Effective lower bound for the class number of a certain family of real quadratic fields

ADDENDUM

Kostadinka Lapkova (Budapest)
Email: k.lapkova@gmail.com

August 14, 2012

I thank Stéphane Louboutin for his remarks on my paper [1]. This addendum answers his comments. In [1] the following main result is shown (there Theorem 1.2).

Theorem 1. *Let $n = m(m^2 - 306)$ for a positive odd integer m, and $N = 2^3 \cdot 3^3 \cdot 103 \cdot 10303$. If $d = n^2 + 4$ is square-free and $\left(\dfrac{d}{N}\right) = -1$, then for every $\epsilon > 0$ there exists an effective computable constant $c_\epsilon > 0$, depending only on ϵ, such that*

$$h(d) = h(n^2 + 4) > c_\epsilon \left(\log d\right)^{1-\epsilon} .$$

As Gergely Harcos had suspected the condition $\left(\dfrac{d}{N}\right) = -1$ yields a stronger bound $h(d) \gg \log d$ because for some prime divisor p of the conductor N we have $\left(\frac{d}{p}\right) = 1$. Louboutin pointed out to me a proof of this fact, and more precisely of the bound

$$h(d) \geq \frac{\log \frac{1}{2}\sqrt{d}}{\log 10303}, \tag{1}$$

which can be found in [2]. It means that in [1] a weaker result was proven than an already existing one.

The method of [1], however, can be used for new families as well. If we take a look at Table 1 from [1], we see that we can formulate

Theorem 2. *Let $n = m(m^2 - 3k)$ for a positive odd integer m and even k. Let $d = n^2 + 4$ be square-free and $\left(\dfrac{d}{p}\right) = -1$ for $p \in \mathcal{A}$ for the set of primes $\mathcal{A}$. Then in the cases*

i) $k = 136$, $\mathcal{A} = \{3, 7, 43, 61, 137\}$,

ii) $k = 184$, $\mathcal{A} = \{3, 5, 7, 151, 223\}$,

we have the following claim. For every $\epsilon > 0$ there exists an effective computable constant $c_\epsilon > 0$, depending only on ϵ, such that

$$h(d) = h(n^2 + 4) > c_\epsilon \left(\log d\right)^{1-\epsilon}$$

The proof of the theorem assumes that the analytic rank of the elliptic curves E_{136} and E_{184} is three.

k	conductor N_k
65	$2^5 \cdot 3^3 \cdot 11 \cdot 19 \cdot 73$
102	$2^3 \cdot 3^3 \cdot 103 \cdot 10303$
114	$2^3 \cdot 3^3 \cdot 5 \cdot 13 \cdot 23 \cdot 991$
129	$2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 337$
136	$2^2 \cdot 3^3 \cdot 7 \cdot 43 \cdot 61 \cdot 137$
141	$2^5 \cdot 3^3 \cdot 19 \cdot 71 \cdot 1039$
145	$2^5 \cdot 3^3 \cdot 7 \cdot 19 \cdot 73 \cdot 157$
162	$2^3 \cdot 3^3 \cdot 163 \cdot 26083$
184	$2^2 \cdot 3^3 \cdot 5 \cdot 37 \cdot 151 \cdot 223$
187	$2^4 \cdot 3^3 \cdot 7 \cdot 47 \cdot 4969$
191	$2^4 \cdot 3^3 \cdot 12097$

Table 1: Elliptic curves E_k of analytic rank 3

In the proof of (1) the continued fractional expansion of $(1+\sqrt{d})/2$ is used. After Theorem 4 [3] we see that for example for the family of square-free $d = n^2 + 8$ the surd $\sqrt{d}$ is with unknown such expansion (the lowest period of the continued fractional expansion tends to infinity together with n). So no analogue of (1) is known for these discriminants. Our method works in this case too.

We need to consider the family of elliptic curves

$$\mathcal{E}_k : y^2 = x^3 - 3k^2 x + (2k^3 + 8).$$

SAGE gives that for example the curves $\mathcal{E}_{174}$ and $\mathcal{E}_{192}$ are of analytic rank three. Here k is even, and now we do not worry whether the parameterizing elliptic curve has odd or even number of prime divisors of its conductor.

Theorem 3. *Let $n = m(m^2 - 3k)$ for a positive odd integer m and even k. Let $d = n^2 + 8$ be square-free and $\left(\dfrac{d}{N}\right) = -1$ for a certain positive integer N. Then in the cases*

i) $k = 174$, $N = 2^6 \cdot 3^2 \cdot 2634013$,

ii) $k = 192$, $N = 2^6 \cdot 3^2 \cdot 5 \cdot 707789$,
we have the following claim. For every $\epsilon > 0$ there exists an effective computable constant $c_\epsilon > 0$, depending only on ϵ, such that

$$h(d) = h(n^2 + 8) > c_\epsilon \,(\log d)^{1-\epsilon}$$

References

[1] Lapkova, K., *Effective lower bound for the class number of a certain family of real quadratic fields*, J. Number Theory 132 (2012), no. 12, 2736–2747, DOI: 10.1016/j.jnt.2012.05.029

[2] Louboutin, St., *Continued Fractions and Real Quadratic Fields*, J. Number Theory 30 (1988), 167–176

[3] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6 (1960-1961), 393–413