Journal of Number Theory 178 (2017) 40–46

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Imaginary quadratic fields of class number 2 and Levy–Hendy quadratics

Viet Kh. Nguyen

Fpt University, 8 Ton That Thuyet, My Dinh, Tu Liem Hanoi, Viet Nam

ARTICLE INFO

Article history:
Received 29 November 2016
Received in revised form 28 February 2017
Accepted 28 February 2017
Available online 3 April 2017
Communicated by D. Goss

In memory of V.A. Iskovskikh

MSC:
primary 11G30, 11R29, 11R11

Keywords:
Imaginary quadratic fields
Class number
Euler
Levy
Hendy
Prime quadratics

ABSTRACT

Let $d = pq \equiv 3 \pmod 4$ with prime p, q and $q < p$. We prove a precise bound in Hendy's theorem on imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with class number $h(-d) = 2$ which is a full analogue of Frobenius–Rabinowitsch theorem (the case of class number one). Namely it is shown that $h(-d) = 2$ if and only if the Levy–Hendy quadratic $L_d(x) = qx^2 + qx + \ell_0$ with $\ell_0 = \dfrac{p+q}{4}$ takes only prime values for integers x in the interval $0 \le x \le \ell_0 - 2$. We discuss also two related conjectures in connection with generalizing a result of Chowla et al. ([1]) on the class number and the least prime quadratic residue.

1. Introduction

In 1772 Euler discovered that for primes $\ell = 3, 5, 11, 17, 41$ the quadratic polynomial

$$E_{4\ell-1}(x) = x^2 + x + \ell$$

E-mail address: vietnk@fe.edu.vn.

http://dx.doi.org/10.1016/j.jnt.2017.02.014
0022-314X/

takes only prime values for integers $x,\ 0 \le x \le \ell - 2$. In fact the values $d = 4\ell - 1$ are precisely those for which the field $\mathbb{Q}(\sqrt{-d})$ has class number one (two values $d = 3, 7$ are exceptions in a trivial sense) – the fact that was proved independently by Frobenius and Rabinowitsch in 1912.

Theorem 1.1. *The quadratic polynomial $E_{4\ell-1}(x)$ assumes prime values for integers x in the interval $0 \le x \le \ell - 2$ if and only if $\mathbb{Q}(\sqrt{1-4\ell})$ has class number one.*

In 1914 Levy noticed another quadratic polynomial with a long sequence of prime values for 22 consecutive integers, namely

$$L_{267}(x) = 3x^2 + 3x + 23$$

is prime for $0 \le x \le 21$. This observation is related to the fact that the field $\mathbb{Q}(\sqrt{-267})$ has class number two (for the above facts *cf.* [4,6] and references therein).

In 1974 Hendy succeeded in generalizing Theorem 1.1 for imaginary quadratic fields of class number two.

Theorem 1.2 *([3]). Let $d = pq \equiv 3\ (4)$ with prime p, q and $q < p$. We denote the Levy–Hendy quadratic by*

$$L_d(x) = qx^2 + qx + \ell_0,\ \ell_0 = \frac{p+q}{4}.$$

Then $\mathbb{Q}(\sqrt{-d})$ has class number $h(-d) = 2$ if and only if the quadratic $L_d(x)$ takes only prime values for integers x in the interval $0 \le x \le \sqrt{pq/12} - 1/2$.

The method of proof of Theorem 1.2 is elementary in the sense that it does not rely on a deep result of Baker and Stark completely determining all imaginary quadratic fields with class number two by transcendental methods. The upper bound $\sqrt{pq/12} - 1/2$ in Theorem 1.2 was improved to $p/4 - 1$ in [4] (*cf.* also [6] for a slightly better bound $p/4 - 1/2 - 1/2q$). Note that these bounds are sharp in the case $q = 3$, *e.g.* as in the case of Levy polynomial.

In this note by elementary means (*i.e.* using the only arithmetic in the ring of integers of $\mathbb{Q}(\sqrt{-d})$, as in [3]) we shall prove the following theorem which is a full analogue of Theorem 1.1.

Theorem 1.3. *In the notation of Theorem 1.2 the field $\mathbb{Q}(\sqrt{-d})$ has class number $h(-d) = 2$ if and only if the quadratic $L_d(x)$ takes only prime values for integers x in the interval $0 \le x \le \ell_0 - 2$.*

It should be noted that in this way one finds an interesting relationship with Thue equations to prime factorizations of $E_d(x)$, $L_d(x)$ as x goes large. We have carried out nu-

merous computations in the big range for $E_{163}(x)$ and $L_{267}(x)$. Details will be submitted elsewhere.

The paper is organized as follows. In §2 we discuss two conjectures on the least split prime and class number two. §3 is devoted to the proof of our main theorem (Theorem 1.3).

Notation. Throughout this note we shall keep the following notation

$d = pq \equiv 3\ (4)$ with prime p, q, $q < p$, $\ell_0 = \dfrac{p+q}{4}$;
$h(-d)$ – the class number of the field $\mathbb{Q}(\sqrt{-d})$;
ρ_d – the least split prime, *i.e.* the least among those with Jacobi symbol $\left(\dfrac{\bullet}{d}\right) = 1$;
$L_d(x) = qx^2 + qx + \ell_0$ – the Levy–Hendy quadratic;
$Q_0(x,y) = x^2 + xy + \dfrac{d+1}{4}y^2$, $Q_1(x,y) = qx^2 + qxy + \ell_0 y^2$;
$\mathcal{E}$ (resp. $\mathcal{A}$) – the set of (rational) integers represented by Q_0 (resp. by Q_1).

2. The least split prime and class number two

It is well known that there is another characterization of imaginary quadratic fields with class number one due to Chowla et al. ([1], *cf.* also [5]).

Theorem 2.1. *Let p be a prime > 3 and $\equiv 3\ (8)$. Then $h(-p) = 1$ if and only if $\rho_p = \dfrac{p+1}{4}$.*

The proof of Theorem 2.1 uses the binary quadratic form (bQF for short) language. We sometimes write a bQF $ax^2 + bxy + cy^2$ as $[a,b,c]$. We are interested in positive definite forms, *i.e.* forms with negative discriminant: $b^2 - 4ac < 0$. In our case $Q_1(x,y)$ corresponds to $[q,q,\ell_0]$ which is an ambiguous form, *i.e.* representing an element of order 2 in the class group $\mathcal{C}(-d)$. A bQF $[a,b,c]$ is called reduced, if $|b| \le a \le c$ (and $b \ge 0$, if either equality holds in these conditions). Two forms are equivalent if there exists a unimodular transformation from one form to another. The form $Q_1(x,y)$ is reduced if and only if $3q < p$. In the case $p < 3q$ the reduction algorithm gives a transformation to the reduced form

$$[q,q,\ell_0] \quad \sim \quad [\ell_0, 2\ell_0 - q, \ell_0].$$

Our aim in this section is to give a partial generalization of Theorem 2.1 for the class number two case and discuss some related conjectures. Note that if $d \equiv 7\ (8)$, then $\left(\dfrac{2}{d}\right) = 1$. So one has the only field $\mathbb{Q}(\sqrt{-15})$ with class number two. The statement is, in a sense, trivially true.

The following conjecture fits into the frame of well-known conjectures (*cf.* [6])

Conjecture 2.2. *In the notation above $h(-d) = 2$ if and only if $\rho_d = \ell_0$.*

A deeper phenomenon could be the following

Conjecture 2.3. *In the same notation if $\left(\frac{q}{p}\right) = -1$, and $h(-d) > 2$, then there is a quadratic residue modulo d less than ℓ_0.*

Theorem 2.4. *Conjecture 2.2 is true, provided $p > 3q$.*

Proof. First assume $h(-d) = 2$. If ℓ is an odd prime with $\left(\frac{\ell}{d}\right) = 1$, then $\left(\frac{-d}{\ell}\right) = 1$. By Lemma 2.5 ([2], I, §2) ℓ is represented by either Q_0, or Q_1. If $\ell = Q_0(x, y),\ y \neq 0$, then

$$\ell = \frac{(2x+y)^2}{4} + \frac{dy^2}{4} \geq \frac{d+1}{4}$$

as if $2x + y = 0$, then $y^2 \geq 4$. Similarly in the case $\ell = Q_1(x, y),\ y \neq 0$: $\ell \geq \ell_0$. In view of Hendy's theorem $\ell_0 = L_d(0)$ is prime. Also ℓ_0 is a split prime, so one concludes that $\rho_d = \ell_0$.

Conversely assuming $\rho_d = \ell_0$ consider a reduced bQF $[a, b, c]$ with discriminant $b^2 - 4ac = -d$. Since $d \equiv 3\ (8)$: a is odd. If $a = 1$, we get Q_0. So let's assume $a > 1$. Clearly for any prime divisor $\ell\ (\neq q)$ of a: $\left(\frac{\ell}{d}\right) = 1$. From the reduced condition $|b| \leq a \leq c$, it follows that $a < \sqrt{\frac{d}{3}}$ which is less than ℓ_0 as $p > 3q$. By the assumption $\rho_d = \ell_0$, a can have only q as a prime divisor. If $a = qa'$, then $b = qb'$, and

$$qb'^2 - 4a'c = -p, \quad |b'| \leq a' \leq \frac{c}{q}.$$

Hence $a' < \sqrt{\frac{p}{3q}}$, and by the same reason $a' = 1$. So $[a, b, c]$ is Q_1. The proof is complete.

3. Proof of Theorem 1.3

The proof is divided into several steps.

1) Every prime divisor ℓ of $L_d(x)$ is a split prime (the converse is also true, *cf.* [6]). Indeed, we may write $\ell s = qx^2 + qx + \frac{p+q}{4}$ for some integer s, so $p = -q(2x+1)^2 + 4\ell s$. One has

$$\left(\frac{\ell}{d}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{d}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{q}{\ell}\right)\left(\frac{p}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{q}{\ell}\right)\left(\frac{-q(2x+1)^2 + 4\ell s}{\ell}\right) =$$
$$= \left(\frac{-1}{\ell}\right)\left(\frac{q}{\ell}\right)\left(\frac{-q(2x+1)^2}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{q}{\ell}\right)\left(\frac{-q}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{q}{\ell}\right)\left(\frac{-1}{\ell}\right)\left(\frac{q}{\ell}\right) = 1$$

as claimed.

2) For $\ell \in \mathcal{E}$: $\ell \geq \dfrac{d+1}{4}$ and for $\ell \in \mathcal{A}$: $\ell \geq \ell_0$ (as in the proof of Theorem 2.4).

3) It is easy to see for $x \in [0, \ell_0 - 1]$

$$qL_d(x) < \frac{d^2}{4} \tag{3.1}$$

Indeed

$$qL_d(x) \leq qL_d(\ell_0 - 1) < q^2\ell_0^2 < q^2\left(\frac{p}{2}\right)^2 = \frac{d^2}{4}.$$

4) As noted in §2: $Q_1(x, y)$ is an ambiguous form, *i.e.* representing an element of order 2 in the class group $\mathcal{C}(-d)$. In fact we have the following useful formulae while working in the ring of integers of $\mathbb{Q}(\sqrt{-d})$

$$\begin{aligned} Q_0(x,y) &= \left[\frac{2x+y}{2} + \frac{y}{2}\sqrt{-d}\right]\left[\frac{2x+y}{2} - \frac{y}{2}\sqrt{-d}\right] \\ Q_1(x,y) &= \left[\frac{\sqrt{q}(2x+y)}{2} + \frac{y}{2}\sqrt{-p}\right]\left[\frac{\sqrt{q}(2x+y)}{2} - \frac{y}{2}\sqrt{-p}\right] \\ Q_1(x,y)Q_1(u,v) &= \gamma(x,y,u,v)\overline{\gamma(x,y,u,v)} \end{aligned} \tag{3.2}$$

where $\gamma(x, y, u, v) = \dfrac{q(2x+y)(2u+v) - yvp}{4} + \dfrac{v(2x+y) + y(2u+v)}{4}\sqrt{-d}$.

The main identity we shall use is

$$qL_q(n) = N(\alpha(n)) := \alpha(n)\overline{\alpha(n)} \tag{3.3}$$

where $\alpha(n) = \dfrac{q(2n+1)}{2} + \dfrac{1}{2}\sqrt{-d}$.

5) For all p, q as in Theorems 1.2 and 1.3 one has

$$\lfloor \sqrt{pq/12} - 1/2 \rfloor \leq \ell_0 - 2.$$

So in view of Hendy's theorem (Theorem 1.2) it suffices to prove the necessity. In fact we shall show that if $h(-d) = 2$, then in the sequence $L_d(0), L_d(1), L_d(2), \cdots$, the first composite value is $L_d(\ell_0 - 1)$.

Assume for some $n_0 \in [0, \ell_0 - 1]$: $L_d(n_0)$ is composite. Clearly $n_0 > 0$, as $L_d(0)$ is prime by Hendy's theorem. Since $h(-d) = 2$ and by Step 1) every prime factor of $L_d(n_0)$ is represented by Q_0, or Q_1. In view of (3.2), (3.3) the number of (not necessarily distinct) prime factors of $L_d(n)$, belonging to $\mathcal{A}$, must be odd. Thus one may assume that there is a non-trivial decomposition $L_d(n_0) = m_0a_1$ with $m_0 \in \mathcal{E}$, $a_1 \in \mathcal{A}$ meaning $m_0 = Q_0(x_0, y_0)$, $a_1 = Q_1(x_1, y_1)$ for certain integers $x_i, y_i,\ i = 0, 1$. We have

$$qL_q(n_0) = N(\alpha(n_0)) := \alpha(n_0)\overline{\alpha(n_0)} \tag{3.4}$$

where $\alpha(n_0) = \dfrac{q(2n_0+1)}{2} + \dfrac{1}{2}\sqrt{-d}$. By putting $\alpha_i := 2x_i + y_i,\ \beta_i := y_i,\ i = 0, 1$ and using (3.2), one has

$$\begin{cases} m_0 = \beta(m_0)\overline{\beta(m_0)} \\ qa_1 = \gamma(a_1)\overline{\gamma(a_1)} \end{cases} \tag{3.5}$$

where $\beta(m_0) = \dfrac{\alpha_0}{2} + \dfrac{\beta_0}{2}\sqrt{-d}$ and $\gamma(a_1) = \dfrac{q\alpha_1}{2} + \dfrac{\beta_1}{2}\sqrt{-d}$. So (3.4), (3.5) give us the following system of Diophantine equations

$$\begin{cases} 4n_0 + 2 = \alpha_0\alpha_1 - \beta_0\beta_1 p \\ \alpha_0\beta_1 + \alpha_1\beta_0 q = 2 \end{cases} \tag{3.6}$$

Also from the non-trivial decomposition $\alpha(n_0) = \beta(m_0)\gamma(a_1)$ and the fact that the coefficient of $\sqrt{-d}/2$ in $\alpha(n_0)$ is 1, it follows

$$\beta_0\beta_1 \neq 0 \tag{3.7}$$

From (3.1), (3.4) and

$$N(\alpha) = \frac{1}{16}(\alpha_0^2 + \beta_0^2 d)(\alpha_1^2 q^2 + \beta_1^2 d) = \frac{1}{16}\left[\alpha_0^2\alpha_1^2 + d(\alpha_0^2\beta_1^2 + \alpha_1^2\beta_0^2 q^2) + \beta_0^2\beta_1^2 d^2\right]$$

one concludes that $\beta_0^2\beta_1^2 < 4$, therefore

$$\beta_0^2\beta_1^2 = 1 \tag{3.8}$$

We claim that the only integer solutions to (3.6), (3.8), up to sign, are $\alpha_0 = q-2,\ \alpha_1 = 1$ which correspond to $n_0 = \ell_0 - 1$. Indeed from (3.7), (3.8), $\beta_0\beta_1 = \pm 1$. If $\beta_0\beta_1 = 1$, then $\alpha_0\alpha_1 > 0$ and either $\beta_0 = \beta_1 = 1$, or $\beta_0 = \beta_1 = -1$. In either case the second equation of (3.6) is not soluble. It remains to consider the case $\beta_0\beta_1 = -1$, *i.e.*, either $\beta_0 = 1,\ \beta_1 = -1$, or $\beta_0 = -1,\ \beta_1 = 1$. Let us first consider the case $\beta_0 = 1,\ \beta_1 = -1$. From (3.6) it follows that

$$4n_0 + 2 = p + \alpha_1(\alpha_1 q - 2) \geq p + q - 2 \tag{3.9}$$

or equivalently

$$n_0 \geq \ell_0 - 1$$

which implies $n_0 = \ell_0 - 1$, as claimed. Note that in (3.9) we used the fact that $\alpha_1 = 2x_1 + \beta_1$, so $\alpha_1 \neq 0$.

Similarly for the case $\beta_0 = -1,\ \beta_1 = 1$. The theorem is proved.

Acknowledgments

I would like to thank the referee for several suggestions and improvements. This paper is in a series dedicated to the memory of my teacher V.A. Iskovskikh with profound admiration.

References

[1] S. Chowla, J. Cowles, M. Cowles, The least prime quadratic residue and the class number, J. Number Theory 22 (1986) 1–3.
[2] D.A. Cox, Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication, Wiley, New York, 1989.
[3] M.D. Hendy, Prime quadratics associated with complex quadratic fields of class number two, Proc. Amer. Math. Soc. 43 (1974) 253–260.
[4] R.A. Mollin, Quadratic polynomials producing consecutive, distinct primes and class groups of complex quadratic fields, Acta Arith. 74 (1996) 17–30.
[5] T. Nagell, Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Semin. Hamb. Univ. 1 (1922) 140–150.
[6] K. Shimizu, Imaginary quadratic fields whose exponents are less than or equal to two, II, RIMS Kôkyûroku Bessatsu (2012) 255–269.