Iwasawa-Cohen-Lenstra heuristics

Cornelius Greither

Abstract.

In this note we propose an analog of the well-known Cohen-Lenstra heuristics for modules over the Iwasawa algebra Λ. It turns out that only the analog of the real-quadratic situation leads to a convergent series and hence to potential predictions. We determine the sum of this series, which runs over all isomorphism classes of finite Λ-modules, and we discuss the partial sum that arises by restricting to cyclic Λ-modules. We demonstrate that this subsum is almost as large as the total sum. No attempt is made to test the heuristics numerically.

§ Introduction and background

The classical Cohen-Lenstra heuristics [CL] make predictions about the distribution of class groups. Let us describe the prototypical cases that started the whole development. An odd prime p is fixed, and one lets K vary through the family of all real quadratic fields (case 1) or all imaginary quadratic fields (case 2), looking at the frequency of the event that the p-part $Cl_K\{p\}$ of Cl_K is isomorphic to a given finite abelian p-group G. Of course, the bigger G is, the less "likely" this event should be. But the central discovery of Cohen and Lenstra was that the order of G alone is not decisive; in a nutshell, there is a strong bias against non-cyclic groups. To take the simplest example, it is observed far more frequently that $Cl_K\{p\}$ is cyclic of order p^2 than non-cyclic of that same order. The key to this is that the non-cyclic group of order p^2 has many more automorphisms than the cyclic group of order p^2. More precisely, heuristical arguments show that the likelihood of "$Cl_K\{p\} \cong G$" should

Received November 10 2017.
Revised October 12 2018.
2010 *Mathematics Subject Classification.* 11R23; 13H05.
Key words and phrases. Cohen Lenstra heuristics; Λ-modules; Iwasawa theory.

be proportional to

$$1/(|G| \cdot |\operatorname{Aut}(G)|), \quad \textit{in case 1 (real),}$$

and to

$$1/|\operatorname{Aut}(G)|, \quad \textit{in case 2 (imaginary).}$$

Proven results in this direction are rare to this day, but there is an excellent plausibility test. If these guessed probability distributions are to make any sense, the sum of the above terms over all G modulo isomorphism had better converge to a finite value, say S in case 1 and S' in case 2; this then determines the proportionality factor. We call sums of this type Cohen-Lenstra sums, or CL sums for short. And indeed, at least in case 2 this sum had been calculated long before the CL heuristics came up; Philip Hall [Ha] proved that

$$\frac{1}{S'} = \prod_{k=1}^{\infty}(1 - p^{-k}).$$

The original CL heuristics have been extended in many and various directions, and we will not even try to mention all the main developments. We only select one line of thought. In the original setting, there is no usable Galois action, because one knows to begin with that the action of $\mathrm{Gal}(K/\mathbb{Q})$ (a group of order 2) is totally predictable: the nontrivial automorphism inverts every element of the class group. But one may take, just for example, a fixed abelian p-group Δ and study families of real abelian Δ-extensions $K/\mathbb{Q}$, or of imaginary abelian $\Delta \times \mathbb{Z}/2$-extensions $L/\mathbb{Q}$. One may postulate similar heuristics, where finite abelian p-groups (that is, $\mathbb{Z}_p$-modules) are replaced by finite $\mathbb{Z}_p[\Delta]$-modules. Just as above, certain sums of CL type arise, and in some cases it is possible to calculate them, and to do some modest testing of the resulting heuristics. See [Gr] and [Wi].

The purpose of the present note is to introduce a new twist on this, for whatever it is worth. We replace the group ring $\mathbb{Z}_p[\Delta]$ by the completed group ring $\Lambda = \mathbb{Z}_p[[\Gamma]]$, where $\Gamma \cong \mathbb{Z}_p$ is the pro-p-free group on one generator. This completed group ring plays a central role in Iwasawa theory; the modules over it that come from certain towers of field extensions are called Iwasawa modules.

The question is which terms we should take to form a CL sum for the ring Λ: as in case 1, or as in case 2, or would both make sense? The simple answer is that the case 2 sum

$$\sum_M 1/|\operatorname{Aut}_\Lambda(M)|$$

over all finite Λ-modules M up to isomorphism diverges. This can be deduced easily from Wittmann's results on CL sums for group rings of cyclic order p^n groups, letting n go to infinity, and we will explain this at the end of the next section. As a consequence, let us forget about case 2.

The main result of this note (see Theorem 5 below) shows that the case 1 sum $S_\Lambda = \sum_M 1/(|M||\operatorname{Aut}_\Lambda(M)|)$ does converge. In fact we prove that

$$S_\Lambda = \prod_{k\geq 2}(1-q^k)^{1-k},$$

where we have put $q = 1/p$. We also consider a similar sum that only runs over the cyclic Λ-modules, and relate it to a value of a Kähler zeta function at $s = 2$. It appears that cyclic modules dominate almost as strongly in this new setting as in the classical one. We did not undertake any numerical testing of this new heuristics over Λ, and we are not sure how far one could go. But at least a little positive evidence can be extracted from calculations done by Sumida-Takahashi in 2007 and perhaps also from even earlier results of Kraft and Schoof, as will be explained at the end of the paper.

There is one crude justification of our approach that does come from nature, that is, from Iwasawa modules. In case 1 one should consider totally real fields K, their p-cyclotomic $\mathbb{Z}_p$-extension K_∞/K, and the Iwasawa module $X_K = \text{proj.lim}_n Cl_{K_n}\{p\}$. Here we have Greenberg's conjecture, which states that the Λ-module X_K should always be finite, so our CL sum encompasses the correct class of modules. If on the contrary K is a CM field and we consider the minus part of X_K, which is a very common object to be studied, then the Λ-modules that we get from nature tend to be infinite or zero. This means that the very idea of a heuristic using the inverse order of automorphism groups seems to lead nowhere in the imaginary case.

Acknowledgements: This note is based on a talk given at the conference "Arithmetic statistics and the Cohen-Lenstra heuristics" held in 2016 at the University of Warwick, and I would like to thank the main organizer Alex Bartel for inviting me to speak. I am likewise grateful to the local organizers of the Iwasawa 2017 conference at the University of Tokyo, Masato Kurihara in particular, for encouraging me to submit this note to the Proceedings, even though there was no related talk at that event. Another word of thanks is due to Masato for directing me to the paper [Su] and for suggesting a comparison with the classical case; in fact this led to the discovery and removal of an error in a comment. I am

grateful to René Schoof for pointing out the existence of Paoluzi's thesis (quoted near the end of this paper) and sending me the full text of this unpublished work. Last not least I would like to thank the referee for some very apposite and helpful suggestions concerning the exposition.

§1. Calculating the sum S_Λ

We first fix some notation.

By Λ we will always denote the classical Iwasawa algebra $\mathbb{Z}_p[[T]]$, where p is a fixed prime number, which may be 2. It is well known and very important that Λ is isomorphic to $\mathbb{Z}_p[[\Gamma]]$ with $\Gamma \cong \mathbb{Z}_p$, but this aspect will rarely be needed in our algebraic considerations. The typical notations for Λ-modules and $\mathbb{Z}_p$-modules will be M and G respectively. If nothing else is said, all modules M and G are supposed to be finite.

To give a Λ-module M is equivalent to specifying a pair (G, φ) consisting of a $\mathbb{Z}_p$-module G together with a nilpotent endomorphism φ which describes the action of T on G. Plainly, (G, φ) and (G, ψ) are isomorphic as Λ-modules if and only φ is conjugate to ψ under the group $\mathrm{Aut}(G)$ of $\mathbb{Z}_p$-automorphisms of G. For any Λ-module M, the underlying $\mathbb{Z}_p$-module will be written G_M.

For any module N over a ring R, the notations $\mathrm{End}_R(N)$, $\mathrm{Nil}_R(N)$, $\mathrm{Aut}_R(N)$ will denote, respectively: the ring of R-endomorphisms of N; the subset of $\mathrm{End}_R(N)$ consisting of all nilpotent endomorphisms of N; and the group of R-automorphisms of N. The subscript R will be dropped when context permits. By $\mathrm{nil}_R(N)$ and $\mathrm{aut}_R(N)$ we denote the cardinality of $\mathrm{Nil}_R(N)$ and $\mathrm{Aut}_R(N)$ respectively.

Our main goal is the calculation of the following sum of Cohen-Lenstra type:

$$S_\Lambda = \sum_{M \in \Lambda - mod} \Big(|M| \cdot \mathrm{aut}(M) \Big)^{-1}.$$

Here the sum is of course not over all modules but over all isomorphism classes of (finite!) Λ-modules; aut means aut_Λ. It is clearly possible to rewrite this sum, sorting it by the underlying $\mathbb{Z}_p$-modules:

$$S_\Lambda = \sum_{G \in \mathbb{Z}_p - mod} \sum_{\substack{M \in \Lambda - mod \\ G_M \cong G}} \Big(|M| \cdot \mathrm{aut}(M) \Big)^{-1}.$$

Let us abbreviate the inner sum (over all M with G_M isomorphic to a given G) by S_G. The first step in our calculation is the following lemma.

Lemma 1. *For every $\mathbb{Z}_p$-module G we have*

$$S_G = |G|^{-1} \cdot \frac{\mathrm{nil}(G)}{\mathrm{aut}(G)}.$$

PROOF: For every $\varphi \in \mathrm{Nil}(G)$, let $Z(\varphi) \subset \mathrm{Aut}(G)$ be the centralizer of φ. Then the number of $\psi \in \mathrm{Nil}(G)$ such that $(G,\varphi) \cong (G,\psi)$ is $\mathrm{aut}(G)/|Z(\varphi)|$, and $\mathrm{Aut}_\Lambda(G,\varphi)$ is easily seen to identify with $Z(\varphi)$. Let $\mathrm{Nil}(G)/\mathrm{Aut}(G)$ denote the set of orbits of $\mathrm{Nil}(G)$ under the action of $\mathrm{Aut}(G)$ by conjugation. We therefore obtain:

$$\begin{aligned}
\sum_{\varphi \in \mathrm{Nil}(G)/\mathrm{Aut}(G)} \frac{1}{aut_\Lambda(G,\varphi)} &= \sum_{\varphi \in \mathrm{Nil}(G)} \frac{1}{[\mathrm{Aut}(G) : Z(\varphi)]} \cdot \frac{1}{aut_\Lambda(G,\varphi)} \\
&= \sum_{\varphi \in \mathrm{Nil}(G)} \frac{|Z(\varphi)|}{\mathrm{aut}(G)} \cdot \frac{1}{|Z(\varphi)|} \\
&= \frac{1}{\mathrm{aut}(G)} \sum_{\varphi \in \mathrm{Nil}(G)} 1 \\
&= \frac{\mathrm{nil}(G)}{\mathrm{aut}(G)}.
\end{aligned}$$

Since all Λ-modules M such that $G_M \cong G$ have the form (G,φ), and since for all of them the factor $1/|M|$ equals $1/|G|$, the lemma follows. QED

We now look at the possible $\mathbb{Z}_p$-modules G more closely. We fix a positive integer n, and recall the notation

$$(p)_a = (1-p^{-1})(1-p^{-2})\cdots(1-p^{-a}), \quad a \in \mathbb{N}.$$

Let us recall that there is a canonical bijection between the set of isomorphism classes of abelian groups of order p^n and the set of partitions of n, that is, the set of vectors $(a_1,\ldots,a_k)$ of natural numbers of any length k such that $a_1 + 2a_2 + \cdots + ka_k = n$. The bijection maps such a vector to the group $G = (\mathbb{Z}/p)^{a_1} \oplus \ldots \oplus (\mathbb{Z}/p^k)^{a_k}$. We will need a description of the endomorphisms of such a group G. What we are going to explain now is a very special case of the general fact that Hom commutes with finite direct sums in either argument. Let $m = a_1 + \ldots + a_k$. Then if we think of the elements of G as column vectors of length m with entries in the appropriate rings $\mathbb{Z}/p^i$, every endomorphism φ of G is given as left multiplication by some matrix $A \in \mathbb{Z}^{m,m}$. Now φ may be identified with a "matrix" $(\varphi_{i,j})_{1\le i,j\le k}$ with $\varphi_{i,j} \in \mathrm{Hom}((\mathbb{Z}/p^j)^{a_j}, (\mathbb{Z}/p^i)^{a_i})$. This

corresponds to a partition of A into block matrices $A_{i,j} \in \mathbb{Z}^{a_i,a_j}$, where for all $1 \leq i,j \leq k$, the matrix $A_{i,j}$ represents $\varphi_{i,j}$.

The following observation will be needed in the next lemma. A matrix A composed of block matrices $A_{i,j}$ as just explained defines an endomorphism of $G = (Z/p)^{a_1} \oplus \ldots \oplus (\mathbb{Z}/p^k)^{a_k}$ if and only if all entries of $A_{i,j}$ are multiples of p^{i-j} for all pairs $i > j$.

Lemma 2. *Let $(a_1, \ldots, a_k)$ be a vector of natural numbers. Let*

$$G = (\mathbb{Z}/p)^{a_1} \oplus (\mathbb{Z}/p^2)^{a_2} \oplus \cdots \oplus (\mathbb{Z}/p^k)^{a_k}.$$

Then the following hold:

(a) If the square matrix A of size $m = a_1 + \cdots + a_k$ is a block matrix with k^2 blocks $A_{i,j}$, defining an endomorphism φ of G as explained above, then φ is nilpotent if and only if all the diagonal blocks $A_{i,i}$ of A are nilpotent modulo p^i.

(b) We have the formula

$$\frac{\mathrm{nil}(G)}{\mathrm{aut}(G)} = \prod_{i=1}^{k} p^{-a_i}/(p)_{a_i}.$$

Proof: (a) All the blocks $A_{i,j}$ with $i > j$ (that is, below the diagonal) have coefficients divisible by p^{i-j} as pointed out before the Lemma, and hence all these blocks are congruent to zero modulo p. Clearly φ is nilpotent if and only if A is nilpotent modulo p^k; this in turn is equivalent to saying that the reduction $\bar{A}$ of A modulo p is nilpotent. But in that reduction all blocks below the diagonal have become zero, so it is nilpotent exactly if all blocks $\bar{A}_{i,i}$ on the diagonal are nilpotent.

(b) By a quite similar reasoning we see that if A defines an endomorphism φ, then φ is an automorphism if and only if all blocks on the diagonal are invertible modulo p^i, and again this is the same as saying that all reductions $\bar{A}_{i,i}$ mod p are invertible. Since the non-diagonal blocks do not matter, either for invertibility or for nilpotency, we only have to take the quotient of $N(a_i, p)$, the number of nilpotent $a_i \times a_i$ matrices modulo p, by the number $I(a_i, p)$ of invertible $a_i \times a_i$ matrices modulo p, and multiply those quotients up for $i = 1, \ldots, k$. Here a theorem of Fine and Herstein [FH] comes to the rescue; it says that $N(a_i, p) = p^{a_i(a_i-1)}$. (For a somewhat simpler proof than in [FH], see [Ge].) Since it is well known that $I(a_i, p) = p^{a_i^2}(p)_{a_i}$, the claimed formula follows. QED

This leads to the following intermediary result.

Proposition 3. *If* $G = \bigoplus_{i=1}^{k} (\mathbb{Z}/p^i)^{a_i}$ *as before, then*

$$S_G = p^{-\sum_i (i+1)a_i} \cdot \prod_i (p)_{a_i}^{-1},$$

with the sum and the product running from 1 to k*.*

PROOF: This is a consequence of the preceding two lemmas and the observation that $|G|^{-1} = p^{-\sum_i i a_i}$. QED

We will now take this formula and sum it over all partitions $(a_1, \ldots, a_k)$ with k arbitrary. (The number $n = a_1 + 2a_2 + \ldots + ka_k$ will not appear explicitly any longer.) To avoid duplication, we use formally infinite vectors $\underline{a} = (a_1, a_2, \ldots,)$ with the prescription that they only contain finitely many nonzero entries. This will cover all (finite) $\mathbb{Z}_p$-modules G, and the sum will be the desired quantity S_Λ. In the process, we will need a certain family of infinite sums. We put

$$R(k) = \sum_{b=0}^{\infty} q^{kb}/(p)_b, \quad k = 1, 2, 3, \ldots$$

Then we may state

Proposition 4.

$$S_\Lambda = R(2) \cdot R(3) \cdot R(4) \ldots = \prod_{k \geq 2} R(k).$$

PROOF: From Prop. 3 and the remarks following it we have

$$S_\Lambda = \sum_{\underline{a}} \Big(p^{-\sum_i (i+1)a_i} \cdot \prod_i (p)_{a_i}^{-1} \Big).$$

Here the trivial module $G = 0$ corresponds to the partition $(0, 0, \ldots)$, which does give the correct summand 1 on the right hand. The point is now to process this sum. It is helpful to consider it as a power series in $q = p^{-1}$. This simplifies our notation a bit: now $(p)_b = (1-q)(1-q^2)\cdots(1-q^b)$; and one sees that S_Λ factors as the product

$$\sum_{a_1=0}^{\infty} q^{-2a_1}/(p)_{a_1} \cdot \sum_{a_2=0}^{\infty} q^{-3a_2}/(p)_{a_2} \cdot \cdots.$$

By the definition of the quantities $R(k)$, this simply means that

$$S_\Lambda = R(2) \cdot R(3) \cdot R(4) \ldots = \prod_{k \geq 2} R(k).$$

Convergence of all occurring series is easy to show and we will not write out any details. QED

We now can state and prove our main result.

Theorem 5. *The Iwasawa-Cohen-Lenstra sum S_Λ converges, and we have the equality (recall $q = 1/p$)*

$$S_\Lambda = \prod_{k\geq 2} (1-q^k)^{1-k}.$$

PROOF: From Prop. 4, one sees that it suffices to establish the following equality for all $k \geq 2$:

$$R(k) = \prod_{j\geq k} (1-q^j)^{-1}.$$

Indeed we will establish it for all $k \geq 1$.

Let us begin by calculating the product $R(1)(1-q)$. We find

$$\begin{aligned} R(1)(1-q) &= 1 + \Big(\frac{q}{(p)_1} - q\Big) + \Big(\frac{q^2}{(p)_2} - \frac{q^2}{(p)_1}\Big) + \Big(\frac{q^3}{(p)_3} - \frac{q^3}{(p)_2}\Big) + \cdots \\ &= 1 + \frac{q}{(p_1)}\big(1-(1-q)\big) + \frac{q^2}{(p_2)}\big(1-(1-q)\big) + \cdots \\ &= 1 + \frac{q^2}{(p)_1} + \frac{q^4}{(p)_2} + \frac{q^6}{(p)_3} + \cdots \\ &= R(2). \end{aligned}$$

Quite similar calculations show that $R(2)(1-q^2) = R(3)$, $R(3)(1-q^3) = R(4)$ and so on. The punchline is now that $R(k)$ converges to 1 for $k \to \infty$; indeed it is not hard to show $1 \leq R(k) \leq 1 + cq^k$ for a suitable positive constant c. From this and the backward recursion $R(k)(1-q^k) = R(k+1)$ one can now easily deduce that $R(k) = (1-q^k)^{-1}(1-q^{k+1})^{-1}(1-q^{k+2})^{-1}\cdots$ as claimed.

This finishes the calculation of $R(k)$ as an infinite product, and hence the proof of the theorem. QED

The infinite product in the theorem converges for every prime p. In fact if we think of it as a power series in the real variable q, it has radius of convergence 1. Let us give a few values, to seven decimal places.

p	S_Λ
2	2.8971188
3	1.2947899
5	1.0654427
7	1.0283933
11	1.0100854

To conclude this section, we explain why the case 2 sum S'_Λ (the one without the factor $|M|$ in the denominator) diverges. Recall that

$$S'_\Lambda = \sum_{M \in \Lambda - mod} 1/\operatorname{aut}(M).$$

Now for every n, the group ring $R_n := \mathbb{Z}_p[\Gamma_n]$ is an epimorphic image of Λ, with Γ_n denoting the cyclic group of order p^n. (Here for once we use the identification $\Lambda = \mathbb{Z}_p[[\Gamma]]$.) This implies of course that S'_Λ cannot be smaller than the corresponding sum S'_{R_n}. But Wittmann [Wi] proved that $S'_{R_n} = {S'}^{n+1}$, where S' is the classical CL sum for the ring $\mathbb{Z}_p$, and in particular $S' > 1$. Since we may choose n as large as we want, it follows that $S'_\Lambda = +\infty$.

§2. Cyclic Λ-modules and a connection with Kähler's zeta function

We define a variant of S_Λ as follows. The convention that all modules are assumed finite is still in force. Define

$$S_{\Lambda,c} = \sum_{\substack{M \in \Lambda - mod \\ M \text{ cyclic}}} \Big(|M| \cdot \operatorname{aut}(M)\Big)^{-1}.$$

Of course we have $S_{\Lambda,c} \le S_\Lambda$, and the inequality is strict, since there exist finite non-cyclic Λ-modules. It is our goal to compare the two quantities, and to link the new quantity with an object that was studied a long time ago and is now more or less forgotten. By this we mean Kähler's zeta function $\tilde{\zeta}_R(s) = \sum_I [R : I]^{-s}$, where R is any commutative ring and the sum is over all ideals of finite index. (Warning: It may very well happen that for a given ring R, this sum diverges for every $s \in \mathbb{R}$.)

Every nonzero cyclic Λ-module M is (up to isomorphism) of the form $M = \Lambda/I$ for a uniquely determined ideal I contained in the radical $\mathfrak{m} = (p, T)$ of Λ. We have $\operatorname{Aut}_\Lambda(\Lambda/I) = (\Lambda/I)^\times$. Since $\Lambda/\mathfrak{m} = \mathbb{F}_p$ and an element of Λ/I is a unit precisely if its image in $\mathbb{F}_p$ is nonzero, we find

that $\mathrm{aut}(M) = \frac{p-1}{p}|M|$ for all nonzero cyclic modules M. This permits to link up $S_{\Lambda,c}$ with a value of a Kähler zeta function as follows.

Proposition 6. *(a)* $S_{\Lambda,c} = 1 + \frac{p}{p-1}\big(\tilde{\zeta}_\Lambda(2) - 1\big)$.

(b) Using the standard notation $(p)_\infty = \prod_{k=1}^{\infty}(1-q^k)$*, we have the equality*

$$S_{\Lambda,c} = 1 + (p)_\infty - \frac{1}{1-q}.$$

Proof: (a) We calculate as follows.

$$\begin{aligned} S_{\Lambda,c} &= 1 + \sum_{0\neq M \text{ cyc.}} |M|^{-1}\,\mathrm{aut}(M)^{-1} \\ &= 1 + \frac{p}{p-1}\sum_{0\neq M \text{ cyc.}} |M|^{-2} \\ &= 1 + \frac{p}{p-1}\Big(\sum_I [\Lambda : I]^{-2} - 1\Big). \end{aligned}$$

The last sum runs over all ideals I in Λ of finite index. This sum is a value of a Kähler zeta function; indeed we have

$$S_{\Lambda,c} = 1 + \frac{p}{p-1}(\tilde{\zeta}_\Lambda(2) - 1)$$

as claimed.

(b) Berndt has given the following formula for real $s > 1$, see [Be], or p.874 in [Ka]:

$$\tilde{\zeta}_\Lambda(s) = \Big((1-q^s)(1-q^{2s-1})(1-q^{3s-2})\cdots\Big)^{-1}.$$

In particular this gives

$$\tilde{\zeta}_\Lambda(2) = \big((1-q^2)(1-q^3)(1-q^4)\cdots\big)^{-1} = 1/\prod_{k\geq 2}(1-q^k).$$

If we plug this into the formula for $S_{\Lambda,c}$ given in part (a) and simplify a little, we obtain the claimed equality. QED

If we now compare the resulting power series for $S_{\Lambda,c}$ with the power series that gives S_Λ, we find that both begin with

$$1 + q^2 + 2q^3 + 4q^4 + 6q^5.$$

The degree 6 terms are $10q^6$ and $12q^6$, respectively. We guess that for every monomial q^k, the coefficient in $S_{\Lambda,c}$ is dominated by the coefficient

in $S_{\Lambda,c}$, and verified this by PARI up to degree 50, but we do not have a proof. Anyway, the difference between these two sums counting all modules, and cyclic modules respectively, is $2q^6 + O(q^7)$.

It is perhaps interesting to compare this with the classical heuristic, that is, with the corresponding sums $S_{\mathbb{Z}_p}$ and $S_{\mathbb{Z}_p,c}$. The former sum is known to be equal to the inverse of $\prod_{k=2}^{\infty}(1-q^k)$, and the latter is easily calculated; its value is $1 + (q^2 + q^4 + q^6 + \ldots)/(1-q)$. The difference between the two series turns out to be $q^6 + O(q^7)$; note that the coefficient at q^6 is now 1. This can be interpreted as follows. The probability that the p-part A of the class group of a totally real field K is not cyclic is predicted to be, very roughly, half the probability that the corresponding Iwasawa module X attached to K_∞ is not cyclic over Λ. If we restrict ourselves to the classical case where K is real quadratic, and $p > 2$, then we have a surjection $X \to A$, so A non-cyclic *implies* X non-cyclic, but not vice versa. So our heuristics seem to pass at least a naive and crude comparison with the classical case, and this may be regarded as a small plausibility test.

We repeat the table given above, now with the values of $S_{\Lambda,c}$ included.

p	S_Λ	$S_{\Lambda,c}$
2	2.8971188	2.4627465
3	1.2947899	1.2853123
5	1.0654427	1.0652136
7	1.0283933	1.0283686
11	1.0100854	1.0100840

The table plainly shows that except for $p = 2$ the values in the middle and right hand column are very close to each other; this means that almost the entire Iwasawa-Cohen-Lenstra sum comes from cyclic Λ-modules, even though, as explained in the previous paragraph, non-cyclic Λ-modules should be somewhat more frequent than non-cyclic $\mathbb{Z}_p$-modules in the classical case. We note that in the classical case the observed scarcity of non-cyclic modules occurring in nature (as class groups) may well have led to the Cohen-Lenstra heuristics in the first place. Unfortunately we do not have sufficiently many observations (yet) in the setting of Λ-modules considered here, but the "guess" induced by the heuristics is that Iwasawa modules X_K attached to the cyclotomic $\mathbb{Z}_p$-extension of a totally real field K should only rarely be non-cyclic as Λ-modules.

As it happens, there does exist some evidence for our heuristics in the literature. We are referring to the papers [Su] of Sumida-Takahashi and [KS] of Kraft and Schoof; let us discuss them in turn.

In [Su] the author considers a doubly indexed family of fields $K = K_{f,p} = \mathbb{Q}(\sqrt{-f}, \zeta_p)^+$; the prime p ranges through $5 \leq p \leq 100000$, and $-f$ ranges through the 62 fundamental discriminants with $1 < f < 200$. It is shown by calculation that the Iwasawa module X is cyclic in all cases considered. For more detail, see Prop. 2 in that paper. Most of the time, the module X_K is zero or $\mathbb{Z}/p$, and in one instance we have $X = \mathbb{Z}/p^2$. Thus, cyclicity over Λ is quite obvious. To appraise these findings in the light of our heuristics, remember it predicts that for a given p and varying totally real fields K the probability that $X = X_K$ is not cyclic is something like $2p^{-6}$. Hence, if we take 62 fields for one prime p, we should have a chance of roughly $124p^{-6}$ of observing one non-cyclic X. If we sum this quantity over $5 \leq p \leq 100000$, we obtain a total chance of 0.0090947, in other words, less than one per cent. Hence the fact that all modules in this range were found to be cyclic by Sumida-Takahashi is in line with our heuristics. The preceding arguments should not be taken too seriously, since the degree of the fields K considered depends on p, and we think that in an experimental study focussed on our heuristics this should be avoided.

In contrast with [Su], the paper [KS] considers only a single prime, that is $p = 3$, and the family of real quadratic fields $K = \mathbb{Q}(\sqrt{f})$, where f ranges through the fundamental discriminants less than 10000, with the important restriction that $f \not\equiv 1$ modulo 3. It is not very difficult to deduce from Table 5.2 in [KS] that X_K is always cyclic as a Λ-module. Looking at our heuristics, one might have expected non-cyclic X in maybe 0.6 per cent of all cases; but probably the condition $f \not\equiv 1$ modulo 3 introduces a bias, and we perhaps also have a phenomenon of "small numbers". From the unpublished thesis [Pa] of M. Paoluzi one can extract that for example the choice $f = 32009$ leads to a non-cyclic Λ-module X of order 27.

After discussing this numerical material, let us conclude by saying that in our opinion, many more tests on various classes of fields would be necessary in order to get a better understanding of how reasonable our heuristical predictions are.

References

[Be] R. Bernd, *Über die Konvergenz einer Zetareihe eines Stellenrings,* PhD thesis, Universität Hamburg 1969

[CL] H. Cohen, H. W. Lenstra, Heuristics on class groups of number fields, *Number Theory Noordwijkerhout 1983,* 33-62, LNM **1068,** Springer 1984

[FH] N. J. Fine and I. N. Herstein, The probability that a matrix be nilpotent, *Illinois J. Math.* **2** (1959), 499-504

[Ge] M. Gerstenhaber, On the number of nilpotent matrices with coefficients in a finite field, *Illinois J. Math.* **5** (1961), 330-333

[Gr] C. Greither, Galois-Cohen-Lenstra heuristics, *Acta Math. et Inf. Univ. Ostraviensis* **8** (2000), 33-43

[Ha] P. Hall, A partition formula connected with Abelian groups, *Comment. Math. Helv.* **11** (1938-39), 126-129

[Ka] E. Kähler, *Mathematische Werke,* edited by R. Berndt and O. Riemenschneider, Walter de Gruyter 2003

[KS] J. Kraft and R. Schoof, Computing Iwasawa modules of real quadratic number fields, *Compositio Math.* **97** (1995), 135-155; Erratum *Compositio Math.* **103** (1996), 241

[Pa] M. Paoluzi, *La congettura di Greenberg per campi quadratici reali,* PhD thesis, Università di Roma La Sapienza 2002

[Su] H. Sumida-Takahashi, Computation of the p-part of the ideal class group of certain real abelian fields, *Math. Comp.* **76** (2007), 1059-1071

[Wi] C. Wittmann, Cohen-Lenstra sums over local rings, *J. Théor. Nombres Bordeaux* **16** (2004), 817-838.

Fakultät INF
Universität der Bundeswehr München
85577 Neubiberg, Germany

E-mail address: cornelius.greither@unibw.de