

By (13), we have

$$g_i \geq \prod_{\substack{p \text{ inert in } K \\ (p+1) | M_{x_i}}} 2 > \exp \left((\log 2) \exp \left(C \frac{\log x_i}{\log \log x_i} \right) \right) > i$$

for sufficiently large i . Moreover, we have $L(g_i) \mid M_{x_i}$, which implies that

$$L(g_i) \leq M_{x_i} \leq x_i^2 = (\log i)^{(4/C) \log \log \log i} < (\log g_i)^{c_0 \log \log \log g_i}$$

for sufficiently large i , where $c_0 := 4/C$. The asserted upper bound follows by extracting a strictly monotonic subsequence $\{f_i\}_{i \geq 1}$ from $\{g_i\}_{i \geq 1}$.

5. MINIMAL ORDER IN THE REAL CASE: PROOF OF THEOREM 1.4

Let K be a real quadratic field. We remind the reader that ϵ denotes the fundamental unit of K , and we set

$$\delta = \begin{cases} 1 & \text{if } N_{K/\mathbb{Q}}(\epsilon) = 1, \\ 2 & \text{if } N_{K/\mathbb{Q}}(\epsilon) = -1. \end{cases}$$

If p is a prime inert in K , then its associated Frobenius element is conjugation on K (the nontrivial element of $\text{Gal}(K/\mathbb{Q})$). Hence,

$$\epsilon^{p+1} \equiv \epsilon^p \epsilon \equiv N_{K/\mathbb{Q}}(\epsilon) \pmod{p\mathcal{O}_K},$$

and

$$\epsilon^{\delta(p+1)} \equiv N_{K/\mathbb{Q}}(\epsilon)^\delta \equiv 1 \pmod{p\mathcal{O}_K}.$$

Thus, the order of ϵ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ is a divisor of $\delta(p+1)$. We will base our proof of Theorem 1.4 on the following result of Roskam [Ros00].

Proposition 5.1 (conditional on GRH). *There are infinitely many primes p , inert in K , for which the order of ϵ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ is precisely $\delta(p+1)$.*

(In fact, Roskam shows that the order is $\delta(p+1)$ not only for infinitely many inert primes, but for a positive proportion of all inert primes. The weaker version here is sufficient for our purposes.) Theorem 1.4 is an immediate consequence of Proposition 5.1 in conjunction with the next assertion.

Proposition 5.2. *If p is a prime inert in K for which ϵ has order $\delta(p+1)$ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$, then*

$$\rho(\mathcal{O}_p) \leq h_K + \frac{3}{2}.$$

Proof. Let p be as in the proposition. Then $\epsilon^{\ell(p)} \equiv n \pmod{p\mathcal{O}_K}$ for some rational integer n prime to p . By Fermat's little theorem,

$$\epsilon^{(p-1)\ell(p)} \equiv 1 \pmod{p\mathcal{O}_K}.$$

We are assuming that ϵ has order $\delta(p+1)$ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$. Hence, the displayed congruence forces

$$p+1 \mid \delta(p+1) \mid (p-1)\ell(p).$$

Writing $(p-1)\ell(p) = (p+1)\ell(p) - 2\ell(p)$, we deduce that $p+1 \mid 2\ell(p)$. In particular,

$$\ell(p) \geq \frac{p+1}{2}.$$