A Note on the Negative Pell Equation

Valentin Blomer

To the memory of Wolfgang Schwarz

Abstract Nagell conjectured in the 1930s that the set of discriminants for which the negative Pell equation has an integral solution has an explicitly given positive proportion within the set of discriminants having no prime factor congruent to 3 modulo 4. In a series of papers, Fouvry and Klüners succeeded in showing that the order of magnitude of such discriminants up to x is indeed $x(\log x)^{-1/2}$. Here we present a short independent argument that the order of magnitude is at least $x(\log x)^{-0.62}$.

Keywords Fundamental unit • Negative norm • Number of discriminants • Pell equation

2010 Mathematics subject classification: Primary 11N45; Secondary 11D09

1 Introduction

There are many open questions in connection with the solvability and the size of possible solutions of Pell-type equations

$$x^2 - dy^2 = C, \quad x, y \in \mathbb{Z}, \tag{1.1}$$

for given squarefree d > 0. Let us write $K := \mathbb{Q}(\sqrt{d})$ and

$$D := \operatorname{disc} K/\mathbb{Q} = f^2 d, \quad f \in \{1, 2\}.$$

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*, DOI 10.1007/978-3-319-28203-9_2

V. Blomer (🖂)

Universität Göttingen, Bunsenstr. 3-5, 37073 Göttingen, Germany e-mail: vblomer@math.uni-goettingen.de

[©] Springer International Publishing Switzerland 2016

While (1.1) has always integral solutions for C = 1, only some d admit integral solutions to

$$x^2 - dy^2 = -1. (1.2)$$

This is tantamount to asking for which real quadratic discriminants D the fundamental unit ϵ_D has negative norm, $N\epsilon_D = -1$. Let \mathfrak{D} be the set of such discriminants. It is well known that $D \in \mathfrak{D}$ if and only if the period length of the continued fraction of \sqrt{d} is odd (which, however, might be as long as about \sqrt{d}). In more algebraic terms, (1.2) is solvable in $x, y \in \mathbb{Z}$ if and only if the class group of K coincides with the narrow class group, in other words if the narrow Hilbert class field of K is real. It is, however, a hard problem to find necessary and sufficient criteria for \mathfrak{D} that are both efficient from an algorithmic point of view and simple enough for theoretical purposes, e.g. counting the number of $D \in \mathfrak{D}$ up to x.

Let S be the set of integers having no prime divisor $p \equiv 3 \pmod{4}$. By the Hasse principle we see that (1.2) admits *rational* solutions if and only if $d \in S$, in particular

$$#\{D \le x \mid D \in \mathfrak{D}\} \le #\{\text{discriminants } D \le x \mid D \in \mathcal{S}\} \ll \frac{x}{\sqrt{\log x}}.$$

On the other hand, by an observation of Redei the negative Pell equation does have integral solutions if $d \in S$ and in addition the two-part C[2] of the class group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(D)-1}$, that is, the class group C of K has no element of order 4. For, in the latter case, the narrow 2-Hilbert class field coincides with the genus field and is in particular real. In other words, if D denotes the set of discriminants of real quadratic fields in S with no element of order 4 in the class group, then $D \subseteq \mathfrak{D}$.

On probabilistic grounds, one may expect

$$\#\{D \le x \mid D \in \mathfrak{D}\} \asymp \frac{x}{\sqrt{\log x}};\tag{1.3}$$

more precisely, there is theoretical and (some) empirical evidence [8] that

$$\frac{\#\{D \le x \mid D \in \mathfrak{D}\}}{\#\{\text{discriminants } D \le x \mid D \in \mathcal{S}\}} \sim 1 - \prod_{j=1}^{\infty} \left(1 - \frac{1}{2^{2j-1}}\right) \approx 0.581, \quad x \to \infty.$$
(1.4)

Nagell [6] conjectured more than 80 years ago that the limit (1.4) exists in the open interval (0, 1), but no proof has been found so far. The beauty in this conjecture lies in the mix of analytic and algebraic number theory that is already apparent in the formulation of the problem.

A first step was made by Cremona and Odoni who proved ([1], see also [8])

$$\frac{\#\{D \le x \mid D \in \mathcal{D}, \omega(D) = n\}}{\#\{\text{discriminants } D \le x \mid D \in \mathcal{S}, \omega(D) = n\}} \sim \prod_{j=1}^{n/2} \left(1 - \frac{1}{2^{2j-1}}\right), \quad x \to \infty$$

$$(1.5)$$

for each fixed $n \in \mathbb{N}$, so that in particular

$$\#\{D \le x \mid D \in \mathfrak{D}\} \gg_n \frac{x(\log \log x)^n}{\log x}.$$
(1.6)

In an impressive series of long and difficult papers, Fouvry and Klüners [3-5] made great progress and essentially solved the problem (along with several related questions) by showing that the left-hand side of (1.4) is asymptotically bounded between two constants:

$$0.524 \le \frac{5}{4} \prod_{j=1}^{\infty} \left(1 - \frac{1}{2^{2j-1}} \right) + o(1) \le \frac{\#\{D \le x \mid D \in \mathfrak{D}\}}{\#\{\text{discriminants } D \le x \mid D \in \mathcal{S}\}} \le \frac{2}{3} + o(1).$$

Our goal in this note is much more modest. Here we show that a short argument suffices to bring us half-way between (1.6) and the correct order of magnitude $x(\log x)^{-1/2}$.

Theorem 1.1 Let $\alpha_0 = 0.616...$ be the minimum of the function

$$f(\alpha) := 1 - \alpha \left(1 + \log \frac{1 - \alpha \log 2}{2\alpha} \right).$$

Then

$$\#\{D \le x \mid D \in \mathfrak{D}\} \gg_{\varepsilon} \frac{x}{(\log x)^{\alpha_0 + \varepsilon}}$$

for any $\varepsilon > 0$.

The general approach is similar as in [1], but we modify the argument as follows: (a) we only aim at getting lower bounds for the quantity on the left-hand side of (1.5), (b) we use the large sieve to estimate primes in arithmetic progressions on average and (c) we exclude exceptional (Siegel) discriminants at an early stage of the argument. The idea of the method dates back several years, and Theorem 1.1 is already mentioned in [4].

2 Proof of the Theorem

We start with the Siegel–Walfisz Theorem (e.g. [2, Sect. 20]). Let (a, q) = 1. There is a constant C > 0 such that

$$\pi(x;q,a) := \sum_{\substack{n \le x \\ n \equiv a \,(\text{mod }q)}} 1 = \frac{1}{\phi(q)} \int_2^x \frac{dt}{\log t} + O\left(xe^{-C\sqrt{\log x}}\right)$$
(2.1)

for all $q \leq e^{\sqrt{\log x}}$, except possibly for a thin sequence $q_1 < q_2 < \ldots$ satisfying $q_{j+1} > q_j^2$. In particular, there is a set of rational primes $\mathcal{P} := \{\pi_1, \pi_2, \ldots\}$ with $\pi_n > 2^{2^{n-1}}$ such that (2.1) holds for all $q \leq e^{\sqrt{\log x}}$ not divisible by any of the π_j .

Our aim is to find a lower bound for the number of $D \in \mathcal{D}$ which implies automatically a lower bound for the number of $D \in \mathfrak{D}$. To this end we utilize a criterion of Redei–Reichardt to characterize the 4-rank of the class group. Let

$$\mathcal{D}^* := \{ D \in \mathbb{N} \mid \mu^2(D) = 1, p \mid D \Rightarrow (p \equiv 1 \pmod{4}, p \notin \mathcal{P}) \},\$$
$$\mathcal{D}^*_n := \{ D \in \mathcal{D}^* \mid \omega(D) = n \},\$$

and let

$$\mathfrak{U}_n := \{(u_{ij})_{1 \le i, j \le n} \mid u_{ij} = 0 \text{ for } j \ge i, u_{ij} \in \{\pm 1\} \text{ for } 1 \le i < j \le n\} = \left\{ \begin{pmatrix} 0 & \pm 1 \\ & \ddots \\ & & 0 \end{pmatrix} \right\}.$$

For any $D = \prod_{i=1}^{n} p_i \in \mathcal{D}_n^*$ let $(\varepsilon_{ij}) =: \mathcal{U}(D) \in \mathfrak{U}_n$ be given by $\varepsilon_{ij} := \left(\frac{p_i}{p_j}\right)$ for i < j. Then the 4-rank of the class group of $\mathbb{Q}(\sqrt{D})$ is determined by $\mathcal{U}(D)$ in the following way. Let $\tilde{\mathcal{U}}(D) := (\eta_{ij}) \in \mathbb{F}_2^{n \times n}$ be defined by $(-1)^{\eta_{ij}} = \varepsilon_{ij}$ for i < j, $\eta_{ij} = \eta_{ji}$ and $\eta_{ii} = \sum_{j \neq i} \eta_{ij}$. Then by a criterion of Redei–Reichardt [7] (see also [8]),

4-rank of the class group of $\mathbb{Q}(\sqrt{D}) = n - 1 - \mathrm{rk}_{\mathbb{F}_2} \tilde{\mathcal{U}}(D).$ (2.2)

We shall need the following lemma [1, Proposition 2.5]:

Lemma 2.1 Out of the $2^{\binom{n}{2}}$ matrices $\mathcal{U} \in \mathfrak{U}_n$ exactly

$$2^{\binom{n}{2}} \prod_{j=1}^{n/2} \left(1 - \frac{1}{2^{2j-1}} \right) \gg 2^{\binom{n}{2}}$$

matrices give rise to a matrix $\tilde{\mathcal{U}}$ having rank n-1 over \mathbb{F}_2 .

For any $\mathcal{V} \in \mathfrak{U}_n$ let

$$\mathcal{D}_n^*(x,\mathcal{V}) := \#\{D \in \mathcal{D}_n^* \mid D \le x, \mathcal{U}(D) = \mathcal{V}\}.$$

The idea is to estimate this quantity from below, sum over all admissible \mathcal{V} and then optimize the value of *n*. To this end, let us fix a small $\varepsilon > 0$, let $C(\varepsilon)$ be a sufficiently large constant depending only on ε , and let

$$\gamma_n := C(\varepsilon)^{(2+4\varepsilon)^{n-1}}.$$

In the following, all implied constant may depend on ε , but not on *n*. We shall show by induction:

$$\mathcal{D}_n^*(x,\mathcal{V}) \gg_{\varepsilon} \Xi_n 2^{-\binom{n}{2}} \frac{x}{\log x} \frac{\left(\log\log x - \log\log \gamma_n\right)^{n-1}}{2^n(n-1)!}$$
(2.3)

for any $\mathcal{V} \in \mathfrak{U}_n$ and $x > \gamma_n$ where

$$\Xi_n := \prod_{j=1}^n \left(1 - \frac{c(\varepsilon) \exp(j^2)}{\exp(c_1 \sqrt{\log \gamma_j})} \right) \gg 1$$

for a suitable constant $c(\varepsilon) > 0$. Here we choose $C(\varepsilon)$ large enough (in terms of $c(\varepsilon)$ and c_1) so that each factor is positive. We will also choose $n \le \log \log x$, so that $\gamma_n \le \exp(\log C(\varepsilon) \cdot (\log x)^{0.7})$ for ε sufficiently small and the condition $\gamma_n < x$ is not void.

From Lemma 2.1, (2.2), (2.3) and the definition of \mathcal{D} , we find

$$\#\{D \in \mathcal{D} \mid D \le x\} \gg \frac{x}{\log x} \frac{(\log \log x - (n-1)\log(2+4\varepsilon) - \log \log C(\varepsilon))^{n-1}}{2^n(n-1)!}$$

for $n \le \log \log x$ (and sufficiently large *x*). Choosing $n = [\alpha \log \log x]$ for some real $0 < \alpha < 1$, this is by Stirling's formula

$$\gg \frac{x}{\log x} \left(\frac{1-\alpha \log 2}{2} \frac{e}{\alpha}\right)^{(\alpha+o(1))\log\log x} = x(\log x)^{f(\alpha)+o(1)},$$

with $f(\alpha)$ as in Theorem 1.1, and the proof follows.

The rest of the paper is devoted to the proof of (2.3). This is certainly true for n = 1 by the prime number theorem (or Chebyshev-type estimates) for the progression 1 (mod 4). Suppose now (2.3) holds for some $n \in \mathbb{N}$, and let $\mathcal{V} = (\varepsilon_{ij})_{1 \le i,j \le n+1} \in \mathfrak{U}_{n+1}$ be given. Let $\mathcal{U} := (\varepsilon_{ij})_{1 \le i,j \le n} \in \mathfrak{U}_n$ be obtained by deleting the last row and column from \mathcal{V} . Let us consider some $t = \prod_{i=1}^{n} p_i \in \mathcal{D}^*(x, \mathcal{U})$. We denote by \mathcal{A}_t the set of

residue classes a (mod 4t) satisfying

$$a \equiv 1 \pmod{4}$$
 and $\left(\frac{p_i}{a}\right) = \varepsilon_{i,n+1}, 1 \le i \le n.$

By the Chinese remainder theorem we have

$$#\mathcal{A}_t = \frac{\phi(4t)}{2^{n+1}}.$$

If *p* satisfies the three conditions $p \equiv a \pmod{4t}$ for some $a \in A_t$, $p_n , and <math>p \notin \mathcal{P}$, then $pt \in \mathcal{D}_{n+1}^*(x, \mathcal{V})$. Let us assume $x > \gamma_{n+1}$, and write

$$y := x^{(1-\varepsilon)/2}.$$

Without loss of generality we also assume that $x = [x] + \frac{1}{2}$ is a half-integer. Then we have

$$\mathcal{D}_{n+1}^{*}(x,\mathcal{V}) \geq \sum_{t=\prod p_{t}\in\mathcal{D}_{n}^{*}(y,\mathcal{U})} \sum_{a\in\mathcal{A}_{t}} \#\left\{p_{n}
$$= \sum_{t\in\mathcal{D}_{n}^{*}(y,\mathcal{U})} \sum_{a\in\mathcal{A}_{t}} \pi\left(\frac{x}{t}; 4t, a\right) + O\left(\sum_{t\leq y}^{*} (\pi(t) + \#\{\pi \leq x \mid \pi \in \mathcal{P}\})\right)$$

$$= \frac{1}{2^{n+1}} \sum_{t\in\mathcal{D}_{n}^{*}(y,\mathcal{U})} \pi\left(\frac{x}{t}\right) + O\left(\sum_{t\leq y}^{*} \sum_{a\in\mathcal{A}_{t}} \left|\pi\left(\frac{x}{t}; 4t, a\right) - \frac{\pi(x/t)}{\phi(4t)}\right|\right)$$

$$+ O(x^{1-\varepsilon}),$$
(2.4)$$

where \sum^* indicates that the summation is taken over *t* coprime to all $\pi \in \mathcal{P}$. By the prime number theorem and partial summation, the main term is

$$\geq \frac{1}{2^{n+1}} \sum_{t \in \mathcal{D}_n^*(y,\mathcal{U})} \int_2^{x/t} \frac{dt}{\log t} + O\left(\sum_{t \leq y} \frac{x/t}{\exp(c_2 \sqrt{\log(x/t)})}\right)$$

$$\geq \frac{x}{2^{n+1}} \int_{\gamma_n}^y \frac{\mathcal{D}_n^*(u,\mathcal{V})}{u^2 \log(x/u)} du + O\left(\frac{x}{\exp(c_3 \sqrt{\log x})}\right);$$

(2.5)

note that $y \le x^{1/2}$, so that $\log \frac{x}{t} \gg \log x$. By the induction hypothesis (2.3) the main term here is

$$\geq \Xi_n 2^{-\binom{n}{2}} \frac{x}{2^{n+1} \log x} \int_{\gamma_n}^{\gamma} \frac{(\log \log u - \log \log \gamma_n)^{n-1}}{2^n (n-1)! u \log u} du$$

= $\Xi_n 2^{-\binom{n}{2}} \frac{x}{2^{n+1} \log x} \frac{(\log \log y - \log \log \gamma_n)^n}{2^n n!}$ (2.6)
= $\Xi_n 2^{-\binom{n+1}{2}} \frac{x}{\log x} \frac{(\log \log x - \log \frac{2}{1-\varepsilon} - \log \log \gamma_n)^n}{2^{n+1} n!}.$

It remains to estimate the first error term on the right-hand side of (2.4). This is a standard application of the large sieve. We split the *t*-sum in $O(\log x)$ dyadic segments. A typical of these terms is at most

$$\sum_{z \le t \le 2z} * \sum_{a \pmod{4t}} * \left| \sum_{\substack{p \le x/t \\ p \equiv a \pmod{4t}}} 1 - \frac{1}{\phi(4t)} \sum_{p \le x/t} 1 \right|$$
(2.7)

for $z \le y$. It is convenient to make the summation range independent of t by replacing the condition $p \le x/t$ with $p \le x/z$. This can be easily done by integral transforms. We use the formula (see, e.g., [2, p. 165])

$$\int_{-T}^{T} e^{i\xi\alpha} \frac{\sin(\xi\beta)}{\pi\xi} d\xi = \begin{cases} 1 + O((T(\beta - |\alpha|))^{-1}), \ |\alpha| < \beta, \\ O((T(|\alpha| - \beta))^{-1}), \ |\alpha| > \beta \end{cases}$$

for $T, \beta > 0$ with $\beta = \log X, \alpha = \log m$ getting

$$\sum_{m \le X} a_m = \int_{-T}^{T} \sum_{m \le Y} a_m m^{i\xi} \frac{\sin(\xi \log X)}{\pi \xi} d\xi + O\left(\frac{1}{T} \sum_{m \le Y} |a_m| \left|\log \frac{m}{X}\right|^{-1}\right)$$

for real numbers $Y \ge X$ and any sequence (a_m) . In particular, (2.7) is at most

$$\int_{-T}^{T} \sum_{z \le t \le 2z} \sum_{a \pmod{4t}}^{*} \left| \sum_{\substack{p \le x/z \\ p \equiv a \pmod{4t}}} p^{i\xi} - \frac{1}{\phi(4t)} \sum_{p \le x/z} p^{i\xi} \right| \min\left(\frac{1}{|\xi|}, \log x\right) d\xi + O\left(\frac{1}{T} \sum_{z \le t \le 2z} \sum_{a \pmod{4t}}^{*} \left(\sum_{\substack{p \le x/z \\ p \equiv a \pmod{4t}}} \left|\log\frac{pt}{x}\right|^{-1} + \frac{1}{\phi(4t)} \sum_{p \le x/z} \left|\log\frac{pt}{x}\right|^{-1}\right)\right)$$
(2.8)

for some 0 < T < x to be chosen later. Gluing together t and p, the error term in (2.8) is at most

$$\ll \frac{1}{T} \sum_{q \le 2x} d(q) \left| \log \frac{q}{x} \right|^{-1} \ll \frac{x(\log x)^2}{T};$$
(2.9)

here we need our assumption that x is not too close to an integer. The main term in (2.8) is by Cauchy's inequality

$$\ll \int_{-T}^{T} \left(\sum_{z \le t \le 2z} \sum_{a \pmod{4t}}^{*} \left| \frac{1}{\phi(4t)} \sum_{\chi \ne \chi_0} \bar{\chi}(a) \sum_{p \le x/z} \chi(p) p^{i\xi} \right|^2 \right)^{1/2} z \min\left(\frac{1}{|\xi|}, \log x\right) d\xi.$$

We open the square and express each character modulo 4*t* in terms of its underlying primitive character modulo $t' = 4t/\ell$. Using $\phi(\ell t') \ge \phi(\ell)\phi(t')$ we get

$$\int_{-T}^{T} \left(\sum_{\ell \le x} \frac{1}{\phi(\ell)} \sum_{\frac{4z}{\ell} \le t' \le \frac{8z}{\ell}}^{*} \frac{1}{\phi(t')} \sum_{\chi \bmod t'} \sum_{\substack{p \le x/z \\ (p,\ell) = 1}}^{*} \chi(p) p^{i\xi} \Big|^2 \right)^{1/2} z \min\left(\frac{1}{|\xi|}, \log x\right) d\xi.$$

$$(2.10)$$

We recall that the asterisk at the *t*'-sum denotes non-exceptional discriminants and the asterisk at the χ -sum denotes primitivity. We split the *t*'-sum into two parts, $t' \ge P$ and t' < P for some $P \le \exp(\sqrt{\log x})$ to be chosen later. By the large sieve inequality (e.g. [2, p. 160]), the *t*'-sum restricted to $t' \ge P$ can be bounded by

$$\ll \left(\frac{x}{zP} + \frac{z}{\ell}\right)\pi\left(\frac{x}{z}\right);$$

summing over ℓ and integrating over ξ we get

$$\frac{x(\log x)^{3/2}}{\sqrt{P}} + x^{1-\frac{\varepsilon}{2}}\log x \tag{2.11}$$

since $z \le y = x^{(1-\varepsilon)/2}$. Let us now deal with the terms t' < P. In this case, the innermost *p*-sum in (2.10) equals

$$\sum_{\substack{b \pmod{t'}} p \equiv b \pmod{t'}} \chi(b) \sum_{\substack{p \leq x/z \\ p \equiv b \pmod{t'} \\ (p,\ell)=1}} p^{i\xi}.$$

By partial summation, and (2.1) where we use the fact that we have excluded exceptional characters, this double sum is

$$\ll t'\frac{x}{z}\exp\left(-C'\sqrt{\log\frac{x}{z}}\right)(1+|\xi|)$$

for some absolute constant 0 < C' < 1 (without loss of generality). Therefore the terms t' < P contribute at most

$$P^{3/2}x(T + \log x) \exp\left(-\frac{C'}{2}\sqrt{\log\frac{x}{z}}\right) \ll P^{3/2}x(T + \log x) \exp\left(-\frac{C'}{4}\sqrt{\log x}\right)$$
(2.12)

to (2.10) where we used again $z \le x^{1/2}$. Now we choose

$$T := \exp\left(\frac{C'}{20}\sqrt{\log x}\right), \quad P := \exp\left(\frac{C'}{10}\sqrt{\log x}\right).$$

Collecting the error terms (2.9), (2.11) and (2.12), we see that (2.7) is

$$\ll x(\log x)^2 \exp\left(-\frac{C'}{20}\sqrt{\log x}\right),$$

and thus the total error in (2.4) and (2.5) is at most

$$O\left(x\exp\left(-\min\left(\frac{C'}{30},c_3\right)\sqrt{\log x}\right)\right).$$

For $x \ge \gamma_{n+1}$, the main term (2.6) is

$$\gg 2^{-\binom{n+1}{2}} \frac{x}{\log x} \frac{(\log(1+\varepsilon-2\varepsilon^2))^n}{2^{n+1}n!} \gg_{\varepsilon} \frac{x}{\log x} 2^{-(n+1)^2}.$$

Thus we can bound (2.4) from below by

$$\Xi_{n}2^{-\binom{n+1}{2}}\frac{x}{\log x}\frac{(\log\log x - \log\log \gamma_{n+1})^{n}}{2^{n+1}n!}\left(1 - O_{\varepsilon}\left(\frac{\exp((n+1)^{2})}{\exp(c_{1}\sqrt{\log \gamma_{n+1}})}\right)\right)$$

for $x \ge \gamma_{n+1}$ and some $c_1 > 0$. This is exactly (2.3) for n + 1.

References

- 1. J.E. Cremona, R.W.K. Odoni, Some density results for negative Pell equations; an application of graph theory. J. Lond. Math. Soc. **39**, 16–28 (1989)
- 2. H. Davenport, Multiplicative Number Theory, 2nd edn. (Springer, New York, 1980)
- É. Fouvry, J. Klüners, On the 4-rank of class groups of quadratic number fields. Invent. Math. 167, 455–513 (2007)
- 4. É. Fouvry, J. Klüners, On the negative Pell equation. Ann. Math. 172, 2035–2104 (2010)
- 5. É. Fouvry, J. Klüners, The parity of the period of the continued fraction of \sqrt{d} . Proc. Lond. Math. Soc. **101**, 337–391 (2010)
- 6. T. Nagell, Über die Lösbarkeit der Gleichung $x^2 Dy^2 = -1$, Ark. Mat. 23B, Nr. 6, 5 pp. (1933)
- 7. L. Redei, E. Reichardt, Die Anzahl der durch 4 teilbaren Invarianaten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. J. Reine Angew. Math. **170**, 69–74 (1934)
- P. Stevenhagen, The number of real quadratic fields having units of negative norm. Exp. Math. 2, 121–136 (1993)