ACTA ARITHMETICA
LV (1990)

On the smallest solution to the general binary quadratic diophantine equation

by

DANIEL M. KORNHAUSER (Ann Arbor, Mich.)

1. Introduction. Consider the diophantine equation

$$ax^2+bxy+cy^2+dx+ey+f=0 \tag{0}$$

with integer coefficients a, b, c, d, e, f, and let $H = \max(|a|, |b|, |c|, |d|, |e|, |f|)$. We wish to bound the size of an integer solution, in the following sense: provide an effectively computable function g as "small as possible" with the property that, if (0) has some integer solution, then there is an integer solution with $\max(|x|, |y|) \leqslant g(H)$.

Schinzel [5] showed that one may take $g(H) = (3H)^{300H^3}$, but he remarked that there is no reason to believe that this estimate is sharp. In the other direction, Schinzel [5], Lagarias [3] and others have given examples which imply that $g(H)$ must exceed $c^{\sqrt{H}}$ for some $c > 1$ and infinitely many H.

In this paper I obtain the following improvements to these results.

THEOREM 1. *If (0) has some integer solution, then there is an integer solution with* $\max(|x|, |y|) \leqslant (14H)^{5H}$.

THEOREM 2. *There is an infinite collection of equations* (0) (*even with* $b = d = e = 0$) *having integer solutions but none with* $\max(|x|, |y|) \leqslant 2^{H/5}$.

Theorem 1 indicates that we can take $g(H) \leqslant (14H)^{5H} = \exp(5H\cdot\log(14H))$ and Theorem 2 implies that $g(H)$ must exceed $2^{H/5}$ for infinitely many H. The two theorems taken together imply that both results are almost optimal, since only a $O(\log H)$ factor in the exponent separates the corresponding estimates for $g(H)$.

The plan of this paper is as follows. First, in Section 2, we prove Theorem 1 by reducing (0) to a Pell equation with congruence conditions. This is essentially the strategy of Schinzel [5], but our tactics are somewhat different.

Then, in Section 3, we prove Theorem 2 by considering generalized Pell equations of the form $ax^2+cy^2 = 1$. This extends the work of Lagarias [3] and others.

Finally, in Section 4, we make more precise the connections between the Pell equation and the general quadratic equation (0).

2. The upper bound $(14H)^{5H}$: Proof of Theorem 1. We reduce the general quadratic equation to a Pell equation with congruence side conditions, and then use an upper bound, due to Hua [2], for the least positive solution of the Pell equation.

For most of the proof we assume $a \neq 0$, $\delta = b^2-4ac$ nonsquare > 0. At the end we treat the remaining cases.

First, remove the cross term: multiply (0) by $4a$ $(a \neq 0)$ to get the equivalent equation

$$(2ax+by)^2-\delta y^2+4adx+4aey+4af = 0.$$

Let

$$u = 2ax+by, \quad v = y. \tag{1}$$

Then integers x, y satisfy (0) if and only if corresponding integers u, v (via (1)) satisfy the system:

$$\begin{aligned} &u^2-\delta v^2+2du-(2bd-4ae)v+4af = 0,\\ &u \equiv bv \pmod{2a}. \end{aligned} \tag{2}$$

(If integers x, y satisfy (0) then the corresponding integers u, v satisfy system (2). Conversely, if integers u, v satisfy system (2), then the corresponding x, y $(x = (u-bv)/2a,\ y = v)$ satisfy (0), and x, y are integers.)

Now remove the linear terms: rewrite the equation in (2) as:

$$(u+d)^2-\delta v^2-(2bd-4ae)v-d^2+4af = 0. \tag{3}$$

Multiply by $-\delta$ $(\delta \neq 0$ by assumption):

$$(\delta v+bd-2ae)^2-\delta(u+d)^2-(bd-2ae)^2+\delta d^2-4\delta af = 0.$$

Letting

$$u' = u+d, \quad v' = \delta v+bd-2ae, \tag{4}$$

we see that the last equation is equivalent, via (4), to the system:

$$\begin{aligned} &v'^2-\delta u'^2 = (bd-2ae)^2-\delta d^2+4\delta af,\\ &v' \equiv bd-2ae \pmod{\delta}. \end{aligned}$$

Now it is clear that integers u, v satisfy system (2) if and only if corresponding integers u, v, u', v' (via (4)) satisfy

$$\begin{aligned} &v'^2-\delta u'^2 = (bd-2ae)^2-\delta d^2+4\delta af,\\ &v' \equiv bd-2ae \pmod{\delta},\\ &u \equiv bv \pmod{2a}. \end{aligned} \tag{5}$$

Hence we have reduced equation (0), via (1) and (4), to system (5).

Now consider system (5). Let

$$L = (bd-2ae)^2-\delta d^2+4\delta af \tag{6}$$

denote the right-hand side of the equation in (5). We can assume that $L \neq 0$: for if $L = 0$, then we have $v'^2 = \delta u'^2$, whose only solution is $u' = v' = 0$. By (1) and (4), this forces

$$x = -d/2a+b(bd-2ae)/2a\delta, \quad y = -(bd-2ae)/\delta,$$

from which it follows easily that $\max(|x|, |y|) \leqslant 3H^3 < (14H)^{5H}$, which verifies the Theorem in this case.

Let α, β be the least positive integers satisfying

$$\alpha^2-\delta\beta^2 = 1 \tag{7}$$

(recall the current assumption that δ is a positive nonsquare), and let α_k, β_k be defined by

$$\alpha_k+\beta_k\sqrt{\delta} = (\alpha+\beta\sqrt{\delta})^{2k} \tag{8}$$

where k is an arbitrary integer. Consider the product

$$(v'+u'\sqrt{\delta})(\alpha_k+\beta_k\sqrt{\delta}) = v'_k+u'_k\sqrt{\delta} \tag{9}$$

where

$$u'_k = v'\beta_k+u'\alpha_k, \quad v'_k = v'\alpha_k+\delta u'\beta_k. \tag{10}$$

By the theory of the Pell equation, we know that if integers u', v' satisfy the equation in (5), then for all integral k, the integers u'_k, v'_k satisfy the same equation.

Let integers u_k, v_k correspond to u'_k, v'_k via (4) in the same way that u, v correspond to u', v'; that is,

$$u_k = u'_k-d, \quad v_k = (v'_k-(bd-2ae))/\delta. \tag{11}$$

CLAIM. *If u', v' and corresponding u, v are integers which satisfy the congruences in (5), then u'_k, v'_k and corresponding u_k, v_k are integers which also satisfy these congruences.*

Proof of Claim. Assume the hypotheses. By (7), $\alpha^2 \equiv 1 \pmod{\delta}$, so by (8), $\alpha_1 = \alpha^2+\delta\beta^2 \equiv \alpha^2 \equiv 1 \pmod{\delta}$. Since $\alpha_k+\beta_k\sqrt{\delta} = (\alpha_1+\beta_1\sqrt{\delta})^k$, by the binomial expansion we see that $\alpha_k \equiv \alpha_1^k \equiv 1 \pmod{\delta}$ for all nonnegative k. Since $\alpha_k = \alpha_{-k}$, we have

$$\alpha_k \equiv 1 \pmod{\delta} \tag{12}$$

for all integral k. Using this and (5), we see that

$$v'_k = v'\alpha_k+\delta u'\beta_k \equiv v'\alpha_k \equiv v' \equiv bd-2ae \pmod{\delta}.$$

Thus v'_k satisfies the relevant congruence condition in (5).

Also from (4), (10), and (11) we find that

$$u_k - bv_k = (u-bv)\,\alpha_k + (\delta v - 2ae - bu)\,\beta_k + ((\alpha_k - 1)/\delta)(d\delta - b(bd-2ae)).$$

But by (12), $(\alpha_k - 1)/\delta$ is an integer; and we also have

$$\delta = b^2 - 4ac \equiv b^2 \pmod{2a}.$$

Finally $u - bv \equiv 0 \pmod{2a}$, and these give the required congruence

$$u_k - bv_k \equiv 0 \pmod{2a}.$$

This completes the verification of the claim.

Thus we have shown: If u', v' and corresponding u, v are integers which satisfy system (5), then for all integral k, u'_k, v'_k and corresponding u_k, v_k are integers which also satisfy this system.

Now for a suitable choice of k, we will get a good upper bound for $|u'_k|$, $|v'_k|$ in terms of α_1, β_1. Then by (1) and (11), we get a similar upper bound for $|u_k|$, $|v_k|$, $|x_k|$, $|y_k|$, where x_k, y_k correspond to u_k, v_k via (1).

We proceed as follows. By multiplying by an appropriate integral power k of

$$\eta_1 = \alpha_1 + \beta_1\sqrt{\delta}$$

as in (9) $(\alpha_1 + \beta_1\sqrt{\delta} > 1)$, we can get

(13) $$\sqrt{|L|/\eta_1} < |v'_k + u'_k\sqrt{\delta}| \leqslant \sqrt{|L|\,\eta_1}.$$

Now $v'_k - u'_k\sqrt{\delta} = L/(v'_k + u'_k\sqrt{\delta})$, so by (13) we have

(14) $$\sqrt{|L|/\eta_1} \leqslant |v'_k - u'_k\sqrt{\delta}| < \sqrt{|L|\,\eta_1}.$$

Using (13) and (14), we see that

(15) $$|u'_k|,\ |v'_k| < \sqrt{|L|\,\eta_1}.$$

Now we estimate η_1, by appealing to the following result of Hua [2]: If $D \equiv 0$ or $1 \pmod 4$ is a positive nonsquare integer, then the least positive integer solution z, t of the equation $z^2 - Dt^2 = 4$ satisfies

(16) $$(z + t\sqrt{D})/2 < D^{\sqrt{D}/2}\exp(\sqrt{D}).$$

(We note in passing that Pintz [4] improves the exponent $\sqrt{D}/2$ in (16) to $(1 - 1/\sqrt{e} + o(1))\sqrt{D}/4$ for sufficiently large D.) Since $z = 2\alpha$, $t = \beta$ clearly provide the smallest positive solution of

(17) $$z^2 - 4\delta t^2 = 4,$$

by Hua we have

$$\begin{aligned}\alpha + \beta\sqrt{\delta} &= z/2 + t\sqrt{\delta} = (z + t\sqrt{4\delta})/2 < (4\delta)^{\sqrt{4\delta}/2}\exp(\sqrt{4\delta})\\ &\leqslant (20H^2)^{\sqrt{20H^2}/2}\exp(\sqrt{20H^2}) \qquad (\delta = b^2 - 4ac \leqslant 5H^2)\\ &< (4.48H)^{4.48H}\,2.72^{4.48H} < (12.19H)^{4.48H}.\end{aligned}$$

Hence

(18) $$\eta_1 = (\alpha + \beta\sqrt{\delta})^2 < (12.19H)^{8.96H}.$$

We now estimate $|L|$. By (6),

$$L = (bd-2ae)^2 - \delta d^2 + 4\delta af = -4abde + 4a^2e^2 + 4acd^2 + 4\delta af,$$

so we easily find that

(19) $$|L| \leqslant 32H^4.$$

Estimate $|u'_k|$, $|v'_k|$, $|u_k|$, $|v_k|$, $|x_k|$, $|y_k|$: by (15), (18), and (19),

$$|u'_k|,\ |v'_k| < \sqrt{|L|\,\eta_1} \leqslant \sqrt{32H^4\,\eta_1} < 5.66H^2(12.19H)^{4.48H} = D \text{ (say)}.$$

By (11),

$$|u_k| \leqslant |u'_k| + |d| < D + H,$$
$$\delta\,|v_k| \leqslant |v'_k| + |bd - 2ae| < D + 3H^2$$

so

$$|u_k|,\ |v_k| < D + 3H^2.$$

By (1),

$$|y_k| = |v_k| < D + 3H^2,$$

and

$$|2ax_k| \leqslant |u_k| + |by_k| < (D + 3H^2) + H(D + 3H^2) = (H+1)(D + 3H^2)$$

so

$$|x_k| < (H+1)(D + 3H^2)/2.$$

By the above, we see that this is also a bound for $|y_k|$. One can easily verify that $3H^2 < .02H^2(12.19H)^{4.48H}$, hence the above bound for $|x_k|$, $|y_k|$ is less than

$$(H+1)(5.68H^2(12.19H)^{4.48H})/2 = 2.84H^2(H+1)(12.19H)^{4.48H} = E \text{ (say)}.$$

For $H \geqslant 8$ we have

$$\begin{aligned}E &< 2.84H^2(2H)(14H)^{4.5H} = 5.68H^3(14H)^{4.5H}\\ &< H^4(14H)^{4.5H} < (14H)^{4.5H+4} \leqslant (14H)^{5H},\end{aligned}$$

and for $H < 8$, one can verify by direct calculation that $E < (14H)^{5H}$. Hence we have shown that $|x_k|$, $|y_k| < (14H)^{5H}$.

To summarize: we started with a solution x, y to (0), derived from this a solution u', v', u, v to (5), then obtained a 'small' solution u'_k, v'_k, u_k, v_k to (5), and finally derived a small solution x_k, y_k to (0).

We have proved: if $a \neq 0$, δ is nonsquare > 0 and (0) has an integer solution, then there is an integer solution with $|x|$, $|y| < (14H)^{5H}$.

It remains to consider the other cases; these are easier to handle. Schinzel [5] has already treated the nondegenerate cases among these; for completeness we give the details here.

We first need the following (best possible) linear analogue of Theorem 1.

LEMMA. *If $Ax+By = C$ (A, B, C integers) has an integer solution, then there is one with* $\max(|x|, |y|) \leqslant H$ *where* $H = \max(|A|, |B|, |C|)$.

Proof. Assume without loss of generality that $C \neq 0$ (the result is trivial for $C = 0$) and $|A| \leqslant |B|$. Let x_0, y_0 be a solution. Then $B \neq 0$ (since otherwise we have $A = B = 0$ and then the equation has no solutions), and $x = x_0+Bt$, $y = y_0-At$ is also a solution for any integer t. Clearly we can choose t so that $-|B| \leqslant x \leqslant |B|$ and Ax has the same sign as C. Then $|x| \leqslant |B| \leqslant H$, and

$$|y| = |C-Ax|/|B| \leqslant \max(|C|, |Ax|)/|B| \leqslant \max(|C|, |x|) \leqslant H.$$

This completes the proof of the Lemma.

We now tackle the remaining cases.

$a \neq 0$, δ square > 0. Let $\delta = \Delta^2$. Then equation (6) can be written as the hyperbola (possibly degenerate)

$$(v'-\Delta u')(v'+\Delta u') = L.$$

First assume that $L \neq 0$. If there is a solution, then we necessarily have $|v'-\Delta u'|$, $|v'+\Delta u'| \leqslant |L|$, hence (19) implies that $|u'|$, $|v'| \leqslant |L| \leqslant 32H^4$. From this and (1), (4) we then easily verify that

$$|x|,\ |y| \leqslant 35H^5 < (14H)^{5H}.$$

Now assume that $L = 0$. Then the equation becomes $(v'-\Delta u') \times (v'+\Delta u') = 0$, so we have $v' = \pm\Delta u'$. After making the substitutions (1) and (4), we see that system (5) reduces to the single linear equation

$$Ax+By = C$$

where

$$A = \mp 2a\Delta, \quad B = \Delta^2 \mp b\Delta, \quad C = \pm\Delta d - bd + 2ae.$$

Since $|\Delta^2| = |b^2-4ac| \leqslant 5H^2$, by the Lemma we easily find the bound

$$8H^2 < (14H)^{5H} \quad \text{for} \quad \max(|x|, |y|).$$

$a \neq 0$, $\delta < 0$. Let $\delta_1 = -\delta > 0$. Then the equation in (5) has the form $v'^2+\delta_1 u'^2 = L$. This is an ellipse; hence by (19), all points satisfy

$$|u'|,\ |v'| \leqslant \sqrt{|L|} \leqslant \sqrt{32H^4} < 6H^2.$$

As before, these bounds on $|u'|$, $|v'|$ lead to bounds on $|x|$, $|y|$ which are majorized by $(14H)^{5H}$.

$a \neq 0$, $\delta = 0$. Proceed from the beginning of the proof of the main case of the Theorem, up through the equation (3), which becomes (since $\delta = 0$):

$$(u+d)^2-(2bd-4ae)v-d^2+4af = 0.$$

This equation (a parabola) is equivalent to the congruence

$$(u+d)^2 \equiv d^2-4af \pmod{2bd-4ae}.$$

Suppose first that the modulus is nonzero. Then if there is a solution, we can take $0 \leqslant u+d < |2bd-4ae| \leqslant 6H^2$, so $|u| \leqslant 6H^2+H \leqslant 7H^2$. From this bound on $|u|$, it follows that $|v| \leqslant 41H^4$, and from these bounds on $|u|$, $|v|$ we get, as before, bounds on $|x|$, $|y|$ which are majorized by $(14H)^{5H}$.

On the other hand, if the modulus is zero, then we get the equation $(u+d)^2 = d^2-4af$, so $(u+d)^2 \leqslant 5H^2$, hence $|u+d| \leqslant 3H$ which implies $|u| \leqslant 4H$. The only condition on v is given by (cf. system (2)): $u \equiv bv \pmod{2a}$, so if there is a solution then we can take $|v| < |2a| \leqslant 2H$. As above, these bounds lead to bounds on $|x|$, $|y|$ which are less than $(14H)^{5H}$.

$a = 0$, $\delta \neq 0$. If $c \neq 0$, then switch the roles of x and y, and we have one of the previous cases. If $c = 0$, then we have the hyperbola $bxy+dx+ey+f = 0$, which can be factored as

$$(bx+d)(by+e) = de-bf.$$

By reasoning similar to that used in the $a \neq 0$, δ square > 0 case, we get bounds on $|x|$, $|y|$ which are majorized by $(14H)^{5H}$.

Finally, we have the case $a = \delta = 0$. Note that $0 = \delta = b^2-4ac = b^2$, so $b = 0$. If $c \neq 0$, then switch the roles of x and y, and apply the case $a \neq 0$, $\delta = 0$. If $c = 0$, the equation reduces to

$$dx+ey = -f.$$

By the Lemma proved above, if there is a solution, then we can take

$$\max(|x|, |y|) \leqslant H < (14H)^{5H}.$$

This completes the proof of Theorem 1.

Remark. By a slight modification of the proof, one can show that if (0) has some integer solution, then there is an integer solution with

$$\max(|x|, |y|) < (14H_0)^{5H_0} \cdot H_1^2,$$

where

$$H_0 = \max(|a|, |b|, |c|) \quad \text{and} \quad H_1 = \max(|d|, |e|, |f|).$$

Hence the bound depends only polynomially on d, e and f.

3. The lower bound $2^{H/5}$: Proof of Theorem 2. We use a few lemmas. A variant of Lemma 1 below was proved in Lagarias [3]; for completeness, a proof is provided here.

In what follows, let $d > 0$ be nonsquare, and let u, v be the least positive integer solution to

$$U^2 - dV^2 = 1. \tag{20}$$

Define integers $u(k)$, $v(k)$ by

$$u(k) + v(k)\sqrt{d} = (u + v\sqrt{d})^k, \quad k = 0, 1, 2, \ldots \tag{21}$$

LEMMA 1. *Suppose that b, f are positive integers such that b^f divides v and $(v/b^f, b) = 1$. Then for each $n \geqslant 0$,*

(i) *b^{n+f} divides $v(k)$ if and only if b^n divides k,*

(ii) *$(v(b^n)/b^{n+f}, b) = 1$.*

Proof. We use induction on n. Assume that $b > 1$ since the result is trivial for $b = 1$.

Suppose $n = 0$. Then (i) says that b^f divides $v(k)$ for all positive k. But

$$v(k+1) = u \cdot v(k) + v \cdot u(k)$$

so (i) is true by induction on k. (ii) is immediate from the second hypothesis.

Assume that (i), (ii) hold for some $n \geqslant 0$. We prove (i), (ii) for $n+1$. Now the left side of (i) says that b^{n+1+f} divides $v(k)$, *a fortiori* b^{n+f} divides $v(k)$. By the induction hypothesis (i), b^n divides k, so we can write $k = b^n k_1$ and

$$u(k) + v(k)\sqrt{d} = \big(u(b^n) + v(b^n)\sqrt{d}\big)^{k_1},$$

where k_1 is a positive integer.

Since b^{n+f} divides $v(b^n)$ and $3(n+f) \geqslant n+2+f$, the binomial expansion gives

$$v(k) \equiv k_1 \big(u(b^n)\big)^{(k_1-1)} v(b^n) \pmod{b^{n+2+f}}. \tag{22}$$

Also because (20) holds with $U = u(k)$, $V = v(k)$ we have $(u(b^n), b) = 1$. Then since b^{n+1+f} divides $v(k)$, we see that (22) and (ii) of the induction hypothesis imply that b divides k_1. Therefore b^{n+1} divides k. This proves one direction of (i).

For the other direction, take $k = b^n k_1$, k_1 divisible by b. Then (22) implies that b^{n+1+f} divides $v(k)$.

Finally we prove (ii) for $n+1$. From (22) with $k = b^{n+1}$ we find that

$$v(b^{n+1})/b^{n+1+f} \equiv \big(u(b^n)\big)^{b-1} v(b^n)/b^{n+f} \pmod{b}.$$

Since $(u(b^n), b) = 1$, this together with (ii) of the induction hypothesis imply (ii) for $n+1$. This proves Lemma 1.

LEMMA 2. *Suppose that a, e are positive integers, a odd > 1, such that a^e divides u and $(u/a^e, a) = 1$. Then for each $n \geqslant 0$,*

(i) *a^{n+e} divides $u(k)$ if and only if k is odd and a^n divides k,*

(ii) *$(u(a^n)/a^{n+e}, a) = 1$.*

Proof. We use induction on n. Note that $(a, d) = (a, v) = 1$ since a divides u and u, v satisfy (20).

Suppose $n = 0$. Then (i) says that a^e divides $u(k)$ exactly when k is odd. Now

$$u(2) + v(2)\sqrt{d} = (u + v\sqrt{d})^2 = (u^2 + v^2 d) + 2uv\sqrt{d}.$$

Because $(a, d) = (a, v) = 1$, we have $(a, v^2 d) = 1$ and hence $(u(2), a) = 1$. Also, $v(2) = 2uv$ is divisible by a^e, so we have

$$u(k+2) = u(2)u(k) + v(2)v(k)d \equiv u(2)u(k) \pmod{a^e}. \tag{23}$$

Since $u(0) = 1$ and $u(1) = u$, (i) follows from (23) and induction on k. (ii) is immediate from the second hypothesis.

Next assume (i), (ii) hold for some $n \geqslant 0$. We prove (i), (ii) for $n+1$. Now the left side of (i) says that a^{n+1+e} divides $u(k)$, *a fortiori* a^{n+e} divides $u(k)$. By induction hypothesis (i), k is odd and a^n divides k, so we can write $k = a^n k_1$, k_1 odd, and

$$u(k) + v(k)\sqrt{d} = \big(u(a^n) + v(a^n)\sqrt{d}\big)^{k_1}.$$

Since a^{n+e} divides $u(a^n)$ and $3(n+e) \geqslant n+2+e$, the binomial expansion gives

$$u(k) \equiv k_1 u(a^n) \cdot \big(v(a^n)\big)^{(k_1-1)} \cdot d^{(k_1-1)/2} \pmod{a^{n+2+e}}. \tag{24}$$

Because (20) holds with $U = u(k)$, $V = v(k)$, we have $(v(a^n), a) = 1$. Then since a^{n+1+e} divides $u(k)$ and $(a, d) = 1$, we see that (24) and (ii) of the induction hypothesis imply that a divides k_1. Therefore a^{n+1} divides k. This proves one direction of (i).

For the other direction, take $k = a^n k_1$, k_1 odd and divisible by a. Then (24) implies that a^{n+1+e} divides $u(k)$.

Finally we prove (ii) for $n+1$. From (24) with $k = a^{n+1}$ we find that

$$u(a^{n+1})/a^{n+1+e} \equiv u(a^n)/a^{n+e} \cdot \big(v(a^n)\big)^{a-1} \cdot d^{(a-1)/2} \pmod{a}.$$

Since $(a, v(a^n)) = (a, d) = 1$, this together with (ii) of the induction hypothesis imply (ii) for $n+1$. This proves Lemma 2.

LEMMA 3. *Let a, b, e, f be positive integers, $a > 1$, such that a, b are odd, a^e divides u, b^f divides v, $(u/a^e, a) = 1$, and $(v/b^f, b) = 1$. Then for all nonnegative integers m, n, the equation*

$$a^{2(m+e)} x^2 - b^{2(n+f)} dy^2 = 1 \tag{25}$$

has positive integer solutions, and they are all given by the formula

$$a^{m+e} x + b^{n+f} y \sqrt{d} = (u + v\sqrt{d})^{a^m \cdot b^n \cdot L}, \quad L = 1, 3, 5, 7, \ldots \tag{26}$$

Proof. Let $k = a^m \cdot b^n \cdot L$, L an odd positive integer. Then k is odd, and by Lemmas 1 and 2 we see that

$$a^{m+e} \text{ divides } u(k), \quad b^{n+f} \text{ divides } v(k). \tag{27}$$

Thus the values $x = u(k)/a^{m+e}$, $y = v(k)/b^{n+f}$ given by formula (26) satisfy (25).

Conversely, by the theory of the Pell equation, every positive solution of (25) is obtained from (21) for some positive k such that $u(k)$, $v(k)$ satisfy (27). By (i) in Lemmas 1 and 2, a^m divides k, b^n divides k, and k is odd. But $(a, b) = 1$ since a divides u, b divides v, and u, v satisfy (20). Hence $a^m \cdot b^n$ divides k, so $k = a^m \cdot b^n \cdot L$, L an odd positive integer. Therefore all positive solutions to (25) arise from formula (26). This proves Lemma 3.

Proof of Theorem 2. Let d be any positive nonsquare integer for which the least positive integer solution u, v of (20) has the property that u is divisible by 5 but not by 5^2, and v is divisible by 3 but not by 3^2 (for example $d = 11$, $u = 10$, $v = 3$). It follows from taking $a = 5$, $b = 3$, $e = f = 1$ in Lemma 3 that the least positive integer solution to

$$5^{2m+2}x^2 - 3^{2n+2}dy^2 = 1 \tag{28}$$

(m, n nonnegative integers) is given by

$$5^{m+1}x + 3^{n+1}y\sqrt{d} = (u+v\sqrt{d})^{5^m \cdot 3^n}. \tag{29}$$

We shall show that this leads to the lower bound c^H of Theorem 2, for any positive $c < \lambda(d) = (u+v\sqrt{d})^{1/15\sqrt{d}}$.

From [1] we find that when $d = 631$ then

$$u = 4896157531299865003556\text{0},$$
$$v = 194912953757515103642\text{7},$$

and $\lambda(d) > 2^{1/5}$. This will prove Theorem 2.

Let $0 < \varepsilon < 1$. It is easily seen from Kronecker's Theorem applied to the irrational number $\log 5/\log 3$ that there are arbitrarily large positive integers m, n with

$$1-\varepsilon < 5^{2m+2}/(3^{2n+2}d) < (1-\varepsilon)^{-1}.$$

Thus

$$H = \max(5^{2m+2}, 3^{2n+2}d, 1)$$

satisfies

$$(1-\varepsilon)H < 5^{2m+2} \quad \text{and} \quad (1-\varepsilon)H < 3^{2n+2}d$$

and therefore

$$5^m \cdot 3^n > H(1-\varepsilon)/15\sqrt{d}.$$

From (28) we see that $5^{m+1}x > 3^{n+1}y\sqrt{d}$, and thus by (29),

$$5^{m+1}x > \tfrac{1}{2}(u+v\sqrt{d})^{H(1-\varepsilon)/15\sqrt{d}}.$$

Since $5^{m+1} \leqslant \sqrt{H}$, this clearly gives a lower bound of c^H for any positive $c < \lambda(d)$. Since all integer solutions of (28) arise from positive ones by changes of sign, this establishes Theorem 2.

Remarks. 1. By slightly modified arguments, one can show that the least positive integer solution to

$$3^{2m+4}x^2 - 5^{2n+3}y^2 = 1$$

(for given m, $n \geqslant 0$) is provided by

$$3^{m+2}x + 5^{n+1}y\sqrt{5} = (9+4\sqrt{5})^{3^m 5^{n+1}}.$$

This family of equations also gives, for suitable m, n, the lower bound $2^{H/5}$ of Theorem 2.

2. The equation $ax^2+cy^2 = 1$ in Theorem 2 is as simple a form of equation as one can use (there is no cross term, and no linear terms), and still have an exponential lower bound. For if either the x^2 or y^2 term does not appear in (0), then $a = 0$ or $c = 0$, so $\delta = b^2-4ac = b^2$ is a square, and the proof of Theorem 1 for this case shows that we can choose a solution (if any exist) with $|x|$, $|y|$ bounded by a polynomial in H.

4. Concluding remarks. Theorems 1 and 2 imply that we can take $g(H)$ to be at most $c^{H\log H}$ for some c, and that $g(H)$ must infinitely often exceed c_1^H for some $c_1 > 1$, where $g(H)$ bounds the size of the least integer solution (if any) to (0).

Similarly, Hua's estimate and Lemma 1 imply that we can take $g_1(d) \leqslant c_2^{\sqrt{d}\log d}$ for some c_2, and that $g_1(d) > c_3^{\sqrt{d}}$ for some $c_3 > 1$ and infinitely many d, where $g_1(d)$ is an upper bound for the size of the least positive integral solution u, v to (20).

In fact the estimates for g and g_1 are related.

PROPOSITION 1. *If we can take $g_1(d) \leqslant c_1^{\sqrt{d}\phi(d)}$ for some monotone nondecreasing function $\phi \geqslant 1$ and some c_1, then we can take $g(H) \leqslant c^{H\cdot\phi(5H^2)}$ for some* c.

The proof is a straightforward application (as in the proof of Theorem 1) of the bound for g_1 to get a suitable bound for g.

PROPOSITION 2. *Let p be an odd prime. If we can take $g(H) \leqslant c^{H\phi(H)}$ for some function $\phi \geqslant 1$ and some c, then we can take $g_1(d) \leqslant c_1^{\sqrt{d}\phi(d)}$ for some c_1 (depending on p) and all d such that u is divisible by p but not by p^2.*

The proof (of the contrapositive form) is a straightforward application of the ideas of the proof of Lemma 2.

Proposition 1 implies that an improvement in the upper bound for the least positive solution to the Pell equation leads to a corresponding improvement in the upper bound for the least solution to the general quadratic equation. In particular, taking ϕ identically equal to 1, we see that the most optimistic upper bound for the Pell leads to the most optimistic upper bound for the general quadratic.

Proposition 2 gives a partial result for the opposite implication; it would be complete if we could remove the divisibility condition.

Acknowledgement. I wish to thank Professor D. W. Masser for helpful discussions.

References

[1] C. F. Degen, *Canon Pellianus sive tabula simplicissimam aequationis celebratissimae $y^2 = ax^2+1$ solutionem, pro singulis numeri dati valoribus ab 1 usque ad 1000, in numeris rationalibus iisdemque integris exhibens*, Copenhagen 1817.

[2] L. K. Hua, *On the least solution of Pell's equation*, Bull. Amer. Math. Soc. 48 (1942), 731–735.

[3] J. C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation $x^2-dy^2 = -1$*, Trans. Amer. Math. Soc. 260 (2) (1980), 485–508 (Appendix A).

[4] J. Pintz, *Elementary methods in the theory of L-functions, VII. Upper bound for $L(1, \chi)$*, Acta Arith. 32 (1977), 397–406.

[5] A. Schinzel, *Integer points on conics*, Ann. Soc. Math. Polon., Ser. I: Comment. Math. 16 (1972), 133–135 (see also 17 (1973), 305).

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MICHIGAN
Ann Arbor, Michigan 48109
U.S.A.

Received on 14.7.1988 (1850)

ACTA ARITHMETICA
LV (1990)

Über die asymptotische Dichte gewisser Teilmengen der natürlichen Zahlen

von

PETER KUNTH (Frankfurt/Main)

1. Überblick. Wir werden als Verallgemeinerung eines wohlbekannten Ergebnisses von B. Saffari, P. Erdös und R. C. Vaughan (vgl. [3], [8]) zeigen: Unter einschränkenden Bedingungen an eine Teilmenge T der natürlichen Zahlen existiert für die Faktoren M_1, M_2 eines direkten Produkts $T = M_1 \times M_2$ ihre "asymptotische Dichte" stets.

2. Asymptotischer und logarithmischer Mittelwert. Im folgenden ist stets $N := \{1, 2, 3, \ldots\}$ (ohne die Null).

DEFINITION. Gegeben sei eine zahlentheoretische Funktion $f\colon N \to C$.

$$\underline{\delta}(f) := \liminf_{x\to\infty} \frac{1}{\log x}\cdot \sum_{n\leqslant x} \frac{f(n)}{n},$$

$$\overline{\delta}(f) := \limsup_{x\to\infty} \frac{1}{\log x}\cdot \sum_{n\leqslant x} \frac{f(n)}{n}$$

heißen *untere* (resp. *obere*) *logarithmische Dichte* der zahlentheoretischen Funktion f. Gilt dabei sogar

$$\underline{\delta}(f) = \overline{\delta}(f),$$

so besitzt f einen *logarithmischen Mittelwert*

$$\delta(f) := \lim_{x\to\infty} \left\{\frac{1}{\log x}\cdot \sum_{n\leqslant x} \frac{f(n)}{n}\right\}.$$

DEFINITION. Für eine zahlentheoretische Funktion f heißen

$$\underline{M}(f) := \liminf_{x\to\infty} \frac{1}{x}\cdot \sum_{n\leqslant x} f(n),$$

$$\overline{M}(f) := \limsup_{x\to\infty} \frac{1}{x}\cdot \sum_{n\leqslant x} f(n)$$