Ann. Sci. Math. Québec **35**, No 2, (2011), 175–184

SOME CONGRUENCE PROPERTIES OF THE PELL EQUATION

JASBIR S. CHAHAL AND NATHAN PRIDDIS

Dedicated to Professor Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. Nous considérons l'équation de Pell sous différents points de vue et nous investiguons certaines congruences satisfaites par ses solutions.

ABSTRACT. In this paper we look at the Pell equation from various points of view and study some congruence properties of its solutions.

1. Introduction

The number theoretic function $l_n(m)$, which is defined to be the order of the integer $n \neq 0, 1$ in the group $(\mathbb{Z}/m\mathbb{Z})^\times$, appears to be very erratic and difficult to predict. In particular, one would like to know when is $l_n(m)$ the maximum possible number $\lambda(m) = \exp\left((\mathbb{Z}/m\mathbb{Z})^\times\right)$. For a finite group G, its *exponent* is defined by

$$\exp(G) = \max\left\{\mathrm{ord}(a) \,|\, a \in G\right\}.$$

A well-known conjecture of E. Artin states that for a given integer $n \neq 0, 1$, which has no square factor, $l_n(p) = \lambda(p) = p - 1$ for infinitely many primes p. C. Hooley [6] proved it assuming GRH is true. Gupta and Murty [4] have proven this conjecture unconditionally for infinitely many n (see also Heath-Brown's paper [5]).

In this paper, we study this problem for groups defined by the Pell equation. We fix a square-free integer $N > 1$, and consider the Pell equation

$$x^2 - Ny^2 = 1\,. \tag{1.1}$$

Its integer solutions form an abelian group

$$G \;=\; \left\{\, (x, y) \in \mathbb{Z}^2 \,\middle|\, x^2 - Ny^2 = 1 \,\right\},$$

which is an extension by $\{\pm 1\}$ of a cyclic group. This cyclic group is the subgroup of G consisting of the elements (x, y) with $x > 0$, whose generator is its unique element with the smallest $y > 0$. The group G may be realized as a group of 2×2 matrices with integer entries. For an integer $m > 1$, the reduction mod m map from $\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ induces a homomorphism from G to its image in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. The fundamental generator of G (the solution of (1.1) with smallest $x, y > 0$) and thus its image in

Reçu le 20 avril 2009 et, sous forme définitive, le 24 avril 2010.

$\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is hard to predict if N is arbitrary. We obtain some results on the size of the image of G under the reduction mod m homomorphism.

The Pell equation has a long and rich history that goes at least as far back as the time of Archimedes, whose famous cattle problem ([1, p. 151]) leads to the Diophantine equation (1.1) with $N = 4729494$. A non-trivial solution, $y \neq 0$, for this choice of N was not found until two millenia later.

Lagrange was the first to prove that the Pell equation has a non-trivial solution, from which it follows easily that it has infinitely many of them. The most obvious, likely the most inefficient, way to find a solution is to plug $y = 1, 2, 3, \ldots$ in $1 + Ny^2$, until the result is a perfect square x^2. By Lagrange's theorem, this is guaranteed to happen sooner or later, but exactly when is a difficult question. A more efficient way, called *cakravāla* ([8, p. 21]) was devised by the Indian school of mathematicians — Aryabhata (*c.* 476–550), Brahmagupta (*c.* 598–665) and Bhaskara (*c.* 1114–1185). Dirichlet gave the complete description of the integer solutions of the Pell equation.

In ancient times, the Pell equation was used to compute square roots of square-free integers. Brahmagupta composed solutions. He called the composition *bhavana* and used it to approximate $\sqrt{N}$. According to Weil, "to have developed the *cakravāla* and to have applied it successfully to such difficult numerical cases as $N = 61$ or $N = 67$ had been no mean achievement" [9, p. 24]. In fact, Brahmagupta was already exploiting what we call the group structure on the integer solutions of (1.1).

The "Pell equation" is named after John Pell, an Englishman who wrote to Euler, asking some questions about it. Euler later referred to equation (1.1) as the Pell equation.

2. Pell's equation from different perspectives

We now discuss some ways the Pell equation appears in disguise in mathematics. The list is by no means complete. Complete treatment would certainly contain a treatment of continued fractions.

2.1. The Pell equation is a forerunner to Dirichlet's Unit Theorem for number fields, which states that the group $\mathscr{O}_K^\times$ of units (of the ring of integers $\mathscr{O}_K$) of a *number field* K (where K is a subfield of $\mathbb{C}$, whose dimension as a vector space over $\mathbb{Q}$ is finite) is isomorphic to $W_K \times \mathbb{Z}^r$, where W_K is the finite group of roots of unity in K and where $r = r_1 + r_2 - 1$. Here r_1 (resp. r_2) is the number of real (resp. pairs of imaginary) imbeddings of K into $\mathbb{C}$.

For the sake of simplicity, we take the square-free positive integers N to be congruent to $2, 3 \pmod 4$. In the special case of $\mathbb{Q}(\sqrt{N})$, we have that $\mathscr{O}_K = \mathbb{Z}[\sqrt{N}]$ and $\mathscr{O}_K^\times$ consists of the algebraic integers $\alpha = x + y\sqrt{N}$ in $\mathscr{O}_K$ with norm

$$\mathcal{N}(\alpha) = \alpha\bar{\alpha} = x^2 - Ny^2 = \pm 1,$$

where $\bar{\alpha} = x - y\sqrt{N}$ is the algebraic conjugate of α. (It turns out that Dirichlet considered the algebraic integers of arbitrary algebraic number fields.)

2.2. The Pell equation provides the best example to illustrate some aspects of the theory of algebraic groups. An *algebraic group* G is the set of solutions of a finite set of polynomial equations in n variables with coefficients in $\mathbb{Q}$, together with a group structure which is given by polynomial expressions [7, p. 51]. The standard examples are GL_n of $n \times n$ matrices that are invertible and the algebraic group SL_n defined by the polynomial equation $\det(x) = 1$ in n^2 variables x_{ij}, the entries of $x \in \mathrm{SL}_n$. Clearly matrix multiplication xy and x^{-1} are given by polynomial expressions in the entries of x and y.

Let G be the group of solutions of the Pell equation on which we define a binary operation by

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 + Ny_1y_2, x_1y_2 + x_2y_1) \tag{2.1}$$

with identity $(1, 0)$, and $(x, y)^{-1} = (x, -y)$. Clearly, G is an abelian algebraic group.

It is a standard fact that every algebraic group is linear, that is, it is isomorphic (as an algebraic group) to a subgroup of GL_n. In particular, the algebraic group G defined by Pell's equation is isomorphic to the algebraic group G' of 2×2 matrices of determinant one, via the obvious isomorphism

$$(x, y) \mapsto \begin{pmatrix} x & y \\ Ny & x \end{pmatrix}.$$

An algebraic group T is called a *torus* if T is isomorphic to a group of diagonal matrices. We say T *splits* over an extension K of $\mathbb{Q}$ if this isomorphism is given by polynomials with coefficients in K. As an example, G' is a torus which splits over $\mathbb{Q}(\sqrt{N})$,

$$G' \cong g^{-1}Gg = \left\{ \begin{pmatrix} x + y\sqrt{N} & 0 \\ 0 & x - y\sqrt{N} \end{pmatrix} \middle| \; x, y \in \mathbb{Z},\, x^2 - Ny^2 = 1 \right\}$$

with

$$g = \begin{pmatrix} \sqrt{N} & 1 \\ N & -\sqrt{N} \end{pmatrix}.$$

2.3. Consider a conic section defined by a polynomial equation

$$f(x, y) = 0 \tag{2.2}$$

of degree two, that is, the set of points $P = (a, b)$ with a, b real, whose coordinates $x = a$, $y = b$ satisfy (2.2). The classification of the conic sections into parabola, ellipse, hyperbola, *etc.* has been known for at least two millennia. If we take them in the standard form, say circle as $x^2 + y^2 = a^2$ or parabola as $y = ax^2$ ($a > 0$ an integer), a number theoretic problem is to find all the integer solutions. Except in the case of hyperbola, the problem is trivial. On the parabola $y = ax^2$, all the integer solutions are (t, at^2) with $t \in \mathbb{Z}$, whereas the only integer points on the unit circle are $(\pm 1, 0)$ and $(0, \pm 1)$. Thus the Pell equation is rare among conic sections which have a number theoritic significance.

The integer solutions of (1.1) with $x > 0$ form a subgroup H of the group G of all integer solutions of (1.1) and the index $[G : H] = 2$. For a geometric interpretation,

see Figure 1. As a group, H is isomorphic to the additive group $\mathbb{Z}$. The solution $(x_1, y_1) \neq (1, 0)$ of (1.1) in the first quadrant that is nearest to $(1, 0)$ is a generator of H. The isomorphism from $\mathbb{Z}$ to H is given by $n \mapsto (x_n, y_n) = (x_1, y_1)^n$. This generator (x_1, y_1) of H corresponds to the so-called *fundamental unit* $x_1 + y_1\sqrt{N}$ of the quadratic field $\mathbb{Q}(\sqrt{N})$.

Given N, *a priori* one cannot say how large the fundamental unit (meaning how large y, or equivalently x) is going to be. One has to compute it, for which continued fractions provide more or less the most efficient method.

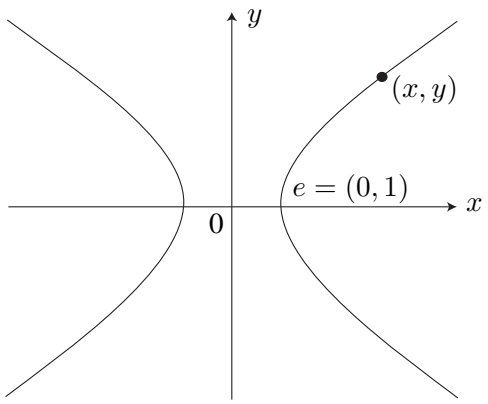

FIGURE 1

2.4. Computing square roots. As an example, take $N = 2$. Then $y = 2$ is the smallest positive integer for which $1 + 2y^2$ is a perfect square (in fact it is the square of 3). Thus from the generator $(3, 2)$ of G, one obtains all the solutions of (1.1) by using the group law (2.1):

$$(3, 2) * (3, 2) = (17, 12),$$
$$(17, 12) * (3, 2) = (99, 70),$$
$$(99, 70) * (17, 12) = (3363, 2378).$$

Now if we write equation (1.1) as

$$N = \frac{x^2}{y^2} - \frac{1}{y^2},$$

the term $1/y^2$ is negligible for large y, hence $\sqrt{N} \approx x/y$. In particular, $\sqrt{2} \approx \frac{3363}{2378} \approx 1.4142136$, is the same as given by a hand-held calculator.

3. Congruence properties

Finally, we come to the main theme of this article. For an integer $m > 1$, we shall denote the reduction mod m map from $\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ by red_m and for $x \in \mathbb{Z}$, $\bar{x} = \mathrm{red}_m(x)$. It is a ring homomorphism. For the remainder of the paper, let G be the group of integer solutions of (1.1) with $x > 0$. The reduction mod m map induces a

group homomorphism $\mathrm{red}_m : G \to \mathrm{GL}_2(Z/m\mathbb{Z})$, where the target group is finite. We shall denote by $g_N(m)$ the order of the image, *i.e.*,

$$g_N(m) = |\mathrm{red}_m(G)|.$$

The following theorems and the corollary sum up our main results.

Theorem 1. *Let p be an odd prime. If $p \mid N$, then $g_N(p) \mid 2p$. If $p \nmid N$, then $g_N(p)$ divides $p-1$ or $p+1$ according as $\bar{N}$ is or is not a square in the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Theorem 1 gives information about the order of the group $\mathrm{red}_p(G)$, for each prime p. When $m > 1$ is composite, $\mathrm{red}_m(G)$ is also a finite cyclic group, so it is reasonable to consider the order of this group as well. The order of $\mathrm{red}_m(G)$ is given by Theorem 2, which follows from Propositions 10 and 11.

Theorem 2. *Let $m = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_r^{\epsilon_r}$, where the p_i's are distinct primes and the ϵ_i's are positive integers. Then*

$$g_N(m) \mid p_1^{\epsilon_1 - 1} g_N(p_1) p_2^{\epsilon_2 - 1} g_N(p_2) \cdots p_r^{\epsilon_r - 1} g_N(p_r).$$

Furthermore,

$$\mathrm{lcm}(g_N(p_1), g_N(p_2), \ldots, g_N(p_r)) \mid g_N(m).$$

The following is an immediate consequence of Theorems 1 and 2.

Corollary 3. *If m is as in Theorem 2, and $\left(\frac{N}{p_i}\right) = 1$ for all odd p_i's, then $g_N(m)$ divides $\phi(N)$.*

Here $\left(\frac{N}{p_i}\right)$ denotes the Legendre symbol and $\phi(N)$, the Euler phi-function.

Without further conditions on N and m, these results (Theorems 1 and 2) are the best possible (see examples below).

Example 4. Consider $N = 7$, *i.e.*, $x^2 - 7y^2 = 1$. The smallest integer solution of this equation, and therefore a generator of G, is $(8, 3)$. We want to consider $\mathrm{red}_5(G)$. We will use bars to denote elements of $\mathbb{Z}/5\mathbb{Z}$. On reduction mod 5, the generator becomes $g = (\bar{3}, \bar{3})$. Now we know that $\mathrm{red}_5(G)$ is cyclic, so to find the order of the group, it suffices to find the smallest d with $g^d = (\bar{1}, \bar{0})$.

$$\begin{aligned}
g^2 &= (\bar{3}, \bar{3}) * (\bar{3}, \bar{3}) = (\bar{2}, \bar{3}),\\
g^3 &= (\bar{3}, \bar{3}) * (\bar{2}, \bar{3}) = (\bar{4}, \bar{0}),\\
g^4 &= (\bar{3}, \bar{3}) * (\bar{4}, \bar{0}) = (\bar{2}, \bar{2}),\\
g^5 &= (\bar{3}, \bar{3}) * (\bar{2}, \bar{2}) = (\bar{3}, \bar{2}),\\
g^6 &= (\bar{3}, \bar{3}) * (\bar{3}, \bar{2}) = (\bar{1}, \bar{0}).
\end{aligned}$$

Therefore the order $g_7(5)$ of $\mathrm{red}_5(G)$ is 6. By Theorem 1, $g_7(5) \mid (5+1)$ so $g_7(5)$ attains the upper bound.

Example 5. Let $N = 11$. The generator for the group of solutions of equation (1.1) is $(10, 3)$. We compute $g_N(m)$ for some values of m. For example,

$$g_N(3) = 1,\ g_N(5) = 4,\ g_N(7) = 3,\ g_N(13) = 7.$$

We see that $g_N(3)$ is as small as possible, whereas $g_N(5) = \phi(5)$, the maximum possible, by Theorem 1. Furthermore,

$$g_N(5^3 \cdot 7 \cdot 13^2) = 27300 = 5^2 \cdot 13 \cdot g_N(5) \cdot g_N(7) \cdot g_N(13)$$

shows that the order of the group with $N = 11$ and $m = 147875$ has attained the upper bound given by Theorem 2.

Example 6. Now let $N = 17$. The generator for G is $(33, 8)$, and we can compute

$$g_N(3) = 4,\ g_N(5) = 6,\ g_N(7) = 8,$$

so we have $g_N(p) = p + 1$ for these three primes. However, we have

$$g_N(3^2 \cdot 5 \cdot 7) = 24 = \operatorname{lcm}(4, 6, 8).$$

In this example, the order of the group attains the lower bound.

Corollary 3 does not hold in general if $\left(\frac{N}{p_i}\right) = -1$ for any p_i. Consider the following example.

Example 7. Suppose $N = 13$. The generator for G with this choice of N is $(649, 180)$. It is not difficult to check that $13 \equiv 6 \pmod 7$ is not square in $\mathbb{F}_7$ and $13 \pmod{19}$ is not square in $\mathbb{F}_{19}$. We have $g_{13}(7) = 8$, and $g_{13}(19) = 20$, and $g_{13}(133) = 40$. However, $\phi(133) = 6 \cdot 18 = 108$.

3.1. Proof of main result. For the proof we need the following techincal lemma (containing a formula which is also given by Lagrange in [3], but with a different proof).

Lemma 8. *If $(x, y) \in G$, then for any positive integer n, $(x, y)^n = (x_n, y_n)$, where for n even, we have*

$$x_n = \binom{n}{0}x^n + \binom{n}{2}Nx^{n-2}y^2 + \cdots + \binom{n}{2k}N^k x^{n-2k}y^{2k} + \cdots + \binom{n}{n}N^{\frac{n}{2}}y^n,$$

$$y_n = \binom{n}{1}x^{n-1}y + \binom{n}{3}Nx^{n-3}y^3 + \cdots + \binom{n}{2k+1}N^k x^{n-2k-1}y^{2k+1} + \cdots + \binom{n}{n-1}N^{\frac{n-2}{2}}xy^{n-1},$$

and where for n odd, we have

$$x_n = \binom{n}{0}x^n + \binom{n}{2}Nx^{n-2}y^2 + \cdots + \binom{n}{2k}N^k x^{n-2k}y^{2k} + \cdots + \binom{n}{n-1}N^{\frac{n-1}{2}}xy^{n-1},$$

$$y_n = \binom{n}{1}x^{n-1}y + \binom{n}{3}Nx^{n-3}y^3 + \cdots + \binom{n}{2k+1}N^k x^{n-2k-1}y^{2k+1} + \cdots + \binom{n}{n}N^{\frac{n-1}{2}}y^n.$$

Proof. We proceed by induction. The lemma is obviously true for $n = 1$. The inductive step is as follows. If n is even, then from (2.1),

$$\begin{aligned}
x_{n+1} &= xx_n + Nyy_n \\
&= x\left(\binom{n}{0}x^n + \binom{n}{2}Nx^{n-2}y^2 + \cdots + \binom{n}{2k}N^k x^{n-2k}y^{2k} + \cdots + \binom{n}{n}N^{\frac{n}{2}}y^n\right) \\
&\quad + Ny\left(\binom{n}{1}x^{n-1}y + \binom{n}{3}Nx^{n-3}y^3 + \cdots \right. \\
&\qquad \left. + \binom{n}{2k+1}N^k x^{n-2k-1}y^{2k+1} + \cdots + \binom{n}{n-1}N^{\frac{n-2}{2}}xy^{n-1}\right) \\
&= x^{n+1} + \left(\binom{n}{1} + \binom{n}{2}\right)Nx^{n-1}y^2 + \cdots \\
&\quad + \left(\binom{n}{2k-1} + \binom{n}{2k}\right)N^k x^{n-2k+1}y^{2k} + \cdots + \left(\binom{n}{n-1} + \binom{n}{n}\right)N^{\frac{n}{2}}xy^n
\end{aligned}$$

and

$$\begin{aligned}
y_{n+1} &= x_n y + xy_n \\
&= \left(\binom{n}{0}x^n + \binom{n}{2}Nx^{n-2}y^2 + \cdots + \binom{n}{2k}N^k x^{n-2k}y^{2k} + \cdots + \binom{n}{n}N^{\frac{n}{2}}y^n\right)y \\
&\quad + x\left(\binom{n}{1}x^{n-1}y + \binom{n}{3}Nx^{n-3}y^3 + \cdots \right. \\
&\qquad \left. + \binom{n}{2k+1}N^k x^{n-2k-1}y^{2k+1} + \cdots + \binom{n}{n-1}N^{\frac{n-2}{2}}xy^{n-1}\right) \\
&= \left(\binom{n}{0} + \binom{n}{1}\right)x^n y + \cdots \\
&\quad + \left(\binom{n}{2k} + \binom{n}{2k+1}\right)N^k x^{n-2k}y^{2k+1} + \cdots + \binom{n}{n}N^{\frac{n}{2}}y^{n+1}.
\end{aligned}$$

By the Binomial Theorem,

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1},$$

so

$$\begin{aligned}
x_{n+1} &= \binom{n+1}{0}x^{n+1} + \binom{n+1}{2}Nx^{n-1}y^2 + \cdots \\
&\qquad + \binom{n+1}{2k}N^k x^{n+1-2k}y^{2k} + \cdots + \binom{n+1}{n}N^{\frac{n}{2}}xy^n, \\
y_{n+1} &= \binom{n+1}{1}x^n y + \binom{n+1}{3}Nx^{n-2}y^3 + \cdots \\
&\qquad + \binom{n+1}{2k+1}N^k x^{(n+1)-2k-1}y^{2k+1} + \cdots + \binom{n+1}{n+1}N^{\frac{n}{2}}y^{n+1},
\end{aligned}$$

as desired. The n odd case can be handled in a similar manner. □

Proof of Theorem 1. The fact $g_N(2) = 1$ or 2 is obvious. If the odd $p \mid N$, then $\mathrm{red}_p(G)$ is isomorphic to a subgroup of

$$\left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} : x, y \in \mathbb{F}_p, x^2 = 1 \right\}.$$

This group has order $2p$. This proves the first statement.

We now consider the case when p is not a factor of N, and $p \neq 2$. To fix notation, we recall some standard facts from basic number theory found, for example, in [2]. Recall that for $x \in \mathbb{F}_p$, $x^p = x$. Consider the group homomorphism $\psi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ defined by $\psi(x) = \bar{x}^{(p-1)/2}$, $\mathbb{F}_p^\times$ being the multiplicative group of non-zero elements of the finite field $\mathbb{F}_p$. The image of the map is $\{\pm 1\}$: If $a \in \mathbb{F}_p^\times$ is a square, then there exists $t \in \mathbb{F}_p$ so that $a = t^2$. Thus, $\psi(a) = (t^2)^{(p-1)/2} = 1$. So we have $(\mathbb{F}_p^\times)^2 \subset \ker \psi$. On the other hand, there exists $b \in \mathbb{F}_p^\times$ such that $\psi(b) = -1$, otherwise the polynomial $x^{(p-1)/2} - 1$ has more roots than its degree. Therefore $\mathbb{F}_p^\times / \ker(\psi) \cong \{\pm 1\}$ and $(\mathbb{F}_p^\times)^2 = \ker \psi$.

To summarize, consider $\bar{N} = \mathrm{red}_p(N)$ as an element of $\mathbb{F}_p$. If $\bar{N}$ is a square then $\bar{N}^{(p-1)/2} = 1$, and if $\bar{N}$ is not a square, then $\bar{N}^{(p-1)/2} = -1$.

Suppose $\bar{N}$ is a square. Since p is odd, Lemma 8 gives

$$\begin{aligned}(\bar{x}, \bar{y})^p &= \left(\bar{x}^p + \cdots + \binom{p}{p-1} \bar{N}^{\frac{p-1}{2}} \bar{x}\bar{y}^{p-1}, \binom{p}{1} \bar{x}^{p-1}\bar{y} + \cdots + \bar{N}^{\frac{p-1}{2}} y^p \right) \\ &= (\bar{x}^p, \bar{N}^{\frac{p-1}{2}} \bar{y}) \\ &= (\bar{x}, \bar{y}).\end{aligned}$$

The second equality follows because $p \mid \binom{p}{k}$ whenever k is not equal to 0 or p. This shows that $(\bar{x}, \bar{y})^{p-1} = (1, 0)$. Therefore $g_N(p) \mid (p-1)$.

Now suppose $\bar{N}$ is not a square. Then we have $\bar{N}^{(p-1)/2} = -1$, and consequently $\bar{N}^{(p+1)/2} = -\bar{N}$. Since $p+1$ is even, Lemma 8 shows that

$$\begin{aligned}(\bar{x}, \bar{y})^{p+1} &= \left(\bar{x}^{p+1} + \cdots + \bar{N}^{\frac{p+1}{2}} \bar{y}^{p+1}, \binom{p+1}{1} \bar{x}^p\bar{y} + \cdots + \binom{p+1}{p} \bar{N}^{\frac{p-1}{2}} \bar{x}\bar{y}^p \right) \\ &= \left(\bar{x}^2 - \bar{N}\bar{y}^2, \bar{x}\bar{y} - \bar{x}\bar{y}\right) \\ &= (1, 0).\end{aligned}$$

The second equatity follows because $p \mid \binom{p+1}{k}$ whenever k is not equal to $0, 1, p$ or $p+1$. Since this is true for any $(\bar{x}, \bar{y}) \in \mathrm{red}_p(G)$, we have $g_N(p) \mid (p+1)$. □

The following corollary gives the divisibility properties of the integer solutions of the Pell equation.

Corollary 9. *Let $p \neq 2$ be a prime number. If (x, y) is a solution of the Pell equation (1.1), then p does not divide x unless $p \nmid N$. Furthermore, there exists a solution (x, y) of equation (1.1) with $p \mid x$ if and only if $4 \mid g_N(p)$.*

Proof. Suppose (x, y) is a solution of (1.1). If $p \mid N$, then on reduction mod p, equation (1.1) becomes $\bar{x}^2 = 1$. Clearly $p \nmid x$ in this case. So suppose p does not divide N.

If $p \mid x$, then $\mathrm{red}_p(G)$ has an element of the form $(0, \bar{y})$ with $\bar{y} \neq 0$ in $\mathbb{F}_p$. But $(0, \bar{y})^2 = (Ny^2, 0) = (-1, 0)$, since $\bar{x}^2 - \bar{N}\bar{y}^2 = 1$, and $(-1, 0)^2 = (1, 0)$. Thus $(0, \bar{y})$ has order 4 in $\mathrm{red}_p(G)$. But if $\mathrm{red}_p(G)$ contains an element of order 4, then $4 \mid g_N(p)$.

To prove the converse, it suffices to check that elements of the form $(0, \bar{y})$ are the only elements of order 4 in $\mathrm{red}_p(G)$.

Suppose $(\bar{x}, \bar{y})$ has order 4. Then

$$\begin{aligned}(\bar{x}, \bar{y})^4 &= (\bar{x}^4 + 6\bar{N}\bar{x}^2\bar{y}^2 + \bar{N}^2\bar{y}^4, 4\bar{x}\bar{y}(\bar{x}^2 + \bar{N}\bar{y}^2)) \\ &= (1, 0).\end{aligned}$$

The second coordinate is zero only if one of the factors is zero. If $\bar{x} \neq 0$, then either $\bar{y} = 0$ or $(\bar{x}^2 + \bar{N}\bar{y}^2) = 0$. In the former case, $\bar{x}^2 = 1$, and so $(\bar{x}, \bar{y})$ has order at most 2. In the latter case, since $(\bar{x}, \bar{y})^2 = (\bar{x}^2 + \bar{N}\bar{y}^2, 2\bar{x}\bar{y}) = (0, \bar{y})$, the order of $(\bar{x}, \bar{y})^2$ is 4, so $(\bar{x}, \bar{y})$ has order 8. □

Proposition 10. *Let $m = p^k$, where k is a positive integer. Then*

$$g_N(m) \,\big|\, p^{k-1} g_N(p)\,.$$

Proof. If $k = 1$, the statement is trivial. So we may assume $k \geq 2$. Consider the map $\varphi : \mathrm{red}_{p^k}(G) \to \mathrm{red}_{p^{k-1}}(G)$ induced by $\mathrm{red}_{p^{k-1}}$. In other words, reduce the entries of elements of $\mathrm{red}_{p^k}(G)$, by p^{k-1}. This is a surjective map, so we have

$$\mathrm{red}_{p^k}(G)/\ker\varphi \cong \mathrm{red}_{p^{k-1}}(G),$$

or in other words, $g_N(p^k) = g_N(p^{k-1}) \cdot |\ker\varphi|$. We will use the bar notation to denote elements of $\mathbb{Z}/p^k\mathbb{Z}$, *i.e.*, if $x \in \mathbb{Z}$, then $\bar{x}$ is its image in $\mathbb{Z}/p^k/\mathbb{Z}$.

To compute the order of $\ker\varphi$, let $(\bar{x}, \bar{y}) \in \ker\varphi$. Then the element $(\bar{x}, \bar{y})$ has the form $(1 + ap^{k-1}, bp^{k-1})$, where $a, b \in \mathbb{Z}/p^k\mathbb{Z}$. But we know that

$$\bar{x}^2 - \bar{N}\bar{y}^2 = 1 + 2ap^{k-1} + b^2\,\bar{p}^{2k-1} - \bar{N}b^2\,\bar{p}^{2k-1} = 1. \tag{3.1}$$

Since $k \geq 2$, $2(k-1) \geq k$, and so $p^k \mid p^{2k-1}$. Now equation (3.1) shows that $a = 0$. Therefore $(\bar{x}, \bar{y})$ has the form $(1, bp^{k-1})$.

If $p \neq 2$ we have

$$\begin{aligned}(\bar{x}, \bar{y})^p = \Bigg(1 + \binom{p}{2}\bar{N}(bp^{k-1})^2 + \cdots + \binom{p}{p-1}\bar{N}^{\frac{p-1}{2}}(bp^{k-1})^{p-1}\,, \\ \binom{p}{1}bp^{k-1} + \cdots + \bar{N}^{\frac{p-1}{2}}(bp^{k-1})^p\Bigg) \\ = (1, 0).\end{aligned}$$

The second equality follows because a power of p^k shows up in every term except the first term of the first entry.

If $p = 2$, then we have

$$\begin{aligned}(\bar{x}, \bar{y})^2 &= \left(1 + \bar{N}(b(2^{k-1}))^2, 2b(2^{k-1})\right) \\ &= (1, 0).\end{aligned}$$

Thus $|\ker \varphi|$ divides p. Then by induction, $g_N(p^k) \mid p^{k-1} g_N(p)$. □

Proposition 11. *Suppose* $m = qr$, *with* $\gcd(q, r) = 1$. *Then*

$$g_N(m) \mid \left(g_N(q) \cdot g_N(r)\right).$$

Proof. The Chinese Remainder Theorem gives an isomorphism of rings

$$\Phi : \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

Consider the obvious group homomorphism

$$\psi : \mathrm{red}_m(G) \to \mathrm{red}_q(G) \times \mathrm{red}_r(G).$$

Since Φ is bijective, so is ψ and we see that $g_N(m) \mid \left(g_N(q) \cdot g_N(r)\right)$. □

Acknowledgements. The authors wish to thank the referee and Professor Gregory Conner, whose comments contributed to the clarity of the exposition.

REFERENCES

[1] R. Calinger, *Classics of Mathematics*, Prentice Hall, Englewood Cliffs, NJ, 1994.

[2] J. S. Chahal, *Topics in Number Theory*, Plenum Press, New York, 1988.

[3] L. Euler, *Elements of Algebra, with the notes of M. Bernoulli and the additions of M. de La Grange*. Third Edition, Longman, Hurst, Rees, Orme, and Co., London, 1822.

[4] R. Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), no. 1, 127–130.

[5] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38.

[6] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[7] J. E. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics, **21**, Springer-Verlag, New York-Heidelberg, 1975.

[8] V. S. Varadarajan, *Algebra in Ancient and Modern Times*, Mathematical World, **12**, American Mathematical Society, Providence, RI; Hindustan Book Agency, Delhi, 1998.

[9] A. Weil, *Number Theory, An approach through history from Hammurapi to Legendre*, Reprint of the 1984 edition. Birkhäuser Boston, Inc., Boston, MA, 2007.

J. S. CHAHAL, DEPT. OF MATH., BRIGHAM YOUNG U., PROVO, UT 84602, USA
jasbir@math.byu.edu

N. PRIDDIS, DEPT. OF MATH., U. OF MICHIGAN, ANN ARBOR, MI 48109, USA
priddisn@gmail.com