ON CATALAN'S CONJECTURE

Preda Mihailescu
(University of Paderborn)

Je ne fais pourtant de mal à personne
En suivant les chemins qui n'mènent pas à Rome
Mais les braves gens n'aiment pas que
L'on suive une autre route qu'eux.
George Brassens

$$x^u - y^v = 1 \ \Rightarrow \ (x, y; u, v) = (3, 2; 2, 3)$$

Proof of Catalan's conjecture

The intriguing pair $3^2 - 2^3 = 1 = 9 - 8$ had been shown in the 13th century to be the only pair of consecutive powers of 3 and 2; this was the Spanish-Jewish astronomer Ben Gershon. In 1844, Catalan conjectured they also are the only consecutive proper powers of integers (different from 0,1). He was right! Considering the equation $x^p - y^q = 1$ with prime exponents p, q the following landmarks had been achieved by 2000: the case $q = 2$ (V. Lebesgue) and $p = 2$ (Ko Chao); Cassels showed that the "I cases of Catalan" had no solutions. Using Baker's theory, Tijdeman showed that the equation might have at most a finite number of solutions and eventually upper bounds on the exponents were improved to $p < 7.10^{11}$ and $q < 7.10^{16}$ (when $p < q$). Lower bounds were gained by verifying algebraic conditions stemming mainly from Inkeri. The lower bound $p, q > 10^6$ was reached in 1999 and in 2000, using a new result, "the double Wieferich conditions", of the lecturer, $p, q > 3.10^8$ was proved. If $\mathbb{Q}(\zeta)$ is the p-th cyclotomic extension and $(x, y; p, q)$ is a solution to Catalan, let $\alpha = \frac{x-\zeta}{1-\zeta} \in \mathbb{Z}[\zeta]$; by Cassels' work, it is known that $N(\alpha) = \nu^q$ and thus the ideal $\mathfrak{a} = (\alpha, \nu) \subset \mathbb{Z}[\zeta]$ has $\mathfrak{a}^q = (\alpha)$. q-primary algebraic numbers of $\mathbb{Q}(\zeta)$ being essentially such ones which are q-adic q-th powers, I prove that for every $\theta \in \mathbb{F}_q[\mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})]$ which annihilates the q-primary cyclotomic units (mod q-th powers, certainly), $(x - \zeta)^\theta = \nu^q$ holds. The algebraic integer ν can then be found by power series expansion: in the reals not only the binomial series converges to ν, but its sum also commutes with Galois action. This strong properties, together with generous lower bounds for x, which were given by Hyyrö, help prove that ν can only be an algebraic integer if $\theta = 0 \mod q$. This again implies that all cyclotomic units should be q-primary, if a new solution to Catalan's equation should exist. However, if $p > q$ one easily shows that all cyclotomic units cannot be q-primary, a contradiction which confirms Catalan's intuition. QED

KUWAIT FOUNDATION LECTURE 30

28 APRIL 2003

PREDA MIHAILESCU

Je ne fais pourtant de mal à personne / En suivant les chemins qui
n'mènent pas à Rome / Mais les braves gens n'aiment pas que / L'on suive
une autre route qu'eux (G. Brassens)

$$x^u - y^v = 1 \Rightarrow (x, y; u, v) = (3, 2; 2, 3)$$

Proof of Catalan's conjecture

The intriguing pair $3^2 - 2^3 = 1 = 9 - 8$ had been shown in the 13th century
to be the only pair of consecutive powers of 3 and 2; this was the
spanish-jewish astronomer Ben Gershon. In 1844, Catalan conjectured
they also are the only consecutive proper powers of integers (diffe-
rent from 0,1). He was right! Considering the equation $x^p - y^q = 1$
with prime exponents p, q, the following landmarks had been achieved
by 2000: the case $q = 2$ - V. Lebesgue and $p = 2$ (Ko Chao); Cassels showed
that the "I cases of Catalan" had no solutions. Using Baker's theory,
Tijdeman showed that the equation might have at most a finite number
of solutions and eventually upper bounds on the exponents were im-
proved to $p < 7 \cdot 10^{11}$ and $q < 7 \cdot 10^{16}$ (when $p < q$). Lower bounds were
gained by verifying algebraic conditions, stemming mainly from Inkeri.
~~Using~~ The lower bound $p, q > 10^6$ was reached in 1999 and in 2000,
using a new result, "the double Wieferich condition", of the lecturer, $p, q > 3 \cdot 10^8$
was proved. If $\mathbb{Q}(\zeta)$ is the p-th cyclotomic extension and $(x, y; p, q)$ is a
solution to Catalan, let $\alpha = \frac{x - \zeta}{1 - \zeta} \in \mathbb{Z}[\zeta]$; by Cassels' work, it is known that
$N(\alpha) = v^q$ and thus the ideal $\mathfrak{a} = (\alpha, v) \subset \mathbb{Z}[\zeta]$ has: $\mathfrak{a}^q = (\alpha)$. q-primary
algebraic numbers of $\mathbb{Q}(\zeta)$ being essentially such ones which are q-adic
q-th powers, I prove that for every $\Theta \in \mathbb{F}_q[\mathrm{Gal}\ \mathbb{Q}(\zeta)^+/\mathbb{Q}]$, which annihi-
lates the q-primary cyclotomic units (mod q-th powers, certainly),
$(x - \zeta)^\Theta = v^q$ holds. The algebraic integer v can then be found by
power series expansion: in the reals not only the binomial series converges
to v, but its sum also commutes with galois action. This strong
propertie, together with generous lower bounds for x, which were given
by Hyyrö, help prove that v can only be an algebraic integer if
$\Theta = 0 \mod q$. This again implies that all cyclotomic units should
be q-primary, if a new solution to Catalan's equation should exist.
However, if $p > q$ one easily shows that all cyclotomic units cannot be
q-primary, a contradiction which confirms Catalan's intuition. QED