MATH. SCAND. 11 (1962), 58–62

ON THE DIOPHANTINE EQUATION $\xi^2 - 2m^2\eta^2 = -1$

CHR. U. JENSEN

1.

On considering the diophantine equation $\xi^2 - 2m^2\eta^2 = -1$ for a prescribed natural number m, one may, as it is well known, without restriction assume m being an odd prime p since the above equation is solvable if and only if the equations arising by replacing m by any of its prime factors are solvable. Now an obvious necessary condition for the solvability of the equation

$$(*) \qquad \xi^2 - 2p^2\eta^2 = -1$$

is that $p \equiv 1 \bmod 4$, which, however, is by no means sufficient; on the other hand it is not hard to show that (*) has solutions in ξ and η for all primes $p \equiv 5 \bmod 8$; from now on p will therefore be assumed to be $\equiv 1 \bmod 8$. For such primes (*) may be solvable or not, and in fact, what is contained in the following, the solvability cannot be predicted from the residue classes (modulo any rational integer) to which p belongs.

However, in an old paper by Perrott [3] which seems to have been overlooked for a long time, the question has been settled for the primes $\equiv 1 \bmod 8$ but $\not\equiv 1 \bmod 16$, that is, $p \equiv 9 \bmod 16$, in terms of the representation of p by a simple binary quadratic form:

THEOREM 1 (J. Perrott). *Let p be a prime $\equiv 1 \bmod 8$ represented by the quadratic form $p = u^2 + 2v^2$; a necessary condition for the solvability of (*) is that $8|v$; for $p \equiv 9 \bmod 16$ this condition is also sufficient.*

In his rather long proof of this theorem Perrott actually deals with what one to-day would call Jacobian sums, which are known to be fairly disagreeable to handle.

In the following we shall in particular sketch how Perrott's result may be proven by means of class field theory, and moreover obtain a more general criterion deciding the solvability for primes $p \equiv 1 \bmod 16$ but $\not\equiv 1 \bmod 32$, that is, $p \equiv 17 \bmod 32$. In the statement of the theorem we need, of course, only consider primes satisfying the necessary condition given by Perrott, i.e. the primes representable by the form $p = u^2 + 128v_1^2$. For $p \equiv 1 \bmod 16$ this involves that 2 is a biquadratic residue

Received July 3, 1961.

mod p which, in turn, by a well-known result of Gauss implies that the representation of p as a sum of two squares takes the form $p = x^2 + 64y^2$. After these prefatory remarks the theorem may be formulated as follows.

THEOREM 2. *Let p be a prime $\equiv 1 \bmod 16$ satisfying the necessary condition of Theorem 1, i.e. representable by the form $p = u^2 + 128v_1^2$ and hence also by $p = x^2 + 64y^2$. Then a necessary condition for the solvability of (*) is that $y + v_1 \equiv \frac{1}{16}(p-1) \bmod 2$; for $p \equiv 17 \bmod 32$ this condition is also sufficient.*

2. Proofs of the theorems.

The question of solvability of (*) is equivalent to that of deciding whether the norm of the fundamental unit in the order of conductor p in the real-quadratic field $\mathsf{P}(2^{\frac{1}{2}})$ is $+1$ or -1. By means of elementary transformations this may as well be settled by the following

LEMMA. *Let $\varepsilon = 1 + 2^{\frac{1}{2}}$ denote the fundamental unit in $\mathsf{P}(2^{\frac{1}{2}})$ and let $2^\lambda \| p-1$; then a necessary and sufficient condition for the solvability of (*) is that*

$$\varepsilon^{(p-1)/2^{\lambda-1}} \equiv -1 \mod p .$$

First we apply this lemma to the theorem of Perrott. We immediately deduce that for primes $\equiv 9 \bmod 16$, (*) is solvable if and only if $\varepsilon^{\frac{1}{2}(p-1)} \equiv -1 \bmod p$, while $\varepsilon^{\frac{1}{2}(p-1)} \equiv +1 \bmod p$ is a necessary condition for the solvability if $p \equiv 1 \bmod 16$. In view of the known splitting theorems from algebraic number theory this means that we have to find the primes splitting fully in the (non-normal) extension $\mathsf{P}(2^{\frac{1}{2}}, \varepsilon^{\frac{1}{2}})$ and those splitting fully in $\mathsf{P}(2^{\frac{1}{2}}, \varepsilon^{\frac{1}{2}})$ but inert in the extension $\mathsf{P}(2^{\frac{1}{2}}, \varepsilon^{\frac{1}{2}})/\mathsf{P}(2^{\frac{1}{2}}, \varepsilon^{\frac{1}{2}})$. Recalling that all primes considered are $\equiv 1 \bmod 4$, we may as well consider the splitting of p in the more convenient absolute normal extension $\Omega = \mathsf{P}(2^{\frac{1}{2}}, i, \varepsilon^{\frac{1}{2}})$. Here it might be worth while to point out that, since this field is clearly non-abelian, it is an easy consequence of the general class field theory (Takagi's inversion theorem) that the primes looked for cannot be described by any congruence group in the field of rational numbers.

However, considering Ω over the imaginary quadratic field $\mathsf{P}((-2)^{\frac{1}{2}})$ we get an abelian extension, its Galois group being in fact cyclic of order 8. It therefore becomes our main task to determine the class groups $\mathfrak{H}_1$ and $\mathfrak{H}_2$ of the two extensions $\mathsf{P}(\varepsilon^{\frac{1}{2}}, 2^{\frac{1}{2}}, i)/\mathsf{P}((-2)^{\frac{1}{2}})$ and $\Omega/\mathsf{P}((-2)^{\frac{1}{2}})$. When first these have been computed, theorem 1 follows almost immediately.

To this purpose we first remark that, since the above extensions may be generated by adjoining square roots, resp. 4^{th} roots of units, the conductors of the two class groups must be powers of the prime divisor of 2 in $\mathsf{P}((-2)^{\frac{1}{2}})$, thus of $(-2)^{\frac{1}{2}}$.

Since the extensions are cyclic of order 4, resp. 8, the general theorem on the isomorphism between the Galois group and the factor group of the group of all ideals with respect to the corresponding class group implies that $\mathfrak{H}_1$ and $\mathfrak{H}_2$ contain all 4^{th}, resp. 8^{th} powers of ideals, in particular, that the conductors must divide $(-2)^{7/2}$, resp. $(-2)^{9/2}$.

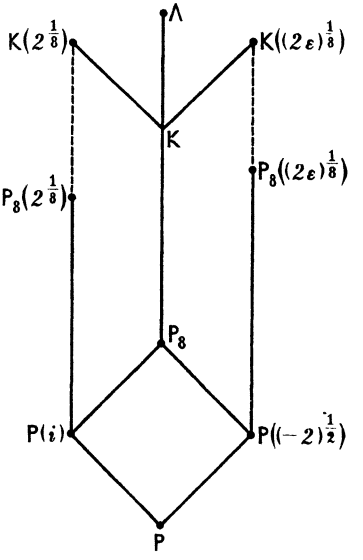
Now an easy calculation shows that the principal ideal (5) belongs to $\mathfrak{H}_1$ which in view of the fact that 5 and the global unit -1 are generators of the group of dyadic units implies that $\mathfrak{H}_1$ must contain all ideals generated by rational numbers.

According to these remarks, $\mathfrak{H}_1$ contains the residue classes $1, 3, \ldots, 15 \bmod 8(-2)^{\frac{1}{2}}$ (precisely: the ideals generated by the numbers in these residue classes) and the dyadic 4^{th} power $(9+4(-2)^{\frac{1}{2}})$ and hence the residue classes $k(9+4(-2)^{\frac{1}{2}})$, $k = 1, 3, \ldots, 15$, as well. The group formed by these has index 4 in the full group of ideals and must therefore be identical with the class group $\mathfrak{H}_1$ looked for. The elements of $\mathfrak{H}_1$ may clearly be characterized as the ideals generated by the numbers in the order $\bmod 4$, that is the numbers $a+b(-2)^{\frac{1}{2}}$ for which $b \equiv 0 \bmod 4$.

The computation of the second class group $\mathfrak{H}_2$ is facilitated if we make use of a sort of crossing method. In fact, we remark that the prime ideals splitting fully in Ω are exactly the primes splitting in $\mathsf{P}(\varepsilon^{\frac{1}{4}}, 2^{\frac{1}{4}}, i)$ which furthermore either split in both of the two extensions $\mathsf{P}(2^{\frac{1}{4}})/\mathsf{P}(\varepsilon^{\frac{1}{4}}, 2^{\frac{1}{4}}, i)$ and $\mathsf{P}((2\varepsilon)^{\frac{1}{4}})/\mathsf{P}(\varepsilon^{\frac{1}{4}}, 2^{\frac{1}{4}}, i)$ or are inert in both of them. Now the class group for $\mathsf{P}(2^{\frac{1}{4}})/\mathsf{P}((-2)^{\frac{1}{2}})$ consists of all ideals $(a+b(-2)^{\frac{1}{2}})$ for which $a \equiv \pm 1 \bmod 8$, $b \equiv 0 \bmod 2$ (this is merely an easy transformation of well-known criteria concerning the biquadratic residue character of 2), while the class group for $\mathsf{P}((2\varepsilon)^{\frac{1}{4}})/\mathsf{P}((-2)^{\frac{1}{2}})$ consists of the ideals $(a+b(-2)^{\frac{1}{2}})$ for which $b \equiv 0 \bmod 8$ (this is verified by an obvious generalization of the argument by which $\mathfrak{H}_1$ was determined). From these facts it readily follows that $\mathfrak{H}_2$ consists of the ideals $(a+b(-2)^{\frac{1}{2}})$ for which $b \equiv 0 \bmod 4$ and $\frac{1}{8}(a^2-1)+\frac{1}{4}b \equiv 0 \bmod 2$. By combining this result with the lemma theorem 1 is easily obtained.

Before we set out to prove theorem 2 we note that a necessary and sufficient condition for the solvability of (*) for primes $\equiv 17 \bmod 32$ cannot be expressed in terms of a single quadratic form; indeed, in view of the lemma this follows at once from the fact that the field $\mathsf{P}(\varepsilon^{\frac{1}{4}}, 2^{\frac{1}{4}}, i)$ is no abelian extension of $\mathsf{P}((-2)^{\frac{1}{2}})$ or of any quadratic field at all. Since we only deal with primes $\equiv 1 \bmod 16$ in theorem 2, we may as well

consider the field $\Lambda = \mathsf{P}(\varepsilon^{\frac{1}{8}}, 2^{\frac{1}{2}}, e^{2\pi i/16})$. Now, Λ being an abelian extension of the cyclotomic field $\mathsf{P}(2^{\frac{1}{2}}, i) = \mathsf{P}_8$ (the field of the 8^{th} roots of unity), a criterion may be obtained by working in this field. However, this would lead to very cumbersome calculations and the practical value of such a criterion might be somewhat questionable. Fortunately, in this



particular case we are able to describe the class group for Λ/P_8 entirely in terms of the two quadratic fields $\mathsf{P}((-2)^{\frac{1}{2}})$ and $\mathsf{P}(i)$ the compositum of which is exactly P_8. To this end we use a similar device as in the computation of $\mathfrak{H}_2$, namely a crossing by $\mathsf{K}(2^{\frac{1}{8}})$ and $\mathsf{K}((2\varepsilon)^{\frac{1}{8}})$, where K stands for the field $\Omega\mathsf{P}_{16} = \Omega(e^{2\pi i/16})$; in fact the primes splitting fully in Λ are the primes which split in K and either split in both $\mathsf{K}(2^{\frac{1}{8}})/\mathsf{K}$ and $\mathsf{K}((2\varepsilon)^{\frac{1}{8}})/\mathsf{K}$ or are inert in both of these. Equivalent to this requirement is that p should split in K and either split in $\mathsf{P}_8(2^{\frac{1}{8}})$ and $\mathsf{P}_8((2\varepsilon)^{\frac{1}{8}})$ or be inert in $\mathsf{P}_8(2^{\frac{1}{8}})/\mathsf{P}_8(2^{\frac{1}{4}})$ and $\mathsf{P}_8((2\varepsilon)^{\frac{1}{8}})/\mathsf{P}_8((2\varepsilon)^{\frac{1}{4}})$ (note that $2^{\frac{1}{4}}$ belongs to K since $2^{\frac{1}{4}} = (e^{2\pi i/16} + e^{-2\pi i/16})\,\varepsilon^{-\frac{1}{2}}$). The point is now that the question of splitting may in this way be reduced to the behaviour of the primes in the *abelian* extensions $\mathsf{P}_8(2^{\frac{1}{8}})/\mathsf{P}(i)$ and $\mathsf{P}_8((2\varepsilon)^{\frac{1}{8}})/\mathsf{P}((-2)^{\frac{1}{4}})$. The Galois groups of these two extensions are cyclic of orders 8 and 16, resp.

The first class group $\mathfrak{G}_1$ consists of all ideals $(c+di)$ for which $d \equiv 0 \bmod 8$ and $\frac{1}{8}(c^2-1) + \frac{1}{8}d \equiv 0 \bmod 2$. Due to an idea of Aigner [1] this is readily proven by means of the relation $2i = (1+i)^2$ and subsequent use of the biquadratic law of reciprocity in $\mathsf{P}(i)$; for

$$\left(\frac{2}{\mathfrak{p}}\right)_8 = \left(\frac{1+i}{\mathfrak{p}}\right)_4 \cdot \left(\frac{-i}{\mathfrak{p}}\right)_8 = \left(\frac{1+i}{\mathfrak{p}}\right)_4 \cdot (-i)^{(N(\mathfrak{p})-1)/8}$$

holds for all prime ideals $\mathfrak{p}$ in $\mathsf{P}(i)$ splitting in P_8.

The second class group $\mathfrak{G}_2$ can be computed by a method due to Aigner and Reichardt [2]; the details are similar to those in the determination of $\mathfrak{H}_1$. Indeed, one first proves that $\mathfrak{G}_2$ contains all 16^{th} powers of ideals in $\mathsf{P}((-2)^{\frac{1}{4}})$; next one shows by considering the generators of the dyadic units that all rational ideals belong to $\mathfrak{G}_2$. From this it is not hard to infer that $\mathfrak{G}_2$ is the group of ideals generated by the numbers in the order mod 16, that is the ideals of the form $(a+b(-2)^{\frac{1}{4}})$, $b \equiv 0 \bmod 16$.

Combining these two class groups according to the indications given above, we conclude that the primes splitting fully in Λ are characterized as those whose components $(a+b(-2)^{\frac{1}{4}})$ and $(c+di)$ in $\mathsf{P}((-2)^{\frac{1}{4}})$ and $\mathsf{P}(i)$ satisfy the relations $b \equiv 0 \bmod 8$, $d \equiv 0 \bmod 8$, $\frac{1}{8}b + \frac{1}{8}d \equiv 0 \bmod 2$.

Finally, by means of the lemma it is only routine work to verify theorem 2.

REFERENCES

1. A. Aigner, *Kriterium zum 8. and 16. Potenzcharakter der Reste* 2 *und* -2, Deutsche Math. 4 (1939), 44–52.
2. A. Aigner und H. Reichardt, *Stufenreihen im Potenzrestcharakter*, J. Reine Angew. Math. 184 (1942), 158–161.
3. J. Perrott, *Sur l'équation* $t^2 - Du^2 = -1$, J. Reine Angew. Math. 102 (1888), 185–223.

UNIVERSITY OF COPENHAGEN, DENMARK