$-(mm'/3)x_2^2 \pmod{m'^2}$. Then if $\varkappa^{\top}$ and $\mu^{\top}$ are given the notations $(k_1\ k_2)$ and $(m_1\ m_2)$, (23) becomes

$$k_1^2 \equiv 1, \quad k_1k_2 \equiv 0, \quad k_2^2 \equiv 0 \pmod{m},$$
$$m_1^2 \equiv 0, \quad m_1m_2 \equiv 0, \quad m_2^2 \equiv 9 \pmod{m'}.$$

Hence k_1 has 2^{ϱ} residues $\bmod m$, while $k_2 \equiv 0$; m_2 has 2^{σ} residues $\bmod m'$, while $m_1 \equiv 0$. Both (24) and (28) are seen to be automatically satisfied.

To sum up, there are $48\cdot 2^{\varrho+\sigma} h_1/u$ simultaneous and primitive representations of m and m' by φ and φ' if $mm' \equiv 1 \bmod 4$, or if $mm' \equiv 3 \bmod 8$ and $(m' \mid 3) = (-1 \mid m)$. There are $48\cdot 2^{\varrho+\sigma}(h_1+h_2)/2$ such representations if $mm' \equiv 7 \bmod 8$ and $(m' \mid 3) = (-1 \mid m)$. There are $48\cdot 2^{\varrho+\sigma} \times h_2/u$ such representations if $mm' \equiv 3 \bmod 8$ and $(m' \mid 3) = -(-1 \mid m)$.

Now, if h denotes the number of properly primitive classes of positive binaries of determinant mm', then it is known that

$$h = \begin{cases} 2^{\varrho+\sigma}h_1 & \text{if} \quad mm' \equiv 1 \pmod 4, \\ 2^{\varrho+\sigma-1}h_1 & \text{if} \quad mm' \equiv 3 \pmod 4; \end{cases} \tag{36}$$

and, if $mm' \equiv 3 \pmod 4$,

$$h_1 = \begin{cases} h_2 & \text{if} \quad mm' = 3, \\ \big(2-(2 \mid mm')\big)h_2 & \text{if} \quad mm' > 3. \end{cases} \tag{37}$$

Also, u (the number of unimodular automorphs of G) is 6 if ψ is i.p. and $mm' = 3$; 4 if $mm' = 1$; and otherwise $u = 2$.

The result stated in the Introduction readily follows.

References

[1] G. Eisenstein, Jour. für Mathematik 35 (1847), pp. 117-136.

[2] H. J. S. Smith, Proc. Roy. Soc. London 16 (1867), pp. 197-208; Collected Mathematical Papers, I, pp. 510-523; II, pp. 623-680.

[3] H. Minkowski, Gesamm. Abh., I.

[4] C. L. Siegel, Annals of Mathematics 36 (1935), pp. 527-606; formula (5).

[5] Any table of positive ternary quadratic forms; e. g. B. W. Jones, Bulletin 97 National Research Council. or see G. Pall, Bull. Amer. Math. Soc., 47(1941), pp. 641-650.

[6] G. Pall, Canadian Jour. of Math. 1 (1949), pp. 344-364; (Theorem 3).

[7] This follows from the fact that the minimum cannot exceed $(4d)^{1/4}$, hence must be 1, and from the corresponding result for ternaries.

LOUISIANA STATE UNIVERSITY

Reçu par la Rédaction le 28. 12. 1963

ACTA ARITHMETICA
IX (1964)

On Catalan's problem

by

K. Inkeri (Turku)

1. Catalan's well-known conjecture that 8 and 9 are the only two consecutive integers larger than 1 which are powers of other integers would be proved if it could be shown that the Diophantine equation

$$x^p - y^q = 1 \tag{1}$$

has only the obvious solutions (x or $y = 0$) for all pairs of prime numbers p and q except for the pair $p = 2$, $q = 3$, for which also $x = \pm 3$, $y = 2$ are solutions. Up to the present this has been proved only for certain special pairs p, q. The case $p = q$ is naturally obvious. Lebesgue [6] has treated the case $q = 2$ and Nagell [7] the cases $p = 3$ and $q = 3$. On the other hand the case $p = 2$ still awaits its final clarification, even though certain strict conditions have been presented. There is, as Obláth [9] has shown, at most one solution. If x, y is the solution, then [5]

$$x \equiv 0 \pmod{q^2}, \qquad y \equiv -1 \pmod{q^3} \tag{2}$$

and (cf. e.g. [4]), in addition,

$$2^q \equiv 2 \pmod{q^2}. \tag{3}$$

As of the primes not exceeding 200183, [10], only 1093 and 3511 fulfil (3), equation (1) is seen not to have a solution for a large number of pairs 2, q.

In this paper we limit ourselves to prime exponents $p > 3$, $q > 3$, of which at least one is of the form $4m+3$ and present proofs for two theorems which yield necessary conditions for the existence of a non-trivial solution of equation (1) that are similar to congruences (2) and (3). As an application, we show that equation (1) is not soluble in non-zero integers for a fairly large number of pairs p, q.

THEOREM 1. *Suppose that p and q are primes >3 and $p\equiv 3\pmod 4$. If q does not divide the class number $h(p)$ of the quadratic field $k(\sqrt{-p})$ and the equation* (1) *has a solution x, y in non-zero integers, then*

$$p^q\equiv p \pmod{q^2} \tag{4}$$

and

$$x\equiv 0 \pmod{q^2},\qquad y\equiv -1 \pmod{q^{2p-1}}. \tag{5}$$

THEOREM 2. *Let p and q be primes with $p\equiv q\equiv 3\pmod 4$, $p>q>3$. If q does not divide the class number $h(p)$ of the field $k(\sqrt{-p})$ and* (1) *has a solution x, y in non-zero integers, then*

$$\begin{aligned} p^q &\equiv p \pmod{q^2}, & q^p &\equiv q \pmod{p^2},\\ x &\equiv 0 \pmod{q^2}, & y &\equiv 0 \pmod{p^2} \end{aligned} \tag{6}$$

and

$$x\equiv 1 \pmod{p^{2q-1}},\qquad y\equiv -1 \pmod{q^{2p-1}}.$$

2. To prove our theorems we introduce certain preliminary results based on the theory of circle-cutting.

The following property of the Gaussian sum is well known:

$$\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)\zeta^m=\sum_a\zeta^a-\sum_b\zeta^b=\sqrt{p^*}\quad \left(p^*=(-1)^{\frac{p-1}{2}}p\right), \tag{7}$$

where p is an odd prime, $\left(\frac{m}{p}\right)$ the Legendre symbol, ζ a primitive pth root of unity, a runs through a complete system of quadratic residues $(\operatorname{mod} p)$ and b through a system of non-residues, and the radical is suitably determined.

Further, one can write ([1], p. 205)

$$4\frac{x^p-1}{x-1}=2A(x)\cdot 2B(x)=Y(x)^2-p^*Z(x)^2, \tag{8}$$

where

$$A(x)=\prod_a(x-\zeta^a),\qquad B(x)=\prod_b(x-\zeta^b) \tag{9}$$

and

$$\begin{cases}2A(x)=Y(x)-Z(x)\sqrt{p^*},\\ 2B(x)=Y(x)+Z(x)\sqrt{p^*},\end{cases}\qquad \begin{cases}Y(x)=A(x)+B(x),\\ Z(x)\sqrt{p^*}=B(x)-A(x)\end{cases} \tag{10}$$

(the radical has the above value). The coefficients of the polynomials $Y(x)$ and $Z(x)$ are rational integers.

We can establish easily by (9) and (10) that

$$Y(x)=(-x)^PY\left(\frac{1}{x}\right),\quad Z(x)=x^PZ\left(\frac{1}{x}\right)\quad \left(P=\frac{p-1}{2},\ p>3\right). \tag{11}$$

Putting

$$Z(x)=a_0+a_1x+\ldots+a_Px^P,$$

we find from (9), (10) and (11) that

$$Z(0)=a_0=a_P=0 \tag{12}$$

and

$$a_1\sqrt{p^*}=a_{P-1}\sqrt{p^*}=\sum_a\zeta^a-\sum_b\zeta^b,$$

whence, by (7), it follows that

$$a_1=1. \tag{13}$$

Suppose now that x, y is a non-trivial solution of the equation (1). Cassels [2] has shown that

$$x\equiv 0 \pmod q,\qquad y\equiv 0 \pmod p. \tag{14}$$

The equation (1) can be written in the form

$$(x-1)\frac{x^p-1}{x-1}=y^q.$$

Since $p\mid y$, the greatest common divisor of the factors on the left is p and the latter factor is not divisible by p^2. Therefore, there exist integers u and v such that

$$x-1=p^{q-1}u^q,\qquad \frac{x^p-1}{x-1}=pv^q. \tag{15}$$

Obviously, v is odd and not divisible by p. From the latter equation it follows, by (8), that

$$pv^q=Y_1^2+pZ_1^2\qquad (Y_1=Y(x)/2,\ Z_1=Z(x)/2),$$

since $p^*=-p$ by $p\equiv 3\pmod 4$. Here the numbers Y_1 and Z_1 are integers. In fact, by (11), $Y(1)=0$ and thus $Y(x)\equiv 0 \pmod 2$ for an odd x, while, by (12), $Z(0)=0$, and therefore $Z(x)\equiv 0 \pmod 2$ for even x. As $p\mid Y_1$, the above equation can be written in the form

$$v^q=Z_2^2+pY_2^2=(Z_2+Y_2\sqrt{-p})(Z_2-Y_2\sqrt{-p}), \tag{16}$$

where $Y_2=\dfrac{Y_1}{p}$, $Z_2=Z_1$. We see easily that $(Y_2, Z_2)=1$; for if a prime r divides this greatest common divisor, then $r>2$, since $r\mid v$ and v is odd. Now $r \mid (A(x), B(x))$, because $r \mid (Y(x), Z(x))$. If $\mathfrak{p}$ is a prime ideal factor of the ideal (r) in the cyclotomic field $k(\zeta)$, we have, by (9),

$$\mathfrak{p} \mid x-\zeta^a, \qquad \mathfrak{p} \mid x-\zeta^b$$

for some a and some b, and therefore $\mathfrak{p} \mid \zeta^a-\zeta^b$ or $r=p$, which is impossible, since $r \mid v$ and v is not divisible by p.

In the quadratic field $k(\sqrt{-p})$ the ideals $(Z_2+Y_2\sqrt{-p})$ and $(Z_2-Y_2\sqrt{-p})$ are relatively prime. For, if $\mathfrak{q}$ is their common prime ideal factor, then $\mathfrak{q} \mid 2Z_2$, and hence $\mathfrak{q} \mid Z_2$, because $\mathfrak{q} \mid v$ and v is odd. But since $(Y_2, Z_2) = 1$, it follows from (16) that $\mathfrak{q} \mid p$, which is contrary to the fact that v is not divisible by p.

It follows now from equation (16) that

$$(Z_2+Y_2\sqrt{-p}) = \mathfrak{a}^q,$$

where $\mathfrak{a}$ is an ideal of $k(\sqrt{-p})$. Since $(q, h(p)) = 1$, $\mathfrak{a}$ is principal, whence

$$Z_2+Y_2\sqrt{-p} = \left(\frac{a+b\sqrt{-p}}{2}\right)^q,$$

where a and b are rational integers with $a \equiv b \pmod 2$. From this equation we deduce, since $Z(x) = 2Z_2$, that

$$2^{q-1}Z(x) = a^q-\binom{q}{2}a^{q-2}b^2p+-\ldots\pm qab^{q-1}p^{\frac{q-1}{2}}.$$

Hence

$$2^{q-1}Z(x) \equiv a^q \pmod{qa}. \tag{17}$$

By (12) and (13), $Z(x) = x(1+a_2x+\ldots)$. Since, by (14), $q \mid x$, it follows from congruence (17) that $q \mid a$. But now $q^2 \mid a^q$ and $q^2 \mid qa$, whence we see from (17) that $q^2 \mid Z(x)$ and thus $q^2 \mid x$, which proves the former of the congruences (5). The latter congruence follows immediately from the original condition (1).

To prove congruence (4) we establish, by (5), that the former of the equations (15) gives

$$p^{q-1}u^q \equiv -1 \pmod{q^2}. \tag{18}$$

By Fermat's theorem, we deduce from this that $u^q \equiv -1 \pmod q$ and further that $u \equiv -1 \pmod q$. Hence $u^q \equiv -1 \pmod{q^2}$ and it follows from (18) that

$$p^{q-1} \equiv 1 \pmod{q^2},$$

which concludes the proof of Theorem 1.

To prove Theorem 2, we note first that (1) can be written in the form

$$(-y)^q-(-x)^p = 1.$$

Moreover, the class number $h(q)$ of the quadratic field $k(\sqrt{-q})$ is not divisible by p, since $p > q > h(q)$ (cf. e.g. [3]). Now Theorem 2 follows immediately from Theorem 1.

Remark. Gut [3] has proved that $h(p) < p/4$. Thus q does not divide the class number of the field $k(\sqrt{-p})$ if it is greater than $p/4$. As is well known, [11], $\log h(p)$ is asymptotically equal to $\log\sqrt{p}$ for $p\to\infty$. Therefore the lower bound for q can be considerably improved if p is large. It seems that for a fixed p there exist very few primes q which fulfil the condition (4). Besides what was said above about the congruence (3), this is confirmed by the fact [5] that the congruence (4) is fulfilled for $p = 3$, $q < 100\,000$ only if $q = 11$. We know no pair p, q of odd primes which satisfies both of the congruences (6).

3. In addition, we consider the prime exponents p, q, which belong to the closed interval (5, 199). There are 44 primes in this interval and 23 of these have the form $4m+3$. There are thus 483 pairs of the form $4m+3$, $4n+1$, 253 pairs $4m+3$, $4n+3$ and 210 pairs $4m+1$, $4n+1$. The last-mentioned pairs remain outside our theorems. The theorems does not apply to the following two sets of pairs $4m+3$, $4n+1$:

(i) $p, 5$ ($p = 47, 79, 103, 127, 131, 179$); 191, 13, for which $q \mid h(p)$;

(ii) $p, 5$ ($p = 7, 43, 107, 151, 199$); p, 13 ($p = 19, 23, 191$); p, 17 ($p = 131, 179$); 19, 137; 107, 97, for which (4) is valid as may be established from data tabulated by Niewiadomski [8].

We can verify that of the pairs $4m+3$, $4n+3$ only 71, 7; 151, 7 and 167, 11 satisfy the condition $q \mid h(p)$ and, according to the data just-mentioned, only the pairs p, 7 ($p = 19, 31, 67, 79$); 127, 19; 19, 43; 67, 47; 71, 47; 11, 71; 31, 79 and 43, 103 satisfy (4). Immediately we see, however, that for all these pairs the latter of the congruences (6) and the condition $q \mid h(q)$ are not valid. Thus equation (1) has only obvious solutions for all pairs $4m+3$, $4n+3$ under consideration. The same has thus been found valid for 718 of the 946 pairs p, q with $5 \leqslant p \leqslant 199$, $5 \leqslant q \leqslant 199$, $p \neq q$.

References

[1] P. Bachmann, *Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie*, 2nd edition, Leipzig u. Berlin 1921.

[2] J. W. S. Cassels, *On the equation $a^x-b^y = 1$, II*, Proc. Cambridge Philos. Soc. 56 (1960), pp. 97-103.

[3] M. Gut, *Abschätzungen für die Klassenzahlen der quadratischen Körper*, Acta Arithm. 8 (1963), pp. 113-122.

[4] K. Inkeri, *Über die Lösbarkeit einiger Diophantischer Gleichungen*, Ann. Acad. Sci. Fenn. A I 334 (1963), pp. 1-15.

[5] K. Inkeri and S. Hyyrö, *On the congruence $3^{p-1} \equiv 1 \pmod{p^2}$ and the Diophantine equation $x^2-1 = y^p$*, Ann. Univ. Turku A 50 (1961), pp. 1-4.

[6] V. A. Lebesgue, *Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2+1$*, Nouv. Ann. de Math. 9 (1850), pp. 178-181.

[7] T. Nagell, *Des équations indéterminées $x^2+x+1 = y^n$ et $x^2+x+1 = 3y^n$*, Norsk Mat. Forenings Skrifter I, 2 (1921), pp. 1-14.

[8] R. Niewiadomski, *Zur Fermatschen Vermutung*, Prace Mat. Fizyczne 42 (1935), pp. 1-10.

[9] R. Obláth, *Über die Zahl x^2-1*, Mathematica B VIII (1939-1940), pp. 161-172.

[10] E. H. Pearson, *On the Congruences $(p-1)! \equiv 1$ and $2^{p-1} \equiv 1 \pmod{p^2}$*, Math. Comp. 17 (1963), pp. 194-195.

[11] C. L. Siegel, *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arithm. 1 (1936), pp. 83-86.

UNIVERSITY OF TURKU, TURKU, FINLAND

Reçu par la Redaction le 28. 12. 1963

ACTA ARITHMETICA
IX (1964)

Diagonal equations over $\mathfrak{p}$-adic fields

by

B. J. Birch (Manchester)

1. It has been conjectured that every form of degree d in at least d^2+1 variables over a $\mathfrak{p}$-adic field K has a non-trivial zero in K. However, as yet it has not even been proved that there is a constant $\Gamma(d)$ independent of K such that every form of degree d in at least $\Gamma(d)$ variables over a $\mathfrak{p}$-adic field has a non-trivial zero in the field. It is the purpose of this note to fill this gap.

In view of the results of Brauer [3], we can deal with general forms (though with an enormously large number of variables) if we can deal with diagonal forms; so it will be enough to prove

THEOREM. *Given d, there is a constant $G(d)$ such that any form*

$$\sum_{i=1}^{s} a_i x_i^d$$

with coefficients in a $\mathfrak{p}$-adic field K and $s \geqslant G(d)$ will have a non-trivial zero x over K.

Our proof of the theorem is a moderately straightforward, though messy, computation; for some of the variables x_j we substitute expansions $1+\sum_{t=1}^{\infty}\pi^t y_{jt}$, where π generates the prime ideal of K and the y_{jt} are units; and in § 2 we analyse what the powers $(1+\sum_{t=1}^{\infty}\pi^t y_{jt})^d$ look like. This enables us to prove our result fairly easily, and fairly efficiently, in certain favourable cases — this is done in § 3. Introducing devices to avoid various difficulties that arise, we gradually widen the scope of our methods, until in § 4 we can prove our theorem in general.

Unfortunately, the arguments of § 4, though not difficult, are inefficient; so our final result involves an inordinately large number of variables.

Our results may be applied to prove theorems about the solutions of equations over algebraic number fields — see [1]. Results similar to our theorem, but with a far better estimate for $G(d)$, have been proved