Putting $k = 1, 0, -1$ in the expression for $S_k(n)$ above, we have the following particular cases:

$$S_1(n) = np(n) = \sum_{r=1}^{n} p(n-r)\sigma(r),$$

$$S_0(n) = \sum_{r=1}^{n} p(n-r)d(r),$$

$$S_{-1}(n) = \sum_{r=1}^{n} \frac{p(n-r)\sigma(r)}{r}.$$

The formula for $S_0(n)$ has appeared on page 218 in [1].

Now let $S_k^*(n)$ denote the sum of all kth powers of all the summands in all the partitions of n into primes. Let $\sigma_k^*(n) = \sum_{p_i|n} p_i^k$, where the p_i are primes and k is any integer.

THEOREM 2. $S_k^*(n) = \sum_{r=1}^{n} q(n-r)\sigma_k^*(r)$, *where $q(n)$ is the number of partitions of n into primes.*

The proof is similar to that of Theorem 1. Putting $k = 1$, we have

$$S_1^*(n) = nq(n) = \sum_{r=1}^{n} q(n-r)\sigma_1^*(r),$$

where $\sigma_1^*(n)$ denotes the sum of all the prime divisors of n.

Finally we note that in Theorem 2, the primes may be replaced by any subset of the natural numbers.

Reference

[1] D. H. Lehmer, *Calculating moments of partitions*, Proceedings of the Second Manitoba Conference on Numerical Mathematics, University Manitoba, Winnipeg, Man. (1972), pp. 217–220.

DEPARTMENT OF MATHEMATICS
KANSAS STATE UNIVERSITY
Manhattan, Kansas, U.S.A.

Received on 14. 9. 1976
and in revised form on 15. 10. 1977 (877)

ACTA ARITHMETICA
XXXVI (1980)

Some remarks on Fermat's conjecture

by

K. INKERI (Turku) and A. J. VAN DER POORTEN (New South Wales)

In a recent note [7] (Theorem 1 cf. also [5]) it was shown: if p is a fixed odd prime, then there exist at most finitely many triples of integers x, y, z which satisfy

$$(1) \qquad x^p + y^p = z^p, \quad (x, y, z) = 1, \quad y > x > 0,$$

and $y - x = k$, where k is a fixed natural number.

Refinements of the effective methods of Baker now allow us to improve the above result. Namely, we can prove:

THEOREM 1. *All solutions in positive integers x, z, and odd primes p, of the equation*

$$(2) \qquad x^p + (x+k)^p = z^p, \quad (x, k) = 1$$

are bounded by effectively computable constants depending only on the positive integer k.

The new feature is that we now can bound the prime p in terms of k; indeed, as we shall see, in terms of the prime factors of k. We shall give explicit bounds for p and establish some improvements of the above theorem.

1. Bounding the exponent. The following lemma is convenient for bounding p in (2).

LEMMA A. *Let a, b, q be integers and let p be an odd prime. If $b > a > 0$, $p > |q|$ then there is an effectively computable absolute constant $C > 0$ such that*

(i) $$|1 - p^q(a/b)^p| > b^{-C(\log p)^3},$$

(ii) *for each prime $l \neq p$*

$$|1 - p^q(a/b)^p|_l > b^{-C(\log p)^3}.$$

The first result is implied by Theorem 2 of van der Poorten and Loxton [9] (or by Theorem 2 of Baker [4]) on noting that for $u \geq \frac{1}{2}$ one has $|\log u| \leq 2|1-u|$. The second, l-adic, result is a special case of Theorem 2 of van der Poorten [10]. The cited references give C explicitly, but make it very large. In this special case, recent calculations of the second author show that the reader may suppose C to be much smaller (certainly, $C = 2^{20}$ would do in Lemma A).

By Abel's well-known formulae (cf. [6], p. 7) we may write as in [7], that (1) implies

I. $z-x = b^p$, $z-y = a^p$ if $p\nmid xy$,

II. $z-x = p^{-1}b^p$, $z-y = a^p$ if $p|y$,

III. $z-x = b^p$, $z-y = p^{p-1}a^p$ if $p|x$

for positive integers a, b (and in case II, $p|b$). Since k is positive we have $b > a$.

Let $l_1, \ldots, l_m$ be distinct positive primes (less than p). We shall suppose that

$$k = k_0 l_1^{w_1} \ldots l_m^{w_m} \tag{3}$$

for non-negative integers $w_1, \ldots, w_m$ and some positive integer k_0, and shall proceed to show that, given (2), p is bounded by a positive constant depending only on k_0 and $l_1, \ldots, l_m$.

In case III we have (recalling that $k = y-x$)

$$k/b^p = 1 - p^{p-1}(a/b)^p.$$

If $l_i|k$ then $l_i\nmid b$ since $(x, k) = 1$. Thus, on applying Lemma A(ii), we have

$$l_i^{w_i} < b^{Cl_i(\log p)^3}, \quad 1 \leqslant i \leqslant m. \tag{4}$$

Now applying Lemma A(i) we obtain

$$k/b^p = |1-p^{p-1}(a/b)^p| > b^{-C(\log p^3)},$$

whence

$$k_0 > b^{p-C(1+l_1+\ldots+l_m)(\log p)^3} = (z-x)^{1-C(1+l_1+\ldots+l_m)(\log p)^3/p}. \tag{5}$$

Since $z-x \geqslant 2^p$, this bounds p as asserted in this case.

In case II we have

$$pk/b^p = 1 - p(a/b)^p$$

and, again, Lemma A(ii) implies the bounds (4). Similarly, after applying Lemma A(i) we obtain

$$pk_0 > b^{p-C(1+l_1+\ldots+l_m)(\log p)^3} = \big(p(z-x)\big)^{1-C(1+l_1+\ldots+l_m)(\log p)^3/p}. \tag{6}$$

Since $z-x = p^{-1}b^p \geqslant p^{p-1}$, this bounds p as asserted in this case.

Finally, in case I we have

$$k/b^p = 1-(a/b)^p,$$

and since $l_i\nmid p$, an elementary estimate implies already that

$$\prod_{i=1}^{m} l_i^{w_i} \leqslant b-a.$$

Here we have, of course, used $l_i < p$ $(1 \leqslant i \leqslant m)$ so that, certainly, $p\nmid(l_i-1)l_i$. On the other hand

$$k = b^p - a^p > b^{p-1},$$

so

$$k_0 > b^{p-2} = (z-x)^{1-2/p}, \tag{7}$$

which bounds p in this case.

In fact we have shown:

THEOREM 2. *Let $l_1, \ldots, l_m$ be distinct positive primes less than p such that $l_i^{w_i}|(y-x)$ $(1 \leqslant i \leqslant m)$. Then* (1) *implies that*

$$(y-x)\Big/\prod_{i=1}^{m} l_i^{w_i} > (z-x)^{1-L(\log p)^3/(p-1)} \tag{8}$$

where $L = C(1+l_1+\ldots+l_m)$, (and $L = C$ if $m = 0$), and C is the constant of Lemma A.

Proof. The bound (6) obtained in case II is the weakest bound for k_0; in that case we have used $p^{-1} \geqslant (z-x)^{-1/(p-1)}$. It is plain that (5) and (7) imply (8).

2. Further results. Once p is supposed bounded in (2) then Theorem 4 of [7] completes the proof of our Theorem 1; here we invoke a deep result of Baker [1] on the solutions of the so-called hyperelliptic equation.

Other than for our appeal to the deep results which imply our Lemma A, the argument of Section 1 above uses only trivial facts concerning eventual solutions of (1). Of course we know a great deal more. For example we readily prove:

THEOREM 3. *If x, z satisfy* (1) *then*

$$z-x > p^{2p}. \tag{9}$$

Moreover, if p, x, y, z with $p\nmid xyz$ are solutions of (1) *such that at least one of the differences $y-x$, $z-x$, $z-y$ is less than $(p^{2-\varepsilon}M)^p$, where ε, M are positive constants, then all of p, x, y, z are bounded by effectively computable constants depending only on ε and M.*

Proof. In the case $p\nmid xyz$ (the "first case of Fermat's Theorem") each of the integers a, b and c (where $c^p = x+y$) has at least one prime factor $\equiv 1 (\mathrm{mod}\, 2p^2)$ (cf. [6], p. 50, Satz XII). Now (9) is immediate in this case, by I. Moreover, $p^{2p} < a^p = z-y \leqslant (p^{2-\varepsilon}M)^p$ and so $p^\varepsilon < M$ whence p is bounded by $M^{1/\varepsilon}$ if indeed $z-y < (p^{2-\varepsilon}M)^p$. Similarly $p^{2p} < b^p$, so we have (9) in this case, and Theorem 2 implies that p is bounded in terms of M and ε if $y-x < (p^{2-\varepsilon}M)^p$. However, in this case, we can obtain a bound on p directly: namely, by $b > p^2$ we have $p^{2(p-1)} < b^{p-1} < (p^{2-\varepsilon}M)^p$, which yields $p^{\varepsilon-2/p} < M$, whence $p^{\varepsilon/2} < M$ if $p > 4/\varepsilon$.

We return to the case $z-y<(p^{2-\varepsilon}M)^p$, when a and p are bounded. By Abel's formula $2y=c^p+b^p-a^p$ (and $b|y$), we have $a^p\equiv(c-b)^p$ (mod b). But $0<c-b<a$ (cf. [6], p. 7), so plainly $a^p>b$ and b is bounded in terms of M and ε. It follows that x, y, z are bounded appropriately, confirming the second part of theorem (cf. [7], p. 252).

Generally $x^p\equiv x$, $y^p\equiv y$, $z^p\equiv z$ (mod p^3) (see [6], p. 5). Hence if $p|x$ (case III above) we have $z-x>z-y=p^{3p-1}a_0^p$ (a_0 an integer), and if $p|y$ (case II above) then $z-x>p^{3p-1}b_0^p$. Finally if $p|z$ (included in case I above), then $c^p=x+y=p^{3p-1}c_0^p$. But $2b>a+b>c$ so $z-x=b^p>(\frac{1}{2}p^{3-1/p})^p>p^{2p}$ as required, completing the proof of (9).

Using (9) we can appropriately restate the inequality (8), and hence Theorem 1 (the notation being that of Theorem 2):

THEOREM 4. *The equation* (1) *has no solutions with*

$$(y-x)/\prod_{i=1}^{m} l_i^{w_i}<p^{2p(1-L(\log p)^3/(p-1))}.$$

3. Remarks. For $p|yz$ the case $z-y=1$ (and the so-called Abel's conjecture) is awaiting solution (see [7], p. 255). The results and ideas given by van der Poorten, Schinzel, Shorey and Tijdeman in the papers [11], [12], [13], [15] make one optimistic about the capabilities of the methods of Baker for coping with this problem.

It has come recently to our attention that Stewart [14] has independently established the following results, which partly overlap with our Theorems 1, 2 and 3: Let x, y, z, p be positive integers satisfying (1). If $y-x<C_0(z-x)^{1-(1/\sqrt{p})}$ for some positive number C_0, then p is less than C, a number which is effectively computable in terms of C_0. If $p\geqslant 3$, $y-x$ is less than a positive number C_0, then x, y, z and p fulfill all a similar condition.

References

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Camb. Phil. Soc. 65 (1969), pp. 439–444.
[2] — *A sharpening of the bounds for linear forms in logarithms I*, Acta Arith. 21 (1972), pp. 117–129.
[3] A. Baker and D. W. Masser (eds.), *Transcendence theory — advances and applications*, Academic Press, London and New York 1977.
[4] A. Baker, *The theory of linear forms in logarithms*, in: *Transcendence theory — advances and applications*, op. cit. pp. 1–27.
[5] C. J. Everett, *Fermat's conjecture, Roth's theorem, Pythagorean triangles, and Pell's equation*, Duke Math. J. 40 (1973), pp. 801–804.
[6] K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. AI, No. 33 (1946), pp. 1–60.
[7] — *A note on Fermat's conjecture*, Acta Arith. 29 (1976), pp. 251–256.

[8] K. Inkeri and S. Hyyrö, *Über die Anzahl der Lösungen einiger diophantischer Gleichungen*, Ann. Univ. Turku, Ser. AI, No. 78 (1964), pp. 1–10.
[9] A. J. van der Poorten and J. H. Loxton, *Computing the effectively computable bound in Baker's inequality for linear forms in logarithms*, and *Multiplicative relations in number fields*, Bull. Austral. Math. Soc. 15 (1976), pp. 33–57, and 16 (1977), pp. 83–98.
[10] A. J. van der Poorten, *Linear forms in logarithms in the* p*-adic case*, in: *Transcendence theory — advances and applications*, op. cit. pp. 29–57.
[11] A. Schinzel and R. Tijdeman, *On the equation* $y^m=P(x)$, Acta Arith. 31 (1976), pp. 199–204.
[12] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, *Applications of the Gelfond–Baker method to diophantine equations*, in: *Transcendence theory — advances and applications*, op. cit. pp. 59–77.
[13] H. M. Stark, *Effective estimates of solutions of some diophantine equations*, Acta Arith. 24 (1973), pp. 251–259.
[14] C. L. Stewart, *A note on the Fermat's equation*, Mathematika 24 (1977), pp. 130–132.
[15] R. Tijdeman, *On the equation of Catalan*, Acta Arith. 29 (1976), pp. 197–209

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU
Turku, Finland

SCHOOL OF MATHEMATICS
UNIVERSITY OF NEW SOUTH WALES
Kensington, Australia

Received on 14. 2. 1977
and in revised form on 4. 7. 1977 (915)