# COMPUTATIONS OF CYCLOTOMIC LATTICES

C. Batut, H.-G. Quebbemann, R. Scharlau

**Abstract**

We study even modular lattices of level $\ell$ and dimension $2(p-1)$, $p$ prime, which arise from the ideal class group of the $p$-th cyclotomic extension of $\mathbb{Q}(\sqrt{-\ell})$. After giving the basic theory we concentrate on Galois-invariant ideals, obtain computational results on minimal vectors and isometries, and identify several old or new extremal lattices.

## 1 Introduction

In this paper (a sequel to [BB], [Q1], [Q2]) we mainly deal with a family of lattices in euclidean spaces which are related to Craig's $A_{p-1}^{(m)}$. Our lattice $B_{n,\ell}^{(m)}$ has dimension $n = 2(p-1)$, contains the tensor product of $A_{p-1}^{(m)}$ with the ring of integers in $\mathbb{Q}(\sqrt{-\ell})$, and is hermitian-unimodular over this ring (therefore similar to its $\mathbb{Z}$-dual, with determinant $\ell^{p-1}$). Like $A_{p-1}^{(m)}$ it admits a simple description as a cyclotomic ideal which displays the affine-linear group $\mathbb{F}_p^+ \rtimes \mathbb{F}_p^*$ as a group of automorphisms. Our family, however, includes more prominent individuals: there are $E_8 = B_{8,1}^{(1)}$, $K_{12} = B_{12,3}^{(1)}$, $\Lambda_{24} = B_{24,1}^{(2)}$, but also Plesken and Nebe's $[2.M_{12}.2]_{20} = B_{20,2}^{(2)}$ and $[2.M_{22}.2]_{20} = B_{20,7}^{(2)}$ (the latter appears to give the highest "isodual Hermite number" known for $n = 20$, and it is one of two "extremal" lattices of minimum 8 we know). On the other hand, our lattices are harder to analyze than Craig's: we cannot give a general lower bound on the minimum, nor theoretically decide eutaxy when $\ell > 3$. Information on these and related questions will be obtained for $p \leq 29$ by machine computations using PARI.

Part of the work on this paper was done during stays of the second author at the University of Bordeaux to which he expresses his gratitude for its hospitality.

## 2 Unimodular cyclotomic lattices over imaginary-quadratic fields

Let $\ell$ be a square-free positive integer, $K = \mathbb{Q}(\sqrt{-\ell})$, and $\mathcal{O}_K$ the ring of integers in $K$. Given a positive definite hermitian space $(V, h)$ of dimension $k$ over $K$, we also consider it as an inner product space of dimension $n = 2k$ over $\mathbb{Q}$ for

[0] *Key words and phrases:* lattice, integral quadratic form, Craig lattice, hermitian lattice, modular lattice, extremal lattice, isodual Hermite number, cyclotomic ideal.

*1991 Mathematics Subject Classification:* 11E12; 11H55, 11R18, 11-04.

$$x \cdot y = c \operatorname{Tr}_{K/\mathbb{Q}} h(x,y), \quad c = \begin{cases} 1 & \ell \equiv 3 \pmod 4 \\ 1/2 & \text{otherwise} \end{cases} \tag{2.1}$$

Then, if $\Lambda$ is an $\mathcal{O}_K$-lattice on $V$, its hermitian dual lattice $\Lambda_h^*$ is $\sqrt{-\ell}\Lambda^*$, where $\Lambda^*$ denotes the euclidean dual. We shall deal with lattices satisfying

$$\Lambda = \Lambda_h^*, \quad \text{and} \quad x \cdot x \in 2\mathbb{Z} \quad \text{for all} \quad x \in \Lambda. \tag{2.2}$$

(Of course, for $\ell \equiv 3 \pmod 4$ the first condition here implies the second one.) As a euclidean lattice such a $\Lambda$ is even and isometric to $\sqrt{\ell}\Lambda^*$, therefore of determinant $\ell^k$.

Let $p$ be an odd prime not dividing $\ell$, and $\zeta$ a non-trivial $p$-th root of unity over $K$. We put $F = K(\zeta)$ and remark that $[F : K] = p - 1$. Consequently, if $p$ divides the order of the isometry group $\mathrm{Aut}_h \Lambda$ for a lattice $\Lambda$ as above, part of $V$ must be a nonzero $F$-vector space, and therefore $p - 1$ is at most equal to $k$. We shall deal with the case $k = p - 1$, and then can assume (cf. [Fe], Section 9)

$$V = F, \quad h(x,y) = \operatorname{Tr}_{F/K}(\delta x \overline{y}), \quad \Lambda = \mathcal{I} \tag{2.3}$$

where $\delta$ is a totally positive element in $F^+ = F \cap \mathbb{R}$ and $\mathcal{I}$ is a fractional ideal of $F$. Note that $\Lambda_h^* = (\delta \overline{\mathcal{I}} \mathcal{D}_{F/K})^{-1}$ where $\mathcal{D}_{F/K} = (1-\zeta)^{p-2}$ is the different. To satisfy (2.2) we therefore require that

$$p \delta \mathcal{I} \overline{\mathcal{I}} = (1 - \zeta). \tag{2.4}$$

Actually (2.4) is equivalent to (2.2) because the absence of dyadic ramification in $F/F^+$ guaranties that $\Lambda$ is even ([BM], Section 3).

**Proposition 1** *Condition (2.4) can be satisfied (with $\delta \in F^+$ totally positive) if and only if we have*

$$\left(\frac{-\ell}{p}\right) = 1 \tag{2.5}$$

**Proof.** The extension $F/F^+$ is unramified at all finite primes, and so class field theory tells us that the left-hand side of (2.4) is in the kernel of the Artin map. In other words, for (2.4) to hold $(1-\zeta)$ must be decomposed in $F$, and so $p$ decomposed in $K$. Conversely, if this is satisfied, we can write

$$(1 - \zeta) = \mathcal{P}\overline{\mathcal{P}} \ \text{ with a prime ideal } \ \mathcal{P} \ \text{ in } \ \mathcal{O}_F, \tag{2.6}$$

and then (2.4) holds with $\delta = 1/p$ and $\mathcal{I} = \mathcal{P}$. ∎

From now on we assume (2.5) and fix $\mathcal{P}$ as in (2.6). In order to satisfy (2.4) with $\delta = 1/p$, we may also put $\mathcal{I} = \mathcal{J}\overline{\mathcal{J}}^{-1}\mathcal{P}$ where $\mathcal{J}$ is any nonzero fractional ideal of $F$. This will turn out to be already the most general case. Namely, let $cl(\mathcal{J})$ denote the ideal class of $\mathcal{J}$, and $Cl(F)$ the class group; put $G = Gal(F/K)$. The $K$-isometry class of the lattice $\Lambda$ will be denoted by $[\Lambda]$.

**Theorem 1** *If $(V,h,\Lambda)$ is given by (2.3) and (2.4) is satisfied, one up to isometry has $\delta = 1/p$. Furthermore, with this choice of $\delta$, the mapping*

$$cl(\mathcal{J}) \longmapsto [\Lambda], \quad \Lambda = \mathcal{J}\overline{\mathcal{J}}^{-1}\mathcal{P}$$

*gives a bijection between $G\backslash(Cl(F)/\mathrm{im}\, Cl(F^+))$ and the set of all $K$-isometry classes of lattices $\Lambda$ as before.*

**Proof.** This is exactly the same as for the case $\ell = 1$ treated in [Q1], Theorem 3, and will not be repeated here. ■

To produce an explicit family of lattices we shall make use of $G$-invariant ideal classes.

**Proposition 2** *The group $Cl(F)^G$ is generated by $\mathrm{im}\, Cl(K)$ and $cl(\mathcal{P})$. Its order is given by*

$$r = h_K(p-1)/u_K, \quad h_K = \#Cl(K), \quad u_K = \#\mathcal{O}_K^*. \tag{2.7}$$

**Proof.** Let $\sigma$ be a generator of $G$. If $cl(\mathcal{J})$ is $G$-invariant, then $\mathcal{J} = \alpha\mathcal{J}^\sigma$ for some $\alpha \in F$ satisfying $N_{F/K}(\alpha) \in \mathcal{O}_K^*$. The local norm at the ramified prime $\mathcal{P}$ is the $(p-1)$-st power (i.e., trivial) on $\mathbb{F}_p$. This shows that $\mathrm{N}_{F/K}(\alpha) = 1$. Then $\alpha = \beta/\beta^\sigma$ for some $\beta \in F^*$ (Hilbert 90), and $J$ may be changed to become a $G$-invariant ideal. Since only $\mathcal{P}$ and $\overline{\mathcal{P}}$ are ramified in $F/K$, then $\mathcal{J}$ is equivalent to a power of $\mathcal{P}$ times an ideal coming from $K$. The value of $r$ is given by the formula of Takagi and Chevalley in [La], Ch. 13, §4. ■

**Definition.** *For $m = 1, \cdots, r$ let $B_{n,\ell}^{(m)}$ denote the unimodular $\mathcal{O}_K$-lattice given as above by (the class of) $\mathcal{J} = \mathcal{P}^{m-1}$. Explicitly,*

$$B_{n,\ell}^{(m)} = \mathcal{P}^m\overline{\mathcal{P}}^{1-m}, \quad h(x,y) = \frac{1}{p}\mathrm{Tr}_{F/K}\, x\overline{y}. \tag{2.8}$$

The relation $cl(\mathcal{P})^r = 1$ implies that $B_{n,\ell}^{(r+1-m)}$ must be isometric to the complex-conjugate of $B_{n,\ell}^{(m)}$. Therefore, being interested in $B_{n,\ell}^{(m)}$ as a euclidean lattice, we can restrict ourselves to the range

$$1 \le m \le [(r+1)/2]. \tag{2.9}$$

We also note that $\mathcal{P}^m\overline{\mathcal{P}}^{1-m}$ contains the ideal $(1-\zeta)^m$, and the latter is just the lattice $A_{p-1}^{(m)}$ of Craig ([CS], Ch.8) tensored with $\mathcal{O}_K$.

**Theorem 2** *Let $B_{n,\ell}^{(m)}$ be considered as a euclidean lattice in dimension $n = 2(p-1)$. Then it is even, of determinant $\ell^{p-1}$, isometric to $\sqrt{\ell}(B_{n,\ell}^{(m)})^*$, and one has*

$$\min B_{n,\ell}^{(m)} \le 2c \min A_{p-1}^{(m)}, \quad c \text{ as in } (2.1). \tag{2.10}$$

*If $\ell \in \{1,2,3,5,7,11,23\}$, i.e., $k_1 = 24/(1+\ell)$ is integral, also*

$$\min B_{n,\ell}^{(m)} \le 2[n/2k_1] + 2\,. \tag{2.11}$$

**Proof.** Only the last statement is not yet obvious. It uses Fricke modular forms and is a general bound based on [Q2], Theorem 7 (for $\ell = 1$ and 3 see [CS], Ch. 7). ■

One has $\min A_{p-1}^{(m)} \geq 2m$, with conjectural equality when $m \leq (p+1)/4$; cf. [BB], §3. However, only in some special cases does $B_{n,\ell}^{(m)}$ attain the minimum value of $4\,mc$ and the right-hand side in (2.11). The computations reported on in the next section will exemplify this. We are particularly interested in examples which attain the bound (2.11). Such lattices are called *extremal* (after Sloane), and their theta-series are uniquely determined by the theory of modular forms ([Q2]).

# 3 Computational results

**Proposition 3** *Let $a \in \mathbb{Z}$ satisfy $a^2 \equiv -\ell \pmod{p}$, and put $\pi = a - \sqrt{-\ell}$. Then $\mathcal{P} = (1-\zeta,\, \pi)$ satisfies (2.6), and*

$$\mathcal{P}^m \overline{\mathcal{P}}^{1-m} = ((1-\zeta)^m,\, (1-\zeta)^{1-m}\pi) \quad \textit{for } \; 1 \leq m < \frac{p}{2}\,. \tag{3.1}$$

**Proof.** Clearly, this $\mathcal{P}$ satisfies $\mathcal{P}\overline{\mathcal{P}} = (1-\zeta)$. Then

$$\mathcal{P}^m \overline{\mathcal{P}}^{1-m} = (1-\zeta)^{1-m}\mathcal{P}^{2m-1},$$

and it suffices to consider the powers $\mathcal{P}^i$ for $1 \leq i \leq p-1$. Now $(\pi, \overline{\pi}) = (1)$ and, after multiplication by $\pi$,

$$(\pi) = (\pi^2,\, \pi\overline{\pi}) \subset (\pi^2,\, (1-\zeta)^i)\,.$$

Then, by induction, $\mathcal{P}^i = ((1-\zeta)^{i-1}, \pi)(1-\zeta, \pi) = ((1-\zeta)^i, \pi)$. ■

Using (3.1) we obtain $2n$ generators of $B_{n,\ell}^{(m)}$ over $\mathbb{Z}$ (in an obvious integral basis of $F/\mathbb{Q}$). After Hermite reduction of the $(n, 2n)$ coefficient matrix, we arrive at a Gram matrix for this lattice. In the following examples the level will be restricted to the five values $\ell = 1, 2, 3, 5, 7$; always $m$ is restricted by (2.9), (2.7).

**Dimension 12** ($p = 7$). Here $\ell = 3$ and 5 are admissible. In the first case we have $r = 1$ and obtain $B_{12,3}^{(1)} = K_{12}$ as in [BM], §4. In the second case we have $r = 6$ and $m \leq 3$. Actually $B_{12,5}^{(2)}$ and $B_{12,5}^{(3)}$ are extremal (minimum 4) and non-isometric (over $\mathbb{Z}$), with automorphism groups of order $2^5 3^2 7$ and $2^5 3^2 5 \cdot 7$, respectively. It has been shown in the course of the work [SH] that there are exactly two further lattices of minimum 4 in this genus. They are modular and have automorphism groups of order not divisible by 7 (order $2^6 3^4, 2^8 3^4 5$ respectively). [1]

**Dimension 20** ($p = 11$), $\ell = 2$ and 7. For both cases, $r = 5$ and so $m \leq 3$. For $\ell = 2$ again two non-isometric extremal lattices arise of which $B_{20,2}^{(2)} = [2.M_{12}.2]_{20}$ has first occurred in [PN]; also $B_{20,2}^{(3)}$ occurs there, but was known before. (In this case

[1] This result has been obtained independently by G. Nebe at Aachen.

the identifications via Gram matrices were done by G. Nebe.) For $\ell = 7$ we obtain one extremal lattice (minimum 8), namely for $m = 2$; $B^{(3)}_{20,7}$ has minimum 6. We have identified $B^{(2)}_{20,7}$ with $[2.M_{22}.2]_{20}$ of [PN] which was commented on in Section 1.

**Dimension 24** ($p = 13$), $\ell = 1$ and 3. For $\ell = 1$ we have $r = 3$, so $m \leq 2$, and $B^{(2)}_{24,1} = \Lambda_{24}$ as in [Q1]. For $\ell = 3$, the value $r = 1$ excludes extremality.

**Dimension 32** ($p = 17$), $\ell = 1$ and 2. In the first case we have $r = 4$, so $m \leq 2$. Actually $B^{(2)}_{32,1}$ is extremal and not isometric to the ubiquitous $BW_{32}$. The latter, however, arises from a non-invariant ideal class; cf. [Q1]. In the case $\ell = 2$ we have $r = 8, m \leq 4$. No extremal lattice is obtained here (for $m = 2, 3, 4$ the minimum is 4 and the number of minimal vectors is $2^3 7 \cdot 17, 2^3 3^2 17$, $2^3 13 \cdot 17$, respectively).

**Dimension 36** ($p = 19$), $\ell = 2$ and 3. For $\ell = 2$ ($r = 9$, $m \leq 5$) we obtain extremal lattices (minimum 6) when $m = 3, 4, 5$. For $\ell = 3$ ($r = 3$, $m \leq 2$) an extremal lattice would have minimum 8 and improve the sphere packing record. However, $B^{(2)}_{36,3}$ has only minimum 6. Now in this case $h_F = 9$, $h_{F^+} = 1$, and we are very grateful to H. Cohen for computing $Cl(F)$ for us. The group turned out to be cyclic and generated by $cl(\mathcal{Q})$, $\mathcal{Q}$ a prime ideal over 37; but also $\Lambda = \mathcal{Q}\overline{\mathcal{Q}}^{-1}\mathcal{P}$ had minimum 6. (The six ideal classes of order 9 make up two $G$-orbits, and the two lattices are complex-conjugate; so all lattices from Theorem 1 have been considered now.)

**Dimension 44** ($p = 23$), $\ell = 5$ and 7. For $\ell = 5$ we have $r = 22$, so $m \leq 11$, and extremality affords that the minimum be 12. However, computation gives the mysterious sequence of minima shown in Table 1. The last row $\tau^*$ in this table shows the number of minimal vectors, divided by $22 \cdot 23$. For $\ell = 7$ extremality is impossible already by the fact that in this case the extremal modular form contains a negative Fourier coefficient.

| $m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| min | 2 | 4 | 6 | 8 | 8 | 8 | 8 | 8 | 10 | 8 | 4 |
| $\tau^*$ | 1 | 5 | 9 | 11 | 2 | 15 | 3 | 5 | 114 | 8 | 1 |

Table 1: Minimum of $B^{(m)}_{44,5}$

**Dimension 56** ($p = 29$), $\ell = 1, 5$ and 7. For $\ell = 1$ we have $r = 7$, $m \leq 4$. For $m = 2$ and 3 the lattices have minimum 4 and $42 \cdot 28 \cdot 29$, resp. $5 \cdot 28 \cdot 29$ minimal vectors. The lattice $B^{(4)}_{56,1}$ turns out to be extremal. An extremal unimodular lattice in dimension 56 had been obtained previously by combining a construction of Ozeki with the existence of a ternary $[56, 28, 15]$-code; see [Oz], Example 5. We did not try to identify $B^{(4)}_{56,1}$ with some lattice coming from this code construction. For $\ell = 5$, the largest minimum of a lattice $B^{(m)}_{56,5}$ is 10. So these lattices are far from being extremal (min = 16). For $\ell = 7$, the extremal modular form has a negative coefficient.

Finally Table 2 summarizes all extremal $B_{n,\ell}^{(m)}$ for $n \leq 56$. Part of the data also follows from theoretical reasons. For example, the number $\tau$ of minimal vectors is predicted by the extremal modular form, and for $\ell = 1$ and 3 all $B_{n,\ell}^{(m)}$ (no matter if extremal or not) are eutactic because then $\mathcal{O}_K^* \times (\mathbb{F}_p^+ \rtimes \mathbb{F}_p^*)$, and therefore $\operatorname{Aut} B_{n,\ell}^{(m)}$, acts $\mathbb{R}$-irreducibly.

| $n$ | $\ell$ | $m$ | min | $\tau$ | perfect? | eutactic? |
|---|---|---|---|---|---|---|
| 4 | 2 | 1 | 2 | 24 | yes | yes |
| 4 | 5 | 1 | 2 | 6 | no | no |
| 4 | 11 | 1 | 4 | 12 | no | no |
| 4 | 23 | 2 | 6 | 12 | no | no |
| 8 | 1 | 1 | 2 | 240 | yes | yes |
| 12 | 3 | 1 | 4 | 756 | yes | yes |
| 12 | 5 | 2 | 4 | 126 | no | no |
| 12 | 5 | 3 | 4 | 126 | no | no |
| 20 | 2 | 2 | 4 | 3960 | yes | yes |
| 20 | 2 | 3 | 4 | 3960 | yes | yes |
| 20 | 7 | 2 | 8 | 6160 | yes | yes |
| 24 | 1 | 2 | 4 | 196560 | yes | yes |
| 32 | 1 | 2 | 4 | 146880 | yes | yes |
| 36 | 2 | 3 | 6 | 164160 | yes | yes |
| 36 | 2 | 4 | 6 | 164160 | yes | yes |
| 36 | 2 | 5 | 6 | 164160 | yes | yes |
| 56 | 1 | 4 | 6 | 15590400 | yes | yes |

Table 2: Extremal $B_{n,\ell}^{(m)}$ for $n \leq 56$

One might hope for the existence of extremal even unimodular lattices in dimensions $n = 72$ and $n = 80$. Actually $B_{80,1}^{(4)}$ and $B_{80,1}^{(5)}$ remain candidates after LLL reduction, but we are unable to verify that the minimum really is 8. All $B_{72,1}^{(m)}$ have minimum at most 6.

## References


[BB] C. Bachoc et C. Batut, "Etude algorithmique de réseaux construits avec la forme trace", Experim. Math. **1** (1992), 184–190

[BM] E. Bayer-Fluckiger et. J. Martinet, "Formes quadratiques liées aux algèbres semi-simples", J. reine angew. Math. **451** (1994), 51–69

[CS] J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices and groups*, Springer-Verlag, New York 1988

[Fe] W. Feit, "On integral representations of finite groups", Proc. London Math. Soc. **29** (1974), 633–683

[La] S. Lang, *Cyclotomic fields* I *and* II, Springer-Verlag, New York 1990

[Oz] M. Ozeki, "Ternary code construction of even unimodular lattices", in: *Thèorie des nombres - Number Theory*, J.-M. De Koninck et. al. (eds.), Walter de Gruyter, Berlin, New York 1989, 772–784

[PN] W. Plesken and G. Nebe, "Finite rational matrix groups", to appear in Memoirs AMS

[Q1] H.-G. Quebbemann, "Unimodular lattices with isometries of large prime order II", Math. Nachr. **256** (1992), 219–224

[Q2] –, "Modular lattices in euclidean spaces", to appear in J. Number Theory

[SH] R. Scharlau and B. Hemkemeier, "Classification of integral lattices with large class number", Universität Bielefeld, SFB-preprint 94-102.



Christian Batut
Mathématiques
Université Bordeaux I
351, cours de la Libération
33405 Talence Cedex
France

Heinz–Georg Quebbemann
FB 6 Mathematik
Universität Oldenburg
D-26111 Oldenburg
Germany

Rudolf Scharlau
FB Mathematik
Universität Dortmund
D-44221 Dortmund
Germany