ARTICLE IN PRESS YJNTH:6085

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the subgroup generated by solutions of Pell's equation

Elena C. Covill, Mohammad Javaheri, Nikolai A. Krylov [*]

Siena College, Department of Mathematics, 515 Loudon Road, Loudonville, NY 12211, United States of America

ARTICLE INFO

Article history:
Received 20 December 2017
Received in revised form 20 July 2018
Accepted 25 July 2018
Available online xxxx
Communicated by F. Pellarin

MSC:
primary 11D09
secondary 11R11, 11A55, 11R20

Keywords:
Pell's equation
Reciprocity laws
Continued fractions
Ideal class group

ABSTRACT

Equivalence classes of solutions of the Diophantine equation $a^2 + mb^2 = c^2$ form an infinitely generated abelian group G_m, where m is a fixed square-free positive integer. Solutions of Pell's equation $x^2 - my^2 = 1$ generate a subgroup P_m of G_m. We prove that P_m and G_m/P_m have infinite rank for all $m > 1$. We also give several examples of m for which G_m/P_m has nontrivial torsion.

1. Introduction

Let m be a fixed, square-free positive integer. Solutions (a_1, b_1, c_1) and (a_2, b_2, c_2) of the Diophantine equation

[*] Corresponding author.
E-mail addresses: ec20covi@siena.edu (E.C. Covill), mjavaheri@siena.edu (M. Javaheri), nkrylov@siena.edu (N.A. Krylov).

https://doi.org/10.1016/j.jnt.2018.07.001
0022-314X/© 2018 Elsevier Inc. All rights reserved.

$$a^2 + mb^2 = c^2 \tag{1.1}$$

produce another solution under the binary operation:

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2 - mb_1b_2, a_1b_2 + a_2b_1, c_1c_2). \tag{1.2}$$

This operation motivates the following definition.

Definition 1. Let $F_m = \mathbb{Q}[\sqrt{-m}] = \{a + b\sqrt{-m} : \ a, b \in \mathbb{Q}\}$ be the quadratic field associated with a square-free positive integer m. Let $\mathcal{S}_m$ denote the multiplicative subgroup of $F_m \backslash \{0\}$ consisting of all nonzero elements such that $a^2 + mb^2$ is a square of a rational number. We let $G_m = \mathcal{S}_m/\mathbb{Q}^*$.

An equivalence class $[a+b\sqrt{-m}] \in G_m$ can be represented by a *primitive* triple (x, y, z) with $x^2+my^2 = z^2$ (a triple (x, y, z) is primitive if $(x, y, z) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{N}$ and $\gcd(x, y, z) = 1$). We denote the equivalence class represented by a primitive triple (x, y, z) by $[x, y, z] \in G_m$. For example, the equivalence class of $[2 + 2\sqrt{-3}] \in G_3$ is denoted by $[1, 1, 2]$. This representation is unique up to the equivalence $[x, y, z] \sim [-x, -y, z]$. The group operation on G_m induced by the operation in (1.2) can be written as

$$[x, y, z] + [a, b, c] = \left[\frac{xa - myb}{g}, \frac{xb + ya}{g}, \frac{zc}{g}\right], \tag{1.3}$$

for $[x, y, z], [a, b, c] \in G_m$ and $g = \gcd(xa - myb, xb + ya, zc)$.

For $m > 1$, the group G_m has been studied by various authors [2,6–8], who have shown, among other results, that G_m is infinitely generated and has nontrivial torsion $\mathbb{Z}/3\mathbb{Z}$ only when $m = 3$.

In this paper, we study the subgroup of G_m generated by the solutions of Pell's equation

$$X^2 - mY^2 = 1. \tag{1.4}$$

Let $P_m \subseteq G_m$ denote the subgroup generated by all $[1, Y, X]$ such that $(1, Y, X)$ is a solution of (1.1), or equivalently (X, Y) is a solution of (1.4). In Section 2, we show that P_m has infinite rank for all square-free $m > 1$ (Proposition 3). We are interested in determining the rank and torsion of G_m/P_m. In Section 3, we prove that G_m/P_m has infinite rank for all square-free $m > 1$. In order to prove this, from a recursion corresponding to the Pell equation, we derive a degree-8 polynomial $f(x)$ and discuss its irreducibility over $\mathbb{Q}$ (see Proposition 6). Regardless of irreducibility of $f(x)$, we show that the splitting field of $f(x)$ does not include $\mathbb{Q}[\zeta_{16}]$, where ζ_{16} is the primitive 16^{th} root of unity (see Corollary 11). We then use the Frobenius Density Theorem to conclude that there exist infinitely many primes $p \not\equiv 1 \pmod{16}$ with the property that $f(x)$ splits completely modulo p (see Proposition 14). For each such p, we associate an

Please cite this article in press as: E.C. Covill et al., On the subgroup generated by solutions of Pell's equation, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.07.001