ACTA ARITHMETICA
XXXIX (1981)

On the generalized Ramanujan—Nagell equation, II

by

F. Beukers (Leiden)

Introduction. In [2] we studied the diophantine equation $x^2+D=2^n$ in integers $x, n \geqslant 1$ in detail. The proofs of the results obtained were based on certain properties of hypergeometric polynomials. In this paper we extend our investigations to the diophantine equation $x^2-D=p^n$ in integers x and $n \geqslant 1$, where D is a positive integer and p is an odd prime not dividing D.

In the introduction of Section 1 some facts about hypergeometric functions are stated. By using these properties we derive the upper bound for the second largest solution of the diophantine equation given in Theorem 1. This result enables us to prove that $x^2-D=p^n$ has at most four solutions in positive integers x, n. On the other hand we show that the equation has at least three solutions if p is of the shape $4a^2+\varepsilon$ and $D=\big((p^l-\varepsilon)/4a\big)^2-p^l$ for some $\varepsilon \in \{-1, 1\}$, $a \in \boldsymbol{N}$, $l \in \boldsymbol{N}$. It would be very interesting to know if there exist equations which have four solutions indeed. So far I have not seen any example and one may suspect that they do not exist.

I have not been able to find references to the equation $x^2-D=p^n$. The equation $x^2+D=p^n$, with $D \in \boldsymbol{N}$ and p an odd prime, has been treated by many authors. In this case there exist at most two solutions as was proved by R. Apéry [1]. For an extensive list of relevant papers see Cohen [3].

1. A few remarks on hypergeometric polynomials. Let $F(\alpha, \beta, \gamma, z)$ be the hypergeometric function given by the series

$$1+\frac{\alpha\cdot\beta}{1\cdot\gamma}z+\frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot 2\cdot\gamma(\gamma+1)}z^2+\ldots,$$

which converges for all $|z|<1$ and for $z=1$ if $\gamma-\alpha-\beta>0$. Let $n_1, n_2, n \in \boldsymbol{N}$ such that $n=n_1+n_2$ and $n_1<\frac{1}{2}n_2$. Define

$$G(z)=F(-\tfrac{1}{2}-n_2, -n_1, -n, z), \qquad H(z)=F(\tfrac{1}{2}-n_1, -n_2, -n, z),$$

$$E(z)=\frac{F(n_2+1, n_1+\frac{1}{2}, n+2, z)}{F(n_2+1, n_1+\frac{1}{2}, n+2, 1)}.$$

According to Lemma 1 in [2] $G(z)$ and $H(z)$ are polynomials of degree n_1 and n_2 respectively, and they satisfy the relation

$$(1)\qquad G(z)-\sqrt{1-z}\,H(z) = z^{n+1}G(1)E(z).$$

According to Lemma 3 of the same paper $\binom{n}{n_1}G(4z)$ and $\binom{n}{n_1}H(4z)$ have integer coefficients as polynomials in z. We prove two more lemmas.

Lemma 1. *Let $|z|>8$, then*

$$\left|\binom{n}{n_1}G(z)\right| < 2^n\left(1+\frac{|z|}{2}\right)^{n_1}, \qquad \left|\binom{n}{n_1}H(z)\right| < 4|z|^{n_2}.$$

Proof.

$$\left|\binom{n}{n_1}G(z)\right| = \left|\sum_{k=0}^{n_1}\binom{n_2+\frac12}{k}\binom{n-k}{n_2}(-z)^k\right| < \sum_{k=0}^{n_1}\binom{n_2+1}{k}\binom{n-k}{n_2}|z|^k$$
$$= \sum_{k=0}^{n_1}\frac{n_2+1}{n_2-k+1}\,\frac{(n-k)!}{n_1!(n_2-k)!}\,\frac{n_1!}{(n_1-k)!k!}\,|z|^k.$$

It is a well-known fact that $\binom{n-k}{n_1}\leqslant 2^{n-k-1}$. Furthermore $\frac{n_2+1}{n_2-k+1}<2$, since $k\leqslant n_1<\frac12 n_2$. Thus we obtain

$$\left|\binom{n}{n_1}G(z)\right| < \sum_{k=0}^{n_1}2\cdot 2^{n-k-1}\binom{n_1}{k}|z|^k = 2^n\left(1+\frac{|z|}{2}\right)^{n_1},$$

as asserted. Furthermore

$$\left|\binom{n}{n_1}H(z)\right| = \left|\sum_{k=0}^{n_2}\binom{n_1-\frac12}{k}\binom{n-k}{n_1}(-z)^k\right|$$
$$< \sum_{k=0}^{n_1}\binom{n_1}{k}\binom{n-k}{n_1}|z|^k + \sum_{k=n_1+1}^{n_2}\frac{n_1!(k-n_1)!}{k!}\binom{n-k}{n_1}|z|^k.$$

Observe that if $k>n/2$, then $n-k<k$ and hence $\binom{n-k}{n_1}\Big/\binom{k}{n_1}<1$. By splitting the second summation on the right-hand side we obtain

$$\left|\binom{n}{n_1}H(z)\right| < 2^n\left(1+\frac{|z|}{2}\right)^{n_1} + \sum_{n_1<k\leqslant n/2}\binom{n-k}{n_1}|z|^k + \sum_{n/2<k\leqslant n_2}|z|^k$$
$$< 2^{n_2}(2+|z|)^{n_1} + \sum_{n_1<k\leqslant n/2}2^{n-k-1}|z|^k + 2|z|^{n_2}$$
$$< 2^{n_2}(2+|z|)^{n_1} + (2|z|)^{n/2} + 2|z|^{n_2}.$$

Since $2n_1<n_2$ and $|z|>8$ we have $2^{n_2}(2+|z|)^{n_1}<(2\sqrt{2+|z|}\,)^{n_2}\leqslant |z|^{n_2}$ and $(2|z|)^{n/2}\leqslant(2|z|)^{3n_2/4}\leqslant|z|^{n_2}$. Hence

$$\left|\binom{n}{n_1}H(z)\right| < 4|z|^{n_2}.$$

Lemma 2. *Let* $\tilde G(z) = F\left(-\frac12-(n_2-1),\ -(n_1+1),\ -n,\ z\right)$ *and* $\tilde H(z) = F\left(\frac12-(n_1+1),\ -(n_2-1),\ -n,\ z\right)$. *Then*

$$\tilde G(z)H(z)-\tilde H(z)G(z) = C\cdot z^{n+1},$$

where C is some non-zero constant.

Proof. According to formula (1) we have

$$G(z)-\sqrt{1-z}\,H(z) = z^{n+1}F(z), \qquad \tilde G(z)-\sqrt{1-z}\,\tilde H(z) = z^{n+1}\tilde F(z)$$

for some power series F and $\tilde F$. Eliminating $\sqrt{1-z}$ we find that $\tilde G(z)H(z)-\tilde H(z)G(z)$ is divisible by z^{n+1}. Since it is a polynomial of degree $n+1$ it must be a multiple of z^{n+1}. The fact that $C\neq 0$ can easily be checked by calculation.

2. Application of hypergeometric polynomials to the equation $x^2-D=p^n$.

Lemma 3. *Let $d\in\boldsymbol{N}$ be square-free and $d\neq 1$. Suppose that there exist integers $\alpha, A, B, r, q\neq 0$ such that*

$$A+B\sqrt d = (r+qB\sqrt d)^\alpha, \qquad \alpha>0.$$

Then $\alpha=1$.

Proof. Without loss of generality we may assume that $r, qB\in\boldsymbol{N}$. Suppose α is odd and $\alpha>1$. Then we observe that $B\sqrt d\geqslant(qB\sqrt d)^\alpha>B\sqrt d$ which is a contradiction. If α is even, then $A+B\sqrt d=(P+QB\sqrt d)^2$ for some integers P, Q. It follows that $B=2PQB$ which is impossible. We therefore conclude $\alpha=1$, as asserted.

Lemma 4. *Let $D\in\boldsymbol{N}$, D not a square. Let p be an odd prime not dividing D. If $A^2-D=p^k$, $A'^2-D=p^{k'}$ for some integers A, A', k, k' with $k'>k$, $p^k>1000D$ then*

$$k' > \frac{\log 2.9D}{4.5}\left(\frac{p^k}{D}\right)^{1/2}.$$

Proof. Choose $B\in\boldsymbol{N}$ such that $D=B^2d$ and d is square-free. Since D s not a square, $d>1$. Factorization of $A^2-B^2d=p^k$ in $\boldsymbol{Q}(\sqrt d)$, gives $(A-B\sqrt d)(A+B\sqrt d)=p^k$. Since $A+B\sqrt d$ and $A-B\sqrt d$ are relatively prime we can write $(A+B\sqrt d)=\mathfrak{a}^k$ for some ideal $\mathfrak{a}$ dividing p. According to the theory of algebraic integers there exists a positive integer e such that

1) $\mathfrak{a}^e = (\alpha+\beta\sqrt{d})$ for some $\alpha, \beta \in \boldsymbol{Z}$ with $B|\beta$,

2) if $\mathfrak{a}^n = (\gamma+\delta\sqrt{d})$ with $B|\delta$, then $e|n$.

This implies $(A+B\sqrt{d}) = (\alpha+\beta\sqrt{d})^{k/e}$ in ideal notation. Hence $A+B\sqrt{d} = \pm\varepsilon\sigma^{k/e}$ where we have put $\sigma = \alpha+\beta\sqrt{d}$ and ε is a unit in $\boldsymbol{Q}(\sqrt{d})$. Notice that ε can be written in the shape $\varepsilon = \varepsilon_1+\varepsilon_2\sqrt{d}$ with $B|\varepsilon_2$. Units which can be written in this shape constitute a cyclic group (mod $\pm$ sign) with generator θ, say. Hence $A+B\sqrt{d} = \pm\theta^r\sigma^{k/e}$ for some $r \in \boldsymbol{Z}$. This implies

$$(2) \qquad |2B\sqrt{d}| = |2\sqrt{D}| = |\theta^r\sigma^{k/e} - \tilde{\theta}^r\tilde{\sigma}^{k/e}|,$$

where $\tilde{\theta}, \tilde{\sigma}$ are the conjugates of θ and σ respectively. Furthermore, by $p^k > 1000D$,

$$|\theta^r\sigma^{k/e}| = |A+B\sqrt{d}| = |A| \pm \sqrt{D} = \sqrt{D+p^k} \pm \sqrt{D} > \frac{30}{31}p^{k/2}.$$

Divide (2) by $|\theta^r\sigma^{k/e}|$, then it follows that

$$\frac{31}{15}\left(\frac{D}{p^k}\right)^{1/2} > \frac{2\sqrt{D}}{|\theta^r\sigma^{k/e}|} = \left|\left(\frac{\tilde{\theta}}{\theta}\right)^r\left(\frac{\tilde{\sigma}}{\sigma}\right)^{k/e} - 1\right|.$$

One easily observes that if $|x-1| < \delta < 1/15$, then $|\log x| < 15\delta/14$. Since $p^k > 1000D$ implies $2(D/p^k)^{1/2} < 1/15.5$ we can apply this inequality and obtain

$$(3) \qquad \left|-r\log\left|\frac{\theta}{\tilde{\theta}}\right| + \frac{k}{e}\log\left|\frac{\tilde{\sigma}}{\sigma}\right|\right| < \frac{31}{14}\left(\frac{D}{p^k}\right)^{1/2}.$$

In a completely analogous way we find that $A'^2 - D = p^{k'}$ implies the existence of an integer r' such that

$$(4) \qquad \left|-r'\log\left|\frac{\theta}{\tilde{\theta}}\right| + \frac{k'}{e}\log\left|\frac{\tilde{\sigma}}{\sigma}\right|\right| < \frac{31}{14}\left(\frac{D}{p^{k'}}\right)^{1/2}.$$

Suppose $r/k = r'/k'$ and $(r, r') = r_1$, $(k, k') = k_1$. Then there exist positive integers α, β such that $r = \alpha r_1$, $k/e = \alpha k_1/e$ and $r' = \beta r_1$, $k'/e = \beta k_1/e$. Since $\beta > \alpha$ we have $\beta > 1$. Now $A+B\sqrt{d} = \pm\theta^{r'}\sigma^{k'/e}$ implies $A+B\sqrt{d} = \pm(p+qB\sqrt{d})^{\beta}$ for some $p, q \in \boldsymbol{Z}$, which is impossible by Lemma 3.

We therefore conclude that $r/k \neq r'/k'$. Put $u = \big|\log|\theta/\tilde{\theta}|\big|$. By eliminating $\log|\tilde{\sigma}/\sigma|$ from the inequalities (3) and (4) we obtain

$$(5) \quad \frac{1}{kk'} \leqslant \left|\frac{r'}{k'} - \frac{r}{k}\right| < \frac{31}{14}\,\frac{1}{u}\left(\frac{1}{k}\left(\frac{D}{p^k}\right)^{1/2} + \frac{1}{k'}\left(\frac{D}{p^{k'}}\right)^{1/2}\right) < \frac{31}{7}\,\frac{1}{u}\,\frac{1}{k}\left(\frac{D}{p^k}\right)^{1/2}.$$

Hence

$$(6) \qquad k' > \frac{u}{4.5}\left(\frac{p^k}{D}\right)^{1/2}.$$

We can determine a lower bound for u as follows. Let $\theta = \xi+\eta\sqrt{d}$ with $B|\eta$. Since θ is a unit, we have $\xi^2-\eta^2 d = \pm 1$. By separating the cases $\xi\eta > 0$ and $\xi\eta < 0$ we can easily find that $u = \big|\log|\theta/\tilde{\theta}|\big| = 2\log(|\xi|+|\eta|\sqrt{d})$. Since $|\xi| = \sqrt{\eta^2 d \pm 1}$ and $\eta^2 d \geqslant B^2 d = D \geqslant 2$, we obtain

$$u = 2\log(|\eta|\sqrt{d} + \sqrt{\eta^2 d \pm 1}) > 2\log\left\{|\eta|\sqrt{d}\left(1+\sqrt{1 \pm \frac{1}{\eta^2 d}}\right)\right\} > \log 2.9D.$$

This inequality, combined with (6), completes the proof of the lemma.

THEOREM 1. *Let $D \in \boldsymbol{N}$, D not a square. Let p be an odd prime not dividing D. If the equation $x^2-D = p^n$ has two solutions $(x, n) = (A, k)$, (A', k') with $k' > k$, then*

$$p^k \leqslant \max(2\cdot 10^6, 600D^2).$$

Proof. Let G, H, n_1, n_2, n be defined as in Section 1. By formula (1) we have

$$G(z) - \sqrt{1-z}\,H(z) = z^{n+1}G(1)E(z).$$

From the introductory remarks in Section 1 we know that the power series expansions of $\binom{n}{n_1}G(4z)$, $\binom{n}{n_1}H(4z)$ and $\sqrt{1-4z}$ in z have integer coefficients. Therefore the power series of $\binom{n}{n_1}G(1)E(z)$ at $z = 0$ has rational coefficients whose denominators are powers of 2. This implies that the power series of $\binom{n}{n_1}G(1)E(z)$ converges in the p-adic number field for all values of z with $\|z\|_p < 1$, where $\|\ \|_p$ is the p-adic valuation. Moreover,

$$(7) \qquad \left\|\binom{n}{n_1}G(1)E(z)\right\|_p \leqslant 1 \quad \text{for all } \|z\|_p \leqslant 1.$$

Consider the identity $G(z) - \sqrt{1-z}\,H(z) = z^{n+1}G(1)E(z)$ as an identity in the p-adic number field and substitute $z = -p^k/D$. On using (7) we find

$$\left\|\binom{n}{n_1}G\left(-\frac{p^k}{D}\right) - \sqrt{1+\frac{p^k}{D}}\binom{n}{n_1}H\left(-\frac{p^k}{D}\right)\right\|_p \leqslant p^{-k(n+1)}$$

and hence

$$(8) \qquad \left\|\binom{n}{n_1}G\left(-\frac{p^k}{D}\right) - \frac{A}{\sqrt{D}}\binom{n}{n_1}H\left(-\frac{p^k}{D}\right)\right\|_p \leqslant p^{-k(n+1)},$$

if the sign of A is correctly chosen. Put $\xi = A(4D)^{n_2}\binom{n}{n_1}H(-p^k/D)$ and $\eta = (4D)^{n_2}\binom{n}{n_1}G(-p^k/D)$ and notice that $\xi, \eta \in \boldsymbol{Z}$. By multiplying (8) with $\sqrt{D}(4D)^{n_2}$ we find that

$$(9) \qquad \|\xi-\eta\sqrt{D}\|_p \leqslant p^{-k(n+1)}.$$

We now assume that $p^k \geqslant \max(2\cdot 10^6, 600D^2)$. According to Lemma 1 we have

$$|\xi| < 4\left|\frac{p^k}{D}\right|^{n_2}|A|(4D)^{n_2} = 4^{n_2+1}p^{n_2k}(D+p^k)^{1/2} < 5\cdot 4^{n_2}p^{(n_2+1/2)k}$$

and

$$|\eta| < 2^n\left(1+\frac{1}{2}\,\frac{p^k}{D}\right)^{n_1}(4D)^{n_2} = 2^{2n_1+n_2}p^{n_1k}\left(\frac{2D}{p^k}+1\right)^{n_1}(4D)^{n_2-n_1}$$
$$< 5^{n_1}2^{n_2}p^{n_1k}(4D)^{n_2-n_1}.$$

Choose the sign of A' such that $\|A'-\sqrt{D}\|_p \leqslant p^{-k'}$. Since $p^k \geqslant \max(2\cdot 10^6, 600D^2)$ we can apply Lemma 4 and obtain

$$k' > \frac{\log 2.9D}{4.5}\left(\frac{p^k}{D}\right)^{1/2} \geqslant k\,\frac{\log 3}{4.5}\,\frac{\log 2.9D}{\log p^k}\left(\frac{p^k}{D}\right)^{1/2}.$$

If $D \geqslant 58$ then

$$k' > k\,\frac{\log 3}{4.5}\,\frac{\log 2.9D}{\log p^k}\,p^{k/4}\left(\frac{p^k}{D^2}\right)^{1/4} > k\,\frac{1}{4.1}\,\frac{\log 2.9D}{\log 600D^2}\cdot 600^{1/2}\cdot D^{1/2} > 15k.$$

If $D \leqslant 58$ then

$$k\,\frac{\log 3}{4.5}\,\frac{\log 2.9D}{D^{1/2}}\,\frac{(2\cdot 10^6)^{1/2}}{\log(2\cdot 10^6)} > 15k.$$

Hence $k' > 15k$. Choose n such that $kn \leqslant k' < k(n+1)$. Notice that $n \geqslant 15$. Choose n_1 such that $\frac{1}{5}n-\frac{6}{5} \leqslant n_1 \leqslant \frac{1}{5}n+\frac{3}{5}$ and such that $\xi-\eta A' \neq 0$. This is possible in view of Lemma 2. Combine $\|A'-\sqrt{D}\|_p \leqslant p^{-k'}$ with inequality (9). Then we obtain

$$\frac{1}{|\xi-\eta A'|} \leqslant \|\xi-\eta A'\|_p \leqslant \max\{p^{-k'}, p^{-k(n+1)}\} = p^{-k'},$$

which implies

$$(10) \quad p^{k'} \leqslant |\xi|+|\eta A'| < 5\cdot 2^{2n_2}p^{(n_2+1/2)k}+5^{n_1}2^{n_2}p^{n_1k}(4D)^{n_2-n_1}\sqrt{D+p^{k'}}.$$

Notice that $\sqrt{p^{k'}+D} < 1.05\cdot p^{k'/2}$ since $p^{k'} > p^k > 600D$. From inequality (10) it follows that at least one of the terms on the right-hand side is larger than $\frac{1}{2}p^{k'}$. Thus we find

$$5\cdot 2^{2n_2}p^{(n_2+1/2)k} > \frac{p^{k'}}{2} \geqslant \frac{p^{nk}}{2}, \quad \text{implying} \quad p^{(n_1-1/2)k} < 10\cdot 2^{2n_2}$$

or

$$1.05\cdot 5^{n_1}2^{n_2}p^{n_1k}(4D)^{n_2-n_1}p^{k'/2} > p^{k'}/2'$$
$$\text{implying} \quad 2.1\cdot 5^{n_1}2^{n_2}(4D)^{n_2-n_1} \geqslant p^{\frac{1}{2}k(n_2-n_1)}.$$

Hence

$$p^k < \max\{10^{\frac{1}{n_1-1/2}}2^{\frac{2n_2}{n_1-1/2}}, (2.1)^{\frac{2}{n_2-n_1}}5^{\frac{2n_1}{n_2-n_1}}2^{\frac{2n_2}{n_2-n_1}}(4D)^2\}.$$

Since $\frac{1}{5}n-\frac{6}{5} \leqslant n_1 \leqslant \frac{1}{5}n+\frac{3}{5}$ and $n \geqslant 15$ it can easily be checked that

$$10^{\frac{1}{n_1-1/2}}2^{\frac{2n_2}{n_1-1/2}} \leqslant 10^{\frac{1}{1.5}}2^{\frac{2\cdot 14}{1.5}} < 2\cdot 10^6$$

and

$$(2.1)^{\frac{2}{n_2-n_1}}5^{\frac{2n_1}{n_2-n_1}}2^{\frac{2n_2}{n_2-n_1}} \leqslant (2.1)^{2/9}5^{\frac{2\cdot 4}{9}}2^{\frac{2\cdot 13}{9}} < 36.8.$$

Thus we obtain

$$p^k < \max(2\cdot 10^6, 600D^2),$$

which proves our theorem.

3. The number of solutions of the equation $x^2-D=p^n$. With the aid of Theorem 1 it is now possible to make some statements about the number of solutions of the equation $x^2-D=p^n$ in positive integers x, n. Before we proceed I want to draw attention to a special class of equations. If $p=4a^2+\varepsilon$ and $D=\big((p^l-\varepsilon)/4a\big)^2-p^l$ for some $a, l \in \boldsymbol{N}$, $\varepsilon \in \{-1, 1\}$ (p not necessarily prime) then the equation $x^2-D=p^n$ has the following solutions

$$(x, n) = \left(\frac{p^l-\varepsilon}{4a}2a, 1\right), \left(\frac{p^l-\varepsilon}{4a}, l\right), \left(2ap^l+\varepsilon\frac{p^l-\varepsilon}{4a}, 2l+1\right).$$

One may notice that this can be generalized to the case where $p^k=4a^2+\varepsilon$ for some $k \in \boldsymbol{N}$. The solutions will be the same, except for the first and third value of the exponent which becomes k, $2l+k$, respectively. From a theorem of Chao Ko [4] however, it follows that $|p^k-4a^2|=1$ with $k>1$ is impossible, so this generalization is useless.

Definition 1. If D and p can be written in the shape given above, the pair (D, p) and the equation $x^2-D=p^n$ will be called *exceptional*.

Lemma 5. *Let $D>0$, and p an odd prime not dividing D. If $x^2-D=p^k$, $y^2-D=p^l$, $z^2-D=p^m$ for some $x, y, z, k, l, m \in \boldsymbol{N}$ with $m>l>k$, then $m-2l$ is an odd positive integer. Moreover, if $m-2l=1$ then $p=4a^2+$ $+\varepsilon$, $D=\big((p^l-\varepsilon)/4a\big)^2-p^l$ for some $a \in \boldsymbol{N}$, $\varepsilon \in \{-1, 1\}$ and $k=1$.*

If $m-2l \geqslant 3$, then $m-2l \geqslant$ $\max\{3, k, \frac{2}{3}(l-1)\}$.

Proof. Note that x, y and z have the same parity and thus it follows that

$$\frac{y-x}{2}\,\frac{y+x}{2}=p^k\,\frac{p^{l-k}-1}{4}\quad\text{and}\quad\frac{z-y}{2}\,\frac{z+y}{2}=p^l\,\frac{p^{m-l}-1}{4}.$$

Notice that p^k divides either $(y-x)/2$ or $(y+x)/2$ and that p^l divides either $(z-y)/2$ or $(z+y)/2$. Put $(y-x)/2=u$, $(y+x)/2=v$ and $(z-y)/2=\alpha p^l$ if $z\equiv y \pmod p$ and $(z+y)/2=\alpha p^l$ if $z\equiv -y \pmod p$. Notice that $\alpha\in \boldsymbol{N}$. Thus we obtain

$$uv=p^k\,\frac{p^{l-k}-1}{4}\quad\text{and}\quad \alpha\big(\alpha p^l+\varepsilon(u+v)\big)=\frac{p^{m-l}-1}{4},\tag{11}$$

where $\varepsilon\in\{-1,1\}$ is determined by $z\equiv \varepsilon y \pmod p$. Notice that

$$u+v\leqslant uv+1=\tfrac14(p^l-p^k)+1\leqslant\tfrac14(p^l+1).$$

Furthermore, it follows from (11) that

$$\left|\frac{(p^{m-2l}-4\alpha^2)p^l-1}{4\alpha}\right|=\left|\frac{p^{m-l}-1}{4\alpha}-\alpha p^l\right|=|u+v|\leqslant\frac14\,(p^l+1)$$

and hence

$$\left|\frac{p^{m-2l}-4\alpha^2}{\alpha}\right|\leqslant p^{-l}+(1+p^{-l}).$$

One easily observes that $m-2l>0$. Put $r=m-2l$. Then we find, by $p^l\geqslant 25$, that

$$|2\alpha-p^{r/2}|\leqslant(2\alpha+p^{r/2})^{-1}\alpha(1+\tfrac{2}{25})\leqslant\frac{1}{2+\sqrt{3}}(1+\tfrac{2}{25})<0.29.\tag{12}$$

We see that α is uniquely determined by p^r and moreover, since r even would imply $|2\alpha-p^{r/2}|\geqslant 1$, we see that r is odd. Thus the first assertion of our lemma is proved.

Eliminate v from the equalities (11). Then we obtain

$$4u\alpha^2p^l+\varepsilon\alpha(p^l-p^k+4u^2)=u(p^{l+r}-1).\tag{13}$$

Since $u<v$, the first equality of (11) implies

$$u(u+v)<\tfrac12(p^l-p^k)<\tfrac12(p^l-1).$$

On using

$$|u+v|=\left|\frac{p^r-4\alpha^2}{4\alpha}p^l-\frac{1}{4\alpha}\right|\geqslant\frac{p^l-1}{4\alpha}$$

we find that

$$|u|<\frac{p^l-1}{2|u+v|}\leqslant 2\alpha.\tag{14}$$

We shall now prove the second assertion of our lemma. Assume $r=1$. Consider (13) modulo p^k. We obtain $4\varepsilon\alpha u^2\equiv -u \pmod{p^k}$ and thus we have either $p^k|u$ or $p^k|(4\varepsilon\alpha u+1)$. By (12) and (14) we have $u<p^{1/2}+0.29$ so $p^k|u$ is impossible. Since $4\alpha u<2(p^{1/2}+0.29)^2<3p-1$, the possibility $p^k|(4\varepsilon\alpha u+1)$ can only occur if $k=1$ and $p=4\alpha u+\varepsilon$. Using this, we can derive from (13) that $(\alpha-u)p^{l+1}=\varepsilon(\alpha-u)p$ and hence $\alpha=u$. We now easily find

$$y=u+v=\alpha+(p^l-p)/4\alpha=(p^l-4\alpha^2-\varepsilon)/4\alpha+\alpha=(p^l-\varepsilon)/4\alpha$$

and hence

$$D=y^2-p^l=\big((p^l-\varepsilon)/4\alpha\big)^2-p^l,$$

as asserted.

We now prove the third assertion. Assume $r\geqslant 3$. Consider (13) modulo p^l. Then we obtain $u+\varepsilon\alpha(-p^k+4u^2)\equiv 0 \pmod{p^l}$. It follows that either $u+\varepsilon\alpha(-p^k+4u^2)=0$ or $|u+\varepsilon\alpha(-p^k+4u^2)|\geqslant p^l$. If the first possibility occurs, then it also follows from (13) that $(4u\alpha+\varepsilon)\alpha=up^r$. These two equalities imply $\alpha|u$ and $u|\alpha$ respectively, hence $\alpha=u$. This implies $p^r=4\alpha^2+\varepsilon$. According to Chao Ko's theorem [4] this can only happen if $r=1$, contradicting $r\geqslant 3$.

We therefore conclude that

$$p^l\leqslant|u+\varepsilon\alpha(-p^k+4u^2)|\leqslant\max\{\alpha p^k,\,u(4\alpha u+\varepsilon)\}.$$

From (13) it also follows that $u(4\alpha u+\varepsilon)\equiv 0 \pmod{p^k}$. Hence we have either $p^k|u$ or $p^k|(4\alpha u+\varepsilon)$. This implies $p^k\leqslant 4\alpha u+1$. Hence

$$p^l\leqslant(4\alpha u+1)\max(\alpha,u).$$

On using (12) and (14) we find $4\alpha u+1<2(p^{r/2}+0.29)^2+1$. Thus $p^k\leqslant 4\alpha u+{}$ $+1$ implies $k\leqslant r$, as asserted. Furthermore

$$p^l<(p^{r/2}+0.29)\big(2(p^{r/2}+0.29)^2+1\big)<2(p^{r/2}+1)^3,$$

and hence

$$p^{2l}<p^{3r+2}\,\frac{4}{p^2}\,(1+p^{-r/2})^6.$$

Since $r\geqslant 3$, we have $p^r\geqslant 27$ and hence

$$4(1+p^{-r/2})^6/p^2\leqslant\frac49\left(1+\frac{1}{\sqrt{27}}\right)^6<3.$$

We therefore conclude that $2l\leqslant 3r+2$ or equivalently, $r\geqslant\frac23(l-1)$.

LEMMA 6. *Let $D\in\boldsymbol{N}$ and p an odd prime not dividing D. Assume $x^2-D=p^k$, $y^2-D=p^l$, $z^2-D=p^m$ for some $k,l,m,x,y,z\in\boldsymbol{N}$ with $m>l>k$. If $m-2l\geqslant 3$ then $m-2l\geqslant\log 10^6/\log p$.*

Proof. We use the same notations as in Lemma 5. In order to prove our lemma we must show that $p^r \geqslant 10^6$. By (12) we have $|2a - p^{r/2}| < 0.29$. Checking this inequality for $p^r < 10^6$ and $r \geqslant 3$ we find the following solutions, $(p^r, 2a) = (17^3, 70)$, $(29^3, 156)$, $(43^3, 282)$, $(47^3, 322)$, $(53^3, 386)$, $(71^3, 598)$, $(73^3, 624)$, $(79^3, 702)$, $(83^3, 756)$, $(5^5, 56)$. We intend to show that none of these solutions is compatible with the assumptions of our lemma and thus $p^r \geqslant 10^6$.

From (11) it follows that $4a$ divides $p^{l+r}-1$. Since $r \geqslant 3$ we can apply Lemma 5 and find $r \geqslant \frac{2}{3}(l-1)$. Suppose $r = 3$ then, by $r \geqslant \frac{2}{3}(l-1)$, we have $l \leqslant 5$ and hence $l+r \leqslant 8$. Moreover $l+r \geqslant 5$ since $l \geqslant 2$. Checking the divisibility of $p^{l+r}-1$ $(5 \leqslant l+r \leqslant 8)$ by $4a$ for our calculated values of p and a we find no other cases than

$$\frac{29^6-1}{312} = 1906485, \qquad \frac{47^6-1}{644} = 16737912.$$

In both cases $l = 3$. Calculating $y = u+v$ by the second equality (11) we find $y = 4143, 22409$, respectively. It is easily checked that the equation $y^2 - x^2 = p^l - p^k$ in the unknowns x and $k < l$ has no solutions for our calculated valies of y, p and l.

Suppose $r = 5$, then $l \leqslant 8$ and $l+r \leqslant 13$. The conditions $112|(5^{l+r}-1)$, $l+r \leqslant 13$ imply $l+r = 12$. Then $(5^{12}-1)/112 = 2179827$ and $y = 7673$. It is easily checked that $7673^2 - x^2 = 5^7 - 5^k$ $(k < 7)$ has no solutions. Thus our lemma is proved.

THEOREM 2. *Let $D > 0$, and p an odd prime not dividing D. Then the equation $x^2 - D = p^n$ has at most four solutions in positive integers x, n. If there are exactly four solutions and $D < 25000$ or $p > (D/40)^{1/2}$, then the pair (D, p) is exceptional.*

Proof. We first deal with the case that $D = d^2$ for some $d \in \mathbf{N}$. Suppose $x^2 - d^2 = p^n$ for some $x, n \in \mathbf{N}$. Then $(x-d)(x+d) = p^n$ and since $x-d$ and $x+d$ are relatively prime, we find $x-d = 1$, $x+d = p^n$ and hence $d = \frac{1}{2}(p^n-1)$. So, if D is a square, then $x^2 - D = p^n$ has at most one solution.

From now on we assume that D is not a square. Assume that (D, p) is an exceptional pair with $p = 4a^2 + \varepsilon$ and $D = \left((p^l - \varepsilon)/4a\right)^2 - p^l$ and suppose that there exists a fourth solution (z, m). Then, by Lemmas 5 and 6, we have $m \geqslant 2(2l+1) + \log 10^6/\log p$. Since $D < (p^l/4a)^2$ it follows that $p^m > 10^6 p^{4l} > 10^6 D^2$ and thus, by Theorem 1, (z, m) is the largest solution. Assume that (D, p) is a non-exceptional pair. Suppose there are three solutions (x_1, n_1), (x_2, n_2), (x_3, n_3) with $n_3 > n_2 > n_1$. By Lemmas 5 and 6 we find $p^{n_3} > 10^6 p^{2n_2}$. We also observe that $p^{n_2} > x_2^2 - x_1^2 \geqslant 4x_1 > 4D^{1/2}$ and hence $p^{n_3} > 16 \cdot 10^6 D$.

Suppose that there exists a fourth solution (x_4, n_4) with $n_4 > n_3$. Then, by Lemma 5, $p^{n_4} > p^{2n_3} > 2 \cdot 10^6 D^2$. According to Theorem 1 (x_4, n_4) is the largest solution.

Suppose $D < 25000$, then $p^{n_3} > 16 \cdot 10^6 D > \max(2 \cdot 10^6, 600D^2)$ and hence (x_3, n_3) is the largest solution according to Theorem 1.

Suppose $p > (D/40)^{1/2}$, then $p^{n_2} \geqslant p^2 > D/40$. Furthermore, $p^{n_3} > 10^6 p^{2n_2} > \max\{3^4 \cdot 10^6,\ 10^6(D/40)^2\} > \max(2 \cdot 10^6, 600D^2)$ and hence (x_3, n_3) is the largest solution according to Theorem 1.

References

[1] R. Apéry, *Sur une équation diophantienne*, C. R. Acad. Sci. Paris, Sér. A 251 (1960), pp. 1451–1452.

[2] F. Beukers, *On the generalised Ramanujan–Nagell equation I*, Acta Arith. 38 (1981), pp. 389–410.

[3] E. L. Cohen, *The diophantine equation $x^2 + 11 = 3^k$ and related questions*, Math. Scand. 38 (1976), pp. 240–246.

[4] Chao Ko, *On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$*, Scientia Sinica (Notes) 14 (1964), pp. 457–460.

Received on 14.4.1978 (1063)