ma
the
ma
tisch

cen
trum

AFDELING ZUIVERE WISKUNDE ZN 75/77 MEI
(DEPARTMENT OF PURE MATHEMATICS)

C.L. STEWART

A NOTE ON THE FERMAT EQUATION

Preprint

amsterdam 1977

stichting
mathematisch
centrum

AFDELING ZUIVERE WISKUNDE ZN 75/77 MEI
(DEPARTMENT OF PURE MATHEMATICS)

C.L. STEWART

A NOTE ON THE FERMAT EQUATION

Preprint

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O).

AMS(MOS) subject classification scheme (1970): 10B15, 10F35

A note on the Fermat equation *)

by

C.L. Stewart

ABSTRACT

Let x,y,z and n denote positive integers with $x < y < z$ and $(x,y,z) = 1$. We prove that if y-x is small in comparison to z there are at most finitely many positive integers n for which the Fermat equation,

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

admits solutions.

KEY WORDS & PHRASES: *Diophantine equations, Fermat, linear forms in logarithms.*

---

*) This report will be published in Mathematika.

Let x,y,z and n denote positive integers with $x < y < z$ and $(x,y,z) = 1$. The purpose of this note is to prove two theorems, the first of which is

THEOREM 1. *If* $y - x < C_0\, z^{1-(1/\sqrt{n})}$ *for some positive number* C_0, *and if*

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

then n *is less than* C, *a number which is effectively computable in terms of* C_0.

Thus if $y - x$ is small in comparison to z there are at most finitely many positive integers n for which the equation (1) admits solutions. We remark that the function $1/\sqrt{n}$ in the exponent of z above was chosen for neatness; it may be replaced by a function which tends to 0 more rapidly with n. The proof of Theorem 1 depends upon a straightforward application of a lower bound, due to Baker [3], for certain linear forms in logarithms. It yields a value for C of $S^2(4 \log S)^6$ where $S = 32^{401} + \log C_0'$ and $C_0' = \max\{e, C_0\}$. Sharper numerical bounds can certainly be obtained for C, however, by reworking the argument of [3] for the case of the particular linear form which arises in the proof of Theorem 1. We note for comparison that Wagstaff [7] has shown that equation (1) has no solutions for n in the range $3 \le n \le 10^5$.

That (1) has only a finite number of solutions x, y and z with $y - x < C_0$ for n a fixed odd prime was proved by Everett [5] by means of the Thue-Siegel-Roth theorem. Recently Inkeri (see Theorem 4 of [6]) generalized the work of Everett. He used estimates due to Baker [2] for the size of solutions of the hyperelliptic equation to show that if $n \ge 3$, (1) holds and either $y - x$ or $z - y$ is less than C_0, then x, y and z are less than a number which is effectively computable in terms of n and C_0 only. It follows from Theorem 1 that if $y - x < C_0$ then n is bounded in terms of C_0. Applying the result of Inkeri we see that in this case x,y and z are also bounded in terms of C_0. Therefore we have

<u>THEOREM</u> 2. *If* $n \geq 3$, $y - x$ *is less than a positive number* C_0 *and*

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

then x, y, z *and* n *are all less than* C, *a number which is effectively computable in terms of* C_0.

Thus, in principle, all the solutions of (1) such that x and y differ by a given number may be explicitly determined. The bound for C in Theorem 2 depends upon the estimates obtained in [2], however, and is so large that a direct computation of the solution set for a given C_0 does not seem feasible. We remark, see below, that Theorem 2 remains valid if the condition $y - x < C_0$ is replaced by $2 < z - y < C_0$. If $z - y = 1$, when the problem is related to Abel's conjecture (see §3 of [6]), or if n is even and $z - y = 2$, then the argument given here does not apply.

Before beginning the proof of Theorem 1 I should like to thank M. Mauclaire for suggesting to me, at the Journées Arithmétique in Caen, that the methods of Baker might be applicable in this context.

Since $(x,y,z) = 1$ we may deduce from [4] or Lemma 1 of [1] that if (1) holds then for some positive integers a and b,

$$(2) \qquad z - x = 2^{\varepsilon_1} d_1^{-1} a^n \quad \text{and} \quad z - y = 2^{\varepsilon_2} d_2^{-1} b^n,$$

where ε_1, similarly ε_2, is either 0 or 1 and where d_1 and d_2 are positive divisors of n. (Both ε_1 and ε_2 are zero if n is odd.) From (2) we see that if $z - y > 2$ then it is necessarily also $\geq 2^n/n$ and so if $2 < z - y < C_0$ then n is bounded in terms of C_0. Therefore, by [6], Theorem 2 holds with this condition in place of $y - x < C_0$. Subtracting $z - y$ from $z - x$ gives

$$(3) \qquad 2^{\varepsilon_1} d_1^{-1} a^n - 2^{\varepsilon_2} d_2^{-1} b^n = y - x.$$

We shall now assume that the conditions of Theorem 1 apply, so that (1) holds and

$$(4) \qquad y - x < C_0\, z^{1-(1/\sqrt{n})}$$

and we shall prove that this implies n is bounded in terms of C_0. Further we shall assume that $C_0 \geq e$ and that $n > 4^6 (\log C_0)^2$; clearly this involves no loss of generality.

We first observe that $z - x > 2$. For if $z - x = 2$ then

$$x^n + (x+1)^n = (x+2)^n,$$

hence certainly $2 < (1+2/x)^n$; and since $\log(1+r) < r$ for $r > 0$, we have $\log 2 < 2n/x$ and thus $x < 3n$. But for $n > 6$ there exist, by Theorems 1 and 5 of [4], primes p_1, p_2 and p_3 congruent to 1 (mod n) which divide x, $x + 1$ and $x + 2$ respectively and therefore $x > 3n$ giving a contradiction. Thus $z - x > 2$ and as a consequence $a \geq 2$. Furthermore since $x < y < z$ we have $2x^n < z^n$ and thus $x < 2^{-1/n} z$ whence, since $n > 4^6$, $z - x > (1-2^{-1/n})\, z > z/2n$. From (4) we deduce that

$$y - x < 2n\, C_0 (z-x)^{1-(1/\sqrt{n})}$$

and since $n - (\log n / \log a) > \frac{1}{2}n$ for $n > 8$, we have from (2) that,

$$(5) \qquad (y-x)/(z-x) < 2n\, C_0\, a^{-\frac{1}{2}\sqrt{n}}.$$

Since $a \geq 2$ and $n > 4^6 (\log C_0)^2$ we find that $(y-x)/(z-x) < \frac{1}{2}$. Further, from (2) and (3) we have

$$(6) \qquad 1 - (y-x)/(z-x) = 2^{\varepsilon_2 - \varepsilon_1} (d_1/d_2)(b/a)^n.$$

Therefore using the inequality $|\log(1-r)| < 2r$, which is valid for $0 < r < \frac{1}{2}$, with $r = (y-x)/(z-x)$ we conclude from (5) and (6) that

$$|\log s + n \log(b/a)| < 4n\, C_0 a^{-\frac{1}{2}\sqrt{n}},$$

where $s = 2^{\varepsilon_2 - \varepsilon_1} d_1/d_2$. Denoting the left hand side of the above inequality by T and taking logarithm yields

(7) $$\log T < \log 4n\, C_0 - \tfrac{1}{2}\sqrt{n} \log a.$$

Recently Baker [3] proved that if b_1 and b_2 are integers with absolute values at most B (≥4), if a_1 and a_2 are rational numbers the numerators and denominators of which are in absolute value at most A_1 (≥4) and A_2 (≥4) respectively and if $b_1 \log a_1 \neq -b_2 \log a_2$ then

(8) $$\log|b_1 \log a_1 + b_2 \log a_2| > - C_1 \log B \log A_1 \log A_2 \operatorname{loglog} A_2,$$

for $C_1 = 32^{400}$. Since $y - x > 0$ we have $\log s \neq - n \log(b/a)$ and thus we may use (8) to obtain a lower bound for log T. Putting $a_1 = b/a$, $a_2 = s$, $b_1 = n$ and $b_2 = 1$ we conclude from (8), since $B = n$, $A_1 \le \max\{4,a,b\}$ and $A_2 \le 2n$, that

$$\log T > - 2C_1 (\log n)^3 \log(\max\{a,b\}).$$

By (6) we have $(a/b)^n > d_1/2d_2 \ge 1/2n \ge 2^{-n}$ from which it follows that $2a > b$.
Therefore

(9) $$\log T > -4C_1 (\log n)^3 \log a.$$

Comparing (7) and (9) we find

$$\sqrt{n} \log a < 8C_1 (\log n)^3 \log a + 2 \log 4nC_0$$

and thus, recall that $C_1 = 32^{400}$ and $n > 4^6 (\log C_0)^2$,

$$\sqrt{n} (\log n)^{-3} < 32^{401} + \log C_0.$$

On setting the right hand side of the above inequality equal to S we conclude that

$$n < S^2(4 \log S)^6$$

as required. This completes the proof of Theorem 1.
Theorem 2 follows as a consequence of Theorem 1.

REFERENCES

[1] Artin, E., *The orders of the linear groups*, Comm. Pure Appl. Math. 8 (1955), pp. 355-366.

[2] Baker, A., *Bounds for the solutions of the hyperelliptic equation*, Proc. Camb. Phil. Soc. 65 (1969), pp. 439-444.

[3] Baker, A., *The theory of linear forms in logarithms*, Transcendence Theory: Advances and Applications (Academic Press, London and New York, 1977).

[4] Birkhoff, G.D. & H.S. Vandiver, *On the integral divisors of* a^n-b^n, Ann. of Math. (2), 5 (1904), pp. 173-180.

[5] Everett, C.J., *Fermat's conjecture, Roth's theorem, Pythagorean triangles and Pell's equation*, Duke Math. J. 40 (1973), pp. 801-804.

[6] Inkeri, K., *A note on Fermat's conjecture*, Acta Arith. 29 (1976), pp. 251-256.

[7] Wagstaff, S.S., *Fermat's last theorem is true for any exponent less than 100,000*, Notices A.M.S. 23 (1976), p. A-53.