Størmer's solution of the unit equation $x - y = 1$

Martin Klazar

August 25, 2010

S-numbers, for a given finite set of primes $S = \{p_1, p_2, \dots, p_r\}$, are the numbers $p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, a_i \in \mathbb{N}_0 = \{0, 1, \dots\}$, built only from the primes in S. For example, the $\{2,3\}$-numbers smaller than 100 are

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, 48, 54, 64, 72, 81, 96.$$

Gaps in this sequence apparently have tendency to grow. How would you prove that for any finite S and any $c \in \mathbb{N} = \{1, 2, \dots\}$ only finitely many pairs of S-numbers are c apart? That is, the equation

$$x - y = c$$

has only finitely many solutions x, y in S-numbers. For example, for $S = \{2,3\}$ and $c = 1$ the only solutions are $2^1 - 1 = 1$, $3^1 - 2^1 = 1$, $2^2 - 3^1 = 1$ and $3^2 - 2^3 = 1$. How do we know that? Why there could not be some other, perhaps gigantic, exponents such that $2^a 3^b - 2^c 3^d = 1$? Shortly we will see why.

Finiteness of solutions to $x - y = c$ in S-numbers follows from the deep theorem on Diophantine equations proved by A. Thue in 1908 [5], which in particular says that any equation

$$ax^3 - by^3 = c, \ \ a, b, c \in \mathbb{N},$$

has only finitely many integral solutions $x, y \in \mathbb{Z}$. Writing the exponents in $p_i^{a_i}$ as $a_i = 3b_i + \varepsilon_i$ with $\varepsilon_i = 0, 1, 2$ we see that all solutions to $x - y = c$ in S-numbers are contained among integral solutions to 9^r Thue equations $ax^3 - by^3 = c$ with a, b of the form $p_1^{\varepsilon_1} \dots p_r^{\varepsilon_r}$, and so there are only finitely many of them. This was observed by G. Pólya [2].

But already one decade before Thue's epoch-making theorem his compatriot Carl Størmer (1874–1957), Norwegian mathematician and physicist famous for investigations, observations and theory of aurora Borealis, could prove ([4]) finiteness of solutions to $x - y = c$ in S-numbers for $c = 1$ and 2. Moreover, unlike the argument using Thue's theorem, Størmer's method is completely effective and gives an algorithm determining for any S all solutions. How Størmer did it without Thue? He used the *Pell equation*

$$x^2 - dy^2 = 1$$

where $d \in \mathbb{N}$ and is not a square. Crazy idea, it seems—already in 1770 J. L. Lagrange proved that each such equation has infinitely many integral solutions, not good for obtaining finiteness results! However, simple algebraic structure of this infinite solution set enables one to prove for Pell equations a finiteness result, discovered by Størmer (Theorem 2 below).

The purpose of this expository note is to review Størmer's argument, a beautiful application of the theory of Pell equation. We follow the book of Ribenboim [3, chapter C.9] which discusses generalizations of Størmer's result. For further information on the unit equation see the book of Bombieri and Gubler [1].

***

Theorem 1 (Størmer, 1897) *Let $S = \{p_1, p_2, \dots, p_r\}$ be r distinct prime numbers. Each of the two equations*

$$x - y = 1 \quad \textit{and} \quad x - y = 2$$

has at most 3^r solutions in S-numbers x, y.

For $d, n \in \mathbb{N}$ we say that n is a *d-number* if every prime factor of n divides d, that is, n is an S-number for S the set of prime divisors of d. The *fundamental solution* of a Pell equation is the positive solution with the smallest x-coordinate (or, equivalently, y-coordinate). Note that if $d = e^2$ is a square then $x^2 - dy^2 = (x - ey)(x + ey) = 1$ has just the trivial integral solution $\pm 1, 0$.

Theorem 2 (Størmer, 1897) *Each equation*

$$x^2 - dy^2 = 1, \ d \in \mathbb{N},$$

has at most one solution $x, y \in \mathbb{N}$ where y is a d-number. In fact, if such solution exists it equals the fundamental solution of the given Pell equation.

Let us see how Theorem 1 follows from Theorem 2. If y and $y + 1$ are both S-numbers, then $2 \in S$ and $4y(y + 1) = (2y + 1)^2 - 1$ is an S-number. Similarly, if y and $y + 2$ are both S-numbers, then $y(y + 2) = (y + 1)^2 - 1$ is an S-number. It suffices to show that at most 3^r S-numbers have form $a^2 - 1$. Let $a^2 - 1 = p_1^{a_1} \dots p_r^{a_r}$ where $a \in \mathbb{N}$ and $a_i \in \mathbb{N}_0$. We define $b_i \in \mathbb{N}_0$ by $b_i = a_i - 1$ if a_i is odd, $b_i = 0$ if $a_i = 0, 2$ and $b_i = a_i - 2$ if $a_i \geq 4$ and is even, and we set $d = p_1^{a_1 - b_1} \dots p_r^{a_r - b_r}$ and $b = p_1^{b_1/2} \dots p_r^{b_r/2}$. Then

$$a^2 - db^2 = 1 \ \text{ and } b \text{ is a } d\text{-number}.$$

We have at most 3^r choices for d because $d = p_1^{\varepsilon_1} \dots p_r^{\varepsilon_r}$ with $\varepsilon_i = 0, 1, 2$ and get at most 3^r equations $x^2 - dy^2 = 1$. Each of them has by Theorem 2 at most one positive solution a, b where b is a d-number. Thus only at most 3^r S-numbers are by one less than a square, which proves Theorem 1.

We prove Theorem 2. From the theory of Pell equation we will not need Lagrange's theorem but only the following easier result whose proof we omit.

Proposition 3 *Suppose that $d \in \mathbb{N}$ and $x^2 - dy^2 = 1$ has at least one positive integral solution. Then d is not a square and all positive solutions form an infinite sequence of pairs $a_n, b_n \in \mathbb{N}$, $n = 1, 2, \ldots$, given by*

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n$$

where $a_1, b_1 \in \mathbb{N}$ is the fundamental (i.e., smallest positive) solution.

Proof of Theorem 2. Suppose that $x^2 - dy^2 = 1$ has a solution $a, b \in \mathbb{N}$ where b is a d-number. Since by Proposition 3 all positive solutions are of the form

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n,\ n = 1, 2, \ldots,$$

where $a_1, b_1 \in \mathbb{N}$ is the fundamental solution, $a = a_m, b = b_m$ for some $m \in \mathbb{N}$. We show that $m = 1$.

First note that $a_1 > 1$ and $(a_1, d) = 1$ since $a_n^2 - db_n^2 = 1$. For $n = kl$, $k, l \in \mathbb{N}$, we get

$$a_{kl} + b_{kl}\sqrt{d} = (a_k + b_k\sqrt{d})^l \quad \text{and} \quad b_{kl} = \binom{l}{1}a_k^{l-1}b_k + \binom{l}{3}a_k^{l-3}b_k^3 d + \ldots$$

It follows that b_k divides b_{kl} and in particular for every $l \in \mathbb{N}$ we have

$$b_l = b_1 c_l,\ c_l \in \mathbb{N}.$$

Setting $k = 1$ and cancelling b_1 in the last but one displayed equality we get the identity

$$c_l = \binom{l}{1}a_1^{l-1} + \binom{l}{3}a_1^{l-3}b_1^2 d + \binom{l}{5}a_1^{l-5}b_1^4 d^2 + \ldots$$

Suppose that $m > 1$ and consider the prime divisors p of the index m of the d-number b_m; we show that there is none. If $p = 2$ then c_2 divides b_m and thus c_2 is a d-number and, by the identity, $c_2 = 2a_1$. Since a_1 is coprime with d, we see that $c_2 = 2^r$ and $a_1 = 2^{r-1}$. If $r \geq 2$ then 2 divides both d and a_1, which is impossible. Thus $r = 1$ and $a_1 = 1$, which is impossible either. If $p \geq 5$ then again c_p divides b_m, is a d-number and each prime factor of c_p divides pa_1^{p-1}. From $(a_1, d) = 1$ it follows that c_p has the only prime factor p and $c_p = p^r$, $r \in \mathbb{N}$. Since $p > 3$, the second summand in the identity (with $l = p$) is divisible by p^2 (as p divides $\binom{p}{3}$ and d) and the following ones are clearly divisible by p^2 as well. Thus if $r \geq 2$ then p^2 divides also the first summand pa_1^{p-1} and p divides a_1 and d, which is impossible. Hence $r = 1$. But then $p = c_p = pa_1^{p-1} + \ldots$ which is impossible either as $a_1 > 1$.

It remains the possibility that $p = 3$ and $m = 3^r$ with $r \in \mathbb{N}$. Then c_3 divides b_m and is a d-number. By the identity,

$$c_3 = 3a_1^2 + b_1^2 d = 4a_1^2 - 1 = (2a_1 - 1)(2a_1 + 1).$$

Again, by $(a_1, d) = 1$ the only prime factor of c_3 may be 3 and $c_3 = 3^s$ with $s \in \mathbb{N}$. Thus $2a_1 - 1$ and $2a_1 + 1$ are powers of 3 differing by 2, which are only

1 and 3, and $a_1 = 1$. But this is impossible as $a_1 > 1$. The assumption $m > 1$ leads to contradiction in all cases and we see that $m = 1$. □

To close let us find all solutions to $x - y = 1$ and $x - y = 2$ in $\{2, 3\}$-numbers. The $9 = 3^2$ corresponding equations $x^2 - dy^2 = 1$ have $d = 1, 2, 3, 4, 6, 9, 12, 18, 36$. Squares $d = 1, 4, 9, 36$ give no solution and in the remaining five cases we have fundamental solutions $(3, 2)$ for $d = 2$, $(2, 1)$ for $d = 3$, $(5, 2)$ for $d = 6$, $(7, 2)$ for $d = 12$ and $(17, 4)$ for $d = 18$. In each of them the y-component is d-number and we get that $x^2 - 1$ is $\{2, 3\}$-number iff $x = 2, 3, 5, 7, 17$. This gives the solutions $3 - 1 = 2$, $4 - 2 = 2$, $6 - 4 = 2$, $8 - 6 = 2$, $18 - 16 = 2$ and (for odd x) $2 - 1 = 1$, $3 - 2 = 1$, $4 - 3 = 1$, $9 - 8 = 1$.

References

[1] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.

[2] G. Pólya, Zur arithmetischen Untersuchungen der Polynome, *Math. Zeit.* **1** (1918), 143–148.

[3] P. Ribenboim, *Catalan's conjecture. Are 8 and 9 the Only Consecutive Powers?*, Academic Press, 1994.

[4] C. Størmer, Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = \pm 1$ et leurs applications, *Christiania Vidensk. Selskab Skrifter*, (I) (1897), No. 2, 48 pp.

[5] A. Thue, Om en generel i store hele tal uløsbar ligning, *Kra. Vidensk. Selsk. Skrifter. I. Mat. Nat. Kl. No. 7. Kra. 1908.* (1908), 13 pp.