Pacific Journal of Mathematics

TWO CLASSES OF DIOPHANTINE EQUATIONS

DONALD JOHN LEWIS

Vol. 11, No. 3 BadMonth 1961

TWO CLASSES OF DIOPHANTINE EQUATIONS

D. J. Lewis

1. Introduction. It is easily shown, by means of the Thue-Siegel-Roth theorem, that the equation

$$x^2 + 7M^2 = N^y , \qquad M \geqq 1 , \quad N \geqq 2 \tag{1}$$

has only a finite number of nonnegative integral solutions x, y. Here we show that this equation cannot have more than $56MN$ integral solutions, and if $(M, 7N) = 1$, it cannot have more than $28N$ solutions. While these are reasonable upper bounds for the number of solutions, they are almost certainly excessively large. With appropriate assumptions on M and N we are able to obtain much smaller bounds.

Previously, Nagell [8] and others [9], [5] showed that the equation $x^2 + 7 = 2^y$ has exactly five solutions. We show that when N is an odd integer the equation $x^2 + 7 = N^y$ has at most two solutions and it has no solution unless N is an odd power of a prime.

In the second part of this paper we determine an upper bound, in terms of M and n, on the number of primitive solutions (i.e. x and y coprime) of the equation

$$x^2 + 7M^2 = y^n , \qquad M \geqq 1 \quad \text{and} \quad n \geqq 3 . \tag{2}$$

In making our calculations, we make use of results which were obtained by means of a p-adic argument.

Nagell has shown that the equation $x^2 + D = y^n$ has at most one solution when $D = 2$ or 8 [7] and has no solution when D is a square free integer congruent to 1 or 2 (modulo 4) [6]. Ljungren [3], [4] has shown that this equation has at most one solution when $D = p^2$ (p a prime) or $D = 1 + 2^s t$ (s and t odd integers $\geqq 3$.)

2. Notation. Let $K = Q(\sqrt{-7})$, where Q is the field of rational numbers. Let $\mathfrak{O}$ be the set of algebraic integers in K, then $\mathfrak{O}$ is a unique factorization ring having ± 1 as its only units. Let $\mathfrak{S}$ denote the set of rational primes which split in $\mathfrak{O}$ into the product of two non-associate conjugate primes. $\mathfrak{S}$ does not contain $7 = (\sqrt{-7})(-\sqrt{-7})$. Let $\mathfrak{I}$ be the set of rational primes not in $\mathfrak{S} \cup (7)$, then all integers in $\mathfrak{I}$ are primes in $\mathfrak{O}$.

Set $\rho = \frac{1}{2}(1 + \sqrt{-7})$, then $2 = \rho \cdot \rho'$ and ρ is a root of the equation $z^2 - z + 2 = 0$. If p is in $\mathfrak{S}$, we write $p = \pi_p \cdot \pi_p'$.

If p is a rational prime and m is a rational integer, we write $\| m \|_p$ for the largest rational integer s such that $p^s \mid m$.

Received August 5, 1960. The author holds a National Science Foundation Fellowship.

A solution shall always refer to one having $x \geqq 0$, thus distinct solutions of (1) or (2) have distinct values or x and y.

I. The equation $x^2 + 7M^2 = N^y$.

3. N divisible by a prime not in $\mathfrak{S}$. Let x, y be a solution of (1). Let $d = (x, M)$. Set $x = d\mathscr{X}$, $M = d\mathscr{M}$, then $(\mathscr{X}, \mathscr{M}) = 1$ and $d^2 \mid N^y$. Furthermore $\| N^y \|_2 > \| d^2 \|_2$ exactly when $\mathscr{X} \equiv \mathscr{M} \equiv 1 \pmod 2$, in which case $4d^2 \mid N^y$. Let

$$\sigma = (x + M\sqrt{-7}, x - M\sqrt{-7}) = d(\mathscr{X} + \mathscr{M}\sqrt{-7}, \mathscr{X} - \mathscr{M}\sqrt{-7}) .$$

Clearly $\sigma = \pm \sigma'$, hence either σ is a rational integer or it is a rational integral multiple of $\sqrt{-7}$. The latter case occures exactly when $7 \mid \mathscr{X}$ and $7 \nmid \mathscr{M}$, hence

$$\| x^2 + 7M^2 \|_7 = 2 \| M \|_7 + 1 = y \| N \|_7 ,$$

and hence this can occur for at most one value of y.

Suppose that σ is a rational integer. Then

$$\begin{aligned} \tau &= (\mathscr{X} + \mathscr{M}\sqrt{-7}, \mathscr{X} - \mathscr{M}\sqrt{-7}) = (2\mathscr{X}, \mathscr{X} + \mathscr{M}\sqrt{-7}) \\ &= (2\mathscr{X}, 2\mathscr{M}\rho + \mathscr{X} - \mathscr{M}) \end{aligned}$$

is a rational integer and $7 \nmid \mathscr{X}$. If $\mathscr{X} \not\equiv \mathscr{M} \pmod 2$, then $\tau = (\mathscr{X}, \mathscr{M}\sqrt{-7}) = 1$. If $\mathscr{X} \equiv \mathscr{M} \pmod 2$, then $\tau = 2(\mathscr{X}, \mathscr{M}\rho + \frac{1}{2}(\mathscr{X} - \mathscr{M})) = 2f$. Now $2 \nmid f$, for otherwise $2 \mid \mathscr{X}$ and $\rho \mid \frac{1}{2}(\mathscr{X} - \mathscr{M})$, hence $4 \mid (\mathscr{X} - \mathscr{M})$ and so $(\mathscr{X}, \mathscr{M}) \geqq 2$. Similarly, if p is an odd prime then $p \nmid f$, otherwise $p \mid \mathscr{X}$ and $p \mid \frac{1}{2}(\mathscr{X} + \mathscr{M}\sqrt{-7})$ and hence $p \mid \mathscr{M}$ and $(\mathscr{X}, \mathscr{M}) > 1$. Thus

$$\sigma = \begin{cases} d\sqrt{-7} & \text{if } 7 \mid \mathscr{X},\ \mathscr{X} \not\equiv \mathscr{M} \pmod 2 , \\ 2d\sqrt{-7} & \text{if } 7 \mid \mathscr{X},\ \mathscr{X} \equiv \mathscr{M} \pmod 2 , \\ d & \text{if } 7 \nmid \mathscr{X},\ \mathscr{X} \not\equiv \mathscr{M} \pmod 2 , \\ 2d & \text{if } 7 \nmid \mathscr{X},\ \mathscr{X} \equiv \mathscr{M} \pmod 2 . \end{cases}$$

Let $\gamma = (x + M\sqrt{-7})/\sigma$, then $(\gamma, \gamma') = 1$ and hence $(p, \gamma) = 1 = (p, \gamma')$ for all p primes p not in $\mathfrak{S}$. Furthermore $N^y = \sigma \cdot \gamma \cdot \gamma'$ and therefore

If x, y is a solution of (1) *and p is in $\mathfrak{S}$ then* $y \| N \|_p = 2 \| d \|_p \leqq 2 \| M \|_p$. *Also either* $y \| N \|_7 = 2 \| x \|_7 \leqq 2 \| M \|_7$ *or* $y \| N \|_7 = 2 \| M \|_7 + 1$.

Thus if N is divisible by a prime not in $\mathfrak{S}$, then the number of solutions is small compared to M. Indeed

If $(N, M) = 1$ and N is divisible by a prime in $\mathfrak{S}$ or if $7^2 \mid N$ then the equation (1) *has no integral solutions. While if $(N, M) = 1$ and $N = 7 \cdot \prod_{p \in \mathfrak{S}} p^{\mu_p}$ then $y = 1$ is the only solution of equation* (1).

Also

If $N = 7^{\mu}\prod_{p\in\mathfrak{S}} p^{\mu_p}$ *then* $x = 0$ *is the only possible solution of equation* (1).
For

$$x^2 + 7M^2 \leqq \prod_{p\notin\mathfrak{S}} p^{||N^y||_p} \leqq \prod_{p\notin\mathfrak{S}} p^{||7M^2||p} \leqq 7M^2 ,$$

hence $x = 0$.

4. N **an odd integer.** Let x, y, with $y = 2z$, be a solution of (1). Set $\mathscr{N} = N^z/d$, then $\mathscr{X}^2 + 7\mathscr{M}^2 = \mathscr{N}^2$. Let $e = (\mathscr{X}, \mathscr{N})$, then $e = 1$, for if p is a prime dividing e then $p^2 \mid 7\mathscr{M}^2$ and hence $p \mid \mathscr{M}$ giving $(\mathscr{X}, \mathscr{M}) > 1$.

We have

$$7\mathscr{M}^2 = \mathscr{N}^2 - \mathscr{X}^2 = (\mathscr{N} + \mathscr{X})(\mathscr{N} - \mathscr{X}) .$$

Suppose $2 \nmid \mathscr{M}$; then $\mathscr{N} \not\equiv \mathscr{X} \pmod 2$ and

$$f = (\mathscr{N} + \mathscr{X}, \mathscr{N} - \mathscr{X}) = (2\mathscr{N}, \mathscr{N} + \mathscr{X}) = 1 .$$

As $\mathscr{N} > \mathscr{X} > 0$, we must have either $\mathscr{N} + \mathscr{X} = 7v^2$ and $\mathscr{N} - \mathscr{X} = u^2$ or $\mathscr{N} + \mathscr{X} = u^2$ and $\mathscr{N} - \mathscr{X} = 7v^2$, where $\mathscr{M} = uv$, $(u, v) = 1 = (u, 7)$. In either case $2\mathscr{N} = u^2 + 7v^2$ and hence $\mathscr{N} \equiv 0 \pmod 4$, since u and v are odd.

On the other hand, if $2 \mid \mathscr{M}$ then $\mathscr{N} \equiv \mathscr{X} \pmod 2$. Furthermore, since $(\mathscr{M}, \mathscr{X}) = 1$ we have $\mathscr{N} \equiv \mathscr{X} \equiv 1 \pmod 2$ and therefore $\mathscr{M} = 0 \pmod 4$. Thus

If N *is an odd integer and* $4 \nmid M$ *and if* x, y *is a solution of* (1) *then* y *is an odd integer.*

Combining this result with those of the previous section, we have

If $4 \nmid M$ *and* N *is an odd integer divisible by an odd power of a prime in* $\mathfrak{S}$ *then the equation* (1) *has no integral solutions.*

If N is odd and $M \equiv 2 \pmod 4$ and x, y is a solution of (1) then x and y are odd integers and

$$1 \equiv x^2 + 7M^2 = N^y \equiv N \pmod 4 .$$

Hence

If $M \equiv 2 \pmod 4$ *and* $N \equiv 3 \pmod 4$ *then the equation* (1) *has no integral solutions.*

Similarly, if $M \equiv N \equiv 1 \pmod 2$ and x, y is a solution of (1) then y is odd and x is even, hence

$$3 \equiv x^2 + 7M^2 = N^y \equiv N \pmod 4 .$$

Thus

If $M \equiv 1 \pmod 2$ *and* $N \equiv 1 \pmod 4$ *then the equation* $x^2 + 7M^2 = N^y$ *has no solutions.*

5. A factorization of N. In this section assume that all prime divisors of N are in $\mathfrak{S}$. Let $t(N)$ denote the number of distinct prime divisors of N, then N has exactly $2^{t(N)-1}$ distinct factorizations of the form $\prod_{p\in\mathfrak{S}} p^{\mu_p} = N = \alpha\alpha'$, $(\alpha, \alpha') = 1$, $\alpha = \frac{1}{2}(a + b\sqrt{-7})$ with $a > 0, b > 0$. For if $p \mid N$ then $p = \pi_p \cdot \pi'_p$, where π_p and π'_p are conjugate nonassociate primes of $\mathfrak{O}$. Then for each vector $(\cdots, e_p, \cdots)$, with $e_p = 0$ or 1, we have a factorization of N into relatively prime conjugate factors, namely

$$\prod_{p\in\mathfrak{S}} \pi_p^{\mu_p e_p} \pi_p'^{\mu_p(1-e_p)} \quad \text{and} \quad \prod_{p\in\mathfrak{S}} \pi_p^{\mu_p(1-e_p)} \pi_p'^{\mu_p e_p}$$

and exactly one of those two factors has the property that a and b are both positive. The vector $(\cdots, e_p, \cdots)$ and the vector $(\cdots, 1 - e_p, \cdots)$ give rise to the same α. As there are $2^{t(N)}$ such vectors, we get at most $2^{t(N)-1}$ possible factorizations. Because $\mathfrak{O}$ is a unique factorization ring, they are all distinct.

If x, y is a solution of (1) then $\sigma^2 \mid N^y$, therefore $p \mid \sigma$ only if $p \mid N$. Hence each factorization

$$N = \alpha\alpha' , \quad (\alpha, \alpha') = 1$$

induces a factorization

$$\sigma^2 = \delta\delta' , \quad (\delta, \delta') = 1 , \quad \delta \mid \alpha .$$

Therefore to each solution x, y of

$$x^2 + 7M^2 = N^y , \quad \text{with} \quad N = \prod_{p\in\mathfrak{S}} p^{\mu_p} ,$$

there exists a factorization of $N = \alpha\alpha'$ such that

$$\frac{x + M\sqrt{-7}}{\sigma} = \mathscr{P}(\alpha^y/\delta) \tag{3}$$

where $\mathscr{P}(c + d\sqrt{-7}) = |c| + |d|\sqrt{-7}$.

Now suppose that $(M, N) = 1$ and $N = \prod_{2\neq p\in\mathfrak{S}} p^{\mu}$; then $\sigma = 1$. If, under these assumptions, x, y is a solution of (1) associated with the factorization $N = \alpha\alpha'$, where $\alpha = a + b\sqrt{-7}$, we have,

$$\pm M = \sum_{i=0}^{\infty} \binom{y}{2i+1} b^{2i+1} a^{y-2i-1} (-7)^i ,$$

and hence $b \mid M$. Since different factorizations give rise to different b,

we have

If $(M, N) = 1$ *and* $N = \prod_{2 \neq p \in \mathfrak{S}} p^{\mu_p}$, *the equation* (1) *has no integral solution if* $t(N) > 1 + \log_2 d(M)$, *where* $d(M)$ *denotes the number of positive divisors of* M.

6. The equation $x^2 + 7 = N^y$, N odd. In view of our discussion in § 3 we may restrict our attention to the case $N = \prod_{2 \neq p \in \mathfrak{S}} p^{\mu_p}$. If the equation

$$x^2 + 7 = N^y , \quad N = \prod_{2 \neq p \in \mathfrak{S}} p^{\mu_p} , \tag{4}$$

has a solution x, y we have seen that y is an odd integer and $N = (a + \sqrt{-7})(a - \sqrt{-7}) = a^2 + 7$. It follows that N is an odd power of an odd prime of the form $a^2 + 7$ and the maximal number of solutions occur when N is a prime of this form. In case N is a prime, $\alpha = a + \sqrt{-7}$ is a root of the equation $z^2 - 2az + N = 0$. Set

$$\alpha^k = S(k) + T(k)\sqrt{-7} , \qquad (k = 0, 1, \cdots) ,$$

then $S(0) = 1$, $S(1) = a$, $T(0) = 0$, $T(1) = 1$ and the functions $S(k)$ and $T(k)$ satisfy the recurrence

$$f(k + 2) = 2af(k + 1) - Nf(k) .$$

Clearly x, y is a solution of (4) exactly when $| T(y) | = 1$.

Now $T(k) = (\alpha^k - \alpha'^k)/(\alpha - \alpha')$, hence if $m \mid n$ then $T(m) \mid T(n)$. Thus if there is a solution of (4) with $y > 1$, there is one with y an odd prime.

Since $2 \mid a$, one shows by induction that $T(2k + 1) \equiv 1 \pmod 4$, $T(2k) \equiv 0 \pmod 4$ $(k = 0, 1, \cdots)$, hence $T(y) \neq -1$. Also, by induction, we see that $T(k) \equiv ka^{k-1} \pmod 7$, hence $T(7u) \neq 1$. Also $S(k) \equiv a^k \pmod 7$. Furthermore

$$T(k) = ka^{k-1} + \binom{k}{3} a^{k-3}(-7) + \cdots + (-7)^{\frac{1}{2}(y-1)} ,$$

hence if y is an odd prime for which $T(y) = 1$, then -7 is a quadratic residue modulo y, so y is of the form $s^2 + 7t^2$, and in particular $3 \neq y$. Thus if y is an integer for which $T(y) = 1$, we have $y \equiv \pm 1 \pmod 6$.

As $7 \nmid N$, we have $7 \nmid a$ and hence $S(6n) \equiv 1 \pmod 7$ while $T(6n) \equiv -na^5 \pmod 7$. Thus

$$T(6n + 1) \equiv 1 - n \pmod 7 ,$$
$$T(6n + 5) \equiv (5 - n)a^4 \pmod 7 .$$

Now $T(6n + 1)$ and $T(6n + 5)$ are 7-adic power series in the variable n and are congruent (modulo 7) to a linear polynomial, and so as shown in [1, § 6]

there is a unique value of n such that $T(6n+1)=1$, namely $n=0$, and there is at most one value of n such that $T(6n+5)=1$. Hence the equation (4), with N a prime of the form a^2+7, has at most two solutions. Summarizing we have

If N is an odd integer, the equation $x^2+7=N^y$ has no integral solution unless N is either of the form $7(1+7c^2)$ or of the form a^2+7 when $y=1$ is a solution; this is the only solution unless N is a prime of the form $a^2+7>7$, when there may be one additional solution.

We conjecture that the equation $x^2+7=N^y$, N odd, has at most one solution.

7. The equation $x^2+28=N^y$, N odd. We may restrict our attention to the case $N=\prod_{2\neq p\in\mathfrak{S}} p^{\mu_p}$. Suppose x, y is a solution of the equation

$$x^2+28=N^y\,,\quad N=\prod_{2\neq p\in\mathfrak{S}} p^{\mu_p}\,. \tag{5}$$

It follows from the discussion in § 4 that $N\equiv 1 \pmod 4$ and y is an odd integer. To this solution there is a factorization $N=\alpha\alpha'$, $\alpha=c+d\sqrt{-7}$, with $d\mid 2$. It follows that $d=2$ (otherwise $N\not\equiv 1 \pmod 4$) and $(c,14)=1$. Since N has only one factorization, N must be a power (in this case an odd power) of a prime of the form c^2+28. Clearly the maximal number of solutions occur when N is a prime.

Now $\alpha=c+2\sqrt{-7}$ is a root of the equation $z^2-2cz+N=0$. Set

$$\alpha^k=S^*(k)+T^*(k)\sqrt{-7}\,,\qquad (k=0,1,\cdots)\,.$$

Then $S^*(k)$ and $T^*(k)$ satisfy the recurrence

$$f(k+2)=2cf(k+1)-Nf(k)\,,$$

where $S^*(0)=1$, $S^*(1)=c$, $T^*(0)=0$ and $T^*(1)=2$. Also $T^*(k)$ is even for all integers k. Clearly x, y is a solution of (5) exactly when $|T^*(y)|=2$.

By induction, one shows that

$$T^*(k)\equiv 2kc^{k-1} \pmod 7\,,\quad S^*(k)\equiv c^k \pmod 7\,,\qquad (k=0,1,\cdots)\,,$$

hence $7\nmid y$. We also have

$$T^*(6n+j)\equiv 2(j-n)c^{j-1} \pmod 7 \qquad (j=0,1,\cdots,5)\,.$$

If $m\mid n$ then $T^*(m)\mid T^*(n)$. Thus if $3\mid y$ then

$$T^*(3)=\pm 2=6c^2-56\,;$$

or $c=3$, $N=37$ and $T^*(3)=-2$. In this case one checks that $|T^*(9)|\neq 2$,

hence $3 \mid y$ only if $N = 37$ and $9 \nmid y$. As in the argument in the preceeding section, $T^*(6n+1) = 2$ has the unique solution $n = 0$, while the relations $T^*(6n+j) = 2$ and $T^*(6n+j) = -2$, ($j = 1, 3$ and 5) each have at most solution. Now $T^*(n+4) \equiv T^*(n) \pmod 8$. As $(6n \pm 1)^2 \equiv 1 \pmod 4$, if $|T^*(y)| = 2$ then $|T^*(y^2)| = 2$ only if $y = 1$; hence every solution of (5) has y square free. Finally one checks that the equation $x^2 + 28 = 37^y$ has at most two solution with $3 \mid y$.

Summarizing, we have

If N is an odd integer, the equation $x^2 + 28 = N^y$ has no solution unless N is either of the form $7(4+7d^2)$ or of the form $a^2 + 28$. If $N = 7(4+7d^2)$ there is exactly one solution, $y = 1$. If $N = 37$ then $y = 1$ and 3 are solutions and there are at most three additional solutions. If $N = a^2 + 28$ is a prime $\neq 37$, there are at most four solutions. If $N = a^2 + 28$ is composite, there are at most two solutions.

8. The general case. Assume that x, y is a solution of (1), with $N = \prod_{p \in \mathscr{S}} p^{\mu_p}$. Then we have seen that there is a factorization of $N = \alpha\alpha'$ with $(\alpha, \alpha') = 1$ and a factorization of $\sigma^2 = \delta\delta'$ such that $\delta \mid \alpha$ and

$$(x + M\sqrt{-7})/\sigma = \mathscr{P}(\alpha^y/\delta) .$$

Futhermore

$$2\alpha = \begin{cases} a + b\sqrt{-7} , & \text{with} \quad (a,b) = 2 , \quad \text{if} \quad 2 \nmid N , \\ a + b\sqrt{-7} , & \text{with} \quad (a,b) = 1 , \quad a \equiv b \equiv 1 \pmod 2 \quad \text{if} \quad 2 \mid N . \end{cases}$$

As $7 \nmid N$, we have $7 \nmid a$.

Set

$$2\alpha^k = S(k) + bT(k)\sqrt{-7} , \qquad (k = 0, 1, \cdots,) ,$$

then $S(k)$ and $T(k)$ satisfy the recurrence

$$f(k+2) = af(k+1) - Nf(k) , \tag{6}$$

with $S(0) = 2$, $S(1) = a$, $T(0) = 0$, and $T(1) = 1$. Set

$$2\delta = u + v\sqrt{-7} ,$$

as $7 \nmid N$ we have $7 \nmid \sigma^2$ and hence $7 \nmid u$.

Now from (3), we have

$$\sigma(x + M\sqrt{-7}) = \mathscr{P}(\alpha^y\delta') ,$$

hence

$$\pm 4\sigma M = buT(y) - vS(y) = F(y) . \tag{7}$$

Clearly x, y is a solution of (1) exactly when y satisfies (7). $F(k)$ satisfies the recurrence (6) and $F(0) = -2v$, $F(1) = bu - av$. Let $L = (F(0), F(1))$, then $F(k) = LG(k)$, with $G(0) = a^*$, $G(1) = b^*$. Obviously $(a, N) = 1$, $\Delta = a^2 - 4N = -7b^2$, $W = \frac{1}{2}(2b^* - a^*a) = buL^{-1}$.

Set $\lambda = ||L||_7$ and $\chi = ||b||_7$. Since $7 \nmid 4\sigma$, if y is a solution of (7) we must have $\nu = ||M||_7 \geqq \lambda$. As $7 \nmid au$, we have $\lambda = \min(||v||_7, ||b||_7) \leqq \chi$. we also have $||\Delta||_7 = 2\chi + 1$ and $||W||_7 = \chi - \lambda$.

By Theorem 4 of [1] if $\lambda = \chi$ the multiplicity of the recurrence $G(k)$ is at most 6. On the other hand, see the proof of Theorem 3 of [1], if $\lambda < \chi$ the multiplicity of the recurrence $G(k)$ is less than $2 \cdot 7^{\lambda+\chi+1}$ and furthermore $7 \nmid G(k)$, i.e. $\lambda = \nu$.

We observe that

$$2 \cdot 7^{\nu}(7 \cdot 7^{\chi}) \leqq 2 \cdot 7^{\nu}(7b) < 4 \cdot 7^{\nu}\sqrt{7N}\,.$$

Obviously $6 < 4 \cdot 7^{\nu}\sqrt{7N}$. Hence the number of y such that $|F(y)| = 4\sigma M$ is at most $8 \cdot 7^{\nu}\sqrt{7N}$.

If $M = 7^{\nu} \prod_{p \neq 7} p^{\nu_p}$, set $M_{\mathfrak{S}} = \prod_{p \in \mathfrak{S}} p^{\nu_p}$. Now each solution x, y of (1) gives rise to a σ^2 and to a factorization of $N = \alpha\alpha'$, and each pair σ, α give rise to a recurrence $F(y)$. Now $\sigma \mid 2M_{\mathfrak{S}}$ and there are $2^{t(N)-1}$ factorizations of N, hence there are at most

$$d(2M_{\mathfrak{S}})2^{t(N)-1} = d(M_{\mathfrak{S}})2^{t(N)} \leqq M_{\mathfrak{S}}2^{t(N)}$$

distinct recurrences. It follows that the number of solutions of (1), with $N = \prod_{p \in \mathfrak{S}} p^{\mu_p}$ is less than

$$8 \cdot 7^{\nu} M_{\mathfrak{S}}\sqrt{7N} \cdot 2^{t(N)}\,.$$

As $2^{t(N)} < \sqrt{7N}$, and $7^{\nu} \cdot M_{\mathfrak{S}} \leqq M$, we have

If $N = \prod_{p \in \mathfrak{S}} p^{\mu_p}$, the number of integral solutions of equation (1) *is less than* $56MN$.

We have seen that when N is divisible by a prime not in $\mathfrak{S}$, the number of solutions of (1) is less than M, hence

The number of integral solutions of the $x^2 + 7M^2 = N^y$ is less than $56MN$.

If $(M, 7N) = 1$, then $\sigma = 1$ or 2 according as $N \equiv 1$ or 2 (mod 2) and hence

If $(M, 7N) = 1$, the number of integral solutions of (1) *is less than* $4\sqrt{7N} \cdot 2^{t(N)} < 28N$.

If N is not a quadratic residue modulo 7^3, then $\chi = 0$ and hence

If N is not a quadratic residue modulo 7^3 the number of integral solutions of (1) *does not exceed*

$$12d(M_{\mathfrak{S}})\cdot 2^{t(N)} \leqq 12d(M)\cdot 2^{t(N)} ;$$

if in addition $(M, 7N) = 1$ *the number of solutions is less than* $6\cdot 2^{t(N)}$.

Our estimates on the number of solutions could be improved by using better estimates for $d(M_{\mathfrak{S}})$ and for $2^{t(N)}$. We have not done so here, because of the belief that the estimate on the multiplicity of the recurrence $F(k)$ is too crude to justify greater precision later.

9. A generalization. The methods just described enable one to estimate an upper bound for the number of integral solutions of

$$B(x^2 + 7M^2) = C\cdot N^y , \quad \text{where} \quad BC \geqq 1 \quad \text{and} \quad N \geqq 2 . \tag{8}$$

We sketch the argument.

We may without loss of generality assume that B and C are positive. If there is a solution there exists a minimal integer, say k, such that $B \mid (C\cdot N^k)$. Let $C\cdot N^k = AB$, then every solution of (8) leads to a solution of

$$x^2 + 7M^2 = A\cdot N^y , \quad \text{where} \quad A \geqq 1 \quad \text{and} \quad N \geqq 2 . \tag{9}$$

If there is a $p \notin \mathfrak{S}$ such that $p \mid A$ and $p^2 \nmid (AN, 7M^2)$ then equation (9) has at most one solution if $p = 7$ and it has no solution if $p \in \mathfrak{I}$. If $p \mid A$ and $p^2 \mid (AN, 7M^2)$ and if x, y is a solution of (9) we can set $x = p\mathscr{X}$, $M = p\mathscr{M}$ and

$$\mathscr{A} = \begin{cases} Ap^{-2} & \text{if} \quad p^2 \mid A \\ ANp^{-2} & \text{if} \quad p \nmid A , \end{cases}$$

then there is a one-to-one correspondence between the solutions of (9) and the equation $\mathscr{X}^2 + 7\mathscr{M}^2 = \mathscr{A}\cdot N^y$. In this way we can reduce the problem to the case where $A = \prod_{p\in\mathfrak{S}} p^{\alpha_p}$. If there is a prime not in $\mathfrak{S}$ which divides N we proceed as in the case where $A = 1$.

Suppose x, y is a solution of (9) with $A = \prod_{p\in\mathfrak{S}} p^{\alpha_p}$, and $N = \prod_{p\in\mathfrak{S}} p^{\mu_p}$. Write $A = A_1A_2$, where $A_1 = (A, N)$. Now to each factorization of N and of A_2 say $4N = \alpha\alpha'$ and $4A_2 = \gamma\gamma'$ into relatively prime factors there are induced factorizations of $4\sigma^2 = \delta\delta'$ and $4A_1 = \tau\tau'$, with $\delta \mid \alpha\gamma$ and $\tau \mid \alpha\gamma$. Then

$$\pm\sigma(x + M\sqrt{-7}) = \mathscr{P}(\tau\gamma\delta'\alpha^y) = \frac{S^\sharp(y) + T^\sharp(y)\sqrt{-7}}{16}$$

or

$$\pm 16\sigma M = T^\sharp(y) , \tag{10}$$

where $T^{\sharp}(y)$ is a linear recurrence of order two. Now using Theorem 3 of [1] one can estimate the number of solutions of (10). There are as many recurrences as there are factorizations of N and A_2 and possible σ. One can estimate the number of possible different recurrences and hence obtain an upper bound on the number of integral solutions of (9) and hence of (8).

II. The Equation $x^2 + 7M^2 = y^n$.

10. The solutions with y odd. We shall call an integral solution x, y of the equation

$$x^2 + 7M^2 = y^n\,, \quad \text{with} \quad M \geqq 1 \quad \text{and} \quad n \geqq 3\,, \tag{2}$$

primitive if x and y are coprime.

If x, y is a primitive solution of (2) then $(x, 7M) = 1$ and

$$\sigma = \begin{cases} 1 & \text{if } y \text{ is odd,} \\ 2 & \text{if } y \text{ is even.} \end{cases}$$

Also, we have seen in the discussion in § 3 that if $p \notin \mathfrak{S}$ and $p \mid y$ then $p \mid (x, M)$; hence $y = \prod_{p \in \mathfrak{S}} p^{\mu_p}$. Thus

$$y = (z + w\rho)(z + w\rho') = z^2 + zw + 2w^2\,,$$

where the factors on the right are relatively prime integers in $\mathfrak{O}$. Since $(z + w\rho)(z + w\rho') = (-z - w\rho)(-z - w\rho')$, we may assume that $w > 0$. Clearly y is odd only if $1 \equiv z \not\equiv w \pmod 2$. Should $2 \mid y$, we may have either $2 \mid z$ (in which case $2 \nmid w$, since the factors are relatively prime) or $z \equiv w \equiv 1 \pmod 2$, whence

$$z + w\rho = (z + w) - w\rho'\,.$$

Thus we may assume that

$$y = (z + w\rho)(z + w\rho')$$

where the factors are relatively prime, $y \equiv z \not\equiv w \pmod 2$ and $w > 0$.

Furthermore

$$(z + w\rho)^n = F_n(z, w) + G_n(z, w)\rho$$

where

$$F_{n+1}(z, w) = zF_n(z, w) - 2wG_n(z, w)\,, \qquad (n = 1, 2, \cdots)\,,$$
$$G_{n+1}(z, w) = (z + w)G_n(z, w) + wF_n(z, w)\,, \qquad (n = 1, 2, \cdots)\,,$$

with $F_0 = 1$, $G_0 = 0$. One easily checks that F_n and G_n are homogeneous forms of degree n and that w divides G_n.

Now if y is odd then $\sigma = 1$ and

$$x^2 + 7M^2 = [(x - M) + 2M\rho][(x - M) + 2M\rho'] ,$$

where the two factors on the right are relatively prime integers in $\mathfrak{O}$. Hence, by the unique factorization property of $\mathfrak{O}$, $\pm(F_n + G_n\rho)$ must be equal to one of these two factors.

Now

$$x - M + 2M\rho' = x + M - 2M\rho .$$

Hence if x, y (with y an odd integer) is a primitive solution of (2) then z, w (w an even integer) is a solution of

$$G_n(z, w) = \pm 2M .$$

In this case w is an even divisor of $2M$ and so there are at most $d(M)$ possibilities for w. To each choice for w there are two equations in z of degree $n - 1$ and therefore at most $2(n - 1)$ possibilities for z. Therefore

The number of primitive solutions of (2), *with y odd, does not exceed* $2(n - 1)d(M)$.

11. The solutions with y even. Suppose x, y (y an even integer), is a primitive solution of (2). Then x and M must be odd integers and $\sigma = 2$. Also

$$(x^2 + 7M^2)/4 = [(x - M)/2 + M\rho][(x - M)/2 + M\rho'] ,$$

where the two factors on the right are relatively prime integers in $\mathfrak{O}$. Now 2 divides the lefthand side of this equation. If $x \equiv M \pmod 4$ then $\rho \mid [(x - M)/2 + M\rho]$, hence

$$x^2 + 7M^2 = \left[x + M - \frac{(x - 3M)}{2}\rho\right]\left[x + M - \frac{(x - 3M)}{2}\rho'\right] ,$$

where the factors on the right are relatively prime and $\rho \mid (x + M)$, hence ρ devides the first factor. If $x \not\equiv M \pmod 4$ then $\rho \mid [(x + M)/2 - M\rho]$ and hence

$$x^2 + 7M^2 = \left[M - x + \frac{(x + 3M)}{2}\rho\right]\left[M - x + \frac{(x + 3M)}{2}\rho'\right] ,$$

where the factors on the right are relatively prime integers in $\mathfrak{O}$ and $\rho \mid (M - x)$, hence ρ divides the first factor.

Now, if y is even so is z, hence $2 \mid F_n(z, w)$ and therefore by the unique factorization property of $\mathfrak{O}$,

$$x + M = \pm F_n \quad \text{and} \quad 3M - x = \pm 2G_n \quad \text{when} \quad x \equiv M \pmod 4$$

$$-x + M = \pm F_n \quad \text{and} \quad 3M + x = \pm 2G_n \quad \text{when} \quad x \not\equiv M \pmod 4 .$$

In either case, we have: if x, y (y and even integer) is a primitive solution of (2) then there exists integers z and w such that

$$H_n(z, w) = F_n(z, w) + 2G_n(z, w) = \pm 4M , \tag{11}$$

with $z \neq 0$, $w > 0$, $(z, w) = 1$ and $2 \mid z$.

One shows by induction that

$$\frac{d}{dz}F_n = nF_{n-1} , \quad \frac{d}{dz}G_n = nG_{n-1} \quad \text{for} \quad n = 1, 2, \cdots ,$$

and hence

$$\frac{d}{dz}H_n = nH_{n-1} \qquad (n = 1, 2, \cdots) .$$

Let

$$L_n = (F_n, G_n) , \qquad (n = 0, 1, \cdots) .$$

Clearly $L_0 = L_1 = 1$. Suppose $L_j = 1$ $(j = 0, 1, \cdots, n)$. Now $L_{n+1} \mid (wF_{n+1} - zG_{n+1})$, i.e. $L_{n+1} \mid (w^2 + zw + z^2)G_n$; also $L_{n+1} \mid [(z + w)F_{n+1} + 2wG_{n+1}]$ or $L_{n+1} \mid (2w^2 + zw + z^2)F_n$. As $(F_n, G_n) = 1$, we have $L_{n+1} \mid (w^2 + zw + z^2, 2w^2 + zw + z^2)$ and hence $L_{n+1} = 1$.

The polynomials H_n $(n = 0, 1, \cdots)$ have non-vanishing discriminant, for

$$\begin{aligned}\left(H_n, \frac{d}{dz}H_n\right) = (H_n, nH_{n-1}) &= (H_n, H_{n-1}) \\ &= ((z + 2w)F_{n-1} + 2zG_{n-1}, F_{n-1} + 2G_{n-1}) \\ &= (2wF_{n-1}, F_{n-1} + 2G_{n-1}) \\ &= (F_{n-1}, G_{n-1}) = 1 .\end{aligned}$$

The heights of the coefficients of F_n and G_n are less than 2^{n+1} and 2^n, respectively. Thus the heights of coefficients of H_n is less than 2^{n+2}. Furthermore $H_n(1, 0) \neq 0 \neq H_n(0, 1)$.

Now the following theorem, which was proved in [2], enables us to estimate the number of solutions for the equation (11), hence of equation (2).

Let $H(z, w)$ be a binary form of degree $n \geqq 3$ with integral coefficients and non-zero discriminant satisfying $F(1, 0) \neq 0$ and $F(0, 1) \neq 0$. Let a be the height of $H(z, w)$; let

$$\alpha = \min_{1 \leqq h \leqq n-1} \left(\frac{n}{h + 1} + h\right) , \qquad \beta = \alpha + \frac{1}{n}$$

and let $p_1, p_2, \cdots, p_t$ *be any finite number of distinct primes. There are not more than*

$$2^{\frac{\beta+2}{\beta-2}}(2n^2a)^{\frac{4n}{\beta-2}} + e(t+1)\left[\frac{\log 48\alpha^2n^8}{\log(\alpha-1)} + 2\right]\left\{\frac{n^3}{n^2-\alpha n+1}\left(\frac{n^3}{\alpha n+1}\right)^{\frac{\alpha n+1}{n^2-\alpha n+1}}\right\}^{t+1}$$

pairs of integers z, w *satisfying*

$$z \neq 0\,, \quad w > 0\,, \quad (z, w) = 1\,, \quad F(z, w) \neq 0$$

for which $F(z, w)$ *has no prime factor distinct from* $p_1, p_2, \cdots, p_t$.

Since we are only interested solutions for which z is even, the term $2^{(\beta+2)/(\beta-1)}(2n^2a)^{4n/(\beta-2)}$ can be replaced by $(2n^2a)^{4n/(\beta-2)}$.

If x, y (y an even integer) is a primitive solution of (2), then M is an odd integer and the number of distinct prime divisors of $4M$ is $1 + t(M)$. It follows that:

The number of primitive solutions of (2) *with* y *even does not exceed*

$$(n^2 2^{n+3})^{\frac{4n}{\beta-2}} + e(2+t(M))\left[\frac{\log 48\alpha^2n^8}{\log(\alpha-1)} + 2\right]\left\{\frac{n^3}{n^2-\alpha n+1}\left(\frac{n^2}{\alpha n+1}\right)^{\frac{\alpha n+1}{n^2-\alpha n+1}}\right\}^{2+t(M)}.$$

12. An extension and a generalization. The methods just demonstrated may be used to obtain an upper bound on the totality of solutions of (2) and not just an upper bound on the number of primitive solutions. We sketch the argument.

Consider the diophantine equation

$$x^2 + 7M^2 = A \cdot y^n\,, \quad \text{with} \quad A \geqq 1 \quad \text{and} \quad n \geqq 3\,. \tag{12}$$

As seen earlier this equation has few solutions if A is divisible by a prime not in $\mathfrak{S}$, hence we assume that $A = \prod_{p \in \mathfrak{S}} p^{\mu_p}$.

If x, y is a solution of (12) with $(x, y) = (x, M) = 1$, then $\sigma = 1$ or 2. There are $2^{t(A)}$ factorizations of A of the form $A = (a + b\rho)(a + b\rho')$. To each factorization, we have

$$Ay^n = (F_n^* + G_n^*\rho)(F_n^* + G_n^*\rho')\,,$$

where $F_n^* + G_n^*\rho = (a + b\rho)(F_n + G_n\rho)$ and hence there is a binary form H_n^* of degree n such that $H_n^* = \pm 4M$. As previously indicated, we can estimate the number of solutions of this equation and hence obtain an upper bound on the number of solutions of (12) with $(x, y) = (x, M) = 1$.

If x, y is a solution of (12) with $(x, y) = 1$ and $(x, M) = d > 1$ then $d^2 \mid Ay^n$, hence $d^2 \mid A$. Set $x = d\mathscr{X}$, $M = d\mathscr{M}$, and $A = d\mathscr{A}$, then

$$\mathscr{X}^2 + 7\mathscr{M}^2 = \mathscr{A} \cdot y^n \quad \text{where} \quad (\mathscr{X}, y) = 1 = (\mathscr{X}, \mathscr{M}) .$$

Since $\mathscr{A} \mid A$, there are at most $d(A)$ such equations, and hence, using the estimates just discussed, we can obtain an upper bound on the number of primitive solutions of equation (12).

Finally let x, y be a solutions of (2). Let $g = (x, y)$ then $g^2 \mid 7M^2$ $g \mid M$. Set $x = g\mathscr{X}$, $y = g\mathscr{Y}$ and $M = g\mathscr{M}$, then $\mathscr{X}, \mathscr{Y}$ is a primitive solution of

$$\mathscr{X}^2 + 7\mathscr{M}^2 = (Ag^{n-2})\mathscr{Y}^n .$$

Since $g \mid M$, there are at most $d(M)$ such equations and hence one can compute an upper bound on the number of solutions of equation (2).

References

1. S. Chowla, M. Dunton and D. J. Lewis, *Linear recurrences of order two*, Pacific J. Math., **11** (1961).
2. D. J. Lewis and K. Mahler, *On the representation of integers by binary forms*, Acta Arith., **6** (1961), 333-363.
3. W. Ljungren, *On the diophantine equation* $x^2 + p^2 = y^n$, Kong. Norske Videnskabers Selskab Forhandl,. v. 16, Nr. 8, Trondheim (1943).
4. W. Ljungren, *On the diophantine equation* $x^2 + D = y^n$, Kong. Norske Nidenskabers Selskab Forhandl., v. 16, Nr. 23, Trondheim (1944).
5. L. J. Mordell, to appear in Arch. Math.
6. T. Nagell, *Sur l'impossibilité de quelques équations à deux indétermintes*, Norsk Matematisk Forenings Skrifter, Ser. I, Nr. 13, Oslo (1923).
7. ———, *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math., **5** (1954), 153-159.
8. ———, Norsk Math. Tidsskrift, **30** (1948), p. 62-64.
9. Th. Skolem, S. Chowla and D. J. Lewis, *The diophantine equation* $2^{n+2} - 7 = x^2$ *and related problems*, Proc. Amer. Math. Soc., **10** (1959), 663-669.

University of Notre Dame and
University of Manchester

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

RALPH S. PHILLIPS
Stanford University
Stanford, California

A. L. WHITEMAN
University of Southern California
Los Angeles 7, California

F. H. BROWNELL
University of Washington
Seattle 5, Washington

L. J. PAIGE
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH
T. M. CHERRY
D. DERRY
M. OHTSUKA
H. L. ROYDEN
E. SPANIER
E. G. STRAUS
F. WOLF

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON

* * *

AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
HUGHES AIRCRAFT COMPANY
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics
Vol. 11, No. 3 BadMonth, 1961