[5] J. F. Koksma, *Some theorems on diophantine inequalities*, Math. Centrum Amsterdam, Scriptum 5 (1950).
[6] H. L. Montgomery, *Extreme values of the Riemann zeta-function*, Comm. Math. Helv. 52 (1977), pp. 511–518.
[7] H. L. Montgomery and R. C. Vaughan, *Hilbert's inequality*, J. London Math. Soc. (2) 8 (1974), pp. 73–82.
[8] R. Paley and N. Wiener, *Fourier Transforms in the complex domain*, AMS Colloq. Publ. XIX, 1934.
[9] G. Pólya und G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Vol. 2, 2. Aufl., Springer, Berlin 1954.
[10] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, Clarendon Press, Oxford 1951.
[11] S. Voronin, *On the distribution of non-zero values of the Riemann zeta-function*, Proc. Steklov Inst. Math. 128 (1972), pp. 153–175.
[12] — *Theorem on the universality of the Riemann zeta-function*, Math. USSR Izv. 9 (1975), pp. 443–453.

THE INSTITUTE FOR ADVANCED STUDY
Princeton, N. J., USA

Received on 2. 11. 1977
and in revised form on 26. 5. 1978 (995)

ACTA ARITHMETICA
XXXVIII (1981)

On the generalized Ramanujan–Nagell equation I

by

F. Beukers (Leiden)

Introduction. In this paper we shall study the diophantine equation $x^2 - D = 2^n$ $(D \in \mathbf{Z})$ in the positive integers x, n. The equation $x^2 + 7 = 2^n$ is known as the Ramanujan–Nagell equation. It was solved by several authors (see Hasse [6]) and has five solutions, namely $(x, n) = (1, 3)$, $(3, 4)$, $(5, 5)$, $(11, 7)$, $(181, 15)$.

In 1960 Apéry [1] proved that the equation $x^2 - D = 2^n$ $(D < 0$, $D \neq -7)$ has at most two solutions. Browkin and Schinzel [4] conjectured that this equation has two solutions if and only if $D = -23$ or $1 - 2^k$ for some $k > 3$. Schinzel ([7], p. 212) partly resolved this conjecture by proving that, unless $D = 1 - 2^k$, the equation has at most one solution with $n > 80$. In Theorem 2 of the present paper we prove the Browkin–Schinzel conjecture.

Theorems 3 and 4 deal with the equation $x^2 - D = 2^n$ $(D > 0)$. In Theorem 4 we prove that this equation has at most four solutions. Surprisingly it turns out to be possible to construct infinitely many equations each one admitting precisely four solutions. In Theorem 3 a complete classification is given for those equations with $0 < D < 10^{12}$ having exactly three or four solutions. I have not found any reference to the case $D > 0$ except for a remark by Hasse ([6], p. 100) and a few congruence considerations by Browkin, Schinzel ([4], p. 311).

Theorems 2, 3 and 4 depend on Corollary 1 of Theorem 1 which states that $n < 435 + 10(\log|D|/\log 2)$ for any solution (x, n). This result makes it possible to solve a given equation $x^2 - D = 2^n$ in finitely many steps. Theorem 1 gives a good lower bound for the approximation to $\sqrt{2}$ by rational numbers whose denominators are a power of two. The proof of this theorem uses so-called hypergeometric functions. In 1937 Siegel [8] introduced these functions in the theory of diophantine approximations. By refining Siegel's method Baker [2] succeeded in giving a good lower bound for the rational approximations to $\sqrt[3]{2}$. The proof of Theorem 1 is in fact an adaptation of Siegel's method.

Theorem 5 is an analogue of Theorem 1 for some integers other than two. We do not work out the applications of this theorem here. The appendix of this paper contains a list of all equations $x^2 - D = 2^n$ with $|D| < 1000$ which have two or more solutions, together with their solutions.

It also contains some numerical results which are used in the proofs. I would like to thank R. Brand for performing the required calculations on a computer and finally Prof. R. Tijdeman, who introduced me to the subject and assisted me during the preparation of this paper.

1. Preliminary remarks on hypergeometric functions. A hypergeometric function $F(\alpha, \beta, \gamma, z)$ is defined by the series

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

which converges for all $|z| < 1$ and for $z = 1$ if $\gamma - \alpha - \beta > 0$. Furthermore $F(\alpha, \beta, \gamma, z)$ satisfies the differential equation

$$z(z-1)F'' + \{(\alpha+\beta+1)z - \gamma\}F' + \alpha\beta F = 0.$$

(For these and other properties of hypergeometric functions see Forsyth [5], Bieberbach [3], Siegel [8], Baker [2] and [9].)

LEMMA 1. *Let n_1, n_2 be positive integers such that $n = n_2 + n_1$, $n_2 \geqslant n_1$. Put $G(z) = F(-\frac{1}{2} - n_2, -n_1, -n, z)$, $H(z) = F(\frac{1}{2} - n_1, -n_2, -n, z)$ and*

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

Then $G(z)$ and $H(z)$ are polynomials of degree n_1 and n_2 respectively and

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

Proof. It is easily checked, that $G(z)$, $\sqrt{1-z}\,H(z)$ and $z^{n+1}F(n_2+1, n_1+\frac{1}{2}, n+2, z)$ satisfy the differential equation

$$z(z-1)F'' + \{(\tfrac{1}{2} - n)z + n\}F' + n_1(n_2 + \tfrac{1}{2})F = 0. \tag{1}$$

Hence there exists a linear relation between these functions. By substituting $z = 0$ and $z = 1$ we find that this relation is given by

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

LEMMA 2. *Let $G(z), H(z), n_1, n_2$ be defined as in Lemma 1. Then*

(a) $|G(z) - \sqrt{1-z}\,H(z)| < G(1)|z|^{n+1}$ *for* $|z| < 1$,

(b) $G(1) < G(z) < G(0) = 1$ *for* $0 < z < 1$,

(c) $G(1) = \binom{n}{n_1}^{-1} \prod_{m=1}^{n_1} \left(1 - \frac{1}{2m}\right)$.

Proof. Since $F(n_2+1, n_1+\frac{1}{2}, n+2, z)$ has only positive coefficients, we have

$$|F(n_2+1, n_1+\tfrac{1}{2}, n+2, z)| < F(n_2+1, n_1+\tfrac{1}{2}, n+2, 1) \quad \text{for} \quad |z| < 1.$$

Hence $|E(z)| < 1$ and by Lemma 1 we find assertion (a). Secondly, notice that

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

$F(-\frac{1}{2} - n_2, -n_1, \frac{1}{2}, 1-z)$ as a polynomial in $1-z$ has positive coefficients, since $n_2 \geqslant n_1$. This implies

$$G(1) < G(z) = G(1)F(-\tfrac{1}{2} - n_2, -n_1, \tfrac{1}{2}, 1-z) < G(0) \quad \text{for} \quad 0 < z < 1.$$

Thirdly, by substituting $z = 0$ we find

$$1 = G(1)\, F(-\tfrac{1}{2} - n_2, -n_1, \tfrac{1}{2}, 1).$$

According to a well-known formula due to Gauss (see [3]) we have

$$F(-\tfrac{1}{2} - n_2, -n_1, \tfrac{1}{2}, 1) = \frac{\Gamma(\frac{1}{2})\,\Gamma(n+1)}{\Gamma(n_2+1)\,\Gamma(n_1+\frac{1}{2})}.$$

Hence

$$G(1) = \binom{n}{n_1}^{-1} \prod_{m=1}^{n_1} \left(1 - \frac{1}{2m}\right).$$

LEMMA 3. *Both $\binom{n}{n_1} G(4z)$ and $\binom{n}{n_1} H(4z)$ are polynomials with integer coefficients.*

Proof.

$$\begin{aligned}
\binom{n}{n_1} G(4z) &= \binom{n}{n_1} \sum_{k=0}^{n_1} \binom{n_2+\frac{1}{2}}{k} \frac{n_1(n_1-1)\dots(n_1-k+1)}{n(n-1)\dots(n-k+1)} (-4z)^k \\
&= \sum_{k=0}^{n_1} \binom{n_2+\frac{1}{2}}{k} \frac{n!}{n_1!\,n_2!} \frac{n_1(n_1-1)\dots(n_1-k+1)}{n(n-1)\dots(n-k+1)} (-4z)^k \\
&= \sum_{k=0}^{n_1} \binom{n_2+\frac{1}{2}}{k} \binom{n-k}{n_2} (-4z)^k.
\end{aligned}$$

Since $\binom{n_2+\frac{1}{2}}{k} 4^k \in \mathbf{Z}$ it follows that $\binom{n}{n_1} G(4z) \in \mathbf{Z}[z]$. In a completely analogous way we find

$$\binom{n}{n_1} H(4z) = \sum_{k=0}^{n_2} \binom{n_1-\frac{1}{2}}{k} \binom{n-k}{n_1} (-4z)^k \in \mathbf{Z}[z].$$

LEMMA 4. *Denote*

$$G^*(z) = F\left(-\tfrac{1}{2}-(n_2+1),\ -(n_1+1),\ -(n+2),\ z\right),$$

$$H^*(z) = F\left(\tfrac{1}{2}-(n_1+1),\ -(n_2+1),\ -(n+2),\ z\right).$$

Then

$$G^*(z)H(z)-H^*(z)G(z) = c\cdot z^{n+1} \quad \text{for some constant } c\neq 0.$$

Proof. According to Lemma 1 we have

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

and

$$G^*(z)-\sqrt{1-z}\,H^*(z) = z^{n+3}F^*(z)$$

for some hypergeometric functions F, F^*. By eliminating $\sqrt{1-z}$ we find that G^*H-H^*G is divisible by z^{n+1}. Since it is a polynomial of degree $n+1$ we find the above lemma. A calculation of the coefficient of z^{n+1} in G^*H-H^*G shows that the constant c is non zero.

2. In this section we prove Theorem 1, which enables us to prove Theorems 2, 3 and 4. Before we proceed, we prove

LEMMA 5. *Let $k, n\in\boldsymbol{N}$. If $n\geqslant 3k$ then $\binom{n}{k} < \frac{1}{2}\left(\frac{3}{4^{1/3}}\right)^n$.*

Proof. Assume $n = 3m+\delta$ for some $m\in\boldsymbol{N}$, $\delta\in\{0,1,2\}$. Then

$$\binom{n}{k} = \binom{3m+\delta}{k} \leqslant \binom{3m+\delta}{m}.$$

Observe that

$$\binom{3m+\delta}{m}\Big/\binom{3(m-1)+\delta}{m-1} = \frac{(3m+\delta)(3m+\delta-1)(3m+\delta-2)}{m(2m+\delta)(2m+\delta-1)} < \frac{27}{4}$$

for all $m\geqslant 2$, $\delta\in\{0,1,2\}$.

This implies

$$\binom{3m+\delta}{m} < \left(\frac{27}{4}\right)^{m-1}\binom{3+\delta}{1} = \left(\frac{4}{27}\right)^{\left(\frac{\delta}{3}+1\right)}(\delta+3)\left(\frac{27}{4}\right)^{\frac{3m+\delta}{3}} < \frac{1}{2}\left(\frac{3}{4^{1/3}}\right)^n.$$

Hence our lemma follows.

THEOREM 1. *Let p be an odd power of 2. Then for all $x\in\boldsymbol{Z}$,*

$$\left|\frac{x}{p^{1/2}}-1\right| > \frac{2^{-43.5}}{p^{0.9}}.$$

Proof. It is well known that $181^2+7 = 2^{15}$. Put $w = 2^{15}$ and $\delta = 7$. Throughout this section G, H, n, n_1, n_2 will be defined as in Section 1.

By Lemma 2 we have

$$\binom{n}{n_1}\left|G(z)-\sqrt{1-z}\,H(z)\right| < G(1)|z|^{n+1}\binom{n}{n_1}.$$

Insert $z = \delta/w$ and put

$$\frac{A}{(4w)^{n_1}} = \binom{n}{n_1}G\left(\frac{\delta}{w}\right), \qquad \frac{B}{(4w)^{n_2}} = \binom{n}{n_1}H\left(\frac{\delta}{w}\right).$$

Then

$$\left|\frac{A}{(4w)^{n_1}}-\frac{181\,B}{w^{1/2}(4w)^{n_2}}\right| < \left(\frac{\delta}{w}\right)^{n+1}G(1)\binom{n}{n_1},$$

where A and B are integers and $A\neq 0$ by Lemmas 2 and 3. Let $x\in\boldsymbol{Z}$ and let p be a positive odd power of 2. Put $\varepsilon = |x/p^{1/2}-1|$. Adding this to

$$\left|1-\frac{181\,B}{w^{1/2}(4w)^{n_2-n_1}A}\right| < \frac{(4w)^{n_1}}{|A|}\left(\frac{\delta}{w}\right)^{n+1}G(1)\binom{n}{n_1},$$

we find

$$K \overset{\text{def}}{=} \left|\frac{x}{p^{1/2}}-\frac{181\,B}{w^{1/2}(4w)^{n_2-n_1}A}\right| < \varepsilon+\frac{(4w)^{n_1}}{|A|}\left(\frac{\delta}{w}\right)^{n+1}G(1)\binom{n}{n_1}. \tag{2}$$

Let $\lambda\in\boldsymbol{N}$ be such that $(4w)^{\lambda}\geqslant(p/w)^{1/2} > (4w)^{\lambda-1}$, and choose n_1, n_2 such that $\frac{2}{3}\lambda-\frac{2}{3}\leqslant n_1\leqslant\frac{2}{3}\lambda+1$, $n_2 = n_1+\lambda$. Notice that we have two choices for n_1. We choose n_1 such that the expression (2) for K is non-zero. This is possible, for if $K = 0$ for both choices of n_1, we would have $(GH^*-G^*H)(\delta/w) = 0$, where G, H correspond to one and G^*, H^* to the other choice of n_1. This is impossible in view of Lemma 4. Since p and w are odd powers of 2, and since $w^{1/2}(4w)^{n_2-n_1} = w^{1/2}(4w)^{\lambda}\geqslant p^{1/2}$ we have

$$\frac{1}{|A|w^{1/2}(4w)^{n_2-n_1}}\leqslant K < \varepsilon+\frac{(4w)^{n_1}}{|A|}\left(\frac{\delta}{w}\right)^{n+1}G(1)\binom{n}{n_1}.$$

Hence

$$1 < \varepsilon|A|w^{1/2}(4w)^{n_2-n_1}+w^{1/2}(4w)^{n_2}\left(\frac{\delta}{w}\right)^{n+1}G(1)\binom{n}{n_1}. \tag{3}$$

Assume $\lambda\geqslant 10$. Then $n_1\geqslant 6$ and by Lemma 2 we find that

$$G(1)\binom{n}{n_1} = \prod_{m=1}^{n_1}\left(1-\frac{1}{2m}\right)\leqslant\prod_{m=1}^{6}\left(1-\frac{1}{2m}\right) < \frac{1}{4}.$$

The second term on the right-hand side of (3) can be estimated by

$$\frac{1}{4}w^{1/2}(4w)^{n_2}\left(\frac{\delta}{w}\right)^{n+1} = \frac{1}{4}\frac{\delta}{w^{1/2}}\left(\frac{4\delta^2}{w}\right)^{n_1}(4\delta)^{\lambda},$$

and since $n_1 \geqslant \frac{2}{3}\lambda - \frac{2}{3}$ this is bounded by

$$\frac{1}{4}\frac{\delta}{w^{1/2}}\frac{w^{2/3}}{(2\delta)^{4/3}}\left(\frac{32\delta^{7/2}}{w}\right)^{2\lambda/3} < \frac{1}{2}.$$

The first term on the right-hand side of (3) can be estimated as follows. We have by Lemma 2 that

$$|A| = (4w)^{n_1}\binom{n}{n_1}G\left(\frac{\delta}{w}\right) < (4w)^{n_1}\binom{n}{n_1}.$$

Since $n = 2n_1+\lambda$, $n_1 \leqslant \frac{2}{3}\lambda+1$ and $\lambda \geqslant 10$ we easily see that $n > 3n_1$, so Lemma 5 can be applied. We now find

$$|A|w^{1/2}(4w)^{n_2-n_1} < \binom{n}{n_1}w^{1/2}(4w)^{\lambda+n_1} < \frac{1}{2}\left(\frac{3}{2^{2/3}}\right)^{2n_1+\lambda}w^{1/2}(4w)^{\lambda+n_1}$$
$$= \frac{w^{1/2}}{2}\left(\frac{12w}{2^{2/3}}\right)^{\lambda}\left(\frac{36w}{2^{4/3}}\right)^{n_1}$$

and since $n_1 \leqslant \frac{2}{3}\lambda+1$ this is bounded by

$$\frac{w^{1/2}}{2}\left\{\frac{3^{2/3}}{2^{14/9}}(12w)^{5/3}\right\}^{\lambda}\frac{36w}{2^{4/3}} < 2^{2.9}w^{3/2}(4w)^{1.8\lambda}.$$

We have chosen λ such that $(4w)^{\lambda} < 4w(p/w)^{1/2}$. Thus we find that the first term on the right-hand side of (3) is bounded by

$$2^{2.9}\varepsilon w^{3/2}(4w)^{1.8\lambda} < 2^{2.9}w^{3/2}(4w^{1/2})^{1.8}\varepsilon p^{0.9} < 2^{42.5}\varepsilon p^{0.9},$$

and finally inequality (3) becomes

$$1 < \varepsilon 2^{42.5}p^{0.9} + \tfrac{1}{2}.$$

Hence $\varepsilon > 2^{-43.5}p^{-0.9}$, and our theorem is proved for the case $\lambda \geqslant 10$. Now assume that $\lambda < 10$. Then $p \leqslant w(4w)^{2\lambda} \leqslant 2^{32.1}$. From $|x^2-p| \geqslant 1$ it follows that

$$\left|\frac{x}{p^{1/2}}-1\right| > \frac{1}{4p} = \frac{1}{4p^{0.1}}p^{-0.9} > \frac{1}{2^{34.1}}p^{-0.9},$$

which proves our theorem.

3. Consequences of Theorem 1. Let $D \in \mathbf{Z}$, $D \neq 0$.

COROLLARY 1. *If the equation $x^2-D = 2^n$ has a solution (x, n), then $n < 435+10(\log|D|/\log 2)$.*

Proof. If n is even then it follows that $|D| = |x^2-2^n| > 2^{n/2}$. Hence $n < 2\log|D|/\log 2$.

If n is odd, then by Theorem 1 we have

$$\left|\frac{x}{2^{n/2}}-1\right| > 2^{-43.5}2^{-0.9n}.$$

On the other hand, $x^2-D = 2^n$ implies $|x/2^{n/2}-1| < |D|2^{-n}$. These two inequalities imply $n < 435+10(\log|D|/\log 2)$.

COROLLARY 2. *If $|D| < 2^{96}$ and $x^2-D = 2^n$ has a solution (x, n), then*

$$n < 18+2\log|D|/\log 2.$$

Proof. We may assume that n is odd. If $|D| < 2^{96}$ then $n < 1395$ according to Corollary 1. Let $\sqrt{2} = \sum_{k=0}^{\infty}a_k2^{-k}$ with $a_k \in \{0, 1\}$ for all k. The values of a_k for $k \leqslant 700$ are given in the appendix. It follows from Table III that $|x-2^{n/2}| \geqslant 2^{-9}$ for $n < 1395$. Combining this estimate with $|x-2^{n/2}| < |D|/2^{n/2}$ we find $n < 18+2\log|D|/\log 2$.

4. THEOREM 2. *Let $D \in \mathbf{N}$ be odd. The equation $x^2+D = 2^n$ has two or more solutions in positive integers x, n if and only if $D = 7$, 23 or 2^k-1 for some $k \geqslant 4$. The solutions in these exceptional cases are given by*

(a) $D = 7$, $(x, n) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$,
(b) $D = 23$, $(x, n) = (3, 5), (45, 11)$,
(c) $D = 2^k-1$ $(k \geqslant 4)$, $(x, n) = (1, k), (2^{k-1}-1, 2k-2)$.

Proof. We first treat the case $D \not\equiv -1 \pmod 8$. Suppose there exist two solutions (y, l) and (z, m) say. Since y and z are odd, we have $1+D \equiv 2^l \pmod 8$ and $1+D \equiv 2^m \pmod 8$. Furthermore, $D \not\equiv -1 \pmod 8$ and hence $l, m < 3$. This implies $1+D \equiv 2^l \not\equiv 2^m \equiv D+1 \pmod 8$, which is a contradiction.

Now assume $D \equiv -1 \pmod 8$. Let e be the smallest positive integer such that $M^2+b^2D = 2^{2+e}$ for some positive integers M, b. The following fact is well known (see Hasse [6], pp. 83–85, Apéry [1]). If there exist integers x, r such that $x^2+D = 2^{2+r}$ then $b = 1$ and $e|r$. Moreover, for the Lucas-sequence given by $a_m = Ma_{m-1}-2^ea_{m-2}$, $a_1 = 1$, $a_0 = 0$ we have $|a_{r/e}| = 1$. Conversely, if there is an index m such that $|a_m| = 1$ then $x^2+D = 2^{2+me}$ for some $x \in \mathbf{N}$ and $D = 2^{2+e}-M^2$. We are going to search for all Lucas-sequences of the type $a_m = Ma_{m-1}-2^ea_{m-2}$, with $|a_m| = 1$ for some $m > 1$.

Assume $|a_m| = 1$ and $m \cdot e$ is even. This implies $x^2+D = 2^{2+me}$ for some $x \in \mathbf{N}$. Observe that $2^{2+e} > D = 2^{2+me}-x^2 > 2^{2+\frac{me}{2}}-1$ and hence $m \leqslant 2$. The solutions for the equation $x^2+D = 2^n$ yielded by $|a_1| = 1$ and $|a_2| = 1$ are $(x, n) = (1, 2+e)$ and $(2^{e+1}-1, 2+2e)$.

Assume $|a_m| = 1$ and $m \cdot e$ is odd. This implies $x^2+D = 2^{2+me}$ for some $x \in \mathbf{N}$. We distinguish two cases depending on whether D exceeds 2^{96} or not.

(I) $D < 2^{96}$. From Corollary 2 of Theorem 1 it follows that $2+me < 18+2\log D/\log 2$. Further $2^{2+e} = M^2+D$ implies $e \geqslant (\log D/\log 2)-2$. Hence, by $D \geqslant 7$,

$$m < 20\,\frac{\log 2}{\log(D/4)}+2 < 27.$$

$D = 7$ implies by definition $e = 1$, $M = 1$. The corresponding recurrent sequence is $a_m = a_{m-1}-2a_{m-2}$. For $m \leqslant 26$ the only values with $|a_m| = 1$ are given by $m = 1, 2, 3, 5, 13$. These values yield the solutions $(x, n) = (1, 3)$, $(3, 4)$, $(5, 5)$, $(11, 7)$, $(181, 15)$ for the equation $x^2+7 = 2^n$. $D = 15$ implies $e = 2$, but we have already dealt with the case e even. $D = 23$ implies $e = 3$, $M = 3$. Let $\{a_m\}$ be the corresponding Lucas-sequence. Then $|a_m| = 1$, $m \leqslant 26$ implies $m = 1, 3$ which yields the solutions $(x, n) = (3, 5)$, $(45, 11)$ for the equation $x^2+23 = 2^n$. $D = 31$ implies $e = 3$, $M = 1$. The corresponding equation $|a_m| = 1$, $m \leqslant 26$ implies $m = 1, 2$ which case we have already dealt with. Assume $D \geqslant 39$. Then $e \geqslant 4$ and, since e is odd, we have $e \geqslant 5$. $D \geqslant 39$ implies

$$m < 20\,\frac{\log 2}{\log(D/4)}+2 < 9$$

and hence $m \leqslant 7$. Since m is odd, we observe that $a_m \equiv 1 \pmod 4$. So $|a_m| = 1$ implies $a_m = 1$. We must check whether $a_3 = 1$, $a_5 = 1$ or $a_7 = 1$ is possible. $a_3 = 1$ implies $M^2-2^e = 1$. Hence $M = 3$, $e = 3$, contradicting $e \geqslant 5$. $a_3 = 1$ implies $M^2-2^e = 1$. Hence $M = 3$, $e = 3$, contradicting $e \geqslant 5$. $a_5 = 1$ implies $M^4-3M^2\,2^e+2^{2e} = 1$ or equivalently, $(M^2-3\cdot 2^{e-1})^2 = 1+5\cdot 2^{2e-2}$. A number of the shape $1+5\cdot 2^{2e-2}$ can only be a square if $2e-2 = 4$, i.e. $e = 3$, contradicting $e \geqslant 5$. $a_7 = 1$ implies $M^6-5M^4\cdot 2^e+6M^2\cdot 2^{2e}-2^{3e} = 1$, hence $M^6 \equiv 1 \pmod{2^e}$. This implies $M^2 \equiv 1 \pmod{2^e}$. Since $M^2+D = 2^{2+e}$, it also follows that $M^2 < 4\cdot 2^e$. Hence $M^2 = 1+\mu 2^e$ for some $0 \leqslant \mu \leqslant 3$. This can only occur if $\mu = 1$, $e = 3$ or $\mu = 3$, $e = 4$ both contradicting $e \geqslant 5$, and if $\mu = 0$, i.e. $M = 1$. If $M = 1$ however, $1-5\cdot 2^e+6\cdot 2^{2e}-2^{3e} = 1$ must have a solution, which is impossible.

(II) $D > 2^{96}$. From Corollary 1 of Theorem 1 it follows that $2+me < 435+10\log D/\log 2$. Together with $e \geqslant (\log D/\log 2)-2$ this implies

$$m < \frac{455}{\log(D/4)}\log 2+10 < 15.$$

Notice that $e \geqslant (\log D/\log 2)-2 > 94$.

It is obvious from the formula $a_m = Ma_{m-1}-2^e a_{m-2}$ that $a_m \equiv M^{m-1} \pmod{2^e}$. Hence $a_m = 1$ implies $M^{m-1} \equiv 1 \pmod{2^e}$. Put $m = 1+2^{t+1}\alpha$ for some odd α. Since $m < 15$ we may assume $t \leqslant 2$. By $M^{m-1} \equiv 1 \pmod{2^e}$ we have $M^2 \equiv 1 \pmod{2^{e-t}}$. Since $M^2 < 2^{2+e}$ we observe that $M^2 = 1+$

$+2^{e-t}\mu$ for some $0 \leqslant \mu < 2^{2+t} \leqslant 16$. Suppose $M = 1$. We can show by induction on m that $a_m \equiv 1-(m-2)2^e \pmod{2^{2e}}$ for all $m \geqslant 2$. So $a_m = 1$ implies $m-2 \equiv 0 \pmod{2^e}$, which contradicts the fact that m is odd. Hence we must assume $M > 1$. Put $M = \pm 1+\varrho\cdot 2^k$ for some $k \geqslant 2$, ϱ odd. Then $1 \pm \varrho\cdot 2^{k+1}+\varrho^2 2^{2k} = 1+\mu\cdot 2^{e-t}$ or equivalently $\varrho\cdot 2^{k+1}(\varrho\cdot 2^{k-1} \pm 1) = \mu\cdot 2^{e-t}$. We divide this equality by 2^{e-t} and obtain $\varrho(\varrho\cdot 2^{k-1} \pm 1) \leqslant \mu$. By $2^{e-t} | 2^{k+1}$ we have $k+1 \geqslant e-t > 92$. Since $\mu < 16$ and $k \geqslant 92$, we find $2^{91}-1 \leqslant \varrho(\varrho\cdot 2^{k-1} \pm 1) \leqslant \mu \leqslant 16$ which is impossible.

Collecting all solutions that we have found we obtain the assertion of Theorem 2.

5. The following lemmas are technical preparations for Theorem 3.

LEMMA 6. *Let $D > 0$, $D \equiv 1 \pmod 8$, D not a square. Suppose there exist positive integers x, y, z, k, l, m such that $x^2-D = 2^k$, $y^2-D = 2^l$, $z^2-D = 2^m$, $m > l > k \geqslant 1$ and $y-x \geqslant 6$. Then either*

(a) $m-2l = 1$ *and*

$$(x, y, z, k, l, m) = \left(\frac{2^{l-2}-17}{3}, \frac{2^{l-2}+1}{3}, \frac{17\cdot 2^{l-2}-1}{3}, 5, l, 2l+1\right)$$

or

(b) $m-2l \geqslant 51$.

Proof. We may assume that $k \geqslant 3$. Notice that $2^l \geqslant y^2-x^2+8 \geqslant 12x+44 > 12\sqrt{8+D}+44$ and since $D \geqslant 17$, this implies $l \geqslant 7$. Suppose $l = 7$. Then it follows from $2^l > 12\sqrt{8+D}+44$ that $D \leqslant 41$. The only value of D such that $D \equiv 1 \pmod 8$, $D \leqslant 41$ and $D+2^7$ is a square, is $D = 41$. It is easily checked by Tables II and III that $z^2-41 = 2^m$ with $7 < m < 65$ has no solutions. From now on we may assume that $l \geqslant 8$.

Note that x, y and z are odd and that

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

Notice that 2^{k-2} divides either $(y-x)/2$ or $(y+x)/2$ and that 2^{l-2} divides either $(z-y)/2$ or $(z+y)/2$. Put $(y-x)/2 = u$, $(y+x)/2 = v$ and $(z-y)/2 = \alpha\cdot 2^{l-2}$ if $z \equiv y \pmod 4$, $(z+y)/2 = \alpha\cdot 2^{l-2}$ if $z \equiv -y \pmod 4$. Thus we obtain

$$uv = 2^{l-2}-2^{k-2} \quad \text{and} \quad \alpha\big(\alpha\cdot 2^{l-2}+\varepsilon(u+v)\big) = 2^{m-l}-1,$$

where $\varepsilon \in \{-1, 1\}$ is determined by $z \equiv \varepsilon y \pmod 4$. Notice that

$(u-3)(v-3) \geqslant 0$, since $v > u \geqslant 3$ and hence $u+v \leqslant \frac{1}{3}uv+3 = \frac{1}{3}(2^{l-2}-2^{k-2})+3 \leqslant \frac{1}{3}(2^{l-2}+7)$. It follows from (4) that a is odd and

$$\varepsilon(u+v) = \frac{2^{m-l}-1}{a} - a\cdot 2^{l-2} = \frac{(2^r-a^2)2^{l-2}-1}{a}, \tag{5}$$

where we have put $r = m-2l+2$. Using $u+v \leqslant \frac{1}{3}(2^{l-2}+7)$ it follows from (5) that

$$|a^2-2^r| \leqslant \frac{a}{3}(1+7\cdot 2^{2-l})+2^{2-l} \leqslant \frac{a}{3}\left(1+\frac{7}{64}\right)+\frac{1}{64}.$$

It is easily seen that $r > 0$ and $|a-2^{r/2}| < \frac{1}{2}$. Hence a is uniquely determined by r and r must be odd. Furthermore we find, on using $l \geqslant 8$, that

$$\left|\frac{a^2-2^r}{a}\right| < 0.373 \quad \text{if} \quad a \geqslant 5. \tag{6}$$

Suppose $r = 1$. Then $a = 1$ and $u+v = 2^{l-2}-1$. Together with $uv = 2^{l-2}-2^{k-2}$ this implies $u = 1$, $v = 2^{l-2}-2$ which contradicts the assumption $u \geqslant 3$. Suppose $r = 3$. Then $a = 3$ and $u+v = (2^{l-2}+1)/3$. Together with $uv = 2^{l-2}-2^{k-2}$ this implies $(u-3)(v-3) = -2^{k-2}+8$. Since $v > u \geqslant 3$ and $l \geqslant 8$ it easily follows from these equations that $u = 3$, $v = (2^{l-2}-8)/3$, $k = 5$. Hence $x = v-u = (2^{l-2}-17)/3$, $y = u+v = (2^{l-2}+1)/3$ and finally $z = (17\cdot 2^{l-2}-1)/3$. This is precisely case (a).

Assume $r \geqslant 5$. Then $a \geqslant 5$ and inequality (6) holds. An inspection of Table II shows that (6) implies $r = 15$ or 31 or $r \geqslant 53$. Next we prove that $r \neq 15, 31$. Since $v > u$ we find that $u(u+v) < 2uv \leqslant 2(2^{l-2}-2)$. Combining this with

$$|u+v| = |(2^r-a^2)2^{l-2}-1|/a \geqslant (|2^r-a^2|2^{l-2}-1)/a$$

we conclude that

$$u \leqslant \frac{2(2^{l-2}-2)}{|2^r-a^2|2^{l-2}-1}a < \frac{2a}{|2^r-a^2|}. \tag{7}$$

Eliminate v from (4) and (5). Then we find after rearranging terms that

$$\big(\varepsilon(2^r-a^2)u-a\big)2^{l-2} = u(au+\varepsilon)-a\cdot 2^{k-2}.$$

Notice that 2^{k-2} divides either u or $au+\varepsilon$ and hence $2^{k-2} \leqslant au+1$. Thus we find

$$|\varepsilon(2^r-a^2)u-a|2^{l-2} \leqslant \max\big(u(au+\varepsilon),\, a\cdot 2^{k-2}\big) \leqslant (au+1)\max(a,u). \tag{8}$$

Suppose $r = 15$. Then $a = 181$, $|a^2-2^r| = 7$. By (7) we find $u < 52$ and by (8) $2^{l-2} < 2^{2l}$. Hence $l \leqslant 22$. From (5) we see that a divides $2^{m-l}-1$ $= 2^{l+13}-1$ and this is impossible if $l \leqslant 22$. Suppose $r = 31$. Then $a = 46341$, $|a^2-2^r| = 4633$. By (7) we find $u < 21$ and by (8) $2^{l-2} < 2^{36}$. Hence $l \leqslant 37$. From (5) we see that 46341 divides $2^{l+29}-1$ and this is impossible if $l \leqslant 37$. We have shown that the assumption $r \geqslant 5$ leads to $r \geqslant 53$, as asserted.

LEMMA 7. *Let $d \in \boldsymbol{N}$ be square-free and $d \equiv 1 \pmod 8$, $d > 1$. Suppose there exist integers $a, A, B, p, q \neq 0$ such that*

$$\frac{A+B\sqrt{d}}{2} = \left(\frac{p+qB\sqrt{d}}{2}\right)^a, \qquad a > 1, \qquad p \equiv qB \pmod 2.$$

Then $a = 2$ and $p, q \in \{-1, 1\}$.

Proof. Without loss of generality we may assume that $p, qB \in \boldsymbol{N}$. If a is odd then

$$\frac{B\sqrt{d}}{2} > \left(\frac{qB\sqrt{d}}{2}\right)^a \geqslant \left(\frac{B\sqrt{d}}{2}\right)^{a-1}\frac{B\sqrt{d}}{2} > \frac{B\sqrt{d}}{2},$$

which is a contradiction. Suppose $a = 4$, then $B = \frac{1}{2}(p^3q+pq^3B^2d)B$, which is impossible. Since every integer $a > 2$ is divisible by an odd prime or by 4, we are left with the case $a = 2$. This implies $B = pqB$ and hence $|p| = |q| = 1$, as asserted.

LEMMA 8. *Let $D > 0$, $D \equiv 1 \pmod 8$, D not a square. If $A'^2-D = 2^{n'}$, $A^2-D = 2^n$ for some A, A', n, n' and $n > n'$, $2^{n'} > 49D$ then*

$$n > \frac{1}{8.8}\frac{\log D}{\log 2}\left(\frac{2^{n'}}{D}\right)^{1/2}.$$

Proof. Choose $B \in \boldsymbol{N}$ such that $D = B^2d$ and d is square-free. Since D is not a square we have $d \neq 1$. Factorise $A^2-B^2d = 2^n$ in $\boldsymbol{Q}(\sqrt{d})$ to obtain $\frac{A-B\sqrt{d}}{2}\cdot\frac{A+B\sqrt{d}}{2} = 2^{n-2}$. Hence $\big((A+B\sqrt{d})/2\big) = \mathfrak{a}^{n-2}$ for some ideal $\mathfrak{a}$ dividing 2. According to the theory of algebraic integers it is possible to find a positive integer e such that

1) $\mathfrak{a}^e = \left(\frac{\alpha+\beta\sqrt{d}}{2}\right)$ for some $\alpha, \beta \in \boldsymbol{Z}$ with $B|\beta$,

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

This implies $\big((A+B\sqrt{d})/2\big) = \big((\alpha+\beta\sqrt{d})/2\big)^{(n-2)/e}$ in ideal notation. Hence $(A+B\sqrt{d})/2 = \pm\varepsilon\sigma^{(n-2)/e}$ where ε is a unit in $\boldsymbol{Q}(\sqrt{d})$ and $\sigma = (\alpha+\beta\sqrt{d})/2$. Notice that ε can be written in the shape $\varepsilon = (\varepsilon_1+\varepsilon_2\sqrt{d})/2$ with $B|\varepsilon_2$. Units which can be written in this shape form a cyclic group (mod $\pm$sign) with generator ν say.

Hence

$$\frac{A+B\sqrt{d}}{2} = \pm\nu^r\sigma^{(n-2)/e} \quad \text{for some } r\in\mathbf{Z}. \tag{9}$$

Let $\tilde\nu$, $\tilde\sigma$ be the conjugate of ν, σ respectively. Then (9) implies

$$|B\sqrt{d}| = |\sqrt{D}| = |\nu^r\sigma^{(n-2)/e} - \tilde\nu^r\tilde\sigma^{(n-2)/e}|. \tag{10}$$

Furthermore,

$$|\nu^r\sigma^{(n-2)/e}| = |A+B\sqrt{d}|/2 = |A|/2 \pm \sqrt{D}/2 = \tfrac{1}{2}(\sqrt{D+2^n}\pm\sqrt{D}) > \tfrac{3}{7}\cdot 2^{n/2}.$$

Divide expression (10) by $|\nu^r\sigma^{(n-2)/e}|$, then

$$\frac{7}{3}\left(\frac{D}{2^n}\right)^{1/2} > \left|\left(\frac{\tilde\nu}{\nu}\right)^r\left(\frac{\tilde\sigma}{\sigma}\right)^{(n-2)/e} - 1\right|.$$

It is easy to see that if $|x-1|<\delta<\frac{1}{3}$ then $|\log x|<1.22\,\delta$. Since $2^n > 2^{n'} > 49D$ implies $\frac{7}{3}(D/2^n)^{1/2} < \frac{1}{3}$ we can apply this inequality and obtain

$$\left| -r\log\left|\frac{\nu}{\tilde\nu}\right| + \frac{n-2}{e}\log\left|\frac{\tilde\sigma}{\sigma}\right|\right| < 2.85\left(\frac{D}{2^n}\right)^{1/2}. \tag{11}$$

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

$$\left| -r'\log\left|\frac{\nu}{\tilde\nu}\right| + \frac{n'-2}{e}\log\left|\frac{\tilde\sigma}{\sigma}\right|\right| < 2.85\left(\frac{D}{2^{n'}}\right)^{1/2}. \tag{12}$$

Suppose $r/(n-2) = r'/(n'-2)$. Let $\alpha = (r', n'-2/e)$, $\beta = (r, n-2/e)$ where (a,b) denotes the largest common divisor of a and b. Suppose $\beta > 2$. Using (9) we find that there exist integers p, q such that $(A+B\sqrt{d})/2 = [(p+qB\sqrt{d})/2]^\beta$ and this contradicts $\beta>2$ by Lemma 7. Suppose $\beta = 2$, then we have $\alpha = 1$, since $\beta > \alpha$. Hence $(A'+B'\sqrt{d})/2 = \pm\big((A+B\sqrt{d})/2\big)^2$ and this implies $A = \pm 1$ by Lemma 7, which is impossible. We conclude that $r/(n-2) \neq r'/(n'-2)$. Eliminate $\log|\tilde\sigma/\sigma|$ from the inequalities (11) and (12). Let $u = |\log|\tilde\nu/\nu||$, then we obtain

$$\frac{1}{(n-2)(n'-2)} \leqslant \left|\frac{r'}{n'-2} - \frac{r}{n-2}\right| < \frac{2.85}{u}\left(\frac{1}{n-2}\left(\frac{D}{2^n}\right)^{1/2} + \frac{1}{n'-2}\left(\frac{D}{2^{n'}}\right)^{1/2}\right) < \frac{5.7}{n'-2}\,\frac{1}{u}\left(\frac{D}{2^{n'}}\right)^{1/2}.$$

Hence

$$n-2 > \frac{u}{5.7}\left(\frac{2^{n'}}{D}\right)^{1/2} > \frac{1}{8.35}\,\frac{u}{\log 2}\left(\frac{2^{n'}}{D}\right)^{1/2}.$$

We determine a lower bound for u as follows. Let $\nu = (\xi+\eta\sqrt{d})/2$ with $B|\eta$. Since ν is a unit, we have $\xi^2-\eta^2 d = \pm 4$. By separating the cases $\xi\eta>0$ and $\xi\eta<0$ we easily calculate that $u = \big|\log|\nu/\tilde\nu|\big| = 2\log\big(\frac{1}{2}(|\xi|+|\eta|\sqrt{d})\big)$. Using the facts $|\xi| = \sqrt{\eta^2 d\pm 4}$ and that $\log\big(\frac{1}{2}(x+\sqrt{x^2-4})\big)/\log x$ is monotonically increasing for $x>2$ and that $D\geqslant 17$, we find that

$$u = 2\log\frac{|\xi|+|\eta|\sqrt{d}}{2} = 2\log\frac{\sqrt{\eta^2 d\pm 4}+|\eta|\sqrt{d}}{2} \geqslant 2\log\frac{\sqrt{D-4}+\sqrt{D}}{2}$$

$$\geqslant \frac{\log\big(\frac{1}{2}(\sqrt{13}+\sqrt{17})\big)}{\log\sqrt{17}}\log D > \frac{\log D}{1.05}.$$

Together with the lower bound for n this estimate for u yields our lemma.

6. The equation $x^2 - D = 2^n$, $D>0$. Before proceeding we note the following peculiarities.

(I) If $D = 2^{2k} - 3\cdot 2^{k+1}+1$ for some $k\geqslant 3$ then $(x,n) = (2^k-3,3)$, $(2^k-1, k+2)$, $(2^k+1, k+3)$, $(3\cdot 2^k-1, 2k+3)$ are solutions of the equation $x^2-D = 2^n$.

(II) If $D = 2^{2l}+2^{2k}-2^{k+l}-2^{k+1}-2^{l+1}+1$ for some $k>1$, $l>k+1$, then $(x,n) = (2^l-2^k-1, k+2)$, $(2^l-2^k+1, l+2)$, $(2^k+2^l-1, k+l+2)$ are solutions of $x^2-D = 2^n$.

(III) If $D = \left(\frac{2^{l-2}-17}{3}\right)^2 - 32$ for some odd $l\geqslant 9$, then $(x,n) = \left(\frac{2^{l-2}-17}{3}, 5\right)$, $\left(\frac{2^{l-2}+1}{3}, l\right)$ and $\left(\frac{17\cdot 2^{l-2}-1}{3}, 2l+1\right)$ are solutions of $x^2-D = 2^n$.

We shall refer to these equations as type **I**, **II** or **III** equations respectively. It is easily checked that a given equation cannot belong to more than one type. Note that for type I equations we have required $k\geqslant 3$ in order to make D positive. If we insert $k=2$ then we find $D=-7$ and the corresponding solutions are $(x,n) = (1,3)$, $(3,4)$, $(5,5)$, $(11,7)$. Insert $k=1$, then $D=-7$ and the solutions are $(x,n) = (-1,3)$, $(1,3)$, $(3,4)$ and $(5,5)$. We can do similarly for type III equations. Insert $l=7$, then $D=-7$ and $(x,n) = (5,5)$, $(11,7)$, $(181,15)$. Insert $l=5$, then $D=-23$ and $(x,n) = (-3,5)$, $(3,5)$, $(45,11)$. Insert $l=3$ then $D=-7$ and $(x,n) = (-5,5)$, $(1,3)$, $(11,7)$. Collecting these solutions we see that we have obtained all solutions of the equations $x^2+7 = 2^n$ and $x^2+23 = 2^n$ (see Theorem 2). One might consider this as an explanation for the occurrence of these two exceptional cases in Theorem 2.

THEOREM 3. *Let $D \in \mathbf{N}$ be odd. Consider the equation $x^2 - D = 2^n$ in positive integers. Then a type* I, II, III *equation has at most* 5, 4, 4 *solutions respectively. All other equations have at most* 3 *solutions. If $D < 10^{12}$ then a type* I, II, III *equation has exactly* 4, 3, 3 *solutions respectively. All other equations with $D < 10^{12}$ have at most* 2 *solutions.*

Proof. We first deal with the cases D a square and $D \not\equiv 1 \pmod 8$. Suppose $D = d^2$ for some $d \in \mathbf{N}$. Then $x^2 - d^2 = 2^n$ implies $\frac{1}{2}(x-d)\frac{1}{2}(x+d) = 2^{n-2}$. Since $(x-d)/2$ and $(x+d)/2$ are relatively prime we conclude $(x-d)/2 = 1$, $(x+d)/2 = 2^{n-2}$ and hence $d = 2^{n-2}-1$. It follows that there is at most one solution. Suppose $D \not\equiv 1 \pmod 8$. Since x is odd we have $x^2 \equiv 1 \pmod 8$. Hence $2^n \equiv 1 - D \not\equiv 0 \pmod 8$ and $n \leqslant 2$. One easily observes that the equation $x^2 - D = 2^n$ cannot have two solutions with $n \leqslant 2$.

From now on we assume that D is not a square and $D \equiv 1 \pmod 8$. Let x, n be the largest solution and x', n' the second largest. According to Corollary 1 of Theorem 1 we have $n < 435 + 10\log D/\log 2$. If $2^{n'} > 49D$ we can apply Lemma 8 to obtain an upper bound for n',

$$\frac{1}{8.8}\left(\frac{2^{n'}}{D}\right)^{1/2}\frac{\log D}{\log 2} < n < 435 + 10\frac{\log D}{\log 2}.$$

Hence

$$2^{n'} \leqslant \max\left\{\left(8.8\left(435\,\frac{\log 2}{\log D} + 10\right)\right)^2 D,\ 49D\right\},$$

and since $D \geqslant 17$ we find $2^{n'} < 2 \cdot 10^6 D$. Hence

$$n' < 21 + \frac{\log D}{\log 2}. \tag{13}$$

If $D < 2^{96}$ we know from Corollary 2 of Theorem 1 that

$$n < 18 + 2\frac{\log D}{\log 2}. \tag{14}$$

We first prove the theorem for type I, II and III equations. Suppose there is a fifth solution (z, m) for a given type I equation. It easily follows from Lemma 6 that $m > 2k+3$. Applying Lemma 6 to the solutions $(2^k+1, k+3)$, $(3\cdot 2^k - 1, 2k+3)$, (z, m) we find that $m \geqslant 51 + 2(2k+3) > 57 + 2\log D/\log 2$. Using (13) we see that (z, m) must be the largest solution. Hence there are at most 5 solutions. If $D < 10^{12}$ then by (14) the solution (z, m) cannot exist at all. Suppose there is a fourth solution (z, m) for a given type II or III equation. In case we have a type II equation, application of Lemma 6 gives $m \geqslant 51 + 2(k+l+2)$. Since

$$D = (2^k + 2^l - 1)^2 - 2^{k+l+2} < (2^k + 2^l)^2 - 2^{k+l+2} = (2^l - 2^k)^2 < 2^{2(l+k+2)-8}$$

we obtain $m \geqslant 51 + 2(k+l+2) > 59 + \log D/\log 2$. In case we have a type III equation, application of Lemma 6 gives $m \geqslant 51 + 2(2l+1) > 51 + 2\log D/\log 2$. Using (13) we see that (z, m) must in both cases be the largest solution. Hence there are at most 4 solutions. If $D < 10^{12}$, then by (14) the solution (z, m) cannot exist.

Assume that the equation $x^2 - D = 2^n$ does not belong to type I, II or III and suppose that there exist at least 3 solutions (x, k), (y, l), (z, m) with $m > l > k \geqslant 1$. Suppose $y - x = 2$. Then $y^2 - x^2 = 2^l - 2^k$ implies $4(x+1) = 2^l - 2^k$ and hence $x = 2^{l-2} - 2^{k-2} - 1$ and $D = x^2 - 2^k = 2^{2l-4} + 2^{2k-4} - 2^{k+l-3} - 2^{l-1} - 2^{k-1} + 1$. This yields either a type I equation (if $k = 3$) or a type II equation, contradicting our assumptions.

Suppose $y - x = 4$. Then $y^2 - x^2 = 2^l - 2^k$ implies $8(x+2) = 2^l - 2^k$ and hence $x + 2 = 2^{l-3} - 2^{k-3}$. Since x is odd, k must be three, so $x = 2^{l-3} - 3$ and $D = x^2 - 2^3 = 2^{2(l-3)} - 3\cdot 2^{l-2} + 1$. This yields a type I equation, contradicting our assumptions.

We therefore conclude that $y - x \geqslant 6$. Applying Lemma 6 we find that $m \geqslant 51 + 2l$. Furthermore $2^l > y^2 - x^2 > 12x > 12D^{1/2}$ and hence $l > \log 12D^{1/2}/\log 2$. Thus $m \geqslant 51 + \log 144/\log 2 + \log D/\log 2 > 58 + \log D/\log 2$.

Using (13) we see that (z, m) is the largest solution. Hence there are at most three solutions.

If $D < 10^{12}$ then it follows from (14) that the solution (z, m) cannot exist.

THEOREM 4. *Let $D \in \mathbf{N}$ be odd. The equation $x^2 - D = 2^n$ has at most four solutions in positive integers x, n.*

Proof. By Theorem 3 it suffices to prove that a type I equation has at most four solutions. Assume $D = 1 - 3\cdot 2^{k+1} + 2^{2k}$ for some $k \geqslant 3$. The functions $\sqrt{1 + z^2 - 6z}$ can be written as a power series in z with integer coefficients. This can be seen as follows. Write

$$\sqrt{1 + z^2 - 6z} = \sqrt{1 + z^2 - 2z - 4z} = (1-z)\sqrt{1 - 4\frac{z}{(1-z)^2}}.$$

Since both $z/(1-z)^2 = z + 2z^2 + \ldots$ and $\sqrt{1-4t} = 1 - 2t + \ldots$ are power series with integer coefficients, our assertion follows. Furthermore $\sqrt{1 + z^2 - 6z} = \sum_{r=0}^{\infty} a_r z^r$ is an analytic function in the complex plane with the

real cut $[3-2\sqrt{2}, 3+2\sqrt{2}]$ deleted. This function can be chosen to ha value 1 for $z=0$. For $0<\varrho<3-2\sqrt{2}$ we have

$$a_r = \frac{1}{2\pi i}\int_{|z|=\varrho} \frac{\sqrt{1+z^2-6z}}{z^{r+1}}\,dz.$$

Write this integral as the sum of an integral over $|z|=M$, $M>3+2$ and an integral over a contour surrounding the cut $[3-2\sqrt{2}, 3+2\sqrt$ If $r\geqslant 2$, the contribution of the integral over $|z|=M$ is zero as we by letting M tend to infinity. By substituting $t=z-3$ we obtain

$$a_r = \frac{1}{\pi}\int_{-2\sqrt{2}}^{2\sqrt{2}} \frac{dt}{(t+3)^{r+1}}\sqrt{8-t^2} \qquad (r\geqslant 2).$$

Observe that $a_r<0$ for all $r\geqslant 2$ and

(15)
$$0<|a_r|<\frac{2\sqrt{2}}{\pi}\int_{-2\sqrt{2}}^{2\sqrt{2}}\frac{dt}{(t+3)^{r+1}}<\frac{2\sqrt{2}}{\pi}\,\frac{1}{r}\left(\frac{1}{3-2\sqrt{2}}\right)^r<\frac{6^r}{r}\leqslant\frac{1}{2}\cdot 6^r \quad (r\geqslant$$

Since $D=1-3\cdot 2^{k+1}+2^{2k}$, $\sqrt{D}$ can be written as the 2-adic series $\sqrt$ $=\sum_{r=0}^{\infty} a_r 2^{rk}$. We know that the equation $x^2-D=2^n$ has at least f solutions. Suppose there is a fifth solution (x,n). By Lemma 6 we ha $n\geqslant 51+2(2k+3)=4k+57$. Choose the sign of x such that $x\equiv 1 \pmod$ Then $x^2-D=2^n$ implies $x\equiv\sqrt{D}\pmod{2^{n-1}}$ and hence

$$x\equiv\sum_{r=0}^{\infty} a_r 2^{kr}\pmod{2^{n-1}}. \tag{16}$$

Furthermore, $x^2-D=2^n$ implies $|x|<2^{(n+1)/2}$ since $n\geqslant 4k+57$. Suppo $n\leqslant 6k$. Since $a_1=-3$, $a_2=-4$, $a_3=-12$ we find that $x\equiv 1-3\cdot 2^k -4\cdot 2^{2k} \pmod{2^{3k+2}}$. Since $|x|<2^{(n+1)/2}\leqslant 2^{3k+4}$ and $|1-3\cdot 2^k-4\cdot 2$ $<2^{2k+3}$ the latter congruence implies $x=1-3\cdot 2^k-4\cdot 2^{2k}$. This is impo ible because x^2-D cannot be a power of 2 for this value of x. We n assume $n\geqslant 6k+1$. Put $R=[(n+1)/2k]+1$. Observe that $(R+2$ $<(n+1)/2+3k\leqslant n$. It follows from congruence (16) that

$$x\equiv\sum_{r=0}^{R} a_r 2^{rk}\pmod{2^{(R+1)k}}. \tag{17}$$

Suppose $6^R<2^{k-2}$. By (15) we have $|a_r|\leqslant\frac{1}{2}\cdot 6^r$ and hence

$$\left|\sum_{r=0}^{R} a_r 2^{rk}\right|<1+\frac{1}{2}\sum_{r=1}^{R}(6\cdot 2^k)^r<(6\cdot 2^k)^R<\frac{1}{2}\cdot 2^{k(R+1)}.$$

Since we also have $|x|<2^{(n+1)/2}<2^{Rk}<\frac{1}{2}\cdot 2^{k(R+1)}$, congruence (17) implies $x=\sum_{r=0}^{R} a_r 2^{rk}$. However it also follows from congruence (16) that

$$x\equiv\sum_{r=0}^{R+1} a_r 2^{kr}\pmod{2^{k(R+2)}}.$$

Together with $x=\sum_{r=0}^{R} a_r 2^{rk}$ this congruence implies $2^k\mid a_{R+1}$. Since $a_{R+1}\neq 0$ and $|a_{R+1}|<\frac{1}{2}\cdot 6^{R+1}$ by (15), we observe that $\frac{1}{2}\cdot 6^{R+1}>|a_{R+1}|\geqslant 2^k$, contradicting $6^R<2^{k-2}$.

We therefore conclude that $6^R\geqslant 2^{k-2}$ and hence $k-2\leqslant R\log 6/\log 2$ $<2.6(1+(n+1)/2k)$. From Corollary 1 of Theorem 1 it follows that $n<435+10\log D/\log 2<435+20k$ and hence

$$k-2<\left(10+1+\frac{218}{k}\right)\cdot(2.6)<29+\frac{567}{k},$$

which implies $k\leqslant 45$ and hence $D<2^{90}$. Application of Corollary 2 of Theorem 1 yields $n<18+2\log D/\log 2<18+4k$, which contradicts $n\geqslant 4k+57$. Hence there exists no fifth solution.

7. All previous results depend on Theorem 1. It is possible to give an analogue of Theorem 1 for other powers than binary powers.

THEOREM 5. *Let N be some positive integer which is not a square. Suppose we can find an integer Δ and an odd power w of N such that $x^2+\Delta=w$ for some $x\in\mathbf{N}$ and $w>\max(2^{\frac{5}{2}(2-e)}|\Delta|^{\frac{7}{2}}, 2^{17-5e})$, where $e=0$ if Δ is odd, $e=1$ if $2\|\Delta$, $e=2$ if $4\mid\Delta$. Put*

$$\nu=\frac{5}{6}+\frac{1}{6}(17-5e)\frac{\log 2}{\log w}.$$

Then

$$\left|\frac{y}{p^{1/2}}-1\right|>\frac{1}{16}w^{-3}p^{-\nu}$$

for every odd power p of N and every $y\in\mathbf{N}$.

Remark. A few values of Δ and w that satisfy the assumptions of Theorem 5 are the following, $(\Delta,w)=(-37,3^{15})$ $(-26,23^5)$ $(-8,46^3)$ $(19,55^5)$ and $(60,76^5)$. In this paper we will not work out the applications of Theorem 5. They can be obtained by the arguments given in the previous sections.

Proof of Theorem 5. We use the hypergeometric polynomials G and H defined in Lemma 1. Since $n \geqslant 2n_1$, we may notice that

$$|G(z)| = \left| \sum_{k=0}^{n_1} \binom{n_2+\frac{1}{2}}{k} \frac{n_1(n_1-1)\dots(n_1-k+1)}{n(n-1)\dots(n-k+1)} (-z)^k \right| < \sum_{k=0}^{n_1} \binom{n_2+1}{k} \left|\frac{z}{2}\right|^k < \left(1+\frac{|z|}{2}\right)^{n_2+1} \tag{18}$$

for all $z \in \mathbb{C}$. From Lemma 2 we know that

$$\binom{n}{n_1} \left| G\left(\frac{\Delta}{w}\right) - \frac{x}{w^{1/2}} H\left(\frac{\Delta}{w}\right) \right| < \left|\frac{\Delta}{w}\right|^{n+1} G(1) \binom{n}{n_1}. \tag{19}$$

On using Lemma 3 and inequality (18) we observe that $\binom{n}{n_1} G(\Delta/w) = A/(2^{2-e}w)^{n_1}$ in which $A \in \mathbb{Z}$ and

$$0 < |A| < (2^{2-e}w)^{n_1} \binom{n}{n_1} \left(1+\frac{|\Delta|}{2w}\right)^{n_2+1}. \tag{20}$$

Furthermore, put $\binom{n}{n_1} H(\Delta/w) = B/(2^{2-e}w)^{n_2}$. Then $B \in \mathbb{Z}$ by Lemma 3. Inequality (19) implies

$$\left| 1 - \frac{x}{w^{1/2}} \frac{B}{A} \frac{1}{(2^{2-e}w)^{n_2-n_1}} \right| < \frac{(2^{2-e}w)^{n_1}}{|A|} \left|\frac{\Delta}{w}\right|^{n+1} \binom{n}{n_1} G(1). \tag{21}$$

Let p be some odd power of N and $y \in \mathbb{N}$ arbitrary. Put $\varepsilon = |y/p^{1/2} - 1|$. Combining this with (2) we obtain

$$K \overset{\text{def}}{=} \left| \frac{y}{p^{1/2}} - \frac{x}{w^{1/2}} \frac{B}{A} \frac{1}{(2^{2-e}w)^{n_2-n_1}} \right| < \varepsilon + \frac{(2^{2-e}w)^{n_1}}{|A|} \left|\frac{\Delta}{w}\right|^{n+1} \binom{n}{n_1} G(1). \tag{22}$$

Let $\lambda \in \mathbb{N}$ be such that $w^\lambda \geqslant (p/w)^{1/2} > w^{\lambda-1}$ and choose n_1, n_2 such that $\frac{2}{3}\lambda - \frac{1}{3} \leqslant n_1 \leqslant \frac{2}{3}\lambda + \frac{4}{3}$ and $n_2 = n_1 + \lambda$. Notice that we have two choices for n_1. We choose n_1 such that expression (22) for K is non-zero. This is possible, for if $K = 0$ for both choices of n_1, we would have $(GH^* - G^*H) \times (\Delta/w) = 0$ where G, H correspond to one and G^*, H^* to the other choice of n_1. This is impossible in view of Lemma 4. Since p and w are odd powers of N and $w^{1/2} w^{n_2-n_1} = w^{\lambda+1/2} \geqslant p^{1/2}$ we have

$$\frac{1}{|A| w^{1/2} (2^{2-e}w)^{n_2-n_1}} \leqslant K < \varepsilon + \frac{(2^{2-e}w)^{n_1}}{|A|} \left|\frac{\Delta}{w}\right|^{n+1} \binom{n}{n_1} G(1).$$

Hence

$$1 < \varepsilon |A| w^{1/2} (2^{2-e}w)^{n_2-n_1} + w^{1/2} (2^{2-e}w)^{n_2} \left|\frac{\Delta}{w}\right|^{n+1} \binom{n}{n_1} G(1). \tag{23}$$

Assume $\lambda \geqslant 9$. Then $n_1 \geqslant 6$ and by Lemma 2 we find that

$$G(1) \binom{n}{n_1} = \prod_{m=1}^{n_1} \left(1 - \frac{1}{2m}\right) \leqslant \prod_{m=1}^{6} \left(1 - \frac{1}{2m}\right) < \frac{1}{4}.$$

The second term on the right-hand side of (23) can be estimated by

$$\tfrac{1}{4} w^{1/2} (2^{2-e}w)^{n_2} \left(\frac{\Delta}{w}\right)^{n+1} = \tfrac{1}{4} \frac{\Delta}{w^{1/2}} \left(\frac{2^{2-e}\Delta^2}{w}\right)^{n_1} (2^{2-e}\Delta)^\lambda,$$

and since $n_1 \geqslant \frac{2}{3}\lambda - \frac{1}{3}$, this is bounded by

$$\tfrac{1}{4} \frac{|\Delta|}{w^{1/2}} \left(\frac{w}{2^{2-e}\Delta^2}\right)^{1/3} (2^{\frac{5}{2}(2-e)} |\Delta|^{7/2}/w)^{2\lambda/3} < \tfrac{1}{4} (|\Delta|/2^{2-e} w^{1/2})^{1/3} < \tfrac{1}{4}.$$

Since $n = 2n_1 + \lambda$, $n_1 \leqslant \frac{2}{3}\lambda + \frac{4}{3}$ and $\lambda \geqslant 9$, we see that $n > 3n_1$. So Lemma 5 can be applied, which yields $\binom{n}{n_1} < \frac{1}{2} \cdot 2^{0.92n}$. From $w > \max\{|\Delta|^{7/2}, 2^7\}$ it follows that $|\Delta/w| < \min\{|\Delta|^{-5/2}, |\Delta| 2^{-7}\} \leqslant 2^{-5}$. Combining these estimates we find $\binom{n}{n_1} (1 + |\Delta/2w|)^{n_2+1} < 2^{n-1}$ and by inequality (20),

$$|A| < (2^{2-e}w)^{n_1} 2^{n-1}.$$

The first term on the right-hand side of (23) can now be estimated as follows,

$$\varepsilon |A| w^{1/2} (2^{2-e}w)^{n_2-n_1} < \frac{\varepsilon}{2} 2^n w^{1/2} (2^{2-e}w)^{n_2}.$$

Since $n_1 \geqslant \frac{2}{3}\lambda + \frac{4}{3}$, we find

$$\varepsilon |A| w^{1/2} (2^{2-e}w)^{n_2-n_1} < \frac{\varepsilon}{2} (2^{4-e}w)^{4/3} w^{1/2} 2^{7\lambda/3} (2^{2-e}w)^{5\lambda/3}.$$

By the definition of ν we have $2^{7/3} (2^{2-e}w)^{5/3} = w^{2\nu}$. Since $w^\lambda < (pw)^{1/2}$, we obtain

$$\varepsilon |A| w^{1/2} (2^{2-e}w)^{n_2-n_1} < \frac{\varepsilon}{2} (2^{4-e}w)^{4/3} w^{1/2} w^\nu p^\nu < \frac{\varepsilon}{2} (2^{4-e}w)^{4/3} w^{3/2} p^\nu.$$

Inequality (23) now implies

$$1 < \frac{1}{4} + \frac{\varepsilon}{2} (2^{4-e}w)^{4/3} w^{3/2} p^\nu,$$

and hence

$$\varepsilon > \frac{3}{2} (2^{4-e}w)^{-4/3} w^{-3/2} p^{-\nu} > \frac{2^{-4}}{w^2} p^{-\nu}.$$

Finally assume $\lambda \leqslant 8$. Then $p \leqslant w^{17}$. From $|y^2-p| \geqslant 1$ it follows that $|y-p^{1/2}| \geqslant \frac{1}{4}p^{-1/2}$ and hence

$$|y/p^{1/2}-1| > \frac{1}{4p} = p^{-5/6}\cdot\frac{1}{4p^{1/6}} > p^{-\nu}\frac{1}{4w^3},$$

which proves our theorem.

8. Appendix

Table I. If $|D| < 1000$ then we know by Corollary 2 of Theorem 1 that $x^2 - D = 2^n$ can only have solutions with $n < 18 + 2\log|D|/\log 2 < 38$. A simple calculation gives all odd values of D such that the equation $x^2 - D = 2^n$ ($|D| < 1000$) has two or more solutions:

	solutions (x, n)
$D = -511$	(1, 9) (255, 16)
-255	(1, 8) (127, 14)
-127	(1, 7) (63, 12)
-63	(1, 6) (31, 10)
-31	(1, 5) (15, 8)
-23	(3, 5) (45, 11)
-15	(1, 4) (7, 6)
-7	(1, 3) (3, 4) (5, 5) (11, 7) (181, 15)
17	(5, 3) (7, 5) (9, 6) (23, 9)
33	(7, 4) (17, 8)
41	(7, 3) (13, 7)

	solutions (x, n)
$D = 65$	(9, 4) (33, 10)
89	(11, 5) (91, 13)
105	(11, 4) (13, 6) (19, 8)
113	(11, 3) (25, 9)
161	(13, 3) (15, 6) (17,7) (47, 11)
217	(15, 3) (27, 9)
257	(17, 5) (129, 14)
273	(17, 4) (23, 8)
329	(19, 5) (29, 9)
345	(19, 4) (37, 10)
353	(19, 3) (49, 11)

	solutions (x, n)
$D = 497$	(23, 5) (25, 7) (39, 10)
513	(23, 4) (257, 16)
665	(27, 6) (69, 12)
697	(27, 5) (363, 17)
713	(27, 4) (29, 7) (35, 9)
721	(27, 3) (183, 15)
777	(29, 6) (131, 14)
825	(29, 4) (43, 10)
833	(29, 3) (31, 7) (33, 8) (95, 13)
945	(31, 4) (71, 12)

Table II. Powers of two and the nearest odd squares

r	2^r	$a \in \mathbf{N}$ such that a is odd and $\lvert a^2-2^r\rvert$ minimal	a^2-2^r	$\left\lvert\frac{a^2-2^r}{a}\right\rvert$
3	8	3	1	0.333
5	32	5	−7	1.200
7	128	11	−7	0.636
9	512	23	17	0.739
11	2048	45	−23	0.511
13	8192	91	89	0.978
15	32768	181	−7	0.039
17	131072	363	697	1.920
19	524288	725	1337	1.844
21	2097152	1449	2449	1.690
23	8388608	2897	4001	1.381
25	33554432	5793	4417	0.762
27	134217728	11585	−5503	0.475
29	536870912	23171	24329	1.050
31	2147483648	46341	4633	0.100
33	8589934592	92681	−166831	1.800
35	34359738368	185363	−296599	1.600
37	137438953472	370727	−444943	1.200
39	549755813888	741455	−296863	0.400
41	2199023255552	1482911	1778369	1.199
43	8796093022208	2965821	1181833	0.398
45	35184372088832	5931641	−7135951	1.203
47	140737488355328	11863283	−4817239	0.406
49	562949953421312	23726567	28184177	1.188
51	2251799813685248	47453133	17830441	0.376

Table III. Binary expansion of $\sqrt{2}$

$\sqrt{2} =$ 1.0110101000001001111001100110011111111001110111100110010010000100010110
0010111110110001001101100110111010101001010101111101001111100011101011
0111101100000101110101000100100111011101010000100110011101101000101111
0101100100001011000001100110011100110010001010101010010101111111001000001
1000001000011101010111000101000101100001110101000101100011111111100110111
1111011100100000111101101100111001000011110111010010101000010111100100
0011100111000111101101001010011110000000010010000111001101100011110111
1110100010011101101000110100100010000000101110100000111010000010101011111
0001111101001110010100110000010110011100011000000000100011011110000110 0
1101111011110010101011000110111100100100010001011010001000010001011 00...

References

[1] R. Apéry, *Sur une équation diophantienne*, C. R. Acad. Sci. Paris Sér. A 251 (1960), 1263–1264.

[2] A. Baker, *Rational approximations to* $\sqrt[3]{2}$ *and other algebraic numbers*, Quart. J. Math. Oxford Ser. (2) 15 (1964), pp. 375–383.

[3] L. Bieberbach, *Theorie der gewöhnlichen Differentialgleichungen*, 2. Auflage, Grundlehren Math. Wiss., Springer Verlag, Berlin 1965, 210 pp.

[4] J. Browkin and A. Schinzel, *On the equation* $2^n - D = y^2$, Bull. Acad. Polon. Sci., Sér. Sci. Math. Astronom. Phys. 8 (1960), pp. 311–318.

[5] A. R. Forsyth, *Lehrbuch der Differentialgleichungen*, 2 Auflage, Vieweg Verlag, Braunschweig 1912, 213 pp.

[6] H. Hasse, *Über eine diphantische Gleichung von Ramanujan–Nagell und ihre Verallgemeinerung*, Nygoya Math.-I. 27 (1966), pp. 77–102.

[7] A. Schinzel, *On two theorems of Gelfond and some of their applications*, Acta Arith. 13 (1967), pp. 177–236.

[8] C. L. Siegel, *Die Gleichung* $ax^n - by^n = c$, Math. Ann. 114 (1937), pp. 57–68.

[9] *Handbook of Mathematical Functions*, ed. by M. Abramowitz and I. A. Stegun, Dover Publ., New York 1964, pp. 556–566.

Received on 8. 3. 1978
and in revised form on 10. 5. 1978 (1050)

ACTA ARITHMETICA
XXXVIII (1981)

Fields with non-trivial Kaplansky's radical and finite square class number

by

M. Kula (Katowice)

Let F be a field of characteristic not 2 and let $g(F) = F^*/F^{*2}$ be the group of square classes of F and $q = |g(F)|$ — the square class number. C. M. Cordes [1] classified the Witt groups of anisotropic quadratic forms over non-real fields with $q = 8$ and obtained 10 non-isomorphic groups for this class of fields. A little later K. Szymiczek [10] classified the Grothendieck groups of quadratic forms over all fields with $q \leqslant 8$ and his classification in the case $q = 8$ gives 7 non-isomorphic Grothendieck groups for non-real fields and 6 non-isomorphic groups for real fields. Having classified Grothendieck groups he was also able to classify Witt groups for all fields with $q = 8$ and for non-real fields he found the 10 groups confirming Cordes' classification and for real fields with $q = 8$ he got 6 non-isomorphic Witt groups. Thus there are at most 16 possible Witt groups for fields with $q = 8$. Both authors also supplied some examples of fields fitting the classifications. But there remained 4 cases (out of the 16 possible) left without any example of field and it was not clear whether the number of different Witt groups can be further lessened or not. In this paper we construct the four missing fields (cf. a remark added in proof, p. 418). The four fields are characterized by the following values of field invariants(cf. [10], Th. 3.2).

(A) $q = 8$, $s = 2$, $q_2 = 8$, $u_2 = 2$ (the case (4.4) of Theorem 3.2 of [10]);

(B) $q = 8$, $s = \infty$, $q_2 = 4$, $u_2 = 1$ (the case (5.2));

(C) $q = 8$, $s = 1$, $q_2 = 8$, $u_2 = 2$ (the case (4.3));

(D) $q = 8$, $s = 2$, $q_2 = 4$, $u_2 = 2$ (the case (4.7)),

where s is the stufe (level) of the field (the minimal number of terms in a representation of -1 as the sum of squares), q_2 is the number of square classes whose elements are represented as the sum of two squares