MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 152
OCTOBER 1980, PAGES 1347–1352

An Efficient Algorithmic Solution of the Diophantine Equation $u^2 + 5v^2 = m$

By Peter Wilker

Abstract. The determination of irreducible elements of the domain $Z[\sqrt{-5}]$ requires the solution of the Diophantine equation $u^2 + 5v^2 = m$, where m represents certain primes or products of two primes. An algorithm of order log m is given for the solution of the equation.

1. Introduction. It is well known that looking for primes of the domain $Z[\sqrt{-1}]$, one has to solve the Diophantine equation $u^2 + v^2 = p$ for rational primes $p \equiv 1 \bmod 4$. An efficient method for an algorithmic solution of the equation has already been presented by Hermite. Recently, J. Brillhart [1] published a considerable simplification of Hermite's method.

If one considers domains like $Z[\sqrt{-5}]$, which have no unique decompositions into irreducibles, the situation is more involved. It can be shown, using methods of algebraic number theory, that the irreducibles of $Z[\sqrt{-5}]$ are

(1) Rational primes $p \equiv 3, 7, 11, 13, 17, 19 \bmod 20$.

(2) The numbers 2 and $\sqrt{-5}$.

(3) Solutions $u + v\sqrt{-5}$ of the Diophantine equation $u^2 + 5v^2 = m$, where m is equal to one of the following:

(a) p, p a prime $\equiv 1, 9 \bmod 20$,

(b) $2p$, p a prime $\equiv 3, 7 \bmod 20$,

(c) pq, p, q primes $\equiv 3, 7 \bmod 20$.

(In case (c) there are always two nonassociate solutions.)

It is the purpose of this note to present an algorithm, shaped after the one used by Brillhart (loc. cit.), to efficiently solve $u^2 + 5v^2 = m$ for appropriate numbers m. The algorithm is easily described, but the proof is more involved as the continued fractions which occur are no longer regular. We prefer a direct approach using methods, but not results, from the theory of continued fractions.

The proof that the algorithm leads to a solution of the equation implies the existence of a solution. Otherwise, to prove existence, one usually relies on results from the theory of quadratic forms. For an approach using Minkowski's theorem, see Mordell [3].

We shall first derive necessary conditions for $u^2 + 5v^2 = m$ to be solvable, next describe the algorithm, and finally present a proof that it always leads to a solution.

Received December 19, 1978.
1980 *Mathematics Subject Classification.* Primary 10A30, 10B05.

Some remarks on the order of the algorithm and possible generalizations will conclude the paper.

2. Necessary Conditions for Solvability. Suppose $u^2 + 5v^2 = m$ is solvable. If m is divisible by 4 or 5, the equation will also be solvable for $m/4$ and $m/5$, respectively. We may therefore assume m not to be divisible by either 4 or 5. As the case $m = 1$ is trivial, we shall also assume $m > 1$.

Suppose m is odd. As $m \equiv u^2 \bmod 5$, m must be $\equiv 1, 4 \bmod 5$ and $m \equiv 1, 9, 11, 19 \bmod 20$. Considering the equation mod 4, one obtains $m \equiv 1, 9, 13, 17 \bmod 20$. Hence $m \equiv 1, 9 \bmod 20$.

If m is even, $m = 2m'$ say, then by the same argument $m' \equiv 2, 3 \bmod 5$ and $m' \equiv 3, 7, 13, 17 \bmod 20$. Considering the equation mod 8, one obtains easily $m' \equiv 3, 7, 11, 19 \bmod 20$. Hence $m' \equiv 3, 7 \bmod 20$.

We want to restrict m somewhat more. Suppose a prime $p \neq 5$ divides m but does not divide u and v. We choose x such that $u \equiv xv \bmod p$. Then $x^2 + 5 \equiv 0 \bmod p$, and -5 is a quadratic residue mod p. Consequently, $p \equiv 1, 3, 7, 9 \bmod 20$ or $p = 2$. If, therefore, p divides m, but $p \equiv 11, 13, 17, 19 \bmod 20$, then p must divide either u or v, hence both, which in turn means that p^2 divides m; u/p and v/p will then be a solution with respect to m/p^2. Thus, we may assume m not to be divisible by any prime $p \equiv 11, 13, 17, 19 \bmod 20$. As a consequence, $x^2 + 5 \equiv 0 \bmod m$ will always be solvable.

We shall use the results and assumptions of this section implicitly in the sequel.

3. Description of the Algorithm. To start the algorithm for a given m, solve $x^2 + 5 \equiv 0 \bmod m$ with $0 < x < m$. (It is sometimes convenient, though not necessary, to choose x such that $0 < x < m/2$.) Next develop the Euclidean algorithm with m and $x = r_0$ as a start:

$$m = f_0 r_0 + r_1,$$
$$r_0 = f_1 r_1 + r_2,$$
$$\cdots\cdots\cdots\cdots$$
$$r_{n-2} = f_{n-1} r_{n-1} + r_n,$$
$$r_{n-1} = f_n r_n + r_{n+1}.$$

We may always assume $r_0^2 \geqslant m$. If $r_0^2 < m$, obviously $x^2 + 5 = m$ and $u = x$; $v = 1$ is already a solution of $u^2 + 5v^2 = m$.

Develop the algorithm to the point where there is a first remainder less than $\sqrt{m}$. Let the notation be so chosen that $r_{n+1}^2 < m$, while $r_n^2 \geqslant m$. We must have $r_{n+1} > 0$, for $r_{n+1} = 0$ implies that r_n is a divisor of x and m, hence of 5. As m does not have the divisor 5, r_n must be equal to 1, contradicting $r_n^2 \geqslant m$.

Define a sequence g_i recursively as follows:

$$g_{-1} = 1, \quad g_0 = f_0, \quad g_i = f_i g_{i-1} + g_{i-2} \qquad (i = 1, \ldots, n).$$

We shall prove in Section 5:

THEOREM 1. $m = r_{n+1}^2 + 5g_n^2$.

As Brillhart in his note, we want to show that the calculation of g_n can be dispensed with. There are two cases to consider.

Case S. r_n is divisible by 5 and $(r_n/5)^2 < m$. We shall prove in Section 6:

THEOREM 2S. $g_n = r_n/5$, *consequently* $m = r_{n+1}^2 + 5(r_n/5)^2$.

Case N. Case S does not apply. We need the following:

LEMMA N. *The linear Diophantine equation* $r_n = r_{n+1}s + 5t$ *is solvable with* $s > 0, 0 < t < r_{n+1}$.

Let $s = f_{n+1}, t = r_{n+2}$.

THEOREM 2N. $g_n = r_{n+2}$, *consequently* $m = r_{n+1}^2 + 5r_{n+2}^2$.

We shall prove Lemma N and Theorem 2N in Section 7.

Let us consider two examples.

Case S. $m = 134, x = 53.$ $134 = 2\cdot 53 + 28,$
$53 = 1\cdot 28 + 25,$
$28 = 1\cdot 25 + 3.$
$g_2 = 5 = r_2/5$. Solution $134 = 3^2 + 5\cdot 5^2$.

Case N. $m = 269, x = 110.$ $269 = 2\cdot 110 + 49,$
$110 = 2\cdot 49 + 12,$
$49 = 2\cdot 12 + 5.5.$
$g_1 = r_3 = 5.$ Solution $269 = 12^2 + 5\cdot 5^2$.

4. Some Identities. In this section we derive some identities between the variables of the algorithm. Though we shall only need a few of them, it is quite as easy to state them in full generality.

$$(1)_i \qquad m = g_i r_i + g_{i-1} r_{i+1} \qquad (i = 0, 1, \ldots, n).$$

This follows immediately from the definition of g_i.

Next we show that there are constants t_{ij} such that

$$r_i r_j = (-1)^{i+j+1} 5 g_{i-1} g_{j-1} + t_{ij} m,$$

for $i, j = 0, 1, \ldots, n + 1$.

By induction, $g_i x \equiv (-1)^{i+1} r_{i+1} \bmod m$, $i = 0, \ldots, n$. Multiplying by x and adding $5g_i$, we get $g_i(x^2 + 5) \equiv 0 \equiv (-1)^{i+1} r_{i+1} x + 5g_i \bmod m$, hence $r_i x \equiv (-1)^{i+1} 5 g_{i-1} \bmod m$, $i = 0, \ldots, n + 1$. Finally, $r_i g_{j-1} x \equiv (-1)^{i+1} 5 g_{i-1} g_{j-1} \equiv (-1)^j r_i r_j \bmod m$.

To simplify notation we introduce $a_i = t_{ii}, b_i = t_{i,i+1}$. The identities just established imply

$$(2)_i \qquad r_i^2 + 5g_{i-1}^2 = a_i m \qquad (i = 0, \ldots, n + 1),$$

$$(3)_i \qquad r_i r_{i+1} - 5g_{i-1} g_i = b_i m \qquad (i = 0, \ldots, n).$$

Multiplying $(1)_i$ by r_{i+1} and using $(2)_{i+1}$ and $(3)_i$, we obtain

$$(4)_i \qquad r_{i+1} = b_i g_i + a_{i+1} g_{i-1} \qquad (i = 0, \ldots, n).$$

We need one inequality

$$(5)_i \qquad \text{If } r_i^2 \geqslant m, \quad \text{then } r_i > g_i.$$

To prove it, by $(1)_i$ write $r_i^2 - m = r_i^2 - g_i r_i - g_{i-1} r_{i+1} = r_i(r_i - g_i) - g_{i-1} r_{i+1} \geqslant 0$. Hence $r_i - g_i > 0$.

LEMMA 1. $a_i \not\equiv 2, 3 \bmod 5$ *and* $a_i \not\equiv 0 \bmod 4$ $(i = 0, \ldots, n+1)$.

Proof. As was shown in Section 2, solvability of $u^2 + 5v^2 = m$ implies $m \equiv 1, 4 \bmod 5$. If $a_i \equiv 2$ or $3 \bmod 5$, then $a_i m \equiv 2$ or $3 \bmod 5$, which contradicts $(2)_i$.

To prove the second assertion, multiply identities $(2)_i$ and $(2)_{i+1}$ together and use $(3)_i$ and $(1)_i$ to get

$$(6)_i \qquad a_i a_{i+1} = b_i^2 + 5.$$

If 4 divides a_i, then 4 divides $b_i^2 + 5$, which is impossible.

5. Proof of Theorem 1. To prove Theorem 1, we have to show that $a_{n+1} = 1$. By $(1)_n$, $(2)_{n+1}$ and $(5)_n$ we get

$$5m = 5g_n r_n + 5g_{n-1} r_{n+1} > 5g_n^2 + 5g_{n-1} r_{n+1}$$
$$= a_{n+1} m + 5g_{n-1} r_{n+1} - r_{n+1}^2 > a_{n+1} m - r_{n+1}^2.$$

From the assumption $r_{n+1}^2 < m$ we infer $6m > a_{n+1} m$, hence $1 \leqslant a_{n+1} \leqslant 5$. By Lemma 1, a_{n+1} cannot be equal to 2, 3 or 4. By $(2)_{n+1}$, $a_{n+1} = 5$ if and only if 5 divides r_{n+1}. (Remember that 5 does not divide m.) We now show that this is impossible. Thus $a_{n+1} = 1$ and Theorem 1 is proved.

LEMMA 2. $r_{n+1} \not\equiv 0 \bmod 5$.

Proof. Suppose $r_{n+1} = 5r'_{n+1}$, hence $a_{n+1} = 5$. $(3)_n$ implies $b_n = 5b'_n$ and $(3)_n$ and $(4)_n$ change to

$$r_n r'_{n+1} - g_{n-1} g_n = b'_n m; \qquad r'_{n+1} = b'_n g_n + g_{n-1}.$$

Because $g_n > g_{n-1}$, we must have $b'_n \geqslant 0$. $b'_n = 0$ leads to $r'_{n+1} = g_{n-1}$ and $r_n = g_n$, contradicting $(5)_n$. Thus $b'_n > 0$, which in turn implies $r'_{n+1} > g_n$. But $a_{n+1} m = 5m = r_{n+1}^2 + 5g_n^2 < r_{n+1}^2 + 5r'^2_{n+1} < 2r_{n+1}^2 < 2m$ is impossible.

Note that $r_{n+1} = 1$ implies $m = 5g_n^2 + 1$. Let $x = 5g_n$; then $x^2 + 5 = 5m$ and $m = g_n x + 1$. This shows $n = 0$. (The argument does not apply to the lowest case $m = 6$.) In the sequel, we may therefore assume $r_{n+1} > 1$.

6. Proof of Theorem 2S. Let us now take up Case S. As r_n is divisible by 5, the same holds for a_n by identity $(2)_n$. We shall write $r_n = 5r'_n$ and $a_n = 5a'_n$. $(2)_n$ changes to

$$(2)'_n \qquad 5r'^2_n + g_{n-1}^2 = a'_n m.$$

Lemma 1, applied to a_n, shows $a'_n \neq 4$. The argument of Lemma 1, applied to identity $(2)'_n$, yields $a'_n \neq 2$ or 3.

We now show that, by our assumption at the end of the preceding section, n cannot be 0. For $n = 0$, $(2)'_0$ would read $5r_0'^2 + 1 = a'_0 m$. As $r_0'^2 < m$, we would get $a'_0 \leqslant 5$. As $a'_0 = 5$ is clearly impossible, $a'_0 = 1$, and consequently $r_1 = 1$, a case we agreed to omit.

$(1)_{n-1}$ and $(5)_{n-1}$ now lead to

$$m = g_{n-1}r_{n-1} + g_{n-2}r_n > g_{n-1}^2 + g_{n-2}r_n$$
$$= a'_n m + g_{n-2}r_n - 5r_n'^2 > a'_n m - 5r_n'^2.$$

As $r_n'^2 < m$, we get $1 \leqslant a'_n \leqslant 5$. We have already excluded $a'_n = 2, 3$ or 4. $a'_n = 5$ would mean that g_{n-1} is divisible by 5, which in turn, by $(1)_n$, would make m divisible by 5. Hence $a'_n = 1$.

Introducing $a_{n+1} = 1$ and $a_n = 5$ into equality $(6)_n$ shows $b_n = 0$. By $(3)_n$ and $(4)_n$ we get $r_{n+1} = g_{n-1}$ and $r_n = 5g_n$. This proves Theorem 2S.

7. **Proof of Lemma N and Theorem 2N.** To establish Lemma N, note that, by Lemma 2, r_{n+1} and 5 are relatively prime. Thus, there is a solution of $r_n = r_{n+1}s - 5t$ with $s > 0$, $0 \leqslant t < r_{n+1}$. We may also assume $t > 0$. For $t = 0$ means that r_{n+1} divides r_n, which is only possible if r_{n+1} divides 5. This in turn means that $r_{n+1} = 1$, a case already dealt with.

Introduce $r_n = r_{n+1}s - 5t$ into $(3)_n$ and use $(2)_{n+1}$ with $a_{n+1} = 1$:

$$r_n r_{n+1} = r_{n+1}^2 s - 5r_{n+1}t = sm - 5sg_{n-1}^2 - 5r_{n+1}t = 5g_{n-1}g_n + b_n m.$$

Thus

$$(s - b_n)m = 5(sg_n^2 + r_{n+1}t + g_{n-1}g_n).$$

Identity $(4)_n$, together with $a_{n+1} = 1$ and $g_n > g_{n-1}$, imply $b_n \geqslant 0$. If $b_n = 0$, then $r_{n+1} = g_{n-1}$ and $r_n = 5g_n$ by $(3)_n$, which can only hold in Case N if $g_n^2 \geqslant m$. But $(2)_{n+1}$ shows $5g_n^2 < m$. Therefore $b_n > 0$.

The equation derived above now implies $0 < s - b_n < s$ and shows at the same time that $s - b_n$ is divisible by 5. This can only hold if $s > 5$. Consequently, we may define $f_{n+1} = s - 5$ and $r_{n+2} = r_{n+1} - t$, which proves Lemma N. Note that the solution as stated in the lemma is clearly unique.

To prove Theorem N, introduce $(4)_n$ into $(1)_n$ and use $(2)_{n+1}$ to obtain

$$r_n = b_n r_{n+1} + 5g_n.$$

As was shown above, $b_n > 0$. From $(4)_n$ we infer $0 < g_n < r_{n+1}$. Hence, as noted, $b_n = f_{n+1}$ and $g_n = r_{n+2}$, which is Theorem 2N.

8. **Efficiency of the Algorithm. Concluding Remarks.** The algorithm presented in Section 3 consists of three parts:

(1) A Euclidean algorithm (with certain tests on the way).

(2) The solution of a linear Diophantine equation.

(3) The solution of $x^2 \equiv -5 \bmod m$.

As is well known, (1) and (2) are problems of order log m. Problem (3) is also of order log m, as has been shown by D. H. Lehmer [2], if the prime factors of m are known. It is unknown to this author if Lehmer's procedure can be generalized to composite m without knowing its factorization. However, if one is interested not in the solution of $u^2 + 5v^2 = m$ for general m, but only in the determination of irreducibles of $Z[\sqrt{-5}]$, the problem does not present itself, though, of course, it is now necessary to determine primes $\equiv 1, 3, 7, 9 \bmod 20$.

The imaginary quadratic number field $Q(\sqrt{-5})$ has class number 2. Recently, all fields of this kind have been determined (H. M. Stark [4]). Of the 13 fields $Q(\sqrt{-d})$ (note that d in our notation does not denote the discriminant) two have prime numbers for d (5 and 37), while the rest has d's with two prime factors.

The author has applied the algorithm presented in this paper to the case $d = 6$. There occurs a new phenomenon, as Theorem 2S is not necessarily true with 6 instead of 5. For instance:

$$m = 4054, \quad x = 544 \qquad 4054 = 7\cdot 544 + 246,$$

$$544 = 2\cdot 246 + 52.$$

246 is divisible by 6 and $41^2 < 4054$. Again, $52^2 < 4054$. Nevertheless, $52^2 + 6\cdot 41^2 = 11850$.

An analysis of the proof shows that Eq. $(2)'_n$ of Section 6, with 6 instead of 5, does not necessarily imply $a'_n = 1$. One can show that in case $a'_n \neq 1$ one has to switch to Case N. In the example above the next line would be

$$246 = 3\cdot 52 + 6\cdot 15$$

and $52^2 + 6\cdot 15^2 = 4054$.

Of course, the reason underlying the different behavior of the algorithms is the fact that 6 is not a prime like 5. It is reasonable to assume that the other cases of quadratic number fields with class number 2 behave like the cases for 5 and 6, but the author has not attempted to treat the remaining cases.

Acknowledgements. The author wishes to thank Heinz Brugesser for bringing Brillhart's paper to his attention as well as Liselotte Kuntner for many stimulating discussions.

Institut für angewandte Mathematik
Universität Bern
Bern, Switzerland

1. J. BRILLHART, "Note on representing a prime as a sum of two squares," *Math. Comp.*, v. 26, 1972, pp. 1011–1013.

2. D. H. LEHMER, "Computer technology applied to the theory of numbers," *Studies in Number Theory,* Math. Assoc. Amer. (distributed by Prentice-Hall, Englewood Cliffs, N. J.), 1969, pp. 117–151.

3. L. J. MORDELL, *Diophantine Equations*, Academic Press, New York, 1969.

4. H. M. STARK, "On complex quadratic fields with class number two," *Math. Comp.*, v. 29, 1975, pp. 289–302.