PACIFIC JOURNAL OF MATHEMATICS
Vol. 181, No. 3, 1997

EMBEDDINGS INTO THE INTEGRAL OCTONIONS

Noam Elkies & Benedict H. Gross

To Olga Taussky-Todd in memoriam

Let $\mathbb{O}$ be the $\mathbb{Q}$-algebra of Cayley's octonions, with basis $\{1, e_1, e_2, \dots, e_7\}$ and multiplication rules:

$$e_i^2 = -1 \qquad \text{all } i$$
$$(e_i e_{i+1})e_{i+3} = e_i(e_{i+1}e_{i+3}) = -1 \qquad \text{all } i \pmod 7.$$

Coxeter discovered a maximal order R in $\mathbb{O}$, which is unique up to the action of $\mathrm{Aut}(\mathbb{O})$, with the property that R/pR is an octonion algebra over $\mathbb{Z}/p\mathbb{Z}$ for all primes p. We review the construction of the order R, and some of its properties, in §1.

In §2, we let K be an imaginary quadratic field, with ring of integers A and discriminant D. We count the number of ring embeddings of A into R, using the L-function $L(\varepsilon, s)$ of the quadratic Dirichlet character $\varepsilon : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$ associated to K.

Theorem 1. *The number of embeddings of A into R is $-252 \cdot L(\varepsilon, -2)$.*

We give two different proofs of this result. The first uses theta series and Eisenstein series of half-integral weight. The second uses the theory of Tamagawa measures, as developed by Siegel and Weil. From the formula in Theorem 1, it follows that the number of embeddings of A into R lies between $3 \cdot |D|^{5/2}$ and $5 \cdot |D|^{5/2}$.

In §3 we let K be a definite quaternion algebra over $\mathbb{Q}$, and let A be a maximal order in K. Let S be the finite set of primes which ramify in K; thus $p \in S$ if and only if $K \otimes \mathbb{Q}_p$ is a division algebra over $\mathbb{Q}_p$. Using the theory of Tamagawa measures, we will prove the following.

Theorem 2. *The number of embeddings of A into R is $504 \cdot \prod_{p \in S}(p^2 - 1)$.*

Our interest in octonions dates from a lecture that Serre gave at Harvard on the subject, in the fall of 1990. The embedding problems which we study are generalizations of the results of Hasse and Eichler (cf. [14, p. 92ff.]) on the embeddings of rings of integers in imaginary quadratic fields into certain orders in rational quaternion algebras. Since Olga loved the arithmetic of quaternion algebras, we felt it was appropriate to dedicate this paper to her memory.

1. Coxeter's order R.

Let M be the $\mathbb{Z}$-order in $\mathbb{O}$ spanned by 1 and the e_i. Then $R/M \simeq (\mathbb{Z}/2\mathbb{Z})^4$, and a basis for R/M is given by [6], [4, p. 14]:

$$\begin{aligned} &\tfrac{1}{2}(1 + e_1 + e_2 + e_4) \\ &\tfrac{1}{2}(1 + e_1 + e_3 + e_7) \\ &\tfrac{1}{2}(1 + e_1 + e_5 + e_6) \\ &\tfrac{1}{2}(e_1 + e_2 + e_3 + e_5). \end{aligned} \tag{1.1}$$

The anti-involution $x \mapsto \overline{x}$ of $\mathbb{O}$, defined by $\overline{1} = 1$ and $\overline{e_i} = -e_i$, stabilizes the order R. The linear map $\mathrm{Tr}(x) = x + \overline{x}$ and the quadratic form $\mathbb{N}(x) = x \cdot \overline{x} = \overline{x} \cdot x$ both take integral values on R, and any x in R satisfies a monic quadratic polynomial over $\mathbb{Z}$:

$$x^2 - \mathrm{Tr}(x) \cdot x + \mathbb{N}(x) = 0. \tag{1.2}$$

The bilinear form $\langle x, y \rangle = \mathrm{Tr}(\overline{x}y)$ is symmetric, even, and positive definite on R. It is also unimodular, so the inner product space $(R, \langle , \rangle)$ over $\mathbb{Z}$ is isomorphic to the E_8-root lattice.

The group $\Gamma = \mathrm{Aut}(R)$ is finite, of order $12096 = 2^6 \cdot 3^3 \cdot 7$, and is isomorphic to $\mathrm{Aut}(R/2R) = G_2(\mathbb{Z}/2\mathbb{Z})$ under reduction mod 2 [4, p. 14].

2. Imaginary quadratic fields.

Let K be an imaginary quadratic field, of discriminant $D < 0$. Let A be the ring of integers of K; then

$$A = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{D + \sqrt{D}}{2}. \tag{2.1}$$

Let $\varepsilon : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$ be the Dirichlet character associated to K. We have $\varepsilon(p) = +1$ if and only if the prime p is split in A. The L-function

$$L(\varepsilon, s) = \sum_{\substack{n \geq 1 \\ (n, D) = 1}} \varepsilon(n) \cdot n^{-s} \tag{2.2}$$

is absolutely convergent for $\mathrm{Re}(s) > 1$, and extends to an entire function in s, taking rational values at negative integers (cf. [3]). The function $\Lambda(s) = \pi^{-\frac{s+1}{2}} \Gamma(\frac{s+1}{2}) L(\varepsilon, s)$ satisfies the functional equation: $\Lambda(1-s) = \Lambda(s) \cdot |D|^{\frac{1}{2}-s}$ [7, p. 71].

Let $\#(A \longrightarrow R)$ denote the number of ring embeddings of A into R. We will give two proofs of the formula of Theorem 1:

$$\#(A \longrightarrow R) = -252 \cdot L(\varepsilon, -2). \tag{2.3}$$

The first is based on (2.1). To give an embedding $f : A \longrightarrow R$ we must specify an x $(= \sqrt{D})$ in R which satisfies:

$$\begin{aligned} \mathrm{Tr}(x) &= 0 \\ \mathbb{N}(x) &= -D \\ x &\equiv D \pmod{2R}. \end{aligned} \tag{2.4}$$

Let L be the subgroup of elements x in $\mathbb{Z} + 2R$ which satisfy $\mathrm{Tr}(x) = 0$. We then have

$$\#(A \longrightarrow R) = \#\{x \in L : \langle x, x \rangle = -2D\}. \tag{2.5}$$

The number on the right of (2.5) is the coefficient of $q^{|D|}$ in the theta function of $(L, \langle , \rangle)$.

Since $(R, \langle , \rangle)$ is isomorphic to the E_8-root lattice, we can identify the lattice L. It is even, of rank 7 and determinant 2^{13}, and has index 2^6 in the E_7-root lattice. In fact, $L = 2 \cdot E_7^*$. Hence the theta function

$$\Theta_L = \sum_{\lambda} q^{\langle \lambda, \lambda \rangle / 2} = \sum_{n \geq 0} a_n q^n \tag{2.6}$$

is a modular form of weight $\frac{7}{2}$ for the group $\Gamma_0(4)$. Since $a_n = 0$ unless $n \equiv 0, 3 \pmod 4$, Θ_L lies in Kohnen's subspace [11]. (More generally, if M is any even lattice of rank n and discriminant 2 then $n \equiv \pm 1 \bmod 8$ and the theta series of $2M^*$ lies in Kohnen's space of modular forms of weight $n/2$ [8].) For weight $\frac{7}{2}$, Kohnen's subspace is one-dimensional, and spanned by the Eisenstein series H_3 introduced by Cohen [3, p. 273]. Since $a_0 = 1$ for Θ_L, a comparison of Fourier coefficients yields:

$$a_{|D|} = -252 \cdot L(\varepsilon, -2). \tag{2.7}$$

This completes the first proof of (2.3).

The second proof is based on the fact that the $\mathbb{Q}$-algebra embeddings $K \longrightarrow \mathbb{O}$ are permuted transitively by the group $G = \mathrm{Aut}(\mathbb{O})$, and the stabilizer of a fixed embedding is the subgroup $H \simeq SU(K^{\perp})$ [10, §3]. The group G is an inner twisting of the split group of type G_2 over $\mathbb{Q}$, and H is an inner twisting of the quasi-split group $SU_3(K)$.

Let

$$\varphi_p : G(\mathbb{Q}_p)/H(\mathbb{Q}_p) \longrightarrow \mathbb{R} \tag{2.8}$$

be the characteristic function of the $\mathbb{Q}_p$-embeddings $K \otimes \mathbb{Q}_p \longrightarrow \mathbb{O} \otimes \mathbb{Q}_p$ which map $A \otimes \mathbb{Z}_p$ into $R \otimes \mathbb{Z}_p$, and put $\varphi_\infty = 1$ on $G(\mathbb{R})/H(\mathbb{R})$. Let $\varphi = \prod \varphi_v$ on the adelic coset space $G(\mathbb{A})/H(\mathbb{A})$, and let dg and dh be the Tamagawa measures on the group $G(\mathbb{A})$ and $H(\mathbb{A})$ respectively. Then by [13, p. 670-671] we have

$$\#(A \longrightarrow R) = \int_{G(\mathbb{A})/H(\mathbb{A})} \varphi(y) dy, \tag{2.9}$$

with $dy = dg/dh$. Indeed, both G and H are simply-connected, so have Tamagawa numbers equal to 1 ([15]), and by [9]:

$$G(\mathbb{A}) = G(\mathbb{Q}) \cdot \left(G(\mathbb{R}) \times \prod G(\mathbb{Z}_p) \right), \tag{2.10}$$

so there is only one class.

We calculate the right hand side of (2.9) by first writing $dy = \prod dy_v$, then calculating the local integrals. To obtain a decomposition $dg = \prod dg_v$ and $dh = \prod dh_v$ of Tamagawa measures, we fix models of G and H over $\mathbb{Z}$, given by the maximal orders R and A. Then G has good reduction at all primes p, and H has good reduction at all $p \not| D$. The base change H/A is isomorphic to SL_3. Let ω_G and ω_H be generators of the invariant differential forms of top degree on G and H over $\mathbb{Z}$. These are determined up to sign, and we define [15, Ch. II]:

$$\begin{aligned} dg_v &= |\omega_G|_v \qquad \text{on } G(\mathbb{Q}_v) \\ dh_v &= |\omega_H|_v \qquad \text{on } H(\mathbb{Q}_v) \\ dy_v &= dg_v/dh_v \quad \text{on } G(\mathbb{Q}_v)/H(\mathbb{Q}_v). \end{aligned} \tag{2.11}$$

Then we have

$$\int_{G(\mathbb{A})/H(\mathbb{A})} \varphi(y) dy = \int_{G(\mathbb{R})/H(\mathbb{R})} dy_\infty \cdot \prod_p \int_{G(\mathbb{Q}_p)/H(\mathbb{Q}_p)} \varphi_p(y_p) dy_p. \tag{2.12}$$

Since $G(\mathbb{Z}_p)$ acts transitively on embeddings $A \otimes \mathbb{Z}_p \longrightarrow R \otimes \mathbb{Z}_p$, with sta-

bilizer $H(\mathbb{Z}_p)$ [15, p. 112], we find

$$\begin{aligned}\int_{G(\mathbb{Q}_p)/H(\mathbb{Q}_p)} \varphi_p(y_p)dy_p &= \int_{G(\mathbb{Z}_p)} dg_p \Big/ \int_{H(\mathbb{Z}_p)} dh_p \\ &= \frac{\#G(\mathbb{Z}/p\mathbb{Z})/p^{\dim G}}{\#H(\mathbb{Z}/p\mathbb{Z})/p^{\dim H}} \\ &= \frac{(1-p^{-6})(1-p^{-2})}{(1-\varepsilon(p)p^{-3})(1-p^{-2})} \\ &= \frac{(1-p^{-6})}{(1-\varepsilon(p)p^{-3})}.\end{aligned}$$

Hence

$$\prod_p \int_{G(\mathbb{Q}_p)/H(\mathbb{Q}_p)} \varphi_p(y_p)dy_p = \zeta(6)^{-1}/L(\varepsilon,3)^{-1}.$$

The real integral is given by ([2, p. 122], [9, p. 269])

$$\begin{aligned}\int_{G(\mathbb{R})/H(\mathbb{R})} dy_\infty &= \int_{G(\mathbb{R})} dg_\infty \Big/ \int_{H(\mathbb{R})} dh_\infty \\ &= \frac{(2\pi)^8}{5!} \Big/ \frac{(2\pi)^5}{2!|D|^{5/2}} \\ &= \frac{(2\pi)^3|D|^{5/2}}{2^2\cdot 3\cdot 5}.\end{aligned}$$

But

$$\begin{aligned}\zeta(6) &= \frac{(2\pi)^6}{2^6\cdot 3^3\cdot 5\cdot 7} \\ L(\varepsilon,3) &= \frac{-(2\pi)^3}{2^2|D|^{5/2}} L(\varepsilon,-2).\end{aligned} \tag{2.13}$$

The first identity is due to Euler, and the second follows from the functional equation of $L(\varepsilon,s)$. Combining (2.9) with (2.12, 2.13), we obtain (2.3).

To estimate $\#(A\longrightarrow R)$ it is better not to invoke the functional equation of $L(\varepsilon,s)$, and to use the formula

$$\frac{\#(A\longrightarrow R)}{|D|^{5/2}} = \frac{126}{\pi^3} L(\varepsilon,3). \tag{2.14}$$

For real $s > 1$,

$$\begin{aligned} L(\varepsilon, s) &= \prod_{p \not| D} (1 - \varepsilon(p)p^{-s})^{-1} \\ &= \prod_{p \not| D} (1 + \varepsilon(p)p^{-s} + \varepsilon(p^2)p^{-2s} + \dots), \end{aligned}$$

with $\varepsilon(p^n) = \pm 1 \leq 1$. Hence the p term in the product is bounded above by

$$(1 - p^{-s})^{-1} = (1 + p^{-s} + p^{-2s} + \dots),$$

and

$$L(\varepsilon, s) \leq \zeta(s) \cdot \prod_{p|D} (1 - p^{-s}).$$

But we also have

$$(1 - \varepsilon(p)p^{-s})(1 + \varepsilon(p)p^{-s}) = (1 - p^{-2s})$$

for all $p \not| D$. Hence

$$\frac{(1 - p^{-2s})^{-1}}{(1 - \varepsilon(p)p^{-s})^{-1}} \leq (1 - p^{-s})^{-1},$$

and

$$\frac{\zeta(2s) \prod_{p|D}(1 - p^{-2s})}{L(\varepsilon, s)} \leq \zeta(s) \cdot \prod_{p|D} (1 - p^{-s}).$$

This gives the upper and lower bounds:

$$\frac{\zeta(2s)}{\zeta(s)} \cdot \prod_{p|D} (1 + p^{-s}) \leq L(\varepsilon, s) \leq \zeta(s) \prod_{p|D} (1 - p^{-s}),$$

which imply the slightly cruder estimates:

$$\frac{\zeta(2s)}{\zeta(s)} \leq L(\varepsilon, s) \leq \zeta(s). \tag{2.15}$$

Taking $s = 3$ in (2.15), and using (2.14), we find

$$\frac{126}{\pi^3} \cdot \frac{\zeta(6)}{\zeta(3)} \leq \frac{\#(A \longrightarrow R)}{|D|^{5/2}} \leq \frac{126}{\pi^3} \cdot \zeta(3). \tag{2.16}$$

Since

$$3.4392 < \frac{126}{\pi^3} \cdot \frac{\zeta(6)}{\zeta(3)} < \frac{126}{\pi^3} \cdot \zeta(3) < 4.8848,$$

this gives the estimate stated in the introduction.

We conclude this section with a short table of numerical values, taken from [3, p. 284] and [5, p. 125]. These values can be computed independently using the formula [16, p. 31]

$$L(\varepsilon, -2) = -\frac{D^2}{3} \sum_{a=1}^{D} \varepsilon(a) B_3(a/D), \tag{2.17}$$

where $B_3(x) = x(x - \frac{1}{2})(x - 1)$ is the third Bernoulli polynomial. In seven cases, namely $-D = 3, 4, 7, 8, 11, 15, 23$, the number of embeddings divides the order $12096 = 2^6 \cdot 3^3 \cdot 7$ of the finite group $\Gamma = \mathrm{Aut}(R)$; it turns out that in each of these cases, Γ acts transitively on the embeddings. In particular for $D = -23$ the action is transitive and free, as we show later, at the end of §3.

Table 2.18.

D	$\#(A \longrightarrow R)$	$\lvert D\rvert^{-5/2}\#(A \longrightarrow R)$
-3	$56 = 2^3 \cdot 7$	3.5924+
-4	$126 = 2 \cdot 3^2 \cdot 7$	3.9375
-7	$576 = 2^6 \cdot 3^2$	4.4430+
-8	$756 = 2^2 \cdot 3^3 \cdot 7$	4.1763+
-11	$1512 = 2^3 \cdot 3^3 \cdot 7$	3.7676+
-15	$4032 = 2^6 \cdot 3^2 \cdot 7$	4.6269+
-19	$5544 = 2^3 \cdot 3^2 \cdot 7 \cdot 11$	3.5232+
-20	$7560 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$	4.2262−
-23	$12096 = 2^6 \cdot 3^3 \cdot 7$	4.7678+
-24	$11592 = 2^3 \cdot 3^2 \cdot 7 \cdot 23$	4.1080−
-31	$24192 = 2^7 \cdot 3^3 \cdot 7$	4.5213+

3. Definite quaternion algebras.

Now let K be a definite quaternion algebra over $\mathbb{Q}$, and let A be a maximal order in K. Let S be the set of primes which ramify in K, and put $D = \prod_{p \in S} p$ [14, Ch. III, §5].

The embeddings of $\mathbb{Q}$-algebras $K \longrightarrow \mathbb{O}$ are again permuted transitively by $G = \mathrm{Aut}(\mathbb{O})$. In this case, the stabilizer of a fixed embedding is the subgroup $H \simeq K^*_{\mathbb{N}=1}$ of elements of norm 1 in K^*, which acts on $K^\perp$ by left multiplication [10]. Over $\overline{\mathbb{Q}}$, this H is a long-root SL_2 subgroup of $G \simeq G_2$. Defining $\varphi = \prod \varphi_v$ on $G(\mathbb{A})/H(\mathbb{A})$ as in §2, we have [13, p. 670-671]

$$\#(A \longrightarrow R) = \int_{G(\mathbb{A})/H(\mathbb{A})} \varphi(y) dg/dh, \tag{3.1}$$

where $dg = \prod dg_v$ as in §2 and dh is Tamagawa measure on $H(\mathbb{A})$.

We obtain a local decomposition for dh by choosing a model for H over $\mathbb{Z}$ (with good reduction at all primes $p \not| D$) corresponding to the order A: $H(\mathbb{Z}) = A^*_{\mathbb{N}=1}$. Let ω_H be a generator of the invariant differentials of top degree on H over $\mathbb{Z}$, and define $dh_v = |\omega_H|_v$, $dy_v = dg_v/dh_v$. Then

$$\int_{G(\mathbb{A})/H(\mathbb{A})} \varphi(y)dy = \int_{G(\mathbb{R})/H(\mathbb{R})} dy_\infty \cdot \prod_p \int_{G(\mathbb{Q}_p)/H(\mathbb{Q}_p)} \varphi_p(y_p)dy_p. \tag{3.2}$$

Again, $G(\mathbb{Z}_p)$ acts transitively on the embeddings $A \otimes \mathbb{Z}_p \longrightarrow R \otimes \mathbb{Z}_p$ [15, p. 112]. If $p \not| D$ the stabilizer is $H(\mathbb{Z}_p)$. If $p|D$ the stabilizer is the subgroup $(1 + \pi(A \otimes \mathbb{Z}_p))_{\mathbb{N}=1}$ of index $(p+1)$ in $H(\mathbb{Z}_p)$, where $\pi \subset A \otimes \mathbb{Z}_p$ is a uniformizing element. Hence if $p \not| D$ we have:

$$\begin{aligned} \int_{G(\mathbb{Q}_p)/H(\mathbb{Q}_p)} \varphi_p(y_p)dy_p &= \int_{G(\mathbb{Z}_p)} dg_p \Big/ \int_{H(\mathbb{Z}_p)} dh_p \\ &= (1-p^{-6})(1-p^{-2}) \Big/ (1-p^{-2}) \\ &= (1-p^{-6}). \end{aligned} \tag{3.3}$$

If $p|D$ we have

$$\begin{aligned} \int_{G(\mathbb{Q}_p)/H(\mathbb{Q}_p)} \varphi_p(y_p)dy_p &= \int_{G(\mathbb{Z}_p)} dg_p \Big/ \frac{1}{p+1} \cdot \int_{H(\mathbb{Z}_p)} dh_p \\ &= (1-p^{-6})(1-p^{-2}) \Big/ \frac{1}{p+1}(1+p^{-1}) \\ &= (1-p^{-6})(p+1)(1-p^{-1}). \end{aligned} \tag{3.4}$$

Hence

$$\begin{aligned} \prod_p \int_{G(\mathbb{Q}_p)/H(\mathbb{Q}_p)} \varphi_p(y_p)dy_p &= \zeta(6)^{-1} \cdot \prod_{p|D}(p+1)(1-p^{-1}) \\ &= \zeta(6)^{-1} \cdot \frac{\prod_{p|D}(p^2-1)}{D}. \end{aligned} \tag{3.5}$$

Over $\mathbb{R}$, we find (cf. [9], [14, p. 54]).

$$\begin{aligned} \int_{G(\mathbb{R})/H(\mathbb{R})} dy_\infty &= \int_{G(\mathbb{R})} dg_\infty \Big/ \int_{H(\mathbb{R})} dh_\infty \\ &= \frac{(2\pi)^8}{5!} \Big/ \frac{(2\pi)^2}{D}. \end{aligned} \tag{3.6}$$

Hence

$$\#(A \longrightarrow R) = 504 \cdot \prod_{p|D}(p^2 - 1), \tag{3.7}$$

as claimed in Theorem 2.

We illustrate Theorem 2 in a few special cases, using the results of Theorem 1. From Table 2.18 we find that the number of $x = i$ in R with $i^2 = -1$ is 126, and the number of $x = \rho$ in R with $\rho^3 = 1$ but $\rho \neq 1$ is 56. For a fixed i and given $a \in \{-1, 0, 1\}$ we want to count the number $N_i(a)$ of ρ with $\langle i, \rho \rangle = a$. To do this we recall (see e.g. [1, Ch. V]) that the only invariants in degree < 6 of the Weyl group of the E_7 lattice are powers of the norm. It follows that if P is any homogeneous polynomial of degree < 6 on $E_7 \otimes \mathbb{R}$ whose average on the unit sphere vanishes then $\sum_\rho P(\rho) = 0$. Taking for P suitable combinations of powers of the norm and of the linear functional $\eta \mapsto \langle \eta, i \rangle$, we obtain several linear equations in the $N_i(a)$, which together with $\sum_{a=-1}^{1} N_i(a) = 56$ determine them uniquely (and, with more equations than unknowns, provide another check on the computations):

$$N_i(-1) = 12, \quad N_i(0) = 32, \quad N_i(1) = 12$$

for each i. Hence the number of pairs (i, ρ) with $\langle i, \rho \rangle = 1$ is $12 \cdot 126 = 3 \cdot 504$. This is the number of embeddings $A \longrightarrow R$ when $D = 2$, as in this case $A = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\rho + \mathbb{Z}i\rho$ with $\langle i, \rho \rangle = 1$.

Similarly, the number of pairs (i, ρ) with $\langle i, \rho \rangle = 0$ is $32 \cdot 126 = 8 \cdot 504$. This is the number of embeddings $A \longrightarrow R$ when $D = 3$, as in this case $A = \mathbb{Z} + \mathbb{Z}\rho + \mathbb{Z}i + \mathbb{Z}i\rho$ with $\langle i, \rho \rangle = 0$.

Finally, assume $D = 7$ and let A_0 be the ring of integers in $\mathbb{Q}(\sqrt{-7})$. Then $A = A_0 + A_0 i$ with i in $A_0^\perp \subset R$. The lattice $A_0^\perp$ is even, of rank 6 and determinant 7^3. It is isomorphic to the lattice associated with the Klein quartic (as described explicitly by Serre, see [12, 235-6]), and has 42 vectors i with $\langle i, i \rangle = 2$ [4, p. 3]. Hence $\#(A \longrightarrow R) = 42 \cdot \#(A_0 \longrightarrow R) = 42 \cdot 576 = 48 \cdot 504$, as claimed.

When $D \neq 2, 3$ the finite group $\mathrm{Aut}(R)$ acts freely on the embeddings of the maximal order A into R. Since this finite group has order $12096 = 24 \cdot 504$, we obtain the formula:

$$\#\{(A \longrightarrow R)/\mathrm{Aut}(R)\} = \frac{\prod_{p|D}(p^2 - 1)}{24}. \tag{3.8}$$

In particular, when $D = 5$ there is a single orbit of embeddings, and when $D = 7$ there are two orbits. When $D = 2$ (resp. $D = 3$) there is a single orbit, with stabilizer a quaternion group of order 8 (resp. a cyclic group of order 3).

We can now also show that $\Gamma = \mathrm{Aut}(R)$ acts simply transitively on the embeddings into R of the quadratic order of discriminant -23. Since the number of such embeddings equals $\#\Gamma$ it is enough to show that any embedding has trivial stabilizer. If some stabilizer were nontrivial, it would contain an element of Γ of order 2, 3, or 7. But the fixed subrings of these automorphisms are quaternion algebras with $D = 2, 3$ and quadratic orders with $D = -3, -7$, and none of these contains an element of discriminant -23. Similar considerations also yield the transitivity of Γ on embeddings of the quadratic orders of the six remaining discriminants $-3, -4, -7, -8, -11, -15$ for which the number of embeddings, as given in Theorem 1 and tabulated in Table 2.18, divides $12096 = \#\Gamma$.

4. Non-maximal orders.

The second proof of Theorem 1, using Tamagawa measures and the group $G = \mathrm{Aut}(\mathbb{O})$, generalized to quaternion algebras. But the first proof, using the results of Kohnen and Cohen on forms of weight $\frac{7}{2}$, also gives the number of embeddings for non-maximal orders A of $K = \mathbb{Q}(\sqrt{D})$. If A has discriminant $\Delta = D \cdot f^2$, then $A = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{\Delta + \sqrt{\Delta}}{2}$ and the embeddings are counted by the Fourier coefficient $a_{|\Delta|}$ of Θ_L. By Cohen's formula [3, p. 273]:

$$\#(A \longrightarrow R) = -252 \cdot L_\Delta(-2), \tag{4.1}$$

where

$$L_\Delta(s) = L(\varepsilon, s) \cdot \sum_{d|f} \mu(d) \cdot \varepsilon(d) \cdot d^{-s} \cdot \sigma_{1-2s}(f/d) \tag{4.2}$$

is the L-function introduced by Zagier [17, p. 130].

For example, if the conductor f of A is a prime p, then

$$\#(A \longrightarrow R) = -252 \cdot L(\varepsilon, -2) \cdot (1 - \varepsilon(p) \cdot p^2 + p^5). \tag{4.3}$$

Can one also obtain these results on non-maximal orders by the method of Tamagawa measures, and generalize them to non-maximal orders in definite quaternion algebras?

References

[1] N. Bourbaki, *Groupes et algèbres de Lie, Chapitres* 4, 5, *et* 6, Hermann, 1981.

[2] ———, *Groupes et algèbres de Lie, Chapitre* 9: *Groupes de Lie réels compacts*, Hermann, 1982.

[3] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math Ann., **217** (1975), 271-285.

[4] J.H. Conway et al., *ATLAS of finite groups*, Oxford, 1985.

[5] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices, and Groups*, Springer Grundlehren, Vol. 290, 1993.

[6] H.M.S. Coxeter, *Integral Cayley numbers*, Duke Math. J., **13** (1946), 567-578.

[7] H. Davenport, *Multiplicative Number Theory*, Springer, GTM 74, 1980.

[8] N.D. Elkies, *Mock-laminated lattices*, in preparation.

[9] B. Gross, *Groups over* $\mathbb{Z}$, Inventiones Math., **124** (1996), 263-279.

[10] N. Jacobson, *Composition algebras and their automorphisms*, Rend. Palermo, **7** (1958), 55-80.

[11] W. Kohnen, *Modular forms of half-integral weight on* $\Gamma_0(4)$, Math Ann., **248** (1980), 249-266.

[12] B. Mazur, *Arithmetic on curves*, Bull. AMS, **14** (1986), 207-259.

[13] J.-P. Serre, *Résumé des cours de* 1982 – 1983, Œuvres 130 (Vol. III), Springer, 1985.

[14] M.-F. Vigneras, *Arithmétique des Algèbres de Quaternions*, SLN 800, 1980.

[15] A. Weil, *Adeles and Algebraic Groups*, Birkhäuser, 1982.

[16] L. Washington, *Introduction to Cyclotomic Fields*, Springer GTM, **83** (1982).

[17] D. Zagier, *Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields*, In Springer Lecture Notes, 627 (1977), 105-169.

Harvard University
Cambridge, MA 02138 USA
E-mail address: elkies@math.harvard.edu, gross@math.harvard.edu