[4] M. Bhaskaran, *Corrections to the paper "Sums of m^{th} powers"*, ibid. 22 (1971), pp. 370–371.

[5] L. E. Dickson, *Linear Groups with an Exposition of the Galois Theory*, Dover Publications, New York, N. Y., 1958.

[6] J. W. Cassels, *On the equation $a^x - b^y = 1$*, Amer. J. Math. 75 (1953), pp. 159–162.

[7] H. Edgar, *The exponential diophantine equation $1+a+a^2+\ldots+a^{x-1} = p^y$*, Amer. Math. Monthly 81 (1974), pp. 758–759.

[8] G. H. Hardy and E. M. Wright, *The Theory of Numbers*, Oxford University Press, Oxford 1946.

[9] K. Inkeri, *On the diophantine equation $a(x^n-1)/(x-1) = y^m$*, Acta Arith. 21 (1972), pp. 299–311.

[10] N. Jacobson, *Structure of Rings*, Amer. Math. Soc. Colloq. Publ. 37, Providence, R. I., 1956.

[11] J. Joly, *Sommes de puissances d-iemes dans un anneaux commutatif*, Acta Arith. 17 (1970), pp. 37–114.

[12] W. LeVeque, *On the equation $a^x - b^y = 1$*, Amer. J. Math. 74 (1952), pp. 325–331.

[13] G. Polya, *Zur arithmetischen Untersuchung der Polynome*, Math. Zeitschr. 1 (1918), pp. 143–148.

[14] A. Schinzel, *On primitive prime factors of Lehmer numbers I*, Acta Arith. 8 (1963), pp. 213–233.

[15] D. Suryanarayana, *Certain diophantine equation*, Math. Student 35 (1967), pp. 197–199.

HARVEY MUDD COLLEGE
Claremont, California, USA

Received on 29. 6. 1974 (591)

ACTA ARITHMETICA
XXIX (1976)

A note on Fermat's conjecture

by

K. Inkeri (Turku)

Introduction. Recently Everett [2] has proved the following theorem.

THEOREM 1. *Let an odd prime $p \geqslant 3$ and an integer $v \geqslant 1$ be fixed. Then there are at most a finite number of relatively prime, positive integer pairs (x, y) on the line $y = x+v$ such that x^p+y^p is the p-th power of an integer.*

The proof is based on Roth's famous theorem, stating that a real algebraic irrational is approximable to no order higher than 2. It is surprising in the proof that $2^{1/p}$ works as the irrational.

Some time ago, the author [3] stated the next theorem.

THEOREM 2. *Let p be a prime $\geqslant 3$. Then there exist at most a finite number of positive integer triples (x, y, z) which satisfy the conditions*

$$x^p+y^p = z^p, \quad (x, y, z) = 1 \tag{1}$$

and for which some difference $|x-y|$, $z-x$, $z-y$ is less than a given positive number M.

Theorem 1 is contained in the case $|x-y| < M$. Theorem 2 can be proved most naturally by the general method given by Inkeri and Hyyrö [5]. Because they only discussed one case (albeit a typical one), we give a complete proof in Section 2. Further we will state a generalization of this theorem. The proof of Theorem 2 given in [3] is of interest for that part which concerns the so-called first case of Fermat's conjecture ($p\nmid xyz$). The method used is completely elementary, and yields also an upper bound in terms of p and M for each of the numbers x, y, z of every solution. On account of Theorem 1, a footnote on p. 52 in [3] is worth mentioning. According to this note, the proof of Theorem 2, excluding the case $z-y < M$, $p|yz$, can be carried out elementarily, using only Thue's theorem concerning (like Roth's), the approximability of an algebraic number by rational numbers. Since Roth's result is fairly deep, we will, in Section 1, prove Theorem 1 by means of Thue's theorem. Our proof is simpler and shorter than that of Everett. In Section 3 our results, and a result of

Baker will be applied to Abel's conjecture (a special case of Fermat's conjecture).

1. Proof of Theorem 1 by Thue's theorem. Let x, y, z be any solution of Fermat's equation (1) in positive integers such that $y-x = v \geqslant 1$, $(x, y) = 1$. Then $0 < x < y < z$, $(x, y, z) = 1$ and, by Abel's well-known formulas (see [6], p. 322, Satz 1044 or [3], pp. 6–8), we may write

$$z-x = b^p, \quad z-y = a^p \quad (0 < a < b) \tag{2}$$

where

(i) a and b are integers if $p \nmid xy$;
(ii) $b^p = p^{p-1}b_0^p$, a and b_0 are integers, if $p|y$;
(iii) $a^p = p^{p-1}a_0^p$, a_0 and b are integers, if $p|x$.

By subtraction it follows from (2) that

$$v = y-x = b^p - a^p. \tag{3}$$

In Case (i) $b^p - a^p > b^p - ab^{p-1} = (b-a)b^{p-1} > b$, since $b-a \geqslant 1$. Thus b is bounded, by (3). Putting $\alpha = p^{1/p}$ (> 1) we obtain in Case (ii), from (2) and (3),

$$pv = (pb_0)^p - pa^p > pb_0(\alpha a)^{p-1} - (\alpha a)^p > |pb_0 - \alpha a|a^{p-1} \tag{4}$$

and hence $|\alpha - pb_0/a| < pv/a^p$. Here α is an algebraic number of degree p $(\geqslant 3)$, because the polynomial $x^p - p$ is irreducible over the field of rational numbers. Now, by Thue's theorem ([6], p. 56, Satz 689), there are only finitely many positive integer pairs (x, y) for which $|\alpha - x/y| < A/y^p$, where A is a positive number. Thus we can conclude that b $(< pb_0)$ is bounded in Case (ii). The same holds also in Case (iii), for it follows as above that

$$pv = pb^p - (pa_0)^p > (\alpha b)^p - pa_0(\alpha b)^{p-1} > |\alpha b - pa_0|b^{p-1}, \tag{5}$$

whence $|\alpha - pa_0/b| < pv/b^p$.

More precisely, we may say that there exists a positive constant M depending only on the fixed v and p such that $b < M$ for every solution (x, y, z) in question. Since, by (1), $2^{1/p}x < z$, we have, according to (2)

$$0 < z(1-2^{-1/p}) < z-x < M^p \quad \text{or} \quad z < M^p/(1-2^{-1/p}),$$

which completes the proof.

Still more quickly than above, cases (ii) and (iii) can be settled using Thue's theorem on binary forms ([6], p. 37) instead of Thue's approximation theorem. From (4) and (5) we immediately see that in Case (ii) $u = pb_0$, $v = a$ and in Case (iii) $u = pa_0$, $v = b$ is an integer solution of the equation

$$|u^p - pv^p| = pv.$$

Since $x^p - p$ is, as mentioned before, an irreducible polynomial of degree $\geqslant 3$ with integer coefficients, this equation has, by Thue's theorem, at most a finite number of solutions in integers u, v. After this, one can proceed as above.

2. The proof and a generalization of Theorem 2. The natural source of results like Theorems 1 and 2 (see [5], where some such results have been stated) is the following fairly general theorem.

THEOREM 3. *Let $m \geqslant 2$, $n \geqslant 2$, $a_0 \neq 0, a_1, \ldots, a_n$ be integers such that m or n is $\geqslant 3$. Then the Diophantine equation*

$$y^m = a_0x^n + a_1x^{n-1} + \ldots + a_n \tag{6}$$

has only finitely many solutions in integers if all zeros of the polynomial on the right of (6) *are simple.*

Siegel ([7], pp. 155–157) has proved this theorem in the case $m = 2$. Applying his method Inkeri and Hyyrö [5] have given a complete proof. The theorem is contained in a more extensive result of LeVeque ([8], p. 210, Theorem 1). Finally, Baker [1] has obtained, using his famous new method and Siegel's techniques, an upper bound for all integer solutions of (6). For $m \geqslant 3$, $n \geqslant 3$ his results implies that

$$\max(|x|, |y|) < \exp\exp\{(5m)^{10}(n^{10n}A)^{n^2}\}, \tag{7}$$

where $A = \max|a_j|$.

It is easily seen that to prove Theorem 2 (and so Theorem 1, too), it suffices to prove the following theorem. (The result with a minus sign in (8) has already been discussed in [5].)

THEOREM 4. *Each of the Diophantine equations*

$$(x+k)^p \pm x^p = y^p, \tag{8}$$

where p is a prime $\geqslant 3$ and k a fixed positive integer, has only finitely many solutions in integers x, y.

Proof. The degrees of the polynomials $f(x) = (x+k)^p \pm x^p$ are $\geqslant p-1 \geqslant 2$. It is seen immediately that

$$pf(x) - (x+k)f'(x) = \mp kpx^{p-1}.$$

Since $f(0) = k^p \neq 0$, we infer from this identity, that $f(x)$ has in the both cases no multiple zero. Now our theorem follows directly from Theorem 3.

To generalize Theorem 4 we consider the equation

$$f(x) \overset{\text{def}}{=} g^p(x) - h^p(x) = y^p, \tag{9}$$

where p is a prime $\geqslant 3$ and g and h are distinct, non-constant polynomials with integer coefficients. Denote by ζ a primitive pth root of unity. Then

$$(10)\qquad f(x) = \big(g(x)-h(x)\big)\big(g(x)-\zeta h(x)\big)\ldots\big(g(x)-\zeta^{p-1}h(x)\big).$$

We have for the degree of the polynomial $f(x)$

$$\deg f = \sum_{r=0}^{p-1} \deg(g-\zeta^r h) \geqslant p-1 \geqslant 2,$$

because $\deg(g-h)\geqslant 0$ and $\deg(g-\zeta^r h)\geqslant 1$ for $1\leqslant r\leqslant p-1$.

By (10), a multiple zero of f is either a multiple zero of some factor on the right of (10), or a common zero at least of two factors and thus also of the polynomials g and h. Now we can conclude that all zeros of f are simple, provided that the discriminants of the factors on the right of (10) and the resultant of g and h satisfy the conditions

$$(11)\qquad D(g-\zeta^r h)\neq 0 \quad (r = 0,1,\ldots,p-1),\quad R(g,h)\neq 0.$$

(For a polynomial $f(x) = a$ of degree 0 we define $D(f) = a^{-2}$.)

The conditions (11) may be replaced by the following

$$(12)\qquad R\big(f(x),\, g(x)h'(x)-g'(x)h(x)\big)\neq 0.$$

Indeed, a simple calculation shows that

$$(13)\qquad pf(x)g'(x)-f'(x)g(x) = ph(x)^{p-1}\big(g(x)h'(x)-g'(x)h(x)\big).$$

A common zero of f and h would be, by (9), a zero of g and thus also of the last factor on the right of (13). But, because of (12), this factor and f have no common zero. Now it follows from (13) that the same also holds for f and f', whence all zeros of f must be simple.

By the way, the equivalence of (11) and (12) is evident from the decompositions

$$R(f, gh'-g'h) = c_1\prod_{r=0}^{p-1} R\big(g-\zeta^r h,\,(g-\zeta^r h)h'-(g'-\zeta^r h')h\big)$$
$$= c_2R^p(g,h)\prod_{r=0}^{p-1} D(g-\zeta^r h),$$

where the c's are numbers $\neq 0$. To verify these one can employ (10) and the following well-known properties of the resultant:

$$R(fg,h) = c_1R(f,h)R(g,h),\qquad R(f,g) = \pm R(g,f),$$
$$R(f,g+hf) = c_2R(f,g),$$

where f, g, h are polynomials and the c's are numbers $\neq 0$.

By Theorem 3, we may sum up the above results as

THEOREM 5. *Let $g(x)$ and $h(x)$ be two different, non-constant polynomials, with integer coefficients. If g and h satisfy the conditions* (11) (*or* (12)), *then the Diophantine equation* (9) *has at most a finite number of solutions in integers x, y.*

This implies as a special case Theorem 4, for if $g(x) = x+k$, $h(x) = \mp x$, we have $gh'-g'h = \mp k$ and hence (12) is valid.

As another example we consider the case $g(x) = ax^2+bx+c$, $h(x) = dx+e$, where the coefficients are integers and $ad\neq 0$. We have

$$R(g,h) = ae^2-bde+cd^2,\qquad D(g-\zeta^r h) = b^2-4ac+(4ae-2bd)\zeta^r+d^2\zeta^{2r}.$$

If $r\not\equiv 0\,(\mathrm{mod}\,p)$, no two of the numbers $0, r, 2r$ are congruent $(\mathrm{mod}\,p)$. Obviously, an equation

$$\sum_{i=0}^{p-1} c_i\zeta^i = 0,$$

where the c_i's are integers, holds iff $c_0 = c_1 = \ldots = c_{p-1}$. Thus the conditions (11) are fulfilled if $ae^2-bde+cd^2\neq 0$, the numbers b^2-4ac, $4ae-2bd$, d^2 are not all equal, and moreover the sum of these numbers is $\neq 0$. For instance, to mention one special case, these three conditions are valid if $d\nmid 4ae^2$, $d\mid(b,c)$.

3. Abel's conjecture and Baker's estimate. Abel has asserted that (1) (with an integer $p\geqslant 3$) has no solution in positive integers x, y, z such that any of the integers x, y, z is a power of a prime. The background and the present state of this problem become apparent from the papers [3], p. 8 and pp. 51–58, in particular, Satz XV and its proof, and [5], p. 6. If x, y, z is such a solution, the following conditions hold:

(i) p is a prime;

(ii) only the smallest of numbers x, y, z (say x) can be a prime power;

(iii) $z-y = 1$; $x\equiv 1$ and $y\equiv 0$ or $-1\,(\mathrm{mod}\,p^3)$.

In addition to these, we have the following fact: There exist only a finite number of solutions of (1) in positive integers x, y, z such that one of x, y, z is a prime power. This follows immediately from (iii) and Theorem 4 $(k = 1)$.

By (iii), we can write (1) in the form

$$(y+1)^p-y^p = \sum_{i=1}^{p} C_i^p y^{p-i} = x^p$$

for any solution in question. We now apply Baker's result (7). By Stirling's formula, the binomial coefficients C_i^p satisfy the conditions

$$C_i^p < \tfrac{4}{5}2^p p^{-1/2},\qquad C_q^p \sim \left(\frac{2}{\pi}\right)^{1/2} 2^p p^{-1/2}\qquad (q = (p-1)/2,\ p\to\infty).$$

Without essential restriction, let $p > 5$. Then

$$(5p)^{10}(\tfrac{4}{5}p^{-1/2})^{(p-1)^2} < 1.$$

Further, by (7), where now $n = p-1$, $m = p$, $A = C_q^p$, we have the estimates

$$x < y < \exp\exp\big(2^p(p-1)^{10(p-1)}\big)^{(p-1)^2} < \exp\exp(2p^{10})^{p^3}.$$

By virtue of estimates given by the author [4] it follows that

$$x > p^{3p-4}, \quad y > \tfrac{1}{2}p^{3p-1},$$

since $p \mid y(y+1)$. Recalling that Fermat's conjecture has been proved for $p < 25000$, the magnitude of each of these bounds is fairly large. However, the differences between the above upper bound and these lower bounds are enormous.

References

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

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

[3] K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. Ser. AI, No. 33 (1946), pp. 1–60.

[4] — *Abschätzungen für eventuelle Lösungen der Gleichung im Fermatschen Problem*, Ann. Univ. Turku, Ser. A, tom. XVI, (1953), pp. 1–9.

[5] K. Inkeri and S. Hyyrö, *Über die Anzahl der Lösungen einiger diophantischer Gleichungen*, Ann. Univ. Turku, Ser. AI, No. 78 (1964), pp. 1–10.

[6] E. Landau, *Vorlesungen über Zahlentheorie*, 3. Bd., Hirzel, Leipzig 1927.

[7] W. J. LeVeque, *Topics in Number Theory*, vol. II, Addison-Wesley, Reading, Massachusetts, 1961.

[8] — *On the equation $y^m = f(x)$*, Acta Arith. 9 (1964), pp. 209–219.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU
Turku, Finland

Received on 12. 7. 1974 (599)

ACTA ARITHMETICA
XXIX (1976)

On the representation of a number in the form $x^2+y^2+p^2+q^2$ where p, q are odd primes

by

G. GREAVES (Cardiff)

1. Introduction. This paper shows that every sufficiently large natural number N that satisfies the necessary condition of incongruence, modulo 8, to 0, 1 or 5 is representable in the form stated in the title. The interest of this result lies partially in the fact that (so far as the author is aware) there is no immediate prospect of any solution of the corresponding "Waring–Goldbach" problem in which the numbers x, y would also be restricted to prime values.

The proof depends on a combination of the mean value theorem of Barban [1] (as re-discovered shortly afterwards by Davenport and Halberstam [3]) with the $\frac{1}{2}$-residue sieve method developed by Rosser (unpublished). An account of this method appears in Iwaniec's paper [7]. Barban's theorem is used in the way described in the author's paper [5] to estimate, with sufficient accuracy for our purposes, the number of pairs of primes p, q that satisfy

$$p^2+q^2 \equiv N \bmod l, \quad p \leqslant Z, \ q \leqslant Z$$

for a modulus l not exceeding $Z/\log^C Z$. Such an estimate is the essential starting point for applications of the sieve method to binary problems involving primes. In this paper the $\frac{1}{2}$-residue sieve method is used in obtaining a positive lower estimate of how often $N-p^2-q^2$ is free of prime factors $\varpi \equiv 3 \bmod 4$, and hence is of the form x^2+y^2.

It is, perhaps, worthy of comment that the $\frac{1}{2}$-residue sieve is sufficiently powerful to establish the existence of numbers that are sums of two squares and lie in a suitable sequence, whereas the 1-residue sieve has not yet been successfully used to establish the existence of primes in any sequence at all.

Iwaniec used his results in his treatment of the number of primes p not exceeding Z that are representable in the form x^2+y^2+A (where, indeed, x^2+y^2 was replaced by an arbitrary quadratic form, positive if