from $x^2 - y^q = 1$ (with q odd prime).

The next special cases dealt were $X^2 - Y^q = 1$, resp. $X^p - Y^2 = 1$ (with p, q primes greater than 3).

Now it happened that one of the above equations was dealt without difficulty and was solved only six years after Catalan's announced his conjecture (1844), thus in 1850, by Lebesgue. Whereas. the other equation, dispite multiple attimpts, required 120 years to be finally solved by Ko in 1964.

Which one is which?

This question is very "à-propos" to stress that sometimes two Diophantine equations may look very much alike but their solution demand methods of a very different level of difficulty.

Lebesgue proved, with a variant of the method of Euler, that $X^p - Y^2 = 1$ (with p prime $p \geq 5$) has only trivial solution.

The proof of Ko (in 1964) that $X^2 - Y^q = 1$ (q prime, $q \geq 5$) has only trivial solution, was much more difficult. Later, Chein used results of Størmer and Nagell from the beginning of this century. to give a clever and much shorter proof of Ko's theorem. Only three pages sufficed!

Once again. mathematicians should not despair from replacing difficult tortuous proofs (which may reflect a lack of complete understanding) by clean and reat -ahbeit clever- proofs [Don't extend what I just said to cover the recent proof of Fermat's last theorem, nor to infer that I believe that a 3-pages proof could be found, if not one in a margin...].

The study of the equations $X^3 - Y^q = 1$, $X^p - Y^3 = 1$ (for p, q primes greater than 3), lead to the equations

$$X^2 + X + 1 = Y^q$$

or

$$X^2 + X + 1 = 3Y^q.$$

These equations were dealt by Nagell, who stated that they have only trivial solutions, provided the solutions of the equation

$$X^3 - 3XY^2 + Y^3 = 1$$

were the ones already known: $(x, y) = (1,0), (0,1), (-1,-1), (2,-1), (1,3)$ and $(-3,-2)$. This was not easy to establish Ljunggren (1942) succeded with a precise analysis of the groups of units in a certain cubic field.

I like to stress that no one dared to attack the equation $X^p - Y^q = 1$ where $\min\{p, q\} \geq 5$, using ad-hoc special methods.

§4. Algebraic Methods

The purpose of these methods relying heavily on the arithmetic of algebraic numbers fields, is to treat simultaneously large classes of exponents. Congruences, units, classes of ideals abound in these considerations.

But first I wish to list some additional conditions which imply that the only non-trivial solution of $X^U - Y^V = 1$ (with exponents at least 2) is $x = 3$, $y = 2$, $u = 2$, $v = 3$, giving 9-8=1.

Namely:

a) If p, q are primes, l prime and $l^p - y^q = \pm 1$, then necessarily $l = 3$, $p = 2$, $y = 2$, $q = 3$.

b) If $x, y \geq 2$ and $x^y - y^x = 1$, then $x = 3$, $y = 2$.

c) The only consecutive powers of consecutive integers are 9, 8, in other words $x^m - y^n = 1$ and $|x - y| = 1$ imply that $x = 3$, $y = 2$, $m = 2$, $n = 3$.

The proof of c) requires an interesting long known arithmetical result on prime divisors of expressions of the form $x^m - 1$.

Cassels gave a remarkable proof of the following result:

If $x^p - y^q = 1$ (with p, q primes), then p divides y and q divides x.

It follows that in the old Euler's lemma, only the second case can actually take place. Thus $x - 1 = p^{q-1}r^q$, $\frac{x^p-1}{x-1} = pr'^q$ and also $y + 1 = q^{p-1}s^p$, $\frac{y^q+1}{y+1} = qs'^p$.

One wonders what would be the importance of Cassels' result. Not knowing the existence of x, y such that $x^p - y^q = 1$, how can one use the fact that $p|y$ and $q|x$?

Surprise! Both Hyyrö (in Finnish) and Mąkowski proved:

There do not exist three consecutive powers.

It seems to be an unwritten rule that every lecture should include at least one proof. So I choose this one for its striking simplicity:

If $x^p < y^q < z^r$ are proper powers with exponents which may be taken to be primes, if $y^q - x^p = 1$, $z^r - y^q = 1$, then by Cassels' result $q|x$ and $q|z$. Hence $q|x^p$, $q|z^r$, so q divides their difference $z^r - x^p = 2$. Thus $q = 2$ and so $z^r - y^2 = 1$. But this is impossible by the result of Lebesgue.

Contradiction and end of proof.

The theorem of Cassels implies that if $x^p - y^q = 1$, then x, y are of special form, namely $x = 1 + p^{q-1}r^q$, $y = -1 + q^{p-1}s^p$, and also $\frac{x^p-1}{x-1}$, $\frac{y^q+1}{y+1}$ are of special form.

Hyyrö explored this idea giving more restrictions which must be satisfied by x, y. But above all, he followed the lead of Wieferich and Inkeri to relate the problem to the congruences obtained by Wieferich for Fermat's last theorem. I explain now the very useful results of Inkeri, which continued the line of Hyyrö's research.

Let p be an odd prime and denote by $H(-p)$ the class number of the field $\mathbf{Q}(\sqrt{-p})$. Here is one of Inkeri's result:

Let $p > 3$, $p \equiv 3 \pmod 4$. If q is a prime, $q > 3$ and

$$\begin{cases} q \nmid H(-p) & \text{and} \\ p^{q-1} \not\equiv 1 & (\text{mod} q^2) \end{cases}$$

then $X^p - Y^q = 1$ has only trivial solution.

Inkeri gave a similar criterion when $q \equiv 3 \pmod 4$ and also a stronger criterion when both $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$, all of this complemented with further precisions in special cases.

The interest of these results for practical purpose is twofold. Firstly it is relatively easy to calculate the class number of an imaginary quadratic field and to check if a given prime divides it. Secondly, it has been observed that the so called Wieferich congruence (with base p) $p^{q-1} \equiv 1 \pmod{q^2}$ occurs very rarely. This and the similar criteria allow after computation, to decide that for many pairs of exponents (p, q) the corresponding equation has only trivial solution.

But even a small pair, like (5,7) cannot be dealt by this criterion. Indeed, $q = 7 \equiv 3$ (mod4) $H(-7) = 1$, 5 does not divide $H(-7)$, however $7^4 \equiv 1 \pmod{5^2}$.

To cover more cases, Inkeri considered also cyclotomic fields. Let h_p denote the class number of the cyclotonic field $\mathbf{Q}(\zeta_p)$ where ζ_p is a primitive pth root of 1.

Inkeri showed:

Assume that $X^p - Y^q = 1$ has non-trivial solution.

1) If p dies not divide h_q then $q^{p-1} \equiv 1 \pmod{p^2}$.

2) If q does not divide h_p, then $p^{q-1} \equiv 1 \pmod{q^2}$.

In particular, the equations $X^5 - Y^7 = \pm 1$ have only trivial solutions. Indeed $5 \nmid h_7$, $7 \nmid h_5$ but $5^6 \not\equiv 1 \pmod{7^2}$.

In a subsequent paper with Aaltonen, many more pairs of exponents were disposed of by this method, after computation of class numbers and Wieferich congruences.

These calculations have been pushed up by Mignotte. The last word is that (with a still unpublished lemma by W. Schwarz) if $\min\{p, q\} \leq 10640$, then $X^p - Y^q = 1$ has only trivial solution.

§5. Analytical Methods

At this moment, I like to stress what is obvious and has been implicit. Namely, equations of three different types have been under consideration

I. $a^U - b^V = 1$ where a, b are given distinct integers greater than 1.
II. $X^m - Y^n = 1$, where m, n are distinct integers greater than 1.
III. $X^U - Y^V = 1$.
So, it is appropriate to discuss in turn each of these equations

I. Equation $a^U - b^V = 1$

The main result is by LeVeque who showed that there exists at most one pair (u, v), with $u \geq 2$, $v \geq 2$ such that $a^u - b^v = 1$.

Cassels gave an algorithm which allows to find the hypothetical solution (if it exists). For $(a, b) \neq (3, 2)$ the algorithm has -up to now- failed to find any solution!

I do want to consider also the variant of this equation, already mentioned at the beginning of this lecture. Let $E = \{p_1, \ldots, p_s\}$ (with $s \geq 1$), be a finite set of primes. Let $k \geq 1$.

Thue proved that there exists an effectively computables constant $C > 0$ such that if

$$p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s} \ldots p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s} = k$$

(with integers $n_i, m_i \geq 0$), then $n_i, m_i < C$ (for all $i = 1, \ldots, s$).

The special cases when $k = 1$ or 2 had been proved earlier by Størmer with a very interesting method involving divigibility properties of terms of linear recurring sequences of order 2 (in other words, analogues to the sequences of Fibonacci numbers and of Lucas numbers).

II. Equation $X^m - Y^n = 1$

Siegel dealt with a more general equation. From his main result, it follows:

If $m, n \geq 2$ with $\max\{m, n\} \geq 3$, if a, b, k are given non-zero integers, then the equation $aX^m - bY^n = k$ has only finitely many solutions in integers.

The result of Siegel did not include any bound on the number or, a fortiori, on the size of the eventual solutions.

It was Baker's great achievement, which earned him a Fields Medal, to invent a new method leading to effective bounds on eventual solutions of many types of diophantine equations.

In the present case, Baker's estimates gave:

If $m, n \geq 2$, $k \geq 1$ and $x^m - y^n = k$, then $|x|, |y| < \exp\exp((3m)^{10} n^{10n^3} |k|^{n^2})$ (and a similar bound exchanging m with n). The bound depends on the strength of estimates of lower bounds for certain linear forms in logarithms. What should be retained is that, presently, the bound involves a double exponentiation and it is therefore very, very large.

It should also be mentioned that for the number of pairs (m, n) such that $X^m - Y^n = 1$ has non-trivial solution, Hyyrö found the following upper bound: $\exp(631 m^2 n^2)$.

Smaller than Baker's, but bigger than 0 -the hoped for bound!

A good support to the conjecture comes from the following density theorem, which I proved using a theorem of Schinzel & Tijdeman: Given a, b, k non-zero integers for each $N > 1$ consider the number $\alpha(N)$ of pairs (m, n) with $2 \leq m, n \leq N$ such that the equation $aX^m - bY^n = k$ has no solution in posiiive integers. Then $\frac{a(N)}{N^2}$ has limit (as N tends to ∞) which is equal to 1.

III. Equation $X^U - Y^V = 1$

It has arrived the moment to state the most significant result thus far obtained about Catalan's conjecture. It was proved in 1976 by Tigdeman, who used twice Baker's inequalities, in a novel clever way:

There exists a constant C such that if p, q are primes, if x, y are positive integers and $x^p - y^q = 1$, then $p, q < C$.

Coupled with the effective result of Baker for the equation (II), one may state:

There is a constant $T > 0$ such that if $x^p - y^q = 1$ with p, q primes $x, y \geq 1$, then $x, y, p, q < T$.

Langevin estimated that T may be taken to be $\exp\exp\exp\exp(730)$ –a number of size defying my imagination (just to think about it, I get a headache).

This theorem does not establish yet the truth of Catalan's conjecture. But it shows that the problem of Catalan is decidable in finitely many steps. Theoretically (if not in practice), it suffices to try, one after the other, all quadruples (x, y, p, q) and to check if $x^p - y^q = 1$.

The consideration of sharper forms of Baker's inequalities in close connection with Catalan's equation has led Mignotle in the one hand, and Glass (and his collaborators) into a race to lower the bound for the exponents. Now, it is already known that if $X^p - Y^q = 1$ has non-trivial solution, then $\max\{p, q\} \leq 10^{26}$.

So, we know that Catalan's conjecture is decidable, but it is not known when will it be decided.

§6. Conclusion

I whish to conclude with an imaginary dialogue. It is now almost ten o'clock in the evening, you heard my lecture with great patience and you will be returning home to face your conjoint. A dialogue between you (V=victim) and the conjoint (C) takes place:

C – You are returning late! Where have you been? I hope you were not in a bar, drinking...

V – Oh! no. I was at the École Normale Supèrieure, listening to a lecture. That place is not a bar.

C – A lecture? About what subject?

V – It concerned numbers which are powers and consecutive.

C – ?? (with a face which called for more explanation)

V – Yes, like the numbers 8 (which is a cube), 9 (which is a square) and have a difference 1.

C – I suppose there must be many like these numbers, because the lecture lasted a very long time.

V – Well this is what is amuzing. No other such numbers are known.

C - Then what did the lecturer talked about?

V - He filled his time with historical developments. Some partial results and many things one says, when one knows not many things.

C - Are you going to listen to the continuation (the conjoint asked, worried that one more evening of bliss would be sacrificed for Philosophy and Mathematics).

V - Oh! no. This Mr. Ribenboim knows nothing more about the problem —this is why he wrote a book.

C - Good! I love ignorance. I will have you home next Monday evening.

V - (with an air of importance and mystery). No. Next Monday I will return to hear how one can move pianos with real algebraic geometry[1]. And since I love the seminar, our happiness has to be limited to Tuesdays, Wednesdays, Thursdays, Fridays, Saturdays and Sundays.

Mondays are for MY happiness.

References

For proofs, remarks, details concerning Catalan's conjecture, you may consult my own book, which contains a fairly complete bibliography about the problem:

P. Ribenboim "Catalan's Conjecture" Academic Press, Boston, 1994.

Previously, I have published a survey on the problem:

P. Ribenboim "Consecutive powers" Expositiones Mathematicae, 2 (1984), 193- 221.

There are also several very recent preprints by A.W. Glass et al., by M. Mignotte and by W. Schwarz, which are concerned with developments in the line of K. Inkeri's criteria and the related calculations, some of whch still unpublished.

The results about prime numbers may be found for example in my own book:

P. Ribenboim "The Book of Prime Number Records" Springer-Verlag, New York (first editions 1987; second edition 1989, third edition 1995).

See also the French abridged version:

P. Ribenboim "Les Nombres Premiers: Mystères et Records", Presses Universitaires de France, Paris, 1994.

[1] M.F. Coste "La complexité du déménagement de pianos".