THE PELL EQUATION IN QUADRATIC FIELDS

IVAN NIVEN

Consider the equation

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

where γ is a given integer of a quadratic field F, and integral solutions ξ, η are sought in F. It has been shown[1] that equation (1) has an infinite number of solutions if and only if γ is not totally negative when F is a real field, and γ is not the square of an integer of F when F is imaginary. We now obtain the following result:

Let γ be such that equation (1) *has an infinite number of solutions. If F is a real field it is possible to find a solution ξ_1, η_1 of* (1) *so that every solution is given by the equations*

$$\begin{aligned} \xi &= \{(\xi_1 + \gamma^{1/2}\eta_1)^n + (\xi_1 - \gamma^{1/2}\eta_1)^n\}/2 \\ \eta &= \{(\xi_1 + \gamma^{1/2}\eta_1)^n - (\xi_1 - \gamma^{1/2}\eta_1)^n\}/(2\gamma^{1/2}), \end{aligned} \qquad n = 1, 2, 3, \cdots, \tag{2}$$

if and only if γ is not a totally positive non-square integer of F. If F is imaginary it is always possible to find a solution ξ_1, η_1 so that all solutions are given by (2).

The latter result is known to hold for the Pell equation in the rational field. The expression $\gamma^{1/2}$ is ambiguous, but no confusion will arise provided it consistently has the same value (we shall specify its value in certain cases). We consider the four sets $\pm\xi$, $\pm\eta$ to be a single solution, so that equations (2) give "every solution" in the sense that one of the four is present for some value of n.

Case 1. *F real, γ positive but not totally positive.* It will be convenient to consider $\gamma^{1/2}$, ξ and η positive. We now show that there is but a finite number of solutions of (1) with ξ bounded, say $\xi < N$. For suppose we have an infinitude of solutions ξ_i, η_i with $\xi_i < N$ for $i = 1, 2, 3, \cdots$. Taking conjugates in equation (1) we would have

$$\bar{\xi}_i^2 - \bar{\gamma}\bar{\eta}_i^2 = 1,$$

and since $-\bar{\gamma}$ is positive, this implies that $\bar{\xi}_i \leqq 1$ for $i = 1, 2, 3, \cdots$. But it is not possible to have an infinite set of real quadratic integers which, along with their conjugates, are bounded.

Presented to the Society, November 28, 1942; received by the editors August 8, 1942.

[1] *Quadratic diophantine equations in the rational and quadratic fields*, Trans. Amer. Math. Soc. vol. 52 (1942) p. 2 Theorem 4. We refer to this paper as (Q).

Hence there exists a least ξ, say ξ_1, among the positive solutions of (1); the corresponding η, say η_1, is also a least value. Thus we have, among the $\xi+\gamma^{1/2}\eta$, a minimum value $\xi_1+\gamma^{1/2}\eta_1$; it is unique, since otherwise $\gamma^{1/2}$ would be an element of F, contrary to hypothesis. Now any solution ξ, η must correspond to a rational integer n such that

$$(\xi_1 + \gamma^{1/2}\eta_1)^n \leqq \xi + \gamma^{1/2}\eta < (\xi_1 + \gamma^{1/2}\eta_1)^{n+1}. \; .$$

Multiplying by $(\xi_1-\gamma^{1/2}\eta_1)^n$ we have

$$1 \leqq (\xi + \gamma^{1/2}\eta)(\xi_1 - \gamma^{1/2}\eta_1)^n < \xi_1 + \gamma^{1/2}\eta_1.$$

The central term is of the form $\xi_2+\gamma^{1/2}\eta_2$, ξ_2 and η_2 being integers of F. On multiplying this central term by $\xi_2-\gamma^{1/2}\eta_2$ we see that ξ_2, η_2 is a solution of (1); also neither ξ_2 nor η_2 is negative. But since $\xi_1+\gamma^{1/2}\eta_1$ is the least with positive ξ and η, we must have $\xi_2=1$, $\eta_2=0$ and hence

$$\xi + \gamma^{1/2}\eta = (\xi_1 + \gamma^{1/2}\eta_1)^n.$$

This implies equations (2).

Case 2. *F real, γ negative but not totally negative.* All solutions of (1) are obtained by taking conjugates of solutions of

$$\xi^2 - \bar{\gamma}\eta^2 = 1, \tag{3}$$

so the problem reduces to Case 1. The particular solution ξ_1, η_1 can be obtained in this case by taking the conjugate of the least positive solution of (3).

Case 3. *F real, γ a perfect square in F (and hence totally positive).* Let $\gamma=\alpha^2$, where α is a positive integer in F. We prove that there is only a finite number of positive solutions of (1) with $\xi+\alpha\eta$ bounded. Any solution gives us two integers of the field $\xi+\alpha\eta$ and $\xi-\alpha\eta$, with product unity. But two integers of a real quadratic field have this property only if one is the conjugate, or the negative of the conjugate, of the other. Hence we can write $\xi+\alpha\eta=\rho$, $\xi-\alpha\eta=\pm\bar{\rho}$. Taking ξ, η and α positive we have $\rho>1$ and $1>|\bar{\rho}|>0$. But there is only a finite number of integers ρ which exceed 1, are bounded, and possess the property $\rho\bar{\rho}=\pm 1$. Thus among the infinitude of solutions of (1) there exists one having $\xi+\alpha\eta$ a minimum. It is unique; for if $\xi_1+\alpha\eta_1=\xi_2+\alpha\eta_2$ with, say, $\xi_1>\xi_2$ and $\eta_1<\eta_2$, then not both ξ_1, η_1 and ξ_2, η_2 can satisfy (1). Hence we proceed as in Case 1 to derive all solutions from this unique smallest one.

Case 4. *F real, γ totally positive but not a perfect square in F.* We shall show that (1) has infinitely many solutions with ξ bounded. In Lemma 2 in §3 of (Q) it is proved that if γ is positive but not totally positive there are infinitely many solutions of (1); we shall make direct use of this proof.

Note first that the infinitude of solutions obtained are such that $\bar{\xi}$ is bounded. To prove this, we observe that the integer ρ introduced in connection with the infinite series (10) in (Q) is bounded, as also is its conjugate; this is seen from inequality (9) and the argument following. And since ξ is obtained in (15) by dividing $\xi_r\xi_s-\gamma\eta_r\eta_s$ by ρ we can obtain $\bar{\xi}$ by multiplying $\bar{\xi}_r\bar{\xi}_s-\bar{\gamma}\bar{\eta}_r\bar{\eta}_s$ by the reciprocal of $\bar{\rho}$, both of which are bounded: the first because of (8), and the second because the reciprocal of $\bar{\rho}$ does not exceed ρ, which is bounded. Instead of obtaining the infinitude of solutions as suggested in (Q) (see the sentence immediately preceding Lemma 3), we can get them by compounding the first pair in (11) with all subsequent pairs, and thus $\bar{\xi}$ is bounded for all resulting solutions.

Next we note that the proof of Lemma 2 in (Q) is valid if γ is a totally positive non-square integer of F. Two remarks should be made in explanation: after inequality (9) the argument used to show that the left side of (7) cannot be zero needs a slight alteration; the result follows from the fact that $\gamma^{1/2}$, or δ, cannot be an element of F, by hypothesis; also the inequality just preceding (10) must be changed since $\bar{\gamma}$ is now positive; the essential idea, that $\bar{\xi}^2-\bar{\gamma}\bar{\eta}^2$ is bounded is still correct.

Thus the proof of Lemma 2 of (Q) can be used to obtain the result that our present equation (1) has infinitely many solutions with $\bar{\xi}$ bounded, γ being totally positive but not a square. But $\bar{\xi}$ and $\bar{\eta}$ are solutions of

$$\bar{\xi}^2 - \bar{\gamma}\bar{\eta}^2 = 1,$$

$\bar{\gamma}$ also being totally positive but not a square; interchanging ξ, η and γ with their conjugates we have the result that our equation (1) has infinitely many solutions with ξ bounded.

Now if there were some least positive solution ξ_1, η_1, we could proceed as in Case 1 and derive all solutions from it by equations (2). But ξ in equations (2) is bounded for only a finite number of values of n. Thus we cannot obtain all solutions by such a scheme.

Case 5. *F imaginary, γ not a perfect square in F.* We first show that, except for trivial solutions ± 1, 0, we cannot have $|\xi+\gamma^{1/2}\eta| = 1$: For otherwise $|\xi-\gamma^{1/2}\eta| = 1$, and the inequality

$$|\xi| \leqq (1/2)\,|\xi + \gamma^{1/2}\eta| + (1/2)\,|\xi - \gamma^{1/2}\eta| \tag{4}$$

would give us $|\xi| \leqq 1$, yielding only a trivial solution. Hence for convenience we can choose the sign of ξ (or η) so that

$$|\xi + \gamma^{1/2}\eta| > 1, \qquad |\xi - \gamma^{1/2}\eta| < 1.$$

Next we show that two essentially different solutions ξ_1, η_1 and ξ_2, η_2 cannot be such that

$$|\xi_1 + \gamma^{1/2}\eta_1| = |\xi_2 + \gamma^{1/2}\eta_2|.$$

For if this were the case we would have another solution ξ_3, η_3 defined by

$$\xi_3 = \xi_1\xi_2 - \gamma\eta_1\eta_2, \qquad \eta_3 = \xi_1\eta_2 - \xi_2\eta_1.$$

It would follow that

$$|\xi_3 + \gamma^{1/2}\eta_3| = |\xi_1 - \gamma^{1/2}\eta_1| \cdot |\xi_2 + \gamma^{1/2}\eta_2| = 1,$$

and by the argument above, $\xi_3 = \pm 1$ and $\eta_3 = 0$. These imply that $\xi_1 = \pm \xi_2$, $\eta_1 = \pm \eta_2$.

Now $|\xi + \gamma^{1/2}\eta|$ is less than any given positive value $N > 1$ for but a finite number of solutions of (1); for by (4) if $|\xi + \gamma^{1/2}\eta|$ is bounded so is $|\xi|$, and this cannot be bounded for an infinite set of integers of an imaginary quadratic field. Hence there exists a unique non-trivial solution of (1) having $|\xi + \gamma^{1/2}\eta|$ a minimum, and we can proceed as in Case 1.

PURDUE UNIVERSITY