Rev.R.Acad.Cienc.Exact.Fis.Nat. (Esp)
Vol. 94, N.º 3, pp 323-332, 2000
Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

HEEGNER POINTS ON MODULAR CURVES[1]

(Heegner point/modular curve/quadratic order/quadratic form/genus)

A. ARENAS*, P. BAYER**

* Facultat de Matemàtiques, Universitat de Barcelona, Gran Vía de les Corts Catalanes, 585. E-08007 Barcelona (arenas@mat.ub.es)
** Facultat de Matemàtiques, Universitat de Barcelona, Gran Vía de les Corts Catalanes, 585. E-08007 Barcelona (bayer@mat.ub.es)

Abstract

In this paper we generalise the concept of Heegner point on the modular curve $X_0(N)$ to the case of any discriminant D, i.e. for D positive or negative and not necessarily fundamental. We reduce their study and evaluation of their number to that of primitive $\mathcal{O}$-ideals of norm N, where $\mathcal{O}$ is the order of discriminant D of a quadratic field and, ultimately, to that of certain integral binary quadratic forms of discriminant D. When $D < 0$, we give a formula expressing the number of Heegner points by using the Minkowski-Siegel theorem concerning representations of integers by genera of quadratic forms.

Resumen

En este artículo, damos una generalización del concepto de puntos de Heegner de la curva modular $X_0(N)$, para cualquier discriminante D; es decir, D puede ser positivo o negativo y no necesariamente fundamental. Reducimos su estudio y la evaluación de su número al de los $\mathcal{O}$-ideales primitivos de norma N, donde $\mathcal{O}$ es el orden de discriminante D de un cuerpo cuadrático y, en última instancia, al de ciertas formas cuadráticas binarias con coeficientes enteros de discriminante D. En el caso $D < 0$, damos una fórmula que expresa el número de puntos de Heegner a partir del teorema de Minkowski-Siegel relativo a las representaciones de enteros por géneros de formas cuadráticas.

Introduction

The central topic of Gauss' *Disquisitiones Arithmeticæ,* written by the author in his youth, is the study of diophantine equations

$$f(X, Y) = n,$$

where $f(X, Y) = aX^2 + bXY + cY^2$ is an integral binary quadratic form, and n is an integer.

One of the most useful tools in Gauss theory is the classification of the forms under the action of the modular group $\mathbf{GL}(2, \mathbb{Z})$, or the special modular group $\mathbf{SL}(2, \mathbb{Z})$. Two forms $f(X, Y), f'(X', Y')$ are defined to be equivalent, respectively properly equivalent, if and only if there exists a change of variables

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \begin{bmatrix} X' \\ Y' \end{bmatrix},$$

defined by a matrix in $\mathbf{GL}(2, \mathbb{Z})$, respectively in $\mathbf{SL}(2, \mathbb{Z})$, which transforms f into f'. All the forms belonging to the same class must have the same discriminant $D = b^2 - 4ac$.

Gauss reduction theory implies that the number of classes of forms of a given discriminant is always finite. A closer investigation of the algebraic properties of the classes of forms led Gauss to the concepts of order, genus, and character.

Extensive tables of class numbers were calculated by Gauss himself. They gave rise to the formulation of several conjectures about the asymptotic behaviour of the class number as $|D|$ tends to infinity. In particular, Gauss claimed that his list of negative discriminants with class number equal to one was probably complete. Nevertheless, he added, a proof of this fact seemed to be very difficult.

The 19th century saw the emergence of a theory that connected integral binary quadratic forms, complex multiplication of elliptic functions, and modular functions. Much of the content of the theory was included in the third volume of the *Lehrbuch der Algebra* of Weber **[We 08]**.

In the 1950's, an initial approach to the solution of the class number one problem was provided by Heegner. By

[1] Partially supported by DGES: PB96-0166.

using the language and tools of Weber's book, Heegner **[He 52]** was the first to prove that the list of negative discriminants for class number one given by Gauss was, indeed, complete. Nevertheless, Heegner's proof was not accepted at first, mainly due to its heavy reliance on the use of modular functions, which were out of favour at that time. After a period of obscurity, solutions to the class number one problem were given, independently, by Baker **[Bak 66]** and Stark **[St 67].**

Heegner's main idea **[He 52]** was to make use of algebraic relations among modular functions in order to produce algebraic equations with integral algebraic coefficients, once the modular functions are evaluated at suitable points.

His article caught the attention of several authors such as Siegel **[Si 68]**, Deuring **[De 68]**, Birch **[Bi 68]**, Stark **[St 69]**, and Cox **[Cox 89]**. Heegner's techniques, which were a source of inspiration to **[Bi 75]**, **[Gr 84]**, **[Gr-Za 86]**, **[Gr-Ko-Za 87]**, today play a central role in the study of diophantine equations of type

$$Y^2 = aX^3 + bX^2 + cX + d, \quad a, b, c, d \in \mathbb{Q};$$

or, more precisely, in the study of rational points of elliptic curves $E/\mathbb{Q}$.

As was conjectured by Poincaré at the beginning of the 20th century, and as follows from a theorem of Mordell **[Mo 22]**, the set of rational points $E(\mathbb{Q})$ of an elliptic curve defined over the rationals is a finitely generated abelian group. The rank of this group is, by definition, the rank of the elliptic curve.

The Birch and Swinnerton-Dyer conjecture **[Bi-SD 65]** predicts that the rank of $E/\mathbb{Q}$ equals the order of vanishing at $s = 1$ of the associated L-series $L(E, s)$. Although there is a great deal of numerical evidence for the truth of this conjecture, until now the most general theoretical results are based on those obtained by Coates and Wiles **[Co-Wi 77]**, Gross and Zagier **[Gr-Za 86]**, and Kolyvagin **[Ko 90]**, some years ago.

Coates and Wiles **[Co-Wi 77]** proved that if the elliptic curve $E/\mathbb{Q}$ has complex multiplication by the ring of integers of an imaginary quadratic field with class number one, and its rank is greater than zero, then the value $L(E, 1)$ must be zero.

Gross and Zagier **[Gr-Za 86]** proved that all modular elliptic curves $E/\mathbb{Q}$ whose L-series has a simple zero at $s = 1$ are of rank greater than zero.

In the articles **[Gr-Za 86]**, **[Gr-Ko-Za 87]**, Gross and Zagier, and Gross, Kohnen, and Zagier produced a remarkable formula relating the heights of explicit rational divisors of degree zero of the modular curve $X_0(N)$, called Heegner divisors, to the derivatives at $s = 1$ of L-series of cusp forms of weight 2 and level N. In particular, if $L(E, 1) = 0$ and $L'(E, 1) \neq 0$, the formula provides a rational point of $E/\mathbb{Q}$ of infinite order and, therefore, infinitely many rational solutions of the defining diophantine equation.

The set $X_0(N)(\mathbb{C})$ of complex points of the modular curve can be parametrised by means of the modular functions $j(z)$, $j(N z)$ of level one and N, respectively. If $z \in \mathbb{C}$ is a quadratic imaginary argument, then the value $j(z)$ is an algebraic integer, extensively studied in the classical theory of complex multiplication. If $z \in \mathbb{C}$ is an algebraic number which is not imaginary quadratic, a theorem of Siegel **[Si 49]** tells us that the value $j(z)$ is transcendental. Therefore, on imaginary quadratic arguments, pairs $(j(z), j(N z))$ define points of $X_0(\mathrm{N})$ whose coordinates lie in the algebraic closure $\overline{\mathbb{Q}} \subset \mathbb{C}$ of the rational field.

But in connection with the theoretical treatment of diophantine problems, such as those just mentioned, other interpretations of the points of the modular curve are currently used. Namely, the points $X_0(N)(K)$, which are rational over a subfield $K \subseteq \mathbb{C}$, are understood as pairs $(E_1 \to E_2)$ consisting of generalised elliptic curves E_i/K linked by a cyclic isogeny defined over K, of degree N. In this setting, a Heegner point of the modular curve $X_0(N)$ is defined as a pair $(E_1 \to E_2)$ in which both elliptic curves E_i have complex multiplication and the rings of complex multiplications $\mathrm{End}(E_1)$, $\mathrm{End}(E_2)$ are isomorphic.

More recently, integral algebraic values of other automorphic functions have been considered and, moreover, several generalizations of the Birch and Swinnerton-Dyer conjecture have been proposed; cf., Shimura **[Sh 67]**, Mazur **[Ma 77]**, Bertolini and Darmon **[Be-Da 98]**, Rück and Tipp **[Rü-Ti 99]**, and Zhang **[Zh 99]**.

Together with this study, quoted **[Ar-Ba 2000-1]**, in this issue we present a series of four more articles: **[Ar-Ba 2000-2]**, **[Ba-Tr 2000-1]**, **[Ba-Tr 2000-2]**, **[Ba-Tr 2000-3]**, whose aim is to provide an approach to the theory of Heegner points and special values of automorphic functions, without neglecting their origins.

We begin **[Ar-Ba 2000-1]** by comparing the modern approach to Heegner points with a definition related to the classical theory of integral binary quadratic forms. In particular, this presentation allows us an easy calculation of the number of Heegner points of a given discriminant D in the modular curve $X_0(N)$, without assuming any condition on the common divisors of N and D. For this purpose, we use a theorem of Minkowski-Siegel which evaluates the number of representations of an integer N by forms in the genus of a given quadratic form.

A special type of Heegner points, called by Mazur complex multiplication points, were considered in **[Ma 77]**. In each level N, only a finite number of discriminants D can yield complex multiplication points of

type (N, D). We study these points in **[Ar-Ba 2000-2]**, where explicit computations are performed.

In **[Ba-Tr 2000-2]**, the theory of integral binary quadratic forms is related to an arithmetic theory of quadratic orders embedded in orders $\mathcal{O}$ of the split quaternion algebra $M(2, \mathbb{Q})$. The embeddings will be classified under the action of groups Γ attached to $\mathcal{O}$. If $\mathcal{O} = M(2, \mathbb{Z})$, then we can take $\Gamma = \mathbf{SL}(2, \mathbb{Z})$. Other examples are obtained when we consider, for each $N \geq 1$, the congruence group $\Gamma_0(N)$ which uniformises $X_0(N)$. It will be shown that the study of the Γ-classes of embeddings is equivalent to the study of the Γ-classes of some integral binary quadratic forms.

Ground material for an arithmetical study of these non-commutative orders is developed in **[Ba-Tr 2000-1]**; it covers some aspects that we were unable to find in the standard references.

Finally, putting together the results obtained in **[Ba-Tr 2000-3]** and **[Ar-Ba 2000-1]**, it is proven that the general theory of Heegner points on the modular curve $X_0(N)$ is equivalent to the theory of $\Gamma_0(N)$-classes of integral binary quadratic forms of level N. By definition, these are the forms of type $aNX^2 + bXY + cY^2$, where a, b, c are integers.

Although most of the time we will restrict ourselves to the modular case, it will be clear throughout that many of the definitions given may fit Heegner points on curves parametrised by arithmetic fuchsian groups other than $\Gamma_0(N)$.

In our articles, the reader will find several formulae which count the number of Heegner points of different sorts. The formulae have been derived by the authors to check that some different definitions appearing in different contexts and expressed in different languages in fact involve the same principles.

1. GENERALISED HEEGNER POINTS ON $X_0(N)$

We fix an integer N > 1 and a discriminant D which may be either positive or negative and not necessarily fundamental. Recall that any discriminant D is of the form $D_0 r^2$, where D_0 is a fundamental discriminant (i. e. $D_0 \equiv 1 \pmod 4$ and D_0 square free; or $D_0 \equiv 0 \pmod 4$, $D_0/4$ square free, and $D_0/4 \equiv 2$ or $3 \pmod 4$), and r is any integer; and that orders in quadratic fields are completely determined by their discriminants.

We next consider triplets $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$, where $\mathcal{O}$ stands for a quadratic order i. e., an order in an arbitrary quadratic field not necessarily imaginary, $\mathfrak{n}$ is an ideal in $\mathcal{O}$ of norm $[\mathcal{O} : \mathfrak{n}] = N \geq 1$, and $[\mathfrak{a}]$ stands for the class of $\mathfrak{a}$ in the group $\mathrm{Pic}^+(\mathcal{O})$. Recall that $\mathrm{Pic}^+(\mathcal{O})$ is the quotient of the abelian group of invertible fractional $\mathcal{O}$-ideals modulo the principal ones defined by generators of positive norm. If we drop the condition of positive norm, we get the usual Picard group $\mathrm{Pic}(\mathcal{O})$. Obviously there is a natural surjection $\mathrm{Pic}^+(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O})$ whose kernel is non-trivial of order 2 if and only if $\mathcal{O}$ is real and all its units have positive norm. Thus, $\mathrm{Pic}^+(\mathcal{O}) \simeq \mathrm{Pic}(\mathcal{O})$ if either $\mathcal{O}$ is imaginary (i. e., its discriminant D is negative) or $\mathcal{O}$ is real and has a unit of negative norm.

With this data we introduce the following

Definition 1.1. *A Heegner triplet $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ of type (N, D) is given by an order $\mathcal{O}$ of a quadratic field of discriminant D, a primitive $\mathcal{O}$-ideal $\mathfrak{n}$ of norm N (i. e., $\mathcal{O}/\mathfrak{n}$ is a cyclic group of order N), and an element $[\mathfrak{a}]$ of* $\mathrm{Pic}^+(\mathcal{O})$.

In our next considerations, we will show why this definition is consistent with the usual concept of Heegner point on $X_0(N)$.

Recall that the open modular curve $Y_0(N)$ over the rational field classifies ordered pairs $(E_1 \to E_2)$ of elliptic curves linked by a cyclic isogeny of degree N. Its complex points, $Y_0(N)(\mathbb{C})$, have the structure of a Riemann surface which is analytically isomorphic to the quotient space $\mathbb{H}/\Gamma_0(N)$ of the upper half-plane, $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$, by the action of the congruence group

$$\Gamma_0(N) = \left\{ \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathbf{SL}(2, \mathbb{Z}) \mid \gamma \equiv 0 (\mathrm{mod}\ N) \right\}.$$

To the point $y = (E_1 \to E_2)$ in $Y_0(N)(\mathbb{C})$ we may associate a pair of tori $(\mathbb{C}/L_1 \to \mathbb{C}/L_2)$ linked by a cyclic isogeny of degree N. Applying to the lattice L_1 a homothety, if necessary, we may assume that $L_1 \subset L_2$, and that the isogeny is given by the identity map on the common universal covering space $\mathbb{C}$. Since the quotient group L_2/L_1 is cyclic of order N, there exists an oriented $\mathbb{Z}$-basis (ω_1, ω_2), i. e., $z = \omega_2/\omega_1$ is in $\mathbb{H}$, such that $L_1 = \langle \omega_1, \omega_2 \rangle$, and $L_2 = \langle \omega_1, \omega_2/N \rangle$. Then the analytical isomorphism assigns to the point y the $\Gamma_0(N)$-orbit of z, which is well defined. To see that the map is surjective, we associate to each z in $\mathbb{H}/\Gamma_0(N)$ the class defined by the ordered pair of elliptic curves $(E_1 = \mathbb{C}/\langle 1, z \rangle \to E_2 = \mathbb{C}/\langle 1, z/N \rangle)$, related by the obvious cyclic isogeny of degree N.

Let $X_0(N)$ be the natural compactification of $Y_0(N)$. This is the modular curve which classifies pairs of generalised elliptic curves linked by cyclic isogenies of degree N. The complex points $X_0(N)(\mathbb{C})$ may be identified with the quotient $\mathbb{H}^*/\Gamma_0(N)$, where $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. The finite set $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$ consists of the cusps of $X_0(N)$.

Modifying slightly Birch's **[Bi 75]** definition, we can give the following geometric description of a Heegner point.

Definition 1.2. *A point $y = (E_1 \to E_2)$ in $Y_0(N)(\mathbb{C})$ is called a Heegner point attached to an order $\mathcal{O}$ of an imaginary quadratic field K if the endomorphism rings $End(E_1)$ and $End(E_2)$ are both isomorphic to $\mathcal{O}$.*

The next proposition gives a condition which guarantees the existence of Heegner points on $X_0(N)$ attached to an order $\mathcal{O}$ of discriminant $D < 0$ in a quadratic field.

Proposition 1.3. *Given an order $\mathcal{O}$ of discriminant $D < 0$ in a quadratic field, the modular curve $Y_0(N)$ has Heegner points attached to $\mathcal{O}$ if and only if there exists a primitive $\mathcal{O}$-ideal $\mathfrak{n}$ of norm N.*

Proof. If $y = (E_1 \to E_2)$ is a Heegner point attached to $\mathcal{O}$, then the associated lattices $\mathfrak{a}_1 := L_1$, $\mathfrak{a}_2 := L_2$ are both invertible fractional $\mathcal{O}$-ideals, since for any lattice $\mathfrak{a} \subset \mathbb{C}$, we clearly have $\mathrm{End}(\mathbb{C}/\mathfrak{a}) \simeq \{x \in \mathbb{C} \mid x\mathfrak{a} \subseteq \mathfrak{a}\}$. As remarked previously, we may assume that $\mathfrak{a}_1 \subset \mathfrak{a}_2$ and that $\mathbb{C}/\mathfrak{a}_1 \to \mathbb{C}/\mathfrak{a}_2$ is the natural map. Then $\mathfrak{n} = \mathfrak{a}_1 \mathfrak{a}_2^{-1}$ is an invertible $\mathcal{O}$-ideal contained in $\mathcal{O}$ which defines a quotient group $\mathcal{O}/\mathfrak{n}$ cyclic of order N; that is, $\mathfrak{n}$ is a primitive ideal of norm N. Conversely, if such an ideal $\mathfrak{n}$ exists in $\mathcal{O}$, we may construct Heegner points with $\mathcal{O} = \mathrm{End}(E_1) = \mathrm{End}(E_2)$ as follows. Let $\mathfrak{a}$ be an invertible fractional $\mathcal{O}$-ideal. We write $E_1(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$, $E_2(\mathbb{C}) = \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$. These curves are related by the obvious isogeny with kernel $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a}$. But as the following lemma will show, we have $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \simeq \mathcal{O}/\mathfrak{n}$. Therefore, in particular, the obvious isogeny is cyclic of degree N. □

Lemma 1.4. *Let $\mathcal{O}$ be an order of a quadratic field K, $\mathfrak{n}$ an $\mathcal{O}$-ideal of norm N and $\mathfrak{a}$ an invertible fractional $\mathcal{O}$-ideal. Then the $\mathcal{O}$-modules $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a}$, $\mathcal{O}/\mathfrak{n}$ and $\mathfrak{a}/\mathfrak{a}\mathfrak{n}$ are all isomorphic.*

Proof. Since $\mathcal{O}$ is a noetherian integral domain of dimension one **[Ne 92]**, and $\mathfrak{n}$ is a non-zero ideal, there are a finite number of maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$, containing $\mathfrak{n}$. Localising with respect to the multiplicative system $S = \mathcal{O} \setminus \cup_{i=1}^{t} \mathfrak{m}_i$, we obtain a semilocal domain $\mathcal{O}_S$ and as $\mathfrak{a}$ is $\mathcal{O}$-invertible, then $\mathfrak{a}_S$ is $\mathcal{O}_S$-invertible and, hence, principal (cf. **[Ka 70]**); i. e., $\mathfrak{a}_S = \mathcal{O}_S a$, for some a, which can be taken in $\mathfrak{a}$. Now multiplication by a induces an $\mathcal{O}$-homomorphism:

$$\mathcal{O}/\mathfrak{n} \xrightarrow{a.} \mathfrak{a}/\mathfrak{a}\mathfrak{n} \qquad (1)$$

which localised at S clearly yields an $\mathcal{O}_S$-isomorphism:

$$\mathcal{O}_S/\mathfrak{n}_S \simeq (\mathcal{O}/\mathfrak{n})_S \xrightarrow{a.} (\mathfrak{a}/\mathfrak{a}\mathfrak{n})_S \simeq \mathfrak{a}_S/\mathfrak{a}_S\mathfrak{n}_S = \mathcal{O}_S a/(a)\mathfrak{n}_S.$$

Localising a little further (localising is transitive), we obtain $(\mathcal{O}/\mathfrak{n})_{\mathfrak{m}_i} \simeq (\mathfrak{a}/\mathfrak{n}\mathfrak{a})_{\mathfrak{m}_i}$ for $i = 1, \ldots, t$. For the other maximal ideals $\mathfrak{m}$, we clearly have $(\mathcal{O}/\mathfrak{n})_{\mathfrak{m}} \simeq 0 \simeq (\mathfrak{a}/\mathfrak{n}\mathfrak{a})_{\mathfrak{m}}$. Thus (1) is an $\mathcal{O}$-isomorphism, since an $\mathcal{O}$-homomorphism is an $\mathcal{O}$-isomorphism if and only if all its localisations at the maximal ideals of $\mathcal{O}$ are so. To see that $\mathcal{O}/\mathfrak{n}$ is isomorphic with $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a}$, we proceed similarly: we have now $\mathfrak{n}_S = \mathcal{O}_S x$, for some x in $\mathfrak{n}$, and then we consider the map from $\mathcal{O}/\mathfrak{n}$ into $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a}$ induced by multiplication by a/x and localise. □

Since for any λ in K^*, λ has positive norm because K is imaginary and multiplication by λ induces an isomorphism from $\mathbb{C}/\mathfrak{a}$ into $\mathbb{C}/\lambda\mathfrak{a}$, for any invertible $\mathcal{O}$-fractional ideal $\mathfrak{a}$, we see that the curves $E_1(\mathbb{C})$ and $E_2(\mathbb{C})$ depend only on the class $[\mathfrak{a}]$ of $\mathfrak{a}$ in $\mathrm{Pic}^+(\mathcal{O})$. This justifies our generalised definition of Heegner point (cf. **[Gr 84]**).

2. PRIMITIVE IDEALS

In this section, we characterise the existence of primitive $\mathcal{O}$-ideals of norm N in terms of binary quadratic forms.

Proposition 2.1. *Given a quadratic order $\mathcal{O}$ of discriminant D, there exists a primitive $\mathcal{O}$-ideal $\mathfrak{n}$ of norm N if and only if there exists an integral primitive binary quadratic form of discriminant D which primitively represents N.*

Proof. Given a primitive integral binary quadratic form $f(X, Y)$ of discriminant D, it is well known that there exists an invertible fractional $\mathcal{O}$-ideal $\mathfrak{a} = \langle \alpha, \beta \rangle$ such that

$$f(x, y) = \frac{n(x\alpha - y\beta)}{n(\mathfrak{a})} \quad \text{for all } (x, y) \in \mathbb{Z}^2.$$

Here n stands for the norm of an element of $\mathbb{Q}(\sqrt{D})$ or, respectively, for the norm of a fractional ideal in $\mathcal{O}$.

Now assume that there exists $(x_0, y_0) \in \mathbb{Z}^2$ with $\gcd(x_0, y_0) = 1$ and $f(x_0, y_0) = N$. Thus there exists an element $\xi \in \mathfrak{a}$, $\xi = x_0\alpha - y_0\beta$, such that $n(\xi) = Nn(\mathfrak{a})$. The fact that (x_0, y_0) is primitive allows us to extend ξ to a $\mathbb{Z}$-basis of $\mathfrak{a}$; i. e., there exists $\eta \in K$ such that $\mathfrak{a} = \langle \xi, \eta \rangle = \xi\langle 1, z \rangle$, $z = \eta/\xi$.

Let $aX^2 + bX + c$ be the $\mathbb{Z}$-irreducible equation of z, with $a > 0$. Then $b^2 - 4ac = D$ and $\mathcal{O} = \langle 1, az \rangle$ (cf. **[Bo-Sh 66** chap. 2]). Moreover, $n(\mathfrak{a}) = |n(\xi)| n(\langle 1, z \rangle) = n(\xi)a^{-1}$. Then, from this result and from $n(\xi) = Nn(\mathfrak{a})$, we have $a = N$. Therefore, $\mathcal{O} = \langle 1, Nz \rangle$. If (′) stands for conjugation, we have now: $\mathfrak{n} := \xi\mathfrak{a}^{-1} = \xi n(\mathfrak{a})^{-1}\mathfrak{a}' = \xi n(\mathfrak{a})^{-1}\xi'\langle 1, z' \rangle = n(\xi)n(\mathfrak{a})^{-1}\langle 1, z' \rangle = N\langle 1, z' \rangle = \langle N, Nz' \rangle$. But $\mathcal{O}$ is also the ring of coefficients of $\mathfrak{a}'$ and then $\mathcal{O} = \langle 1, Nz' \rangle$, so that $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$.

Conversely, let $\mathfrak{n} \subseteq \mathcal{O}$ be a primitive $\mathcal{O}$-ideal of norm N and let k be the smallest positive integer in $\mathfrak{n}$. We claim it can be extended to a $\mathbb{Z}$-basis of $\mathfrak{n}$. In fact, express k in

any $\mathbb{Z}$-basis $\{\alpha, \beta\}$ of $\mathfrak{n}$: $k = \lambda\alpha + \mu\beta$, and observe that λ, μ have to be coprime rational integers, for otherwise we could write $k = d(\lambda_1\alpha + \mu_1\beta)$, for some integer $d > 1$, with $\lambda_1, \mu_1 \in \mathbb{Z}$, and then k/d would be a positive integer in $\mathfrak{n}$ smaller than k, since $k/d \in \mathbb{Q} \cap \mathfrak{n} \subseteq \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$. This establishes our claim and we can write $\mathfrak{n} = \langle k, k\gamma\rangle$, for a certain γ. As usual, let us consider the irreducible equation for γ over $\mathbb{Z}$: $aX^2 + bX + c$, with $a > 0$ and $\gcd(a, b, c) = 1$. Since $\mathcal{O} = \langle 1, a\gamma\rangle$ and $\mathfrak{n} \subset \mathcal{O}$, we see that $a \mid k$; i. e., $k = as$ with $s \in \mathbb{Z}$. But then from $\mathfrak{n} = \langle as, as\gamma\rangle$, we obtain $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/as\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$, which tells us that $\mathcal{O}/\mathfrak{n}$ is cyclic of order N if and only if $s = 1$ and, consequently, $a = N = k$, so that the quadratic form $aX^2 + bXY + cY^2$ represents N primitively and satisfies all our requirements. □

Corollary 2.2. *There exists a primitive $\mathcal{O}$-ideal of norm N if and only if the equation $D = B^2 - 4NC$ can be solved in integers with $\gcd(N, B, C) = 1$.*

Proof. If there exists a primitive $\mathcal{O}$-ideal of norm N, then there exists a primitive binary quadratic form $f(X, Y) = aX^2 + bXY + cY^2$ which primitively represents N; i. e., there exists a pair of integers (x_0, y_0) such that $f(x_0, y_0) = N$ and $\gcd(x_0, y_0) = 1$. Then there also exist $z, t \in \mathbb{Z}$ such that $x_0z - y_0t = 1$. And we have

$$\begin{bmatrix} x_0 & y_0 \\ t & z \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x_0 & t \\ y_0 & z \end{bmatrix} = \begin{bmatrix} N & * \\ * & * \end{bmatrix};$$

that is, $f(X, Y)$ is $\mathbf{SL}(2, \mathbb{Z})$-equivalent to a primitive form of type $NX^2 + BXY + CY^2$ with $B^2 - 4NC = D$.

Conversely, if the equation $B^2 - 4NC = D$ can be solved in integers such that $\gcd(N, B, C) = 1$, then we can construct a primitive binary quadratic form $NX^2 + BXY + CY^2$ of discriminant D which obviously represents N primitively. □

Now it is easy to determine the primitive ideals $\mathfrak{n}$ in $\mathcal{O}$ of norm N. But, first, let us recall that a basis (α, β) of $\mathfrak{a}$ is said to be oriented if $\begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} < 0$ in the real case, i. e., when $D > 0$; and if $\sqrt{-1}\begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} > 0$ (or, equivalently, when $\beta/\alpha \in \mathbb{H}$) in the imaginary case, i. e., when $D < 0$.

Proposition 2.3. *The number of primitive ideals $\mathfrak{n}$ in $\mathcal{O}$ of norm N equals the number of integral solutions (b, c) of the equation $Y^2 - 4NZ = D$ with $\gcd(N, b, c) = 1$ and $-N \le b < N$. These ideals can be expressed by*

$$\mathfrak{n} = N\left\langle 1, \frac{-b + \sqrt{D}}{2N}\right\rangle.$$

Proof. We proceed as in the proof of proposition 2.1 and observe that we can write $\mathfrak{n} = N\langle 1, \gamma\rangle$ for a certain γ satisfying a quadratic equation of type $NX^2 + bX + c = 0$ with $\gcd(N, b, c) = 1$, $b^2 - 4Nc = D$. But, if $\mathfrak{n} = N\langle 1, \gamma_1\rangle$, then, obviously, $\gamma_1 \equiv \pm\gamma (\mathrm{mod}\ \mathbb{Z})$. The case of minus sign, however, leads to a non-oriented basis. Thus γ is uniquely determined if we require its rational part to lie in $[-1/2, 1/2)$, and γ either to lie in $\mathbb{H}$ (for non real γ), or to have positive irrational part (for real γ). The rest is obvious. □

3. THE CLASS SET $H(N, D)$

The next two lemmas aim to establish that the automorphisms of a binary quadratic form of discriminant D belonging to the proper class associated with the strict class of an invertible fractional $\mathcal{O}$-ideal can be identified with the units of $\mathcal{O}$ of positive norm.

Lemma 3.1. *If $\mathfrak{a}$ is an invertible fractional $\mathcal{O}$-ideal and λ belongs to $\mathbb{Q}(\sqrt{D})$, then $\lambda\mathfrak{a} = \mathfrak{a}$ if and only if $\lambda \in \mathcal{O}^*$. Furthermore, if (α, β) is an oriented basis of $\mathfrak{a}$ and λ lies in $\mathcal{O}^*$, then $(\lambda\alpha, \lambda\beta)$ is another oriented basis of $\mathfrak{a}$ if and only if λ has norm $+1$.*

Proof. For a given element $\lambda \in \mathbb{Q}(\sqrt{D})$, we have that $\lambda \in \mathcal{O}^*$ if and only if $\lambda\mathcal{O} = \mathcal{O}$. So, if λ is a unit, $\lambda\mathfrak{a} = \mathfrak{a}$. Conversely, if for $\lambda \in \mathbb{Q}(\sqrt{D})$ is $\lambda\mathfrak{a} = \mathfrak{a}$, then $0 \neq \lambda \in \mathcal{O}$, and multiplying by λ^{-1} we obtain $\mathfrak{a} = \lambda^{-1}\mathfrak{a}$; so $\lambda^{-1} \in \mathcal{O}$, i. e., $\lambda \in \mathcal{O}^*$. This proves the first assertion. Next, if we write $\begin{bmatrix} \lambda\alpha \\ \lambda\beta \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, with $\begin{bmatrix} r & s \\ t & u \end{bmatrix} \in \mathbf{GL}(2, \mathbb{Z})$, as we obviously have (primes denoting conjugates) $\begin{bmatrix} \lambda\alpha & \lambda'\alpha' \\ \lambda\beta & \lambda'\beta' \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix}\begin{bmatrix} \alpha & \alpha' \\ \beta & \beta' \end{bmatrix}$, by taking determinants, we have

$$n(\lambda)\begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix} = \begin{vmatrix} r & s \\ t & u \end{vmatrix}\begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix}.$$

So the orientations are preserved if and only if

$$n(\lambda) = \begin{vmatrix} r & s \\ t & u \end{vmatrix} = +1. \qquad \square$$

Lemma 3.2. *Let $\mathfrak{a}$ be an invertible fractional $\mathcal{O}$-ideal and select an oriented basis (α, β) in $\mathfrak{a}$. Then the group $\mathcal{O}_1^*$ of elements of norm 1 in $\mathcal{O}^*$ is isomorphic to the isotropy group $\mathbf{O}^+(f) \subset \mathbf{SL}(2, \mathbb{Z})$ of the binary quadratic form associated with the oriented basis chosen in $\mathfrak{a}$, i. e.*

$$f(X, Y) = \frac{n(X\alpha - Y\beta)}{n(\mathfrak{a})}.$$

Proof. For $\lambda \in \mathcal{O}_1^*$, $(\lambda\alpha, \lambda\beta)$ is by the previous lemma another oriented basis of $\mathfrak{a}$, so that $\lambda\alpha = r\alpha + s\beta$, $\lambda\beta = t\alpha + u\beta$ with $\begin{bmatrix} r & s \\ t & u \end{bmatrix} \in \mathbf{SL}(2, \mathbb{Z})$. Then we have

$$\frac{n(X\alpha - Y\beta)}{n(\mathfrak{a})} = \frac{n(X\lambda\alpha - Y\lambda\beta)}{n(\mathfrak{a})} = \frac{n[(Xr - Yt)\alpha - (-Xs + Yu)\beta]}{n(\mathfrak{a})}.$$

This shows that $\lambda \mapsto \begin{bmatrix} r & -t \\ -s & u \end{bmatrix}$ is a well-defined map from $\mathcal{O}_1^*$ into the isotropy group $\mathbf{O}^+(f)$ of f under the action of $\mathbf{SL}(2, \mathbb{Z})$. It is clearly injective. We next show it is surjective. By **[Za 81]**, we know that an element of $\mathbf{O}^+(f)$ may be written as

$$\begin{bmatrix} \frac{\mu - bv}{2} & -cv \\ av & \frac{\mu + bv}{2} \end{bmatrix},$$

for certain integers μ, v and where we assume $f(X, Y) = aX^2 + bXY + cY^2$. Now we realise that, from the definition of the map it suffices to check that the equality

$$\frac{\mu - bv}{2} - av\frac{\beta}{\alpha} = cv\frac{\alpha}{\beta} + \frac{\mu + bv}{2}$$

holds, since this equality trivially implies (cf. lemma above) that the element occurring in it has to lie in $\mathcal{O}^*$, and actually in $\mathcal{O}_1^*$, as the determinant of the preceding matrix is +1. But the preceding equality can be simplified to $\frac{-b}{2} - a\frac{\beta}{\alpha} = c\frac{\alpha}{\beta} + \frac{b}{2}$, which is easily seen to hold if we multiply through by β/α and recall that β/α has to be a root of $f(X, 1)$. That this bijective map is a group isomorphism is clear from a routine checking. □

Remark 3.3. *For imaginary quadratic fields, of course, $\mathcal{O}_1^* = \mathcal{O}^*$, since all elements have non-negative norm.*

Given an order $\mathcal{O}$ of discriminant D and an integer $N \geq 1$, let us denote by $\mathcal{H}(N, D)$ the set of integral quadratic forms of type $aNX^2 + bXY + cY^2$, with $D = b^2 - 4Nac$, $\gcd(aN, b, c) = \gcd(a, b, Nc) = 1$.

Theorem 3.4. *The group $\Gamma_0(N)$ operates on $\mathcal{H}(N, D)$. The quotient $H(N, D) := \mathcal{H}(N, D)/\Gamma_0(N)$ is a finite set. Moreover there is a bijection between $H(N, D)$ and the set of pairs $(\mathfrak{n}, [\mathfrak{a}])$, where $\mathfrak{n}$ is a primitive $\mathcal{O}$-ideal of norm N and $[\mathfrak{a}]$ is the proper class, i. e., in $Pic^+(\mathcal{O})$, of an invertible fractional $\mathcal{O}$-ideal $\mathfrak{a}$.*

Proof. If $\begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix} \in \Gamma_0(N)$, computation of

$$\begin{bmatrix} \alpha & \gamma N \\ \beta & \delta \end{bmatrix} \begin{bmatrix} aN & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix}$$

shows that $aNX^2 + bXY + cY^2$ is transformed into a form of type $a_1NX^2 + b_1XY + c_1Y^2$ with $a_1, b_1, c_1 \in \mathbb{Z}$ and, of course,

$$\gcd(a_1N, b_1, c_1) = \gcd(aN, b, c).$$

But then it is immediately checked that $\begin{bmatrix} \alpha & \beta N \\ \gamma & \delta \end{bmatrix} \in \mathbf{SL}(2, \mathbb{Z})$ transforms $aX^2 + bXY + cNY^2$ into $a_1X^2 + b_1XY + c_1NY^2$. It follows that $\gcd(a_1, b_1, c_1N) = \gcd(a, b, cN)$. This shows that $\Gamma_0(N)$ does operate on $\mathcal{H}(N, D)$. That the set $H(N, D)$ is finite is a trivial consequence of the finiteness of the number of classes of binary quadratic forms of discriminant D under $\mathbf{SL}(2, \mathbb{Z})$-equivalence, together with the fact that $\Gamma_0(N)$ has finite index in $\mathbf{SL}(2, \mathbb{Z})$.

In order to establish the asserted bijection, we proceed as follows: Take a pair $(\mathfrak{n}, [\mathfrak{a}])$. Then, by lemma 1.4, $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \simeq \mathbb{Z}/N\mathbb{Z}$, so that, by the theory of elementary divisors, we can write $\mathfrak{a} = \langle \omega_1, \omega_2 \rangle = \omega_1\langle 1, \tau \rangle$ and $\mathfrak{a}\mathfrak{n}^{-1} = \langle \omega_1/N, \omega_2 \rangle = \omega_1\langle 1/N, \tau \rangle = N^{-1}\omega_1\langle 1, N\tau \rangle$, for a suitable oriented basis (ω_1, ω_2).

Let the $\mathbb{Z}$-irreducible polynomial of τ be $aX^2 + bX + c$, with $a > 0$ and that of $N\tau$ be $AX^2 + BX + C$, with $A > 0$. Taking norms, we have, on the one hand, $n(\mathfrak{a}\mathfrak{n}^{-1}) = n(\mathfrak{a})n(\mathfrak{n})^{-1} = N^{-1}n(\mathfrak{a}) = N^{-1}|n(\omega_1)|a^{-1}$, and, on the other, $n(\mathfrak{a}\mathfrak{n}^{-1}) = n(N^{-1}\omega_1\langle 1, N\tau \rangle) = N^{-2}A^{-1}|n(\omega_1)|$, whence $aN = AN^2$; i. e., $a = AN$. Furthermore, the equation $A(N\tau)^2 + B(N\tau) + C = 0$ yields $AN\tau^2 + B\tau + CN^{-1} = 0$, from which we obtain $B = b$, $CN^{-1} = c$. Then it follows that $f(x, y) = ax^2 + bxy + cy^2 \in \mathcal{H}(N, D)$ and it is this form that we associate to $(\mathfrak{n}, [\mathfrak{a}])$. Now, it is easy to check that a different oriented $\mathbb{Z}$-basis $(\tilde{\omega}_1, \tilde{\omega}_2)$ of $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{n}^{-1} = \left\langle \frac{\tilde{\omega}_1}{N}, \tilde{\omega}_2 \right\rangle$ would yield a $\Gamma_0(N)$-equivalent quadratic form in $\mathcal{H}(N, D)$. In fact, if we express $\tilde{\omega}_1 = \alpha\omega_1 + \beta\omega_2$ and $\tilde{\omega}_2 = \gamma\omega_1 + \delta\omega_2$ and do the same for $\frac{\tilde{\omega}_1}{N}$ and $\tilde{\omega}_2$ with respect to $\frac{\omega_1}{N}$ and ω_2, we immediately obtain $\beta \equiv 0 \pmod{N}$. But $\tilde{\tau} = \frac{\tilde{\omega}_2}{\tilde{\omega}_1} = \frac{\delta\tau + \gamma}{\beta\tau + \alpha}$, and from this, it is easy to see that the corresponding quadratic forms for τ and $\tilde{\tau}$ *are* $\Gamma_0(N)$-equivalent and that, if we consider $\lambda\mathfrak{a}$ with $n(\lambda) > 0$ instead of $\mathfrak{a}$, we can proceed with the oriented basis $(\lambda\omega_1, \lambda\omega_2)$ to obtain the same results (observe that if $n(\lambda) < 0$, then $(\lambda\omega_1, \lambda\omega_2)$ is not oriented by lemma 3.1). This establishes a map from the set $\{(\mathfrak{n}, [\mathfrak{a}])\}$ into $H(N, D)$.

Conversely, for a quadratic form $f(X, Y) = aNX^2 + bXY + cY^2 \in \mathcal{H}(N, D)$, let τ be the root of the polynomial $aNX^2 + bX + c$ such that the $\mathbb{Z}$-basis $(1, \tau)$ is oriented. Then, we can associate to $f(X, Y)$ the pair $(\mathfrak{n}, [\mathfrak{a}])$, where $[\mathfrak{a}]$ is the class of $\langle 1, \tau\rangle$ in $\mathrm{Pic}^+(\mathcal{O})$ and $\mathfrak{n}$ is just $\langle 1, \tau\rangle\langle 1/N, \tau\rangle^{-1}$.

If we consider another form $\Gamma_0(N)$-equivalent to our original one, and $\tilde{\tau}$ is the corresponding root of the dehomogenised form, then there exists a matrix $\begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix} \in \in \mathbf{SL}(2, \mathbb{Z})$, *such that* $\tilde{\tau} = \dfrac{\alpha\tau + \beta}{\gamma N\tau + \delta}$. Now we see that $n(\gamma \mathrm{N}\tau + \delta) > 0$; in fact, only the real case needs to be considered. We have

$$\begin{vmatrix} 1 & \tilde{\tau} \\ 1 & \tilde{\tau}' \end{vmatrix} = \frac{\alpha\tau' + \beta}{\gamma \mathrm{N}\tau' + \delta} - \frac{\alpha\tau + \beta}{\gamma \mathrm{N}\tau + \delta} =$$

$$= n(\gamma N\tau + \delta)^{-1}(\alpha\delta - \beta\gamma N)(\tau' - \tau)$$

and, as both $(1, \tau)$ and $(1, \tilde{\tau})$ are oriented and $(\alpha\delta - \beta\gamma N) = 1$, we obtain $n(\gamma N\tau + \delta) > 0$. But then $\langle 1, \tilde{\tau}\rangle = (\gamma \mathrm{N}\tau + \delta)^{-1} \langle 1, \tau\rangle$, so that $[\mathfrak{a}]$ is well-defined. Since $N\tilde{\tau} = \dfrac{\alpha N\tau + \beta N}{\gamma N\tau + \delta}$, we also have $\langle 1, N\tilde{\tau}\rangle = (\gamma N\tau + \delta)^{-1} \langle 1, N\tau\rangle$, so that $\langle 1, \tau\rangle \langle 1, N\tau\rangle^{-1} = \langle 1, \tilde{\tau}\rangle \langle 1, \mathrm{N}\tilde{\tau}\rangle^{-1}$, and $\mathfrak{n}$ is well-defined too; i. e., we have a well defined map from the set $H(N, D)$ into $\{(\mathfrak{n}, [\mathfrak{a}])\}$. Now it is trivial to check that the two maps are inverse to each other. □

Setting $h(N, D) := \#H(N, D)$, we have the following:

Corollary 3.5. *The class number $h(N, D)$ equals the product of $h^+(D) := \mathrm{Pic}^+(\mathcal{O})$ by the number $s(N, D)$ of primitive $\mathcal{O}$-ideals of norm N. In particular, $h(1, D) = h^+(D)$.*

4. THE EVALUATION OF $H(N, D)$ IN THE IMAGINARY CASE

In this section we obtain a formula for the number $h(N, D)$ of Heegner points of type (N, D) in terms of numbers of representations by the genera of binary quadratic forms of discriminant D. Recall **[Si 35]** that two forms belong to the same genus, in the sense of Siegel, if and only if they are $\mathbf{GL}(2, \mathbb{Z}_p)$-equivalent for each prime p, including $p = \infty$; the genus of a primitive quadratic form f consists of a finite number of classes and, in the case of binary forms, the number of $\mathbf{SL}(2, \mathbb{Z})$-classes in a genus depends only on D. The genus of a quadratic form will be denoted by gen f.

We introduce the following notations for $N \geq 1$:

$$r(N, \mathrm{gen}\, f) := \left(\sum_{k=1}^{\nu} \frac{r(N, f_k)}{o(f_k)}\right) : \left(\sum_{k=1}^{\nu} \frac{1}{o(f_k)}\right),$$

$$r_+(N, \mathrm{gen}\, f) := \left(\sum_{k=1}^{\nu^+} \frac{r(N, f_k)}{o^+(f_k)}\right) : \left(\sum_{k=1}^{\nu^+} \frac{1}{o^+(f_k)}\right),$$

resp. $r^*(N, \mathrm{gen}\, f)$, $r_+^*(N, \mathrm{gen}\, f)$, for the average numbers of representations, resp. primitive representations, of an integer N by all the classes of forms in the genus of f. We understand that the sums run over a complete set of representatives for the ν $\mathbf{GL}(2, \mathbb{Z})$-classes, resp. ν^+ $\mathbf{SL}(2, \mathbb{Z})$-classes, in the genus of f.

Lemma 4.1. *Let f be a binary quadratic form.*

i) If f admits an improper automorphism, i. e., an automorphism of $\mathbf{GL}(2, \mathbb{Z})$ of determinant -1, then

$$r_+(N, \mathrm{gen}\, f) = r(N, \mathrm{gen}\, f), \quad r_+^*(N, \mathrm{gen}\, f) = r^*(N, \mathrm{gen}\, f).$$

ii) If f admits no improper automorphisms, then

$$r_+(N, \mathrm{gen}\, f) = 2r(N, \mathrm{gen}\, f),$$
$$r_+^*(N, \mathrm{gen}\, f) = 2r^*(N, \mathrm{gen}\, f).$$

Proof. In fact, if f admits an improper automorphism, then $o(f) = 2o^+(f)$, but the number of $\mathbf{SL}(2, \mathbb{Z})$-classes coincides with that of $\mathbf{GL}(2, \mathbb{Z})$-classes. If f admits no improper automorphisms, then $o(f) = o^+(f)$, but the number of $\mathbf{SL}(2, \mathbb{Z})$-classes doubles that of $\mathbf{GL}(2, \mathbb{Z})$-classes. □

Theorem 4.2. *The number of Heegner points of type (N, D) is*

$$h(N, D) = h(D) \frac{\nu}{o^+(D)} \sum_{j=1}^{t} \sum_{d^2 \mid N} \mu(d)\, \varepsilon(f_j)\, r(Nd^{-2}, \mathrm{gen}\, f_j).$$

Here ν stands for the number of $\mathbf{SL}(2, \mathbb{Z})$-classes in a genus of any primitive binary quadratic form of discriminant D; t stands for the number of genera of primitive binary quadratic forms of discriminant D; $\mu(-)$ denotes the Möbius function;

$$o^+(D) = \begin{cases} 2 & \text{if } D < -4, \\ 4 & \text{if } D = -4, \\ 6 & \text{if } D = -3, \end{cases}$$

is the number of roots of unity in the quadratic field; and

$$\varepsilon(f) = \begin{cases} 1 & \text{if } f \text{ admits improper automorphisms,} \\ 2 & \text{otherwise.} \end{cases}$$

Proof. Since a Heegner point of type (N, D) is described by the data $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$, we see that their number is

$s(N, D)h(D)$, where $s(N, D)$ denotes the number of primitive $\mathcal{O}$-ideals of norm N. By proposition 2.1 and its proof, to any primitive representation of N by a primitive binary quadratic form f, i. e., $(x, y) \in \mathbb{Z}^2$ with $f(x, y) = N$, $\gcd(x, y) = 1$, we associate an element $\xi = \alpha x - \beta y \in \mathfrak{a}$ of positive norm. The corresponding primitive $\mathcal{O}$-ideal $\mathfrak{n}$ of norm N is $\xi\mathfrak{a}^{-1}$, where $\mathfrak{a}$ is a representative of the class of the invertible fractional $\mathcal{O}$-ideal associated to

$$f(X, Y) = \frac{n(X\alpha - Y\beta)}{n(\mathfrak{a})}, \qquad \mathfrak{a} = \langle \alpha, \beta \rangle.$$

If we take another primitive representation of N by f, i. e., $(x_1, y_1) \in \mathbb{Z}^2$ with $f(x_1, y_1) = N$, $\gcd(x_1, y_1) = 1$, we obtain $\xi_1 \in \mathfrak{a}$ and another primitive $\mathcal{O}$-ideal of norm N, namely $\mathfrak{n}_1 = \xi_1\mathfrak{a}^{-1}$. We have $\xi\xi_1^{-1} \in \mathbb{Q}(\sqrt{D})$ and $n(\xi\xi_1^{-1}) = 1$. Obviously, ξ, ξ_1 are associates if and only if $\xi\xi_1^{-1} \in \mathcal{O}_1^*$. Therefore, if ξ and ξ_1 are not associates, they yield different primitive $\mathcal{O}$-ideals of norm N in the class, defined by $\mathfrak{a}^{-1}$. But by the previous lemma 3.2, ξ and ξ_1 are associates if and only if the corresponding solutions are $\mathbf{O}^+(f)$-equivalent. This shows that $\dfrac{r^*(N, f)}{o^+(f)}$ is precisely the number of distinct primitive $\mathcal{O}$-ideals of norm N in the inverse of the class of invertible fractional $\mathcal{O}$-ideals corresponding to the class of f. By considering all the classes, we have that

$$s(N, D) = \sum_{i=1}^{h(D)} \frac{r^*(N, f_i)}{o^+(f_i)} = \frac{v}{o^+(D)} \sum_{j=1}^{t} r_+^*(N, \operatorname{gen} f_j) = \frac{v}{o^+(D)} \sum_{j=1}^{t} \varepsilon(f_j)\, r^*(N, \operatorname{gen} f_j).$$

But

$$r^*(N, \operatorname{gen} f) = \sum_{d^2 \mid N} \mu(d) r(Nd^{-2}, \operatorname{gen} f),$$

and the claim follows. □

Remarks 4.3. *i) The above formula is also true for $N = 1$. In fact, since the integer 1 is only represented by the forms of the unit class, say $[f_1]$ of the group $H(D)$, and the forms in this class have improper automorphisms, we obtain*

$$r(1, \operatorname{gen} f_1) = \frac{o^+(D)}{v}.$$

Therefore, $h(1, D) = h(D)$.

ii) The value $r(N, \operatorname{gen} f)$ can be determined by means of the so-called p-adic densities. In fact, applying Minkowski-Siegel's main theorem **[Si 35]**, *we have*

$$r(N, \operatorname{gen} f) = \frac{1}{2}\, \partial_\infty(N, f) \prod_p \partial_p(N, f),$$

where, the ∂'s stand for the p-adic densities. In our case,

$$\partial_\infty(N, f) = \frac{2\pi}{\sqrt{|D|}}$$

and

$$\partial_p(N, f) = \frac{r_q(N, f)}{q}$$

with $q = p^a$ and $a > 2v_p(2N)$; $v_p(-)$ stands for the p-adic valuation; $r_q(N, f)$ stands for the number of representations of N by f modulo q.

iii) Since $D = D_0 r^2$, we have (cf., **[Za 81]**)

$$h(D) = \frac{2r}{o^+(D)} \prod_{p \mid r} \left(1 - \frac{\chi_{D_0}(p)}{p}\right) h(D_0).$$

In what follows, for any positive integer N we shall write its factorisation into primes in the form $N = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$, where $\alpha \geq 0$, $r \geq 0$, $s \geq 0$, $p_i \equiv 1$ or $3 \pmod 8$ for $1 \leq i \leq r$, $q_j \equiv 5$ or $7 \pmod 8$ for $1 \leq j \leq s$, and the exponents α_i, β_j are strictly positive (whenever they occur).

We illustrate the preceding results with the following example:

Proposition 4.4. *With the preceding notations, for any positive integer N, we have*

$$h(N, -8) = \begin{cases} 2^r & \text{if } \alpha < 2 \text{ and } s = 0, \\ 0 & \text{otherwise} \end{cases}$$

Proof. In this case, f can be considered to be $X^2 + 2Y^2$ and we have $\operatorname{gen} f = f$, because $h(-8) = 1$. We first observe that for $\alpha \geq 2$, we have $h(N, -8) = 0$, since, by reducing (mod 4), we easily see that $r^*(N, f) = 0$ and, then we just recall that $h(N, -8) = h(-8) \dfrac{r^*(N, f)}{2}$. So, in the sequel, we will always assume $0 \leq \alpha \leq 1$.

By theorem 4.2 we have

$$h(N, -8) = \frac{1}{2} \sum_{d^2 \mid N} \mu(d) r(Nd^{-2}, \operatorname{gen} f). \tag{2}$$

By the Minkowski-Siegel formula, we have, for $m = Nd^{-2}$,

$$r(m, \operatorname{gen} f) = \frac{1}{2} \frac{2\pi}{\sqrt{|D|}}\, \partial_2(m, f) \prod_{i=1}^{r} \partial_{p_i}(m, f) \prod_{\substack{\ell \neq 2 \\ \ell \neq p_i}} \partial_\ell(m, f)$$

and we next evaluate the p-adic densities.

In order to calculate $\partial_2(m, f)$, we distinguish the cases $\alpha = 0$ and $\alpha = 1$. In the former case, we readily obtain $\partial_2(m, f) = \frac{1}{8} r_8(m, f) = 2$. In the latter, as will be shown later in this proof, we will only need to assume all the β's to be even. In this case, an elementary but tedious checking (essentially reduced to computing the powers of 3 (mod 16)) shows that $m \equiv 2, 6, 18, 22 \pmod{32}$ and for these cases, we immediately have $\partial_2(m, f) = \frac{1}{32} r_{32}(m, f) = 2$. Summarising, $\partial_2(m, f) = 2$ in the cases we are interested in.

Next, for the primes $p_i \equiv 1, 3 \pmod 8$ occurring in the factorisation of N, we have (cf. **[Ar-Ba 87]**)

$$\partial_{p_i}(m, f) = \left(v_{p_i}(m) + 1\right) \frac{p_i - 1}{p_i},$$

where, as before, $v_{p_i}(m)$ stands for the p-adic valuation of m.

For $q \mid m$, $q \equiv 5, 7 \pmod 8$, we have

$$\partial_q(m, f) = \begin{cases} \dfrac{q+1}{q} & \text{if } v_q(m) \text{ is even,} \\ 0 & \text{if } v_q(m) \text{ is odd.} \end{cases}$$

For a prime $\ell \nmid m$, we simply have

$$\partial_\ell(m, f) = \left(1 - \left(\frac{-2}{\ell}\right)\frac{1}{\ell}\right).$$

Recalling that

$$L(1, \chi_{-8}) = \prod_\ell \left(1 - \left(\frac{-2}{\ell}\right)\frac{1}{\ell}\right),$$

where the product is extended over all finite primes, and that $h(-8) = \frac{\pi}{2\sqrt{2}} L(1, \chi_{-8})$, we see that

$$r(m, \operatorname{gen} f) = 2 \prod_{i=1}^{r} \left(v_{p_i}(m) + 1\right). \tag{3}$$

Now we compute the right hand side of (2) using (3) in the case $\alpha < 2$, $s = 0$ and $r > 0$. Recalling that $\alpha_i = v_{p_i}(N)$, $1 \le i \le r$, and setting $a := \prod_{i=1}^{r} (\alpha_i + 1)$, we obtain

$$\frac{1}{2} \sum_{d^2 \mid N} \mu(d) r(Nd^{-2}, \operatorname{gen} f) = r(N, \operatorname{gen} f) - \sum_{i=1}^{r} r(Np_i^{-2}, \operatorname{gen} f) +$$

$$+ \sum_{1 \le i < j \le r} r(Np_i^{-2}p_j^{-2}, \operatorname{gen} f) - \sum_{1 \le i < j < k \le r} r(Np_i^{-2}p_j^{-2}p_k^{-2}, \operatorname{gen} f) +$$

$$+ \cdots + (-1)^r r(Np_1^{-2} \cdots p_r^{-2}, \operatorname{gen} f) =$$

$$a\left[1 - \sum_{i=1}^{r} \frac{\alpha_i - 1}{\alpha_i + 1} + \sum_{1 \le i < j \le r} \frac{(\alpha_i - 1)(\alpha_j - 1)}{(\alpha_i + 1)(\alpha_j + 1)} - \cdots + \right.$$

$$\left. + (-1)^r \prod_{i=1}^{r} \frac{\alpha_i - 1}{\alpha_i + 1}\right] = a\left[1 - \sum_{i=1}^{r} (1 - \gamma_i) + \right.$$

$$\left. + \sum_{1 \le i < j \le r} (1 - \gamma_i)(1 - \gamma_j) - \cdots + (-1)^r \prod_{i=1}^{r} (1 - \gamma_i)\right],$$

where γ_i stands for $2(\alpha_i + 1)^{-1}$, $1 \le i \le r$. But the alternating sum in brackets is easily seen to be equal to $\gamma_1 \cdot \cdots \cdot \gamma_r$; just observe that

$$1 - \sum_{i=1}^{r} X_i + \sum_{1 \le i < j \le r} X_i X_j + \cdots + (-1)^r X_1 X_2 \cdot \cdots \cdot X_r =$$

$$= \prod_{i=1}^{r} (1 - X_i),$$

and then substitute $X_i = 1 - \gamma_i$. Consequently, we see in our case

$$h(N, -8) = \frac{1}{2} \sum_{d^2 \mid N} \mu(d) r(Nd^{-2}, \operatorname{gen} f) = a \cdot \prod_{i=1}^{r} \frac{2}{\alpha_i + 1} = 2^r.$$

Observe that this result also holds for $r = 0$, in which case, the preceding sum reduces just to $\frac{1}{2} r(N, \operatorname{gen} f) = 1$.

If $s > 0$ and all the β_j are even, the preceding calculations may still be used, as we explain with a simple example: observe that by our preceding formulae, for instance, $r(Np_i^{-2}p_j^{-2}, \operatorname{gen} f)$ remains unaltered by (3) if we add squares of q's to the denominator and thus all non-vanishing terms $\mu(d) r(Nd^{-2}, \operatorname{gen} f)$ where d is the product of $p_i p_j$ with possibly other q's yield the following contribution to the whole sum:

$$r(Np_i^{-2}p_j^{-2}, \operatorname{gen} f) - \sum_{k=1}^{s} r(Np_i^{-2}p_j^{-2}q_k^{-2}, \operatorname{gen} f) +$$

$$+ \sum_{1 \le k < k' \le s} r(Np_i^{-2}p_j^{-2}q_k^{-2}q_{k'}^{-2}, \operatorname{gen} f) - + \cdots +$$

$$+ (-1)^s r(Np_i^{-2}p_j^{-2}q_1^{-2} \cdot \cdots \cdot q_s^{-2}, \operatorname{gen} f) =$$

$$= a(1 - \gamma_i)(1 - \gamma_j)\left[1 - \binom{s}{1} + \binom{s}{2} - \binom{s}{3} + \cdots + \right.$$

$$\left. + (-1)^s \binom{s}{s}\right] = 0.$$

As the same happens in the remaining cases, the result follows trivially.

Of course, in the case where a prime q appears with an odd exponent, we also obtain the value 0 but, here, we do

not require the preceding calculations; we just observe that $\partial_q(Nd^{-2}, \text{gen}\, f)$ is already zero for all $d^2 | N$ (and this also allows us to get rid of the computation for $\partial_2(Nd^{-2}, \text{gen}\, f)$ when not all β's are even). This completes the proof. □

REFERENCES

1. **[Ar-Ba 87]** Arenas, A. & Bayer, P. (1987). Arithmetic Behaviour of the Sums of Three Squares, *Journal of Number Theory* **27**, 3, 273-284.
2. **[Ar-Ba 2000-2]** Arenas, A. & Bayer, P. (2000), Complex multiplication points on modular curves, *Rev. R. Acad. Cienc. Exact. Fis. Nat., Esp.* **94**, 333-338.
3. **[Bak 66]** Baker, A. (1966), Linear forms in the logarithms of algebraic numbers I, *Mathematika* **13**, 204-216.
4. **[Ba-Tr 2000-1]** Bayer, P. & Travesa, A. (2000), Órdenes matriciales generados por grupos de congruencia, *Rev. R. Acad. Cienc. Exact. Fis. Nat., Esp.* **94**, 339-346.
5. **[Ba-Tr 2000-2]** Bayer, P. & Travesa, A. (2000), Formas cuadráticas ternarias e inmersiones matriciales de órdenes cuadráticos, *Rev. R. Acad. Cienc. Exact. Fis. Nat., Esp.* **94**, 347-356.
6. **[Ba-Tr 2000-3]** Bayer, P. & Travesa, A. (2000), Inmersiones de órdenes cuadráticos en el orden generado por $\Gamma_0(N)$, *Rev. R. Acad. Cienc. Exact. Fis. Nat., Esp.* **94**, 357-376.
7. **[Be-Da 98]** Bertolini, M. & Darmon, H. (1998), Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization, *Invent. math.* **131**, 453-491.
8. **[Bi 68]** Birch, B. J. (1975), Diophantine Analysis and Modular Functions, in the book *Proceedings of the Bombay Colloquium on Algebraic Geometry,* pp 35-42.
9. **[Bi 75]** Birch, B. J. (1975), Heegner Points of Elliptic Curves, in the book *Symp. Math. Ist. d. Alta Mat.,* pp 441-445.
10. **[Bi-SD 65]** Birch, B. J. & Swinnerton-Dyer, H. P. F. (1965), Notes on elliptic curves, II, *J. für die reine u. angew. Math.* **218**, 79-108.
11. **[Bo-Sh 66]** Borevich, Z. I. & Shafarevich, I. R. (1966), *Number Theory*, Academic Press.
12. **[Co-Wi 77]** Coates, J. & Wiles, A. (1977), On the Conjecture of Birch and Swinnerton-Dyer, *Inventiones math.* **39**, 223-251.
13. **[Cox 89]** Cox, D. A. (1989), *Primes of the Form $x^2 + ny^2$*, Wiley & Sons.
14. **[De 68]** Deuring, M. (1968), Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins. *Inventiones math.* **5**, 169-179.
15. **[Ga 1801-96]** Gauss, C. F. (1996), *Disquisitiones Arithmeticæ,* Gerh. Fleischer, Lipsiæ, 1801. Catalan translation by G. Pascual, IEC, Barcelona.
16. **[Gr 84]** Gross, B. H. (1984), Heegner Points on $X_0(N)$, in the book *Modular Forms,* R. A. Rankin, ed., Ellis Horwood Series, Wiley and Sons, 87-105.
17. **[Gr-Ko-Za 87]** Gross, B.; Kohnen, W. & Zagier, D. (1987), Heegner Points and Derivatives of L-Series, II, *Math. Ann.* **278**, 497-562.
18. **[Gr-Za 86]** Gross, B. H. & Zagier, D. B. (1986), Heegner points and derivatives of L-series, *Inventiones math.* **84**, 225-320.
19. **[He 52]** Heegner, K. (1952) Diophantische Analysis und Modulfunktionen, *Mathematische Z.* **56**, 227-253.
20. **[Ka 70]** Kaplansky, I. (1970), *Commutative Rings,* University of Chicago Press.
21. **[Ko 90]** Kolyvagin, V. A. (1990), Euler Systems, in the book *The Grothendieck Festschrift,* II, P. Cartier et al., ed., Birkhäuser, 435-483.
22. **[Ma 77]** Mazur, B. (1977), Modular Curves and the Eisenstein Ideal, *Publ. Math. IHES* **47**, 33-186.
23. **[Mo 22]** Mordell, L. J. (1922), On the rational solutions of the indeterminate equations of the third and four degrees, *Proc. Camb. Philos. Soc.* **21**, 179-192.
24. **[Ne 92]** Neukirch, J. (1992), *Algebraische Zahlentheorie,* Springer.
25. **[Rü-Ti 99]** Rück, H. G. & Tipp, U. (1999), Heegner points and L-series of automorphic cusp forms of Drinfeld type. Preprint.
26. **[Sh 67]** Shimura, G. (1967), Construction of class fields and zeta functions of algebraic curves, *Ann. of Math.* **85**, 58-159.
27. **[Si 35]** Siegel, C. L. (1966), Über die analytische Theorie der quadratischen Formen, *Annals of Math.* **36** (1935), 527-606. In *Gesammelte Abhandlungen,* Band 1, Springer, 1966.
28. **[Si 49]** Siegel, C. L. (1949), *Transcendental numbers,* Princeton Univ. Press.
29. **[Si 68]** Siegel, C. L. (1968), Zum Beweise des Starkschen Satzes, *Inventiones math.* **5**, 180-191.
30. **[St 67]** Stark, H. M. (1967), A complete determination of the complex quadratic fields of class number one, *Michigan Math. J.* **14**, 1-27.
31. **[St 69]** Stark, H. M. (1969), On the «gap» in a theorem of Heegner, *J. Number Theory* **1**, 16-27.
32. **[We 08]** Weber, H. (1962), *Lehrbuch der Algebra, Bd. III,* Vieweg, 1908. Chelsea.
33. **[Zh 99]** Zhang, S. (1999), Heights of Heegner Points on Shimura Curves. Preprint, 1-82.
34. **[Za 81]** Zagier, D. B. (1981), *Zetafunktionen und quadratische Körper,* Hochschultext, Springer, 1981.