MATH. SCAND. 10 (1962), 71–84

ON THE SOLVABILITY OF A CERTAIN CLASS OF NON-PELLIAN EQUATIONS

CHR. U. JENSEN

While Pell's equation $x^2 - Dy^2 = 1$, D a positive non-square integer, has always non-trivial integral solutions in x and y, the equation

$$\xi^2 - D\eta^2 = -1 \tag{0.1}$$

is solvable only for certain values of D. A necessary condition for the solvability of this equation is obviously that all odd prime factors of D be of the form $4n+1$; furthermore, if D is even, it cannot be divisible by 4. However, these conditions are not sufficient. ($D=34$ is the first counterexample.)

There exists an extensive literature concerning the problem of finding criteria for the solvability of (0.1). The most complete, but not very simple treatment of this subject has been given by Redei [6], [7]. After this article had been written, a recent paper by Furuta [1] dealing with the same subject by methods which have points of resemblance with those presented here, came to the author's knowledge.

The author wishes to thank Professor Th. Skolem for helpful comments and suggestions.

1.

In this note we shall consider non-Pellian equations of the form

$$\xi^2 - dm^2\eta^2 = -1\,, \tag{1.1}$$

where d is an odd square-free natural number and the equation is assumed to be solvable for $m=1$. We shall give some criteria for the solvability of the equation for prescribed odd natural numbers m.

It is well known that the solvability of (1.1) is equivalent to that of

$$\xi^2 - dm^2\eta^2 = -4\,. \tag{1.2}$$

Written in this form the problem in question may as well be regarded as that of deciding whether the norm of the fundamental unit of the order

Received February 11, 1961.

I_m of conductor m in the real-quadratic field $\mathsf{P}(d^{\frac{1}{2}})$ is 1 or -1. This has consequences for the structure of the corresponding ring class fields.

We will follow up this point of view somewhat more closely. Let the norm of the fundamental unit ε in the field $\mathsf{P}(d^{\frac{1}{2}})$ be -1. The order I_m is the integral domain consisting of the numbers $\frac{1}{2}(a+bd^{\frac{1}{2}})$, where a and b are rational integers for which $a \equiv b \bmod 2$ and $b \equiv 0 \bmod m$. Any unit α in I_m is a power of ε. If in particular $N\alpha = -1$, then

$$\alpha = \varepsilon^f, \quad f \text{ odd}.$$

Considering congruences in the principal order I, we have

$$\varepsilon^f \equiv \varepsilon'^f \mod m,$$

whence because of $N\varepsilon = -1$

$$\varepsilon^{2f} \equiv -1 \mod m.$$

Conversely, if $\varepsilon^{2f} \equiv -1 \bmod m$, multiplication on both sides by ε'^f yields

$$\varepsilon^f \equiv \varepsilon'^f \mod m$$

which shows that ε^f belongs to I_m, since m is odd. Thus we have proved:

LEMMA 1. *The equation* (1.2) (*subsidiarily* (1.1)) *is solvable if, and only if, there is an odd integer* f *such that* $\varepsilon^{2f} \equiv -1 \bmod m$.

It is obvious that, if (1.2) is solvable for an m having the prime decomposition $m = \prod_i p_i^{\nu_i}$, then it is solvable for $m = p_i$ for all i. On the other hand, let (1.3) be solvable for $m = p$, say

$$a^2 - dp^2b^2 = -4.$$

Then, putting $\alpha = \frac{1}{2}(a+pbd^{\frac{1}{2}}) = \varepsilon^f$, we obtain

$$\alpha^{p^{\nu-1}} = (\tfrac{1}{2})^{p^{\nu-1}} \varepsilon^{fp^{\nu-1}} = (\tfrac{1}{2})^{p^{\nu-1}} \{a^{p^{\nu-1}} + p^{\nu-1} a^{p^{\nu-1}} pbd^{\frac{1}{2}} + \ldots\} = \tfrac{1}{2}(a_\nu + b_\nu d^{\frac{1}{2}}),$$

where $p^\nu | b_\nu$, say $b_\nu = p^\nu c_\nu$. Clearly $N\alpha^{p^{\nu-1}} = -1$, so that

$$a_\nu^2 - dp^{2\nu} c_\nu^2 = -4.$$

Further (1.3) must be solvable for $m = \prod_i p_i^{\nu_i}$ when it is solvable for $m = p_i^{\nu_i}$ for all i. Indeed, there is for every i an odd number f_i such that

$$\varepsilon^{2f_i} \equiv -1 \mod p_i^{\nu_i},$$

whence

$$\varepsilon^{2f} \equiv -1 \mod m,$$

where f denotes the least common multiple of all the f_i. Thus the following statement is proved:

LEMMA 2. *The equation* (1.2) (*subsidiarily* (1.1)) *is solvable for an odd number* m *with the prime decomposition* $m=\prod_i p_i^{\nu_i}$ *if, and only if, it is solvable for* $m=p_i$ *for all* i.

With regard to applications given in the next section we will consider primes p for which $p\equiv 1 \bmod 4$ and $(d/p)=1$. Such primes split in $\mathsf{P}(d^{\frac{1}{2}})$ into distinct prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$. Using the Euler criterion we have

$$\left(\frac{\varepsilon}{\mathfrak{p}}\right) \equiv \varepsilon^{\frac{1}{2}(p-1)} \mod \mathfrak{p} \quad \text{and} \quad \left(\frac{\varepsilon}{\mathfrak{p}'}\right) \equiv \varepsilon^{\frac{1}{2}(p-1)} \mod \mathfrak{p}' .$$

By passing over to the conjugates we infer

$$\left(\frac{\varepsilon}{\mathfrak{p}'}\right) = \left(\frac{\varepsilon'}{\mathfrak{p}}\right) = \left(\frac{\varepsilon^2\varepsilon'}{\mathfrak{p}}\right) = \left(\frac{-\varepsilon}{\mathfrak{p}}\right) = \left(\frac{-1}{\mathfrak{p}}\right)\cdot\left(\frac{\varepsilon}{\mathfrak{p}}\right) = \left(\frac{\varepsilon}{\mathfrak{p}}\right)$$

since

$$\left(\frac{-1}{\mathfrak{p}}\right) = (-1)^{\frac{1}{2}(N\mathfrak{p}-1)} = (-1)^{\frac{1}{2}(p-1)} = 1 .$$

Thus for the primes considered, exactly one of the congruences

$$\varepsilon^{\frac{1}{2}(p-1)} \equiv \pm 1 \mod p$$

must be valid.

By means of Lemma 1 we easily deduce the following lemma concerning the sign in the above congruence.

LEMMA 3. *Let* p *be a prime for which* $(d/p)=1$ *and* $p\equiv 1 \bmod 4$. *If* $p\equiv 5 \bmod 8$ *the diophantine equation* (1.2) *is solvable if and only if* $\varepsilon^{\frac{1}{2}(p-1)}\equiv -1 \bmod p$, *where* ε *denotes the fundamental unit in* $\mathsf{P}(d^{\frac{1}{2}})$. *If* $p\equiv 1 \bmod 8$, *the validity of the congruence* $\varepsilon^{\frac{1}{2}(p-1)}\equiv 1 \bmod p$ *is a necessary* (*but in general not a sufficient*) *condition for the solvability of* (1.2).

PROOF. Let us first consider primes $p\equiv 5 \bmod 8$. If (1.2) is solvable, there is a least positive odd number f_1, such that $\varepsilon^{2f_1}\equiv -1 \bmod p$. Then $4f_1$ is the smallest positive integer for which $\varepsilon^{4f_1}\equiv 1 \bmod p$. Since $\frac{1}{2}(p-1)$ is only divisible by 2, but not by 4, we must have $\varepsilon^{\frac{1}{2}(p-1)}\equiv -1 \bmod p$, because otherwise $4f_1 \mid \frac{1}{2}(p-1)$. If on the other hand $\varepsilon^{\frac{1}{2}(p-1)}\equiv -1 \bmod p$, then $\frac{1}{4}(p-1)$ is just an odd number f such that $\varepsilon^{2f}\equiv -1 \bmod p$.

Now let $p\equiv 1 \bmod 8$, and let (1.2) be solvable. Since $\frac{1}{2}(p-1)$ is now divisible by 4, we see that in this case $4f_1 \mid \frac{1}{2}(p-1)$ and hence $\varepsilon^{\frac{1}{2}(p-1)}\equiv 1 \bmod p$.

By the way, we may state the following more general result: Let $2^\lambda \| (p-1)$, $\lambda \geqq 2$. Then (1.2) is solvable if and only if

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

Indeed, if this congruence is true, then $f=(\frac{1}{2})^{\lambda}(p-1)$ is an odd number such that $\varepsilon^{2f}\equiv -1 \bmod p$ so that (1.2) is solvable. Conversely, let (1.2) be solvable. Then there is a smallest positive odd number f_1 such that $\varepsilon^{2f_1}\equiv -1 \bmod p$. Then $4f_1$ is the smallest positive integer such that $\varepsilon^{4f_1}\equiv 1 \bmod p$, which implies that $4f_1|p-1$, whence $f_1|(\frac{1}{2})^{\lambda}(p-1)$ and the quotient is odd. Hence, $\varepsilon^{2f_1}\equiv -1 \bmod p$ yields $\varepsilon^{(p-1)/2^{\lambda-1}}\equiv -1 \bmod p$.

In the following section we first consider in detail the special case $d=5$, and afterwards, in Section 3, we discuss which of the criteria may be generalized to an arbitrary square-free odd d.

2. The equation $\xi^2-5m\eta^2=-4$.

As shown above in Lemma 2 we may assume that m is a prime $p\equiv 1 \bmod 4$. Now it is elementary and well known that the equation is solvable if $(5/p)=-1$, that is, if $p\equiv \pm 2 \bmod 5$. Therefore we may henceforth assume that $p\equiv 1 \bmod 4$ and $(5/p)=1$, that is, $p\equiv 1$ or $9 \bmod 20$.

The fundamental unit in $\mathsf{P}(5^{\frac{1}{2}})$ is

$$\omega = \tfrac{1}{2}(1+5^{\frac{1}{2}}) .$$

Hence, concerning the solvability of the equation in question, which now takes the form

$$\xi^2-5p^2\eta^2 = -4 , \tag{2.1}$$

we obtain the following statement using Lemma 3 in the preceeding section:

If $p\equiv 5 \bmod 8$, (2.1) *is sovable if and only if* $\omega^{\frac{1}{2}(p-1)}\equiv -1 \bmod p$.

If $p\equiv 1 \bmod 8$, *the validity of the congruence* $\omega^{\frac{1}{2}(p-1)}\equiv 1 \bmod p$ *is a necessary condition for the solvability of* (2.1).

We now establish some simple criteria deciding the sign in the congruence

$$\omega^{\frac{1}{2}(p-1)} \equiv \pm 1 \mod p \tag{2.2}$$

and obtain in this way criteria for the solvability of (2.1). More precisely we are going to prove the following theorem:

THEOREM 1. *Let* p *be a prime for which* $(5/p)=1$ *and* $p\equiv 1 \bmod 4$. *Such primes may be represented by each of the quadratic forms*

I) $p=u^2-5v^2$,
II) $p=s^2+5t^2$,
III) $p=x^2+25y^2$.

Criteria concerning the sign in (2.2) *may be established in terms of any of these representations*:

I′) *The plus sign in* (2.2) *holds if and only if* $|u|+v\equiv 1 \bmod 4$.

II′) *The plus sign in* (2.2) *holds if and only if* t *is even.*

III′) *The plus sign in* (2.2) *holds if and only if* $(x/5)=1$ *or* -1 *according as* y *is even or odd.*

These yield evidently the following criteria for the solvability of (2.1).

I″) *A necessary condition for the solvability of* (2.1) *is that* $|u|\equiv 1 \bmod 4$. *For* $p\equiv 5 \bmod 8$ *this condition is also sufficient.*

II″) *A necessary condition for the solvability of* (2.1) *is that* $\frac{1}{4}(p-1)+t$ *is even. For* $p\equiv 5 \bmod 8$ *this condition is also sufficient.*

III″) *A necessary condition for the solvability of* (2.1) *is that* $(x/5)=1$ *or* -1 *according as* $\frac{1}{4}(p-1)+y$ *is even or odd. For* $p\equiv 5 \bmod 8$ *this condition is also sufficient.*

REMARK. Since we are giving an elementary proof of the theorem at the end of this section, it should be pointed out that the above representations, well-known from algebraic number theory, may be obtained by entirely elementary methods as developed in Nagell [4, Chap. VI].

PROOF OF THEOREM 1. We start the proof by establishing the equivalence of the statements I′), II′), III′) (subsidiarily I″), II″), III″)), that is I′)$\Leftrightarrow$II′) and I′)$\Leftrightarrow$III′). Since the proofs are analogous, we only carry out the first one, I′)$\Leftrightarrow$II′). It consists of two parts:

(a) If $p=s^2+5t^2$ with an even t, then $|u|+v\equiv 1 \bmod 4$.

(b) If $p=s^2+5t^2$ with an odd t, then $|u|+v\equiv -1 \bmod 4$.

ad a): From the representations $p=s^2+5t^2=u^2-5v^2$ we get

$$u^2-s^2 = (|u|+s)(|u|-s) = 5(t^2+v^2)\,.$$

Putting $(t,v)=\mu$ and $t=\mu t_1$, $v=\mu v_1$, where μ obviously is even, this may also be written

$$\tfrac{1}{2}(|u|+s)\cdot\tfrac{1}{2}(|u|-s) = 5(\tfrac{1}{2}\mu)^2({t_1}^2+{v_1}^2)\,.$$

Since $(\frac{1}{2}(|u|+s), \frac{1}{2}(|u|-s), \frac{1}{2}\mu)=1$ we conclude that, with a suitable choice of the signs, $\frac{1}{2}(|u|\pm s)$ and $\frac{1}{2}(|u|\mp s)/(\frac{1}{2}\mu)^2$ are positive integers all odd prime divisors of which are divisors of the quadratic form $5({t_1}^2+{v_1}^2)$ with coprime t_1 and v_1 and must therefore be $\equiv 1 \bmod 4$. We now distinguish between the cases $4|v$ and $2\|v$. Since

$$5(t^2+v^2) = u^2-s^2 \equiv 0 \mod 8\,,$$

$4|v$ implies $4|t$, that is $4|(t,v)=\mu$. We thus obtain

$$|u| = \frac{|u|\pm s}{2} + (\tfrac{1}{2}\mu)^2\frac{|u|\pm s}{2\cdot(\frac{1}{2}\mu)^2} \equiv 1+0 \equiv 1 \mod 4\,.$$

Similarly $2||v$ implies $2||t$, that is $\frac{1}{2}\mu$ is odd, and $2^3||5(t^2+v^2)$. Hence the even one of the numbers $\frac{1}{2}(|u|\pm s)$ and $\frac{1}{2}(|u|\mp s)/(\frac{1}{2}\mu)^2$ cannot be divisible by 4. Therefore we have

$$|u| = \frac{|u|\pm s}{2} + (\tfrac{1}{2}\mu)^2\frac{|u|\mp s}{2\cdot(\frac{1}{2}\mu)^2} \equiv 1+2 \equiv -1 \mod 4\,.$$

In either case we have shown that $|u|+v\equiv 1 \bmod 4$.

ad b): In this case $(t,v)=\mu$ is odd. Since $(|u|-s,|u|+s,\mu)=1$,

$$(|u|-s)(|u|+s) = 5\mu^2(t_1^2+v_1^2)\,,$$

implies that $|u|\pm s$ and $(|u|\mp s)/\mu^2$ with suitably chosen signs are odd integers all of whose prime divisors must be $\equiv 1 \bmod 4$, and which therefore must be $\equiv 1 \bmod 4$ themselves. Since $4|v$ or $2||v$ according as $2||s$ or $4|s$, we conclude that

$$|u| = (|u|\pm s)\mp s \equiv 1\mp(v+2) \mod 4$$

or

$$|u|+v \equiv -1 \mod 4\,.$$

Thus the equivalence I')$\Leftrightarrow$II') has been established. Consequently we have only to prove one of the propositions I'), II') or III'). For the results from class field theory and the theory of reciprocity to be used we refer to Hasse [2].

We first remark that, using the main theorems from class field theory, the existence of criteria of the forms mentioned becomes almost trivial. In fact, one has only to observe that the primes p for which the plus sign in (2.4) is valid, may be characterized as those primes of the rational number field P which are products of distinct prime ideals of degree 1 in the field $\mathsf{P}(i,\omega^{\frac{1}{2}})$. This field is an abelian extension of each of the quadratic fields $\mathsf{P}(5^{\frac{1}{2}})$, $\mathsf{P}((-5)^{\frac{1}{2}})$ and $\mathsf{P}(i)$. Hence, the primes in question, decomposed in these fields, are fully described by the class groups of the extensions. In general the explicit computation of class groups of abelian extensions is, however, by no means straightforward, as is well known to any one, who has tried.

Only in one of the cases considered a direct determination is very simple, viz. for the cyclic extension $\mathsf{P}(\omega^{\frac{1}{2}})/\mathsf{P}((-5)^{\frac{1}{2}})$ of degree 4. Incorporating the intermediate field $\mathsf{P}(i,(-5)^{\frac{1}{2}})$, which is the absolute class field of $\mathsf{P}((-5)^{\frac{1}{2}})$, it is not hard to see that the conductor of the class group

is 2. Since in $\mathsf{P}((-5)^{\frac{1}{4}})$ the only ideal group mod 2 of index 4 is the group of principal ideals (α) generated by numbers α in the ray $\alpha \equiv 1 \bmod 2$, this must be the class group looked for. This accomplishes, the proof of II').

It is true that this suffices for the proof of Theorem 1, but since in the next section it turns out that not all of the criteria included in the theorem can be applied to the general case, we also give direct proofs of I') and III'). Furthermore, at the end of this section we give a purely elementary proof of I') so that in fact each of the criteria may be proved exclusively by the methods of elementary number theory.

For a direct proof of I') we observe that the factorization of p in $\mathsf{P}(5^{\frac{1}{4}})$ is given by $p \simeq \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p} = (u + v5^{\frac{1}{4}})$ and $\mathfrak{p}' = (u - v5^{\frac{1}{4}})$, say, and u chosen positive. In virtue of

$$\left(\frac{\omega}{\mathfrak{p}}\right) = \left(\frac{\omega}{\mathfrak{p}'}\right) \equiv \omega^{\frac{1}{4}(p-1)} \mod p\,,$$

it becomes our task to determine the above quadratic residue symbol. For this purpose we apply the law of quadratic reciprocity in $\mathsf{P}(5^{\frac{1}{4}})$:

$$\left(\frac{\omega}{u+v5^{\frac{1}{4}}}\right)\cdot\left(\frac{u+v5^{\frac{1}{4}}}{\omega}\right) = \left(\frac{\omega, u+v5^{\frac{1}{4}}}{2}\right)\cdot\left(\frac{\omega, u+v5^{\frac{1}{4}}}{\mathfrak{p}_\infty}\right).$$

Here

$$\left(\frac{u+v5^{\frac{1}{4}}}{\omega}\right) = 1 \qquad \text{and} \qquad \left(\frac{\omega, u+v5^{\frac{1}{4}}}{\mathfrak{p}_\infty}\right) = 1\,,$$

the first equality holding because ω is a unit and the latter one because $u + v5^{\frac{1}{4}}$ is totally positive. To find the value of the remaining norm residue symbol we remark that, in consequence of the general theory, the norm residue symbol depends only on the residue classes of the components mod 4. Furthermore, v being an even number, $u + v5^{\frac{1}{4}} \equiv 1$ or $-1 \bmod 4$ according as $u + v \equiv 1$ or $-1 \bmod 4$. Hence

$$\left(\frac{\omega}{\mathfrak{p}}\right) = \left(\frac{\omega, 1}{2}\right) \qquad \text{or} \qquad \left(\frac{\omega}{\mathfrak{p}}\right) = \left(\frac{\omega, -1}{2}\right).$$

Since ω and 1 are units, we conclude

$$\left(\frac{\omega, 1}{2}\right) = \left(\frac{\omega, 1}{\mathfrak{p}_\infty}\right) = 1 \qquad \text{and} \qquad \left(\frac{\omega, -1}{2}\right) = \left(\frac{\omega, -1}{\mathfrak{p}_\infty}\right) = -1\,.$$

Summing up these results, we have proved

$$\omega^{\frac{1}{4}(p-1)} \equiv 1 \text{ or } -1 \mod p \quad \text{according as} \quad u + v \equiv 1 \text{ or } -1 \mod 4\,,$$

and hence I').

In order to prove III') directly we shall compute the class group of the bicyclic extension $\mathsf{P}(i,\omega^{\frac{1}{2}})/\mathsf{P}(i)$. In virtue of

$$(\omega^{\frac{1}{2}}+\omega'^{\frac{1}{2}})^2 = 1+2i\,,$$

where ω' as usual denotes the conjugate of ω, the extension is generated by adjoining the square roots $5^{\frac{1}{2}}$ and $(1+2i)^{\frac{1}{2}}$ to the ground field $\mathsf{P}(i)$. Hence, by a well-known theorem, the primes which split in the extension concerned are exactly those splitting in each of the relative quadratic fields $\mathsf{P}(5^{\frac{1}{2}},i)/\mathsf{P}(i)$ and $\mathsf{P}\big((1+2i)^{\frac{1}{2}}\big)/\mathsf{P}(i)$. Since all of the primes in question split in the first one, we only have to require splitting in $\mathsf{P}\big((1+2i)^{\frac{1}{2}}\big)/\mathsf{P}(i)$, that is, if $p\simeq\mathfrak{P}\mathfrak{P}'$ with $\mathfrak{P}=(x+5yi)$, say, is the factorization of p in $\mathsf{P}(i)$, then

$$\left(\frac{1+2i}{\mathfrak{P}}\right)=\left(\frac{1+2i}{\mathfrak{P}'}\right)=1$$

must hold.

We proceed just as before using the reciprocity law in $\mathsf{P}(i)$, namely

$$\left(\frac{1+2i}{\mathfrak{P}}\right)=\left(\frac{x+5yi}{1+2i}\right)\cdot\left(\frac{x+5yi,\,1+2i}{1+i}\right)=\left(\frac{x}{1+2i}\right)\cdot\left(\frac{x+5yi,\,1+2i}{1+i}\right).$$

Here the first factor is equal to the usual quadratic residue symbol $(x/5)=1$ or -1 according as $x\equiv\pm1$ or $\pm2 \bmod 5$, and the second one 1 or -1 according as y is even or odd. By combination of these results, III') is established.

Finally we point out that, as mentioned above, I') may be proved solely by methods of elementary number theory. In fact, since obviously $5\equiv(u/v)^2 \bmod p$ and $b\equiv0 \bmod p$ in the expression

$$\omega^{\frac{1}{2}(p-1)} = \tfrac{1}{2}(a+b5^{\frac{1}{2}})\,,$$

we get

$$\begin{aligned}2^{\frac{1}{2}(p-3)}a &= \sum_{k=0}^{\frac{1}{2}(p-1)}\binom{\frac{1}{2}(p-1)}{2k}5^k \equiv \sum_{k=0}^{\frac{1}{2}(p-1)}\binom{\frac{1}{2}(p-1)}{2k}\left(\frac{u}{v}\right)^{2k}+b\frac{u}{v}\\ &\equiv \sum_{k=0}^{\frac{1}{2}(p-1)}\binom{\frac{1}{2}(p-1)}{2k}\left(\frac{u}{v}\right)^{2k}+\sum_{k=1}^{\frac{1}{2}(p-1)}\binom{\frac{1}{2}(p-1)}{2k-1}\left(\frac{u}{v}\right)^{2k-1}\\ &\equiv \left(1+\frac{u}{v}\right)^{\frac{1}{2}(p-1)} \bmod p\end{aligned}$$

and thus

$$\omega^{\frac{1}{2}(p-1)}\equiv\left(\frac{1+u/v}{2}\right)^{\frac{1}{2}(p-1)}\equiv\left(\frac{\frac{1}{2}(1+u/v)}{p}\right)\equiv\left(\frac{2v(u+v)}{p}\right) \bmod p\,.$$

Using the reciprocity law in the rational field we see that with u and v chosen positive

$$\left(\frac{u+v}{p}\right) = \left(\frac{p}{u+v}\right) = \left(\frac{u^2-5v^2}{u+v}\right) = \left(\frac{-4v^2}{u+v}\right) = \left(\frac{-1}{u+v}\right) = (-1)^{\frac{1}{2}(u+v-1)}.$$

Hence it only remains to be shown that $(2v/p)=1$. Here we distinguish between the cases $p\equiv 5 \bmod 8$ and $p\equiv 1 \bmod 8$. In the first case we have $2||v$, that is, $v=2v'$ with v' odd. Thus

$$\left(\frac{2v}{p}\right) = \left(\frac{4v'}{p}\right) = \left(\frac{v'}{p}\right) = \left(\frac{p}{v'}\right) = \left(\frac{u^2-5v^2}{v'}\right) = \left(\frac{u^2}{v'}\right) = 1.$$

In the second case we put $v=2^j v'$ with v' odd. Since here $(2/p)=1$, we get

$$\left(\frac{2v}{p}\right) = \left(\frac{v'}{p}\right) = \left(\frac{p}{v'}\right) = \left(\frac{u^2-5v^2}{v'}\right) = \left(\frac{u^2}{v'}\right) = 1,$$

which proves the assertion.

3.

In this section we turn to the solvability of the general equation

$$\xi^2 - dm^2\eta^2 = -1, \tag{3.1}$$

supposed to be solvable for $m=1$. Just as in the preceeding section we need only to consider the case, where m is a prime $p\equiv 1 \bmod 4$. Furthermore, since (3.1) is surely solvable for $(d/p)=-1$, we henceforth assume $(d/p)=1$.

Only part III′ of Theorem 1 applies to the general situation, the two others only if d is a prime q. First we look at this case, distinguishing between the $q\equiv 5 \bmod 8$ and the $q\equiv 1 \bmod 8$. Concerning the solvability of the equation (3.1), which now takes the form

$$\xi^2 - qp^2\eta^2 = -1, \tag{3.2}$$

we actually prove the following in the case $q\equiv 5 \bmod 8$.

THEOREM 2. *Let q be a prime $\equiv 5 \bmod 8$. Primes p for which $(q/p)=1$ and $p\equiv 1 \bmod 4$ possess the following representations*

I) $p^h = u^2 - qv^2$ *or* $p^h = \frac{1}{4}({u_1}^2 - q{v_1}^2)$, u_1 *and* v_1 *odd*; h *being the class number of* $\mathsf{P}(q^{\frac{1}{2}})$.

II) $p^{\frac{1}{2}h'} = u^2 + qv^2$; h' *being the class number of* $\mathsf{P}((-q)^{\frac{1}{2}})$.

With these representations

I) *A necessary condition for the solvability of* (3.2) *is that* $|u|\equiv 1 \bmod 4$ *or* $\frac{1}{2}(|u_1|+1)\equiv\frac{1}{4}(p-1) \bmod 2$, *respectively. If* $p\equiv 5 \bmod 8$, *this condition is also sufficient.*

II) *A necessary condition for the solvability of* (3.2) *is that* $\frac{1}{4}(p-1)+t$ *is even. If* $p \equiv 5 \bmod 8$ *this condition is also sufficient.*

PROOF. ad I): Let $\xi_0+\eta_0 q^{\frac{1}{2}}$ be the fundamental solution of

$$\xi^2 - q\eta^2 = -1 .$$

Exactly as in Section 2 we only have to determine $(\xi_0+\eta_0 q^{\frac{1}{2}})^{\frac{1}{2}(p-1)} \bmod p$, applying Lemma 3 with ε replaced by $\xi_0+\eta_0 q^{\frac{1}{2}}$.

In $\mathsf{P}(q^{\frac{1}{2}})$ the factorization of p is given by $p \simeq \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}$ and $\mathfrak{p}'$ are two conjugate prime ideals. With suitably chosen $\mathfrak{p}$ and $\mathfrak{p}'$, we then have

$$q^{\frac{1}{2}} \equiv \frac{u}{v} \bmod \mathfrak{p} \qquad \text{and} \qquad q^{\frac{1}{2}} \equiv -\frac{u}{v} \bmod \mathfrak{p}'$$

if

$$p^h = u^2 - qv^2 .$$

Hence

$$\left(\frac{\xi_0+\eta_0 q^{\frac{1}{2}}}{\mathfrak{p}}\right) \equiv (\xi_0+\eta_0 q^{\frac{1}{2}})^{\frac{1}{2}(p-1)} \equiv (\xi_0+\eta_0 u/v)^{\frac{1}{2}(p-1)} \equiv \left(\frac{\xi_0+\eta_0 u/v}{p}\right) \bmod \mathfrak{p} ,$$

$$\left(\frac{\xi_0+\eta_0 q^{\frac{1}{2}}}{\mathfrak{p}'}\right) \equiv (\xi_0+\eta_0 q^{\frac{1}{2}})^{\frac{1}{2}(p-1)} \equiv (\xi_0-\eta_0 u/v)^{\frac{1}{2}(p-1)} \equiv \left(\frac{\xi_0-\eta_0 u/v}{p}\right) \bmod \mathfrak{p}' .$$

However, since $\mathsf{P}\big((\xi_0+\eta_0 q^{\frac{1}{2}})^{\frac{1}{2}}, i\big)/\mathsf{P}$ is a normal extension,

$$\left(\frac{\xi_0+\eta_0 u/v}{p}\right) = \left(\frac{\xi_0+\eta_0 q^{\frac{1}{2}}}{\mathfrak{p}}\right)$$

must have the same value as

$$\left(\frac{\xi_0-\eta_0 u/v}{p}\right) = \left(\frac{\xi_0+\eta_0 q^{\frac{1}{2}}}{\mathfrak{p}'}\right)$$

so that we may write

$$(\xi_0+\eta_0 q^{\frac{1}{2}})^{\frac{1}{2}(p-1)} \equiv \left(\frac{\xi_0+\eta_0 u/v}{p}\right) \bmod p .$$

The computation of the above residue symbol may now be accomplished as follows. We assume the numbers ξ_0, η_0, u and v to be chosen positive and obtain then, using the reciprocity law ($p \equiv 1 \bmod 4$) together with the well-known fact that the class number h of $\mathsf{P}(q^{\frac{1}{2}})$ is odd,

$$\left(\frac{\xi_0+\eta_0 u/v}{p}\right) = \left(\frac{v}{p}\right)\cdot\left(\frac{\xi_0 v+\eta_0 u}{p}\right) = \left(\frac{v}{p}\right)\cdot\left(\frac{p}{\xi_0 v+\eta_0 u}\right)$$
$$= \left(\frac{v}{p}\right)\cdot\left(\frac{p^h}{\xi_0 v+\eta_0 u}\right) = \left(\frac{v}{p}\right)\cdot\left(\frac{u^2-qv^2}{\xi_0 v+\eta_0 u}\right)$$
$$= \left(\frac{v}{p}\right)\cdot\left(\frac{\eta_0^2 u^2-qv^2\eta_0^2}{\xi_0 v+\eta_0 u}\right) = \left(\frac{v}{p}\right)\cdot\left(\frac{\xi_0^2 v^2-qv^2\eta_0^2}{\xi_0 v+\eta_0 u}\right)$$
$$= \left(\frac{v}{p}\right)\cdot\left(\frac{v^2(\xi_0^2-q\eta_0^2)}{\xi_0 v+\eta_0 u}\right) = \left(\frac{v}{p}\right)\cdot\left(\frac{-1}{\xi_0 v+\eta_0 u}\right)$$
$$= \left(\frac{v}{p}\right)\cdot(-1)^{\frac{1}{4}(\xi_0 v+\eta_0 u-1)}\left(\frac{v}{p}\right)\cdot(-1)^{\frac{1}{4}(u-1)},$$

where in the last step it is used that ξ_0 and v both are even and that $\eta_0 \equiv 1 \bmod 4$, since η_0 is a divisor of ξ_0^2+1. Putting $v=2^n v'$ with v' odd we obtain

$$\left(\frac{v'}{p}\right) = \left(\frac{p}{v'}\right) = \left(\frac{p^h}{v'}\right) = \left(\frac{u^2-qv^2}{v'}\right) = \left(\frac{u^2}{v'}\right) = 1.$$

Since $2\|v$ exactly for $p\equiv 5 \bmod 8$, we have $(v/p)=(-1)^{\frac{1}{4}(p-1)}$. Summing up these results, we see that

$$(\xi_0+\eta_0 q^{\frac{1}{2}})^{\frac{1}{2}(p-1)} \equiv (-1)^{\frac{1}{4}(p-1)+\frac{1}{4}(u-1)} \bmod p,$$

which suffices for the proof of the first part of I).

The alternative part of I) may be established quite similarly, the essential difference being that here both u_1 and v_1 are odd. Using $2\|\xi_0$, we get as before

$$(\xi_0+\eta_0 q^{\frac{1}{2}})^{\frac{1}{2}(p-1)} \equiv (-1)^{\frac{1}{4}(\xi_0 v_1+\eta_0 u_1-1)} \equiv (-1)^{\frac{1}{4}(u_1+1)} \bmod p,$$

which proves the second part of I).

ad II): For quadratic fields $\mathsf{P}((-q)^{\frac{1}{2}})$ with $q\equiv 5 \bmod 8$ the class number h' is divisible exactly by 2, the number of ideal classes in each genus being odd (Iyanaga [3], Redei [5]). As in the proof of the corresponding theorem in Section 2 we hereby see that the class group of the cyclic extension $\mathsf{P}((\xi_0+\eta_0 q^{\frac{1}{2}})^{\frac{1}{2}},(-q)^{\frac{1}{2}})/\mathsf{P}((-q)^{\frac{1}{2}})$ of degree 4 consists of all ideals whose $(\frac{1}{2}h')$-th powers are principal ideals (α) generated by numbers in the ray $\alpha\equiv 1 \bmod 2$. This proves the statement II).

Concerning the case $q\equiv 1 \bmod 8$ we prove the following

THEOREM 3. *Let q be a prime $\equiv 1 \bmod 8$ and p a prime for which $(q/p)=1$ and $p\equiv 1 \bmod 4$.*

I) *Let p be represented by $p^h = u^2 - qv^2$, where h denotes the class number of $\mathsf{P}(q^{\frac{1}{2}})$. Then $|u| \equiv 1 \bmod 4$ is a necessary condition for the solvability of* (3.2); *for $p \equiv 5 \bmod 8$ this is also sufficient.*

II) *If $p \equiv 5 \bmod 8$, it is necessary and sufficient for the solvability of* (3.2) *that $p^{\frac{1}{4}h'}$, where h' is the class number of $P((-q)^{\frac{1}{2}})$, be not representable by $p^{\frac{1}{4}h'} = s^2 + qt^2$.*

For $p \equiv 1$ mod 8 it is necessary for the solvability of (3.2) *that $p^{\frac{1}{4}h'}$ is representable by the form $p^{\frac{1}{4}h'} = s^2 + qt^2$.*

PROOF. ad I): This part may be proved verbatim as the corresponding part of Theorem 2. It should be noticed that when $q \equiv 1 \bmod 8$ the alternative representation in Theorem 2,I) does not occur, which is easily seen by considering the representation mod 8.

ad II): In a quadratic field $\mathsf{P}((-q)^{\frac{1}{2}})$ with $q \equiv 1 \bmod 8$ the number of ideal classes in each genus is even (Iyanaga [3], Redei [5]) so that the full number of ideal classes h is divisible by 4 (at least). The statement in II) is equivalent to the assertion that precisely the primes p representable by $p^{\frac{1}{4}h'} = s^2 + qt^2$ are splitting in the field $\mathsf{P}((\xi_0 + \eta_0 q^{\frac{1}{2}})^{\frac{1}{2}}, (-q)^{\frac{1}{2}})$. Now, since $\xi_0 \equiv 0 \bmod 4$, it is not hard to see that the cyclic extension

$$\mathsf{P}((\xi_0 + \eta_0 q^{\frac{1}{2}})^{\frac{1}{2}}, (-q)^{\frac{1}{2}})/\mathsf{P}((-q)^{\frac{1}{2}})$$

of degree 4 is unramified (which incidentally makes clear that the class number h must be divisible by 4). Hence the class group of this extension must be the only existing subgroup in the group of ideal classes whose factor group is cyclic of order 4, namely the subgroup consisting of all ideal classes whose $(\frac{1}{4}h')$-th powers are principal.

We now pass over to the generalization of part III) in Theorem 1. Here the restricting assumption of d being a prime is not needed. In fact we only suppose d to be an odd squarefree integer for which the equation (3.1) is solvable for $m = 1$. Under these assumptions we prove the following theorem concerning the solvability of

$$\xi^2 - dp^2\eta^2 = -1 . \tag{3.3}$$

THEOREM 4. *Let $\xi_0 + \eta_0 d^{\frac{1}{2}}$ be the fundamental solution of $\xi^2 - d\eta^2 = -1$ (with arbitrarily chosen signs of ξ_0 and η_0), and let p be a prime for which $(d/p) = 1$ and $p \equiv 1 \bmod 4$, represented by $p = x^2 + 4y^2$.*

A necessary condition for the solvability of (3.3) *is that*

$$\left(\frac{x + 2\xi_0 y}{d}\right) = (-1)^{\frac{1}{4}(p-1)}.$$

For $p \equiv 5 \bmod 8$ this is also sufficient.

REMARK. In particular, if d is a prime, ξ_0 may be replaced by any residue class ξ mod d for which $\xi^2 \equiv -1 \bmod d$.

PROOF OF THEOREM 4. As previously, the theorem is equivalent to the proposition that p splits in the field $\mathsf{P}((\xi_0+\eta_0 d^{\frac{1}{2}})^{\frac{1}{2}}, i)$ if, and only if,

$$\left(\frac{x+2\xi_0 y}{d}\right) = 1 .$$

Now as a consequence of

$$((\xi_0+\eta_0 d^{\frac{1}{2}})^{\frac{1}{2}} + (\xi_0-\eta_0 d^{\frac{1}{2}})^{\frac{1}{2}})^2 = 2(\xi_0+i) = (1-i)^2 i(\xi_0+i)$$

the bicyclic extension $\mathsf{P}((\xi_0+\eta_0 d^{\frac{1}{2}})^{\frac{1}{2}}, i)/\mathsf{P}(i)$ may be generated by adjoining the square roots $d^{\frac{1}{2}}$ and $(i(\xi_0+i))^{\frac{1}{2}}$. The factorization of p in $\mathsf{P}(i)$ is given by $p \simeq \mathfrak{P}\mathfrak{P}'$ with $\mathfrak{P} = (x+2yi)$, say. Since $(d/p) = 1$, p splits in $\mathsf{P}(d^{\frac{1}{2}})$ and thus in $\mathsf{P}(d^{\frac{1}{2}}, i)$ too. Hence we need only require that $\mathfrak{P}$ (and then automatically $\mathfrak{P}'$ as well) splits in $\mathsf{P}\left((i(\xi_0+i))^{\frac{1}{2}}, i\right)$, that is, that

$$\left(\frac{i(\xi_0+i)}{\mathfrak{P}}\right) = 1 .$$

In view of $N(\xi_0+i) = \xi_0^2+1 = d\eta_0^2$ it follows that ξ_0+i may be written in the form

$$i(\xi_0+i) = (\alpha+\beta i)^2(a+2bi) ,$$

where $(a+2bi)$ is a divisor of d in $\mathsf{P}(i)$ determined by

$$\xi_0 \equiv -i \mod (a+2bi) .$$

Since ξ_0 is even, it follows from the law of quadratic reciprocity in $\mathsf{P}(i)$ that

$$\left(\frac{i(\xi_0+i)}{\mathfrak{P}}\right) = \left(\frac{a+2bi}{x+2yi}\right) = \left(\frac{x+2yi}{a+2bi}\right) = \left(\frac{x+2y\xi_0}{a+2bi}\right) = \left(\frac{x+2y\xi_0}{d}\right) ,$$

where the last quadratic residue symbol is to be understood as concerning numbers in the rational field (the signs of x and y are inessential since a change of these only corresponds to the passing over to the conjugates). This obviously accomplishes the proof of the theorem.

REFERENCES

1. Y. Furuta, *Norms of units of quadratic fields*, J. Math. Soc. Japan 2 (1959), 139–145.
2. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jber. Deutsch. Math. Verein. 35 (1926), 36 (1927), Erg. Bd. 6 (1930).

3. S. Iyanaga, *Sur les classes d'ideaux dans les corps quadratiques* (Actualitées sci. et ind. 197), Paris, 1935.
4. T. Nagell, *Introduction to number theory*, Uppsala, 1951.
5. L. Redei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. 171 (1934), 55–61.
6. L. Redei, *Bedingtes Artinsymbol mit Anwendungen in der Klassenkörpertheorie*, Acta Math. Sci. Hung. 4 (1953), 1–29.
7. L. Redei, *Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung*, Acta Math. Sci. Hungar. 4 (1953), 31–87.

UNIVERSITY OF COPENHAGEN, DENMARK