

On (p, i) -regular quadratic number fields

J. Assim, S. Bhihi and Z. Bouazzaoui

MSC 2010 Classifications: Primary 11F37; Secondary 11R11.

Keywords and phrases: Modular forms, L -functions, Quadratic fields.

The authors would like to thank the reviewers and the editor.

Abstract. We discuss some aspects of indivisibility by a fixed prime number p of values of L -functions $L(\chi_d, \cdot)$ associated to the non-trivial character of real quadratic fields $\mathbf{Q}(\sqrt{d})$ at odd negative integers. These values are closely related to the orders of certain cohomology groups. For an even integer $i \geq 2$, we use the Cohen-Eisenstein series to show how to prove the existence of infinitely many real quadratic fields such that $L(\chi_d, 1-i) \not\equiv 0 \pmod{p}$ and $\mathbf{Q}(\sqrt{d})$ satisfies splitting conditions at a finite set of primes.

1 Introduction and Statement of Results

In algebraic number theory, special values of L -functions at integers contain rich arithmetic information. The first example is Riemann's zeta function defined by the series

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^s},$$

for $\Re(s) > 1$. For a number field K , Dedekind zeta function $\zeta_K(s)$ is a generalization of the Riemann zeta function. By definition,

$$\zeta_K(s) = \sum_I \frac{1}{(N_{K/\mathbf{Q}}(I))^s} = \prod_{\mathfrak{p}} \frac{1}{1 - (N_{K/\mathbf{Q}}(\mathfrak{p}))^s},$$

where I ranges over non-zero ideals of the ring of integers $\mathcal{O}_K$, $\mathfrak{p}$ ranges over prime ideals of $\mathcal{O}_K$ and $N_{K/\mathbf{Q}}(I) = [\mathcal{O}_K : I]$ is the norm of I .

Let r_1 (resp. r_2) denote the number of real embeddings (resp. the number of complex embeddings) of K . The function $\zeta_K(s)$ converges absolutely for $\Re(s) > 1$ and extends to a meromorphic function defined for $s \in \mathbb{C} \setminus \{-1\}$ with only one simple pole at $s = 1$. Furthermore, the order of vanishing of $\zeta_K(s)$ at $s = 0$ is equal $r_1 + r_2 - 1 = \dim_{\mathbf{Q}} U_K \otimes \mathbf{Q}$, where U_K is the units group of K . The quantity $\zeta_K^*(0) := \lim_{s \rightarrow 0} \frac{\zeta_K(s)}{s^{r_1+r_2-1}}$ is the first non-zero term in the Taylor expansion of $\zeta_K(s)$ around 0. It is named the special value of $\zeta_K(s)$ at $s = 0$.

The following well-known analytic class number formula is an illustrated example that the special values of L -functions contain global arithmetic information:

$$\zeta_K^*(0) = -\frac{h_K R_K}{w_K},$$

where h_K is the class number of K , R_K is the regulator of K and w_K is the number of roots of unity contained in K .

Lichtenbaum's conjecture [13] is a generalization of the class number formula. It asserts that there is a relation between special values of $\zeta_K(s)$ at negative integers and the orders of certain cohomology groups. Borel shows that the order of vanishing of $\zeta_K(s)$ at $1-i$, $i \geq 2$, is precisely the $\mathbf{Z}$ -rank of the odd K -group $K_{2i-1}\mathcal{O}_K$. When K is a totally real field and $i \geq 2$ is an even

integer, the Lichtenbaum conjecture holds as a consequence of the Main Conjecture in Iwasawa theory, proved by Wiles [21]. In this case, the value $\zeta_K(1-i)$ does not vanish and we have

$$w_i(K)\zeta_K(1-i) \sim_p |H_{\text{ét}}^2(\text{spec}\mathcal{O}_K[1/p], \mathbf{Z}_p(i))|, \quad (1.1)$$

where $w_i(K) = |H^0(K, \mathbf{Q}_p/\mathbf{Z}_p(i))|$ and $\sim_p$ means having the same p -adic valuation. Notice that the étale cohomology group $H_{\text{ét}}^2(\text{spec}\mathcal{O}_K[1/p], \mathbf{Z}_p(i))$ is isomorphic to the p -primary part of the K -theory group $K_{2i-2}\mathcal{O}_K$ and $H^0(K, \mathbf{Q}_p/\mathbf{Z}_p(i))$ is isomorphic to the $\mathbf{Z}_p$ -torsion of $K_{2i-1}\mathcal{O}_K$. Our interest is on the indivisibility by an odd prime number p of the special values of the Dedekind zeta functions of real quadratic fields at odd negative integers.

Hereafter, for a number field K and an odd prime number p , denote by $\mathcal{G}_K$ the Galois group over K of the maximal algebraic extension of K , which is unramified outside p -adic and infinite places of K . The p -adic cohomology groups $H^2(\mathcal{G}_K, \mathbf{Z}_p(i))$, $i \in \mathbf{Z}$, coincide with the étale cohomology groups $H_{\text{ét}}^2(\text{spec}\mathcal{O}_K[1/p], \mathbf{Z}_p(i))$. These cohomological invariants reflect arithmetic properties of K at the prime number p . The number field K is called (p, i) -regular if the cohomology group $H^2(\mathcal{G}_K, \mathbf{Z}/p\mathbf{Z}(i))$ vanishes [1]. In Section 2, we give a characterization of (p, i) -regularity in terms of indivisibility by p of special values of the Dedekind zeta function if K is totally real (Proposition 2.1).

For a given odd prime number p , Wiles proved in [22] that there exists an imaginary quadratic field K such that $p \nmid h_K$, and K satisfies some splitting conditions at a finite set of primes. O. Beckwith quantifies in [4] the theorem of Wiles by proving an estimate for the number of imaginary quadratic fields $K = \mathbf{Q}(\sqrt{-d})$, $d \leq X$, $X > 0$, satisfying Wiles' conditions. The methods used in [4] follow partially [17] which provide a quantitative result for the number of $(p, \frac{p-1}{2})$ -regular quadratic fields $K = \mathbf{Q}(\sqrt{(-1)^{\frac{p-1}{2}}d})$ (but without any local conditions [17, Theorem 1]). We would be interested to prove an analogue result of [4] for (p, i) -regular number fields. We fix some notations that will be used in the text:

For a disjoint union of finite sets of odd primes $S = S_+ \cup S_0 \cup S_-$, we denote by $\mathcal{F}_{2,S}$ the set of real quadratic fields $F = \mathbf{Q}(\sqrt{d})$ such that primes of S_0 ramify in F , primes of S_+ split in F and primes of S_- are inert in F .

Theorem 1.1. *Let $i \geq 2$ be an even integer and let p be an odd prime number such that $p-1 \nmid 2i$. Suppose that there exists a square-free positive integer d_0 such that $\mathbf{Q}(\sqrt{d_0}) \in \mathcal{F}_{2,S}$ is (p, i) -regular.*

Then there are infinitely many real quadratic fields $F = \mathbf{Q}(\sqrt{d})$ satisfying

- (i) F is (p, i) -regular;
- (ii) $F \in \mathcal{F}_{2,S}$.

In fact, we have

$$\#\{0 < d < X : \mathbf{Q}(\sqrt{d}) \text{ satisfies the conditions (1) and (2)}\} \gg \frac{\sqrt{X}}{\log(X)}.$$

In the case $i = 2$, we prove the existence of a real quadratic $(p, 2)$ -regular field satisfying the above local conditions under some additional assumptions on the primes of S . We then obtain the following

Theorem 1.2. *Let $p > 3$ a prime, and $S = S_+ \cup S_0 \cup S_-$ a disjoint union of finite sets of primes. For all $\ell \in S$ we assume that:*

- i. $\ell \not\equiv 0, \pm 1 \pmod{p}$;
- ii. $\ell^2 \not\equiv -1 \pmod{p}$.

Then there exist infinitely many real quadratic fields F satisfying

- (i) F is $(p, 2)$ -regular;
- (ii) $F \in \mathcal{F}_{2,S}$.

To prove these results, we use the theory of modular forms. We construct an adequate modular form that we deduce from the Cohen-Eisenstein series (Lemma 3.1) which are modular forms of half-integer weight and whose Fourier coefficients involve values of L -functions of quadratic fields.

2 (p, i) -regular number fields and values of zeta functions

Let $i \in \mathbf{Z}$. Recall that a number field K is called (p, i) -regular if the Galois cohomology group $H^2(\mathcal{G}_K, \mathbf{Z}/p\mathbf{Z}(i))$ vanishes [1]. Number fields which are $(p, 0)$ -regular are precisely p -rational fields [14] [15], and $(p, 2)$ -regular fields are p -regular fields studied in [9].

The (p, i) -regularity gives arithmetic information about the field at the prime number p . For example, a (p, i) -regular number field satisfies the following twisted analogue of Leopoldt's conjecture

$$H^2(\mathcal{G}_K, \mathbf{Q}_p/\mathbf{Z}_p(i)) = 0 \quad (\text{for } i \neq 1).$$

We have the following useful description of the (p, i) -regularity of totally real number fields.

Proposition 2.1. *Let $i \geq 2$ be an even integer. A totally real number field K is (p, i) -regular if and only if $w_i(K)\zeta_K(1-i)$ is a p -adic unit.*

Proof. By (1.1), we have

$$w_i(K)\zeta_K(1-i) \sim_p |H^2(\mathcal{G}_K, \mathbf{Z}_p(i))|.$$

Furthermore, we have the equivalence

$$H^2(\mathcal{G}_K, \mathbf{Z}/p\mathbf{Z}(i)) = 0 \Leftrightarrow H^2(\mathcal{G}_K, \mathbf{Z}_p(i)) = 0. \quad (2.1)$$

Thus, K is (p, i) -regular precisely when $w_i(K)\zeta_K(1-i)$ is a p -adic unit. $\square$

In particular, a totally real number field is p -rational precisely when $w_{p-1}(K)\zeta_K(2-p)$ is a p -adic unit. In [10], while studying p -rational number fields, Greenberg suggested the following conjecture about the existence of p -rational number fields.

Conjecture 2.2. (Greenberg p -rational conjecture) For any odd prime p and any integer $t \geq 1$, there exists a p -rational field K such that $\text{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^t$.

As an interesting consequence, the conjecture of Greenberg implies the following proposition cf. [10, Proposition 6.2.2].

Proposition 2.3. *Suppose that K is complex with Galois group isomorphic to $(\mathbf{Z}/2\mathbf{Z})^t$, where $t \geq 4$. Suppose also that $4 \leq n \leq 2^{t-1} - 3$. If K is p -rational, there exists a p -adic Galois representation with open image in $\text{GL}_n(\mathbf{Z}_p)$.*

Greenberg's conjecture is known to be true for $t = 1$ since, for every odd prime number p , there exists an imaginary quadratic p -rational field. It is also known to be true for $t = 2$ by a recent result [5]. In fact, for a given prime number, using extensive computations, we can find examples of multi-quadratic p -rational fields of large degree [6]. Otherwise, the conjecture is still open.

In [1] the author studied the notion of (p, i) -regular number fields and gave some characterizations and arithmetic applications. The main result was a going-up theorem of the (p, i) -regularity in p -extensions L/F of number fields, provided that Leopoldt's conjecture holds in the cyclotomic tower $L(\mu_{p^\infty})$. An alternative proof was obtained in [3, Corollary 4.5], without any assumption on Leopoldt's conjecture.

Inspired by the work of Greenberg on p -rational number fields, we can state the analogue of the conjecture of Greenberg for (p, i) -regular fields:

Conjecture 2.4. Let i be an integer and let p be an odd prime number such that $\mathbf{Q}$ is (p, i) -regular. Then, for any integer $t \geq 1$, there exists a (p, i) -regular field K such that $\text{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^t$.

For any integer $t \geq 1$, let K be a number field such that $\text{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^t$. For $i \geq 2$, it is well known that K is (p, i) -regular for all but finitely many primes p , which we denote (if any) $p_1, \dots, p_s$. Looking at tables of number fields with the same Galois group, we expect that for every $p = p_j$ we will find a (p, i) -regular field. For the case of totally real fields, by Proposition

2.1, it reduces to check the values at $1 - i$ of the corresponding Dedekind zeta functions. Let us consider the case of quadratic fields and take for example the field $\mathbf{Q}(\sqrt{2})$. Since

$$\zeta_{\mathbf{Q}(\sqrt{2})}(-3) = \frac{11}{2^3 \cdot 3 \cdot 5},$$

the field $\mathbf{Q}(\sqrt{2})$ is not $(11, 4)$ -regular and is $(p, 4)$ -regular for the rest of odd primes p . We also check that this field is 3-rational and 5-rational. In contrast, if we take $\mathbf{Q}(\sqrt{5})$ we find

$$\zeta_{\mathbf{Q}(\sqrt{5})}(-3) = \frac{1}{2^2 \cdot 3 \cdot 5},$$

and we can see that $\mathbf{Q}(\sqrt{5})$ is $(p, 4)$ -regular for any prime p . Thus, for every odd prime number p there exists a $(p, 4)$ -regular real quadratic field.

3 Cohen-Eisenstein series

We consider the theta series $\theta(z)$ given by the q -expansion

$$\theta(z) = \sum_{n \in \mathbf{Z}} q^{n^2}.$$

The function θ is an element of the space $M_{\frac{1}{2}}(\Gamma_0(4))$ of modular forms of weight $1/2$ for the congruence subgroup $\Gamma_0(4)$ (cf. [12, Proposition 4, page 184]). An interesting example of the arithmetic importance of the Fourier coefficients of half-integral weight modular forms is the following. The 3-power of θ gives a modular form of weight $3/2$ for $\Gamma_0(4)$ such that

$$\theta^3 = \sum_{n \in \mathbf{Z}} r_3(n) q^n,$$

where $r_3(n)$ is the number of representations of n as a sum of three squares. By the work of Gauss we know that

$$r_3(n) = \begin{cases} 12H(4n), & n \equiv 1, 2 \pmod{4}, \\ 24H(n), & n \equiv 3 \pmod{8}, \\ r(n/4), & n \equiv 0 \pmod{4}, \\ 0, & n \equiv 7 \pmod{8}, \end{cases}$$

where $H(n)$ is the Hurwitz-Kronecker class number for $n \equiv 0, 3 \pmod{4}$. Suppose that $n = -dm^2$, where $d < 0$ is a fundamental discriminant. Then

$$H(n) = \frac{h(d)}{w(d)} \sum_{t|n} \mu(t) \left(\frac{d}{t} \right) \sigma_1(n/t),$$

where σ_1 is the usual sum of divisors function, μ is the Möbius function and $h(d)$ (resp. $w(d)$) is the class number of (resp. half of the number of roots of units in) $\mathbf{Q}(\sqrt{d})$.

Let χ be a Dirichlet character and let $L(\cdot, \chi)$ be the associated Dirichlet L -function. Then, for any positive integer i ,

$$L(1 - i, \chi) = -\frac{B(i, \chi)}{i}$$

where $B(i, \chi)$ is the generalized Bernoulli number. If d is a fundamental discriminant, denote by $\chi_d = \left(\frac{d}{\cdot} \right)$ the non-trivial character of $\mathbf{Q}(\sqrt{d})$. Recall that for imaginary quadratic fields $\mathbf{Q}(\sqrt{d})$, the class number formula reads

$$L\left(0, \left(\frac{d}{\cdot} \right)\right) = \frac{h(d)}{w(d)},$$

hence we have a modular form θ^3 , whose Fourier coefficients involve special values of L -functions. This modular form is used to prove the existence of infinitely many imaginary

quadratic fields whose class numbers are not divisible by a given prime number p [11], [17], [18], [7].

H. Cohen introduced, for every positive integer i , the *Cohen-Eisenstein* series given by the q -expansion

$$\mathcal{H}_i(q) = \sum_{n \geq 0} H(i, n) q^n,$$

with

$$H(i, n) = \begin{cases} \zeta(1 - 2i), & n = 0; \\ 0, & (-1)^i n \equiv 2, 3 \pmod{4}; \\ L(1 - i, \chi_d) \sum_{t|m} \mu(t) \chi_d(t) t^{i-1} \sigma_{2i-1}(m/t), & (-1)^i n = dm^2, \end{cases}$$

In particular, if $d = (-1)^i n$ is a negative fundamental discriminant, we obtain

$$H(i, n) = L(1 - i, \chi_d). \quad (3.1)$$

The series $\mathcal{H}_i(q)$ is a modular form of weight $i + \frac{1}{2}$ for $\Gamma_0(4)$ [8].

We need an adequate modular form that we deduce from the Cohen-Eisenstein series and whose coefficients satisfy certain local conditions. For a modular form $g = \sum_{n \geq 0} a_n q^n \in M_{i+\frac{1}{2}}(\Gamma_0(N))$ and an integer m , let us define the modular form $g|B_m \in M_{i+\frac{1}{2}}(\Gamma_0(Nm^2))$ in the usual way [7, p. 598]

$$g|B_m = \sum_{n \geq 0} a_{mn} q^{mn}.$$

Let $S = S_0 \cup S_+ \cup S_-$ be a disjoint union of sets of prime numbers. For $\ell \in S_0$, the modular form

$$\mathcal{H}_i(q) - \mathcal{H}_i|B_\ell(q) = \sum_{(n, \ell)=1} H(i, n) q^n$$

is an element of the space $M_{i+\frac{1}{2}}(\Gamma_0(4\ell^2))$. Doing so for the rest of primes in the set S_0 , we thereby find a modular form $\mathcal{G}_0$ in the space $M_{i+\frac{1}{2}}(\Gamma_0(4M_0^2))$, with $M_0 = \prod_{\ell \in S_0} \ell$, given by the q -expansion

$$\mathcal{G}_0 = \sum_{n \in A_0} H(i, n) q^n,$$

where $A_0 = \{n \mid \forall \ell \in S_0, v_\ell(n) = 1\}$.

Now, we use the twist operator on the above modular form with respect to the characters $(\frac{\cdot}{\ell})$, for the primes $\ell \in S_- \cup S_+$. For a prime $\ell \in S_-$, we have the modular form

$$\frac{1}{2}((\mathcal{G}_0 - \mathcal{G}_0|B_\ell)(q) - (\mathcal{G}_0)_{(\frac{\cdot}{\ell})}(q)) = \sum_{\substack{n \in A_0 \\ (\frac{n}{\ell}) = -1}} H(i, n) q^n \in M_{i+\frac{1}{2}}(\Gamma_0(4M_0^2 \ell^2)).$$

Applying this for the rest of the primes in S_- , we have the modular form

$$\mathcal{G}_1 = \sum_{n \in A_1} H(i, n) q^n \in M_{i+\frac{1}{2}}(\Gamma_0(4M_0^2 M_-^2)),$$

where $M_- = \prod_{\ell \in S_-} \ell$ and $A_1 = \{n \in A_0 \mid \ell \in S_0 \text{ (resp. } \ell \in S_-) \text{ ramifies (resp. is inert) in } \mathbb{Q}(\sqrt{n})\}$.

For a prime $\ell \in S_+$, consider the modular form

$$\frac{1}{2}((\mathcal{G}_1 - \mathcal{G}_1|B_\ell)(q) + (\mathcal{G}_1)_{(\frac{\cdot}{\ell})}(q)) = \sum_{\substack{n \in A_1 \\ (\frac{n}{\ell}) = 1}} H(i, n) q^n \in M_{i+\frac{1}{2}}(\Gamma_0(4M_0^2 M_-^2 \ell^2)).$$

By induction on the primes of S_+ , we obtain the following lemma.

Lemma 3.1. *Let $S = S_0 \cup S_+ \cup S_-$ be a disjoint union of sets of prime numbers. We have a modular form*

$$\mathcal{G}_2 = \sum_{n \in A} H(i, n) q^n \in M_{i+\frac{1}{2}}(\Gamma_0(4M_S^2)),$$

where $M_S = \prod_{\ell \in S} \ell$ and A is the set of square-free integers n for which the extension $\mathbf{Q}(\sqrt{(-1)^i n})/\mathbf{Q}$ ramifies at the primes in S_0 , splits at the primes in S_+ and is inert at the primes of S_- .

The modular form $\mathcal{G}_2$ is used in the following section to prove our main theorem.

4 Proofs

Let f be a modular form $f(z) = \sum_{n \geq 0} a(n) q^n$ in the space $M_k(\Gamma_0(N), \chi)$ with integer Fourier coefficients. We define

$$\text{ord}_p(f) := \min\{n : p \nmid a(n)\},$$

and we say $\text{ord}_p(f) := \infty$ if $p \mid a(n)$ for all n .

Theorem 4.1. ([20]) *Let $f(z) = \sum_{n \geq 0} a(n) q^n \in M_k(\Gamma_0(N), \chi)$ be a modular form with integer Fourier coefficients. If*

$$\text{ord}_p(f) > \frac{k}{12} [\Gamma_0(1) : \Gamma_0(N)],$$

then $\text{ord}_p(f) = \infty$.

Note that Sturm's theorem was first formulated for holomorphic modular forms of integer weight, but the proof carries also over half-integral weight modular forms.

4.1 Proof of Theorem 1.1.

Since the field $\mathbf{Q}(\sqrt{d_0})$ is (p, i) -regular, we have $v_p(L(1 - i, \chi_{d_0})) = 0$. In the following, for every non-square integer n , we denote D_n for the fundamental discriminant of the field $\mathbf{Q}(\sqrt{n})$. We use the operators U and V on spaces of modular forms at prime numbers ([19, Section 3.2]).

Note that there exists an integer $\alpha(p)$ coprime to p such that $\alpha(p)\mathcal{G}_2 \in \mathbf{Z}[[q]]$, where $\mathcal{G}_2$ is as in Lemma 3.1. For an odd prime number Q , we consider the modular forms

$$\alpha(p)\mathcal{G}_2|U_Q = \sum_{nQ \in A} \alpha(p)H(i, nQ)q^n := \sum_n u_{p,Q}(n)q^n,$$

$$\alpha(p)\mathcal{G}_2|V_Q = \sum_{n \in A} \alpha(p)H(i, n)q^{nQ} := \sum_n v_{p,Q}(n)q^n,$$

which are in the space $M_{i+\frac{1}{2}}(\Gamma_0(4Q^2M_S^4))$.

We put $\kappa(p) = \frac{i+\frac{1}{2}}{12} [\Gamma_0(1) : \Gamma_0(4Q^2M_S^4)]/(Q+1)$. If Q is sufficiently large and $g \in M_{i+\frac{1}{2}}(\Gamma_0(4Q^2M_S^4))$ with $\text{ord}_p(g) > \kappa(p)Q$, then by Sturm's theorem $g \equiv 0 \pmod{p}$. We use this result together with the following two observations:

- for every integer $n \leq \kappa(p)$ with $Q \nmid n$, we have $v_{p,Q}(n) = 0$,
- if there is no $n \leq \kappa(p)Q$ coprime to Q such that

$$\alpha(p)H(i, nQ) \not\equiv 0 \pmod{p}.$$

Then we have the congruence

$$\alpha(p)\mathcal{G}_2|U_Q \equiv \alpha(p)(1 - Q^{i-1} + Q^{2i-1})\mathcal{G}_2|V_Q \pmod{p}.$$

Let $\mathcal{D}_p$ be the set of discriminants D_n for $n \leq \kappa(p)$ with $n \in A$. There exists an arithmetic progression $r_p \pmod{t_p}$, such that $(r_p, t_p) = 1$ and $p \mid t_p$, satisfying ([17, page 8])

- $\chi_{D_n}(Q) = 1$ for every prime $Q \equiv r_p \pmod{t_p}$ and $D_n \in \mathcal{D}_p$,
- $\left(\frac{Q}{\ell}\right) = 1$ for every prime $Q \equiv r_p \pmod{t_p}$ and $\ell \in S$,
- $r_p^i \not\equiv 1 \pmod{p}$.

By definition of the coefficients of Cohen-Eisenstein series, for every prime $Q \equiv r_p \pmod{t_p}$, we have the congruence

$$\alpha(p)H(i, d_0 Q^4) \equiv \alpha(p)(1 - r_p^{i-1} - r_p^{3i-2} + r_p^{2i-1} + r_p^{4i-2})H(i, d_0) \pmod{p}.$$

Since $\alpha(p)H(i, d_0) \not\equiv 0 \pmod{p}$, we find that $u_{p,Q}(d_0 Q^3) \not\equiv v_{p,Q}(d_0 Q^3) \pmod{p}$ if and only if $r_p^{4i-2} \not\equiv r_p^{3i-2} \pmod{p}$. This is satisfied by the 3rd property of the arithmetic progression. Hence,

$$\alpha(p)(\mathcal{G}_2|U_Q - \mathcal{G}_2|V_Q) \not\equiv 0 \pmod{p}.$$

Thus, by the theorem of Sturm, there exists an integer $n \leq \kappa(p)Q$ coprime to Q , such that $n \in A$ and $\alpha(p)H(i, nQ) \not\equiv 0 \pmod{p}$. Then the field $\mathbf{Q}(\sqrt{nQ})$ is a (p, i) -regular quadratic field satisfying (1) and (2). To finish, we apply Dirichlet's Theorem on arithmetic progressions to obtain

$$\#\{0 < d < X : \mathbf{Q}(\sqrt{d}) \text{ satisfies the conditions (1) and (2)}\} \gg \frac{\sqrt{X}}{\log(X)}.$$

4.2 Proof of Theorem 1.2.

Let us consider the Cohen-Eisenstein series of weight $5/2$,

$$\mathcal{H}_2(q) = \sum_{n \geq 0} H(2, n)q^n = \zeta(-3) + \zeta(-1)q + \dots$$

For every prime number ℓ , $\mathcal{H}_2$ is an eigenform of the Hecke operators T_ℓ ([19, Chapter 3]) with corresponding eigenvalues

$$\sigma_3(\ell) = 1 + \ell^3.$$

We have $\zeta(-3) = 1/120$ and $\zeta(-1) = -1/12$, we need to omit the constant coefficient because $v_5(\zeta(-3)) = -1$. Let Q be an arbitrary prime number and consider the modular form

$$f = \frac{1}{2}((\mathcal{H}_2 - \mathcal{H}_2|B_Q) + (\mathcal{H}_2)_{(\frac{p}{Q})}) = \sum_{n \geq 1, (\frac{p}{Q})=1} H(2, n)q^n.$$

Since $\mathbb{Q}$ is $(p, 2)$ -regular for every prime $p \geq 5$ (that is $v_p(\zeta(-1)) = 0$), we have $\mathcal{H}_2 \not\equiv 0 \pmod{p}$.

From conditions (a) and (b) we deduce that

$$v_p(\ell^3 + \ell^2 + \ell + 1) = 0$$

and

$$v_p(\ell^3 - \ell^2 - \ell + 1) = 0.$$

By induction on the number of primes in the set S , since $\mathcal{H}_2 \not\equiv 0 \pmod{p}$, Corollary 1. and Lemma 3. of [7] give a fundamental discriminant $d > 0$ such that $v_p(H(2, d)) = 0$ with the desired local conditions at a prime $\ell \in S$ (see for instance the proof of Theorem 3. of [7]). Then the result follows from Theorem 1.1.

References

- [1] Assim, J. *Codescente en K -théorie étale et corps de nombres*, manuscripta math. 86, (1995), 499-518.
- [2] Assim, J. and Bouazzaoui, Z. *Half-integer weight modular forms and real quadratic p -rational fields*. Functiones et Approximatio Commentarii Mathematici (2019).
- [3] Assim, J and Movahhedi, A. *Galois codescent for motivic tame kernels*. Ann. Math. Québec (2025). <https://doi.org/10.1007/s40316-024-00233-8>
- [4] Beckwith, O. *Indivisibility of class numbers of imaginary quadratic fields*. Research in the Mathematical Sciences, 4(1), p.20. (2017).
- [5] Benmerieme, Y. and Movahhedi, A. *Multi-quadratic p -rational Number Fields*. Journal of Pure and Applied Algebra, Volume 225, Issue 9, 2021.
- [6] Bouazzaoui, Z. *Fibonacci numbers and real quadratic p -rational fields*. Period. Math. Hungar. 81 (2020), no. 1, 123–133.
- [7] Bruinier, J.H. *Nonvanishing modulo ℓ of Fourier coefficients of half-integral weight modular forms*. Duke Math. J. 98 (1999), 595-611.
- [8] Cohen, H. *Sums involving the values at negative integers of L -functions of quadratic characters*, Math. Ann. 217 (1975), 271-285.
- [9] Gras, G. and Jaulent, J.F., *Sur les corps de nombres réguliers*. Mathematische Zeitschrift, 202(3), (1989) 343-365.
- [10] Greenberg, R. *Galois representations with open image*, Annales mathématiques du Québec, 40 (2016), 83-119.
- [11] Hartung, P. *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3*, J. Number Theory 6 (1974) 276-278.
- [12] Koblitz, N. *Introduction to elliptic curves and modular forms*, Springer Verlag, 1984.
- [13] Kolster, M. *K -theory and arithmetic*, No. INIS-XA-986. 2003.
- [14] Movahhedi, A. and Nguyen, Q.D. *Sur l'arithmétique des corps de nombres p -rationnels*, Séminaire de théorie des nombres de Paris, 1987-1988, Birkhäuser, Vol 81, (1990) 155-200.
- [15] Movahhedi, A. *Sur les p -extensions des corps p -rationnels*, Math. Nachr., 149, 163-176 (1990).
- [16] Mazur, B., and Wiles, A. *Class fields of abelian extensions of $\mathbb{Q}$* . Invent Math 76, 179–330 (1984).
- [17] Ono, K. *Indivisibility of class numbers of real quadratic fields*, composition math, 119: 1-11 (1999).
- [18] Ono, K. and Skinner, C. *Fourier coefficients of half-integral weight modular forms modulo ℓ* . Annals of mathematics 147.2: 453-470 (1998).
- [19] Ono, K. *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q -series: Arithmetic of the Coefficients of Modular Forms and q -series*. American Mathematical Soc. 102: (2004).
- [20] Sturm, J. *On the congruence of modular forms*. In Number theory (pp. 275-280). Springer Berlin Heidelberg, (1987).
- [21] Wiles, A. *The Iwasawa conjecture for totally real fields*. Annals of mathematics, 131(3), 493-540 (1990).
- [22] Wiles, A. *On class group of imaginary quadratic fields*, J.London Math. soc. (2) 92, 411-426 (2015).

Author information

J. Assim, Department of Mathematics, Faculty of sciences of Meknès (FSM), Morocco.
E-mail: j.assim@umi.ac.ma

S. Bhihi, Department of Mathematics, Faculty of sciences of Meknès (FSM), Morocco.
E-mail: soumia.bhihi@edu.umi.ac.ma

Z. Bouazzaoui, Higher School of Education and Training of Oujda (ESEFO), Morocco.
E-mail: z.bouazzaoui@ump.ac.ma