Vandiver's Conjecture via K-theory

Summer School on Cyclotomic fields, Pune, June 7-30, 1999

Eknath Ghate

1 Introduction

The purpose of this note is to describe some recent work by Soulé [6] on Vandiver's conjecture[1] which uses K-theory.

Let us start by recalling the conjecture. The letter p will always denote an odd prime in what follows.

Conjecture 1 (Vandiver's Conjecture) *Let h^+ denote the class number of the maximal totally real subfield $\mathbb{Q}(\zeta_p)^+$ of $\mathbb{Q}(\zeta_p)$. Then $p \not| \, h^+$.*

At the outset, we should perhaps remind the reader that if p is a 'Vandiver prime', that is an odd prime for which Vandiver's conjecture holds, then much of the theory of the p^{th}-cyclotomic field becomes much 'easier'. For instance, for such p, the proof of the main conjecture is routine (see Theorem 10.16 of [8]).[2]

Here is another example, for which we will need some notation. Let

$$\omega : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p)^\times$$

denote the Teichmuller character. Recall that ω is the canonical character of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ given by the formula

$$\zeta_p^\sigma = \zeta_p^{\omega(\sigma)},$$

[1] Although Conjecture 1 is attributed to Vandiver, it apparently was already stated by Kummer in a letter to Kronecker in the middle of the 19th century (see the Remark on page 158 of [8]).

[2] The main conjecture was established independently of Vandiver's conjecture by Mazur and Wiles [3] by studying the reductions of modular curves. An alternative proof was given by Kolyvagin and Rubin (see [5], or Chapter 15 of [8]), using the more elementary, but ingenious, method of Euler systems.

for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Let σ_a denote the pre-image of $[a] \in (\mathbb{Z}/p)^\times$ under ω.

It will be convenient to regard ω as a p-adic object as follows. Note that $(\mathbb{Z}/p)^\times$ is isomorphic to μ_{p-1}, the group of $(p-1)^{\text{st}}$ roots of 1. By Hensel's lemma, $\mu_{p-1} \subset \mathbb{Z}_p^\times$. Thus we may regard ω as a character

$$\omega : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{Z}_p^\times \subset \mathbb{Z}_p.$$

Let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$. By using a system of orthogonal idempotents of $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$, we may decompose A into 'eigenspaces' for the natural action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ on A (see section 6.3 of [8]):

$$A \quad = \quad \bigoplus_{i=0}^{p-2} A_i,$$

with $A_i = \{a \in A \,\big|\, \sigma(a) = \omega^i(\sigma)a, \text{ for all } \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\}$.

Let $B_k \in \mathbb{Q}$ denote the k^{th} Bernoulli number, and v_p denote the normalized p-adic valuation of $\mathbb{Q}_p$, with $v_p(p) = 1$. We have[3]:

Theorem 1 *(Herbrand-Ribet) Let i be an odd integer with $1 \leq i \leq p-2$. Then*

$$A_i \neq 0 \iff v_p(B_{p-i}) > 0.$$

For i as in Theorem 1 above, we have (see Corollary 5.15 of [8]):

$$B_{1,\omega^{-i}} \equiv \frac{B_{p-i}}{p-i} \ (\mathrm{mod}\ p),$$

where[4]

$$B_{1,\omega^{-i}} := \frac{1}{p} \sum_{a=1}^{p-1} a\omega^{-i}(\sigma_a) \in \mathbb{Z}_p.$$

Thus the following theorem is a refinement of the Herbrand-Ribet theorem[5]:

[3] See the lectures of Katre and Khare in these proceedings, as well as [8], for various proofs of Theorem 1.

[4] The fact that $B_{1,\omega^{-i}}$ lies in $\mathbb{Z}_p$ and not just $\mathbb{Q}_p$ is forced on us by Theorem 2.

[5] Theorem 2 is a consequence of the main conjecture.

Theorem 2 *(Mazur-Wiles) Let i be an odd integer with $1 \leq i \leq p-2$. Then*

$$\mathrm{card}(A_i) = p^{m_i},$$

where $m_i = v_p(B_{1,\omega^{-i}})$.

However, even more is conjectured to be true:

Conjecture 2 *(Iwasawa) When i is odd, $A_i \xrightarrow{\sim} \mathbb{Z}/p^{m_i}$ is cyclic.*

As it turns out (see Corollary 10.15 of [8]), Iwasawa's conjecture is true when p is a Vandiver prime.

The above discussion shows that it is more than simply a matter of curiosity to investigate the validity of Vandiver's conjecture. Numerically, it has been checked that all $p \leq 4 \times 10^6$ are Vandiver primes. However, apparently, this is not sufficient evidence for one to believe that Vandiver's conjecture holds for *all* p. Indeed, a heuristic argument of Washington (see the Remark on page 158 of [8]) shows that the exceptions to Vandiver's conjecture are very rare: the number of exceptions one expects in the range $3 \leq p \leq 4 \times 10^6$ is only 1.36....!

Let us now rephrase Conjecture 1 in a form that will render it more manageable. It is an exercise to check that it is equivalent to the following:

Conjecture 3 (Vandiver's Conjecture) *Let p be an odd prime. Then $A_i = 0$, for all even integers i with $0 \leq i \leq p-3$.*

To place things in context, let us recall that it is well known that $A_0 = A_1 = 0$ and that, moreover, when i is odd, $A_i = 0 \iff p \not| B_{p-i}$ (Herbrand-Ribet theorem). Thus Vandiver's Conjecture says that, on the other hand, when i is even, A_i always vanishes!

As mentioned already, in this note we would like to describe recent work by Soulé on Vandiver's conjecture which uses K-theory.

The story starts with a pretty result of Kurihara [2], who proved that the 'top' even eigenspace always vanishes:

Theorem 3 *(Kurihara) $A_{p-3} = 0$.*

The idea of Kurihara's proof is to note that there is a surjective map

$$K_4(\mathbb{Z}) \otimes \mathbb{Z}/p \to A_{p-3}, \tag{1}$$

and that $K_4(\mathbb{Z})$ is not too big.[6] Last year Soulé [6] was able to extend Kurihara's result. He showed that if n is small (and odd) compared to p then $A_{p-n} = 0$. More precisely, he showed:

Theorem 4 *(Soulé) Assume $n > 1$ is odd. If $\log p > n^{224n^4}$, then*

$$A_{p-n} = 0.$$

The basic idea of Soulé's proof is very similar to Kurihara's. He notes that the 'Chern map' (of which (1) above is a special case):

$$K_{2n-2}(\mathbb{Z}) \otimes \mathbb{Z}/p \to A_{p-n} \tag{2}$$

is surjective. On the other hand the finite abelian group $K_{2n-2}(\mathbb{Z})$, is (essentially) the $(2n-2)^{\text{th}}$ homology group of $SL_N(\mathbb{Z})$ for N large. Classical Voronoi 'reduction theory' gives an explicit cell decomposition of the compactification of the locally symmetric space attached to $SL_N(\mathbb{Z})$. With this in hand, Soulé now implements the following simple remark of Gabber: one may bound the torsion in the homology of a finite CW-complex X purely in terms of data associated with the cellular chain complex $C_.(X)$ of X, such as the number of cells of a fixed degree and the number of faces of each cell. This yields an explicit upper bound for the primes p dividing the order of $K_{2n-2}(\mathbb{Z})$: this is the bound that appears in the statement of Theorem 4 above.

Note that because of the inherent surjectivity of the map (2), the Soulé-Kurihara method has natural limitations: one can only expect it to yield rough results such as Theorem 4 above. On the other hand, as far as we are aware, Theorems 3 and 4 are really the first results towards Vandiver's conjecture of a general nature.

I would like to thank Dinesh Thakur for encouraging me to write up these notes, and V. Srinivas for his comments on a first draft.

2 A quick introduction to K-theory

Let R be a commutative ring with 1. In this section we will introduce the K-groups $K_i(R)$ ($i \geq 0$) attached to R, and describe some of their properties

[6] At the time that Kurihara wrote [2] it was known that $K_4(\mathbb{Z})$ is a finite abelian group whose p primary components were 0, for $p \neq 2, 3$. This was enough to deduce Theorem 3. However recently Rognes has shown that in fact $K_4(\mathbb{Z}) = 0$.

when R is the ring of integers of a number field. References for some of the material described here are Srinivas' book [7] (especially Chapters 1 and 2), and Rosenberg's book [4].

2.1 $K_0(R)$

Here we simply recall the definition of $K_0(R)$. Let $\mathcal{F}$ denote the free abelian group on isomorphism classes of projective R-modules, and let $\mathcal{R}$ denote the subgroup generated by the elements

$$[P \oplus Q] - [P] - [Q],$$

where P and Q are projective R-modules, and [ ] denotes an isomorphism class. Then we set

$$K_0(R) = \mathcal{F}/\mathcal{R}.$$

2.2 Classifying spaces

To introduce the higher K-groups we will need the notion of a classifying space of a discrete group G, which we introduce now.

It is a fact that if G is a group, regarded as a discrete topological group, then there exists a contractible CW-complex X on which G acts freely and cellularly (so properly discontinuously), so that the quotient X/G is a CW-complex (see Theorem 5.1.15 of [4] for an explicit construction of X). We now make the:

Definition 1 *The* classifying space of G *is the quotient space* $BG := X/G$.

It is a fact that BG is well defined up to homotopy equivalence (Theorem 5.1.5. of [4]). Also BG is a $K(G, 1)$-space (see Corollary 5.1.25 of [4]). That is, it is a connected space with

$$\pi_1(BG, x) = G \text{ and } \pi_m(BG, x) = 0, \text{ for } m > 1.$$

Here x is a base point, which we will drop from the subsequent notation.

2.3 The plus construction

Let $\mathrm{GL}_n(R)$ denote the ring of invertible $n \times n$ matrices with entries in R. Then $\mathrm{GL}_n(R) \subset \mathrm{GL}_{n+1}(R)$ via the embedding

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $\mathrm{GL}(R) = \lim_{n\to\infty} \mathrm{GL}_n(R)$, where the limit is taken with respect to these embeddings.

Regard $\mathrm{GL}(R)$ as a topological group with the discrete topology, and let $\mathrm{BGL}(R)$ denote the classifying space of $\mathrm{GL}(R)$. Recall that $\mathrm{BGL}(R)$ is a $K(\mathrm{GL}(R), 1)$ space: i.e. $\mathrm{BGL}(R)$ is a connected space with $\pi_1(\mathrm{BGL}(R)) = \mathrm{GL}(R)$, and $\pi_m(\mathrm{BGL}(R)) = 0$, for $m > 0$.

Now one constructs another space $\mathrm{BGL}(R)^+$ from $\mathrm{BGL}(R)$ by attaching two and three cells. This process is called the plus construction, and is described on page 19 of [7]. Here we will be content in describing some of the properties of $\mathrm{BGL}(R)^+$, that we summarize in the following theorem:

Theorem 5 *1. Let* $\mathrm{E}(R)$ *denote the subgroup of* $\mathrm{GL}(R)$ *generated by the elementary matrices (at finite level, these matrices are just* $n \times n$ *matrices with diagonal entries equal to 1 and at most one non-zero off-diagonal entry). Then* $\mathrm{E}(R)$ *is the commutator subgroup of* $\mathrm{GL}(R)$*, and is a perfect normal subgroup of* $\mathrm{GL}(R)$*. Moreover,*

$$\pi_1(\mathrm{BGL}(R)^+) = \mathrm{GL}(R)/\mathrm{E}(R).$$

2. For each $m \geq 0$ *we have*

$$\mathrm{H}_m(\mathrm{BGL}(R)^+, \mathbb{Z}) = \mathrm{H}_m(\mathrm{BGL}(R), \mathbb{Z}) = \mathrm{H}_m(\mathrm{GL}(R), \mathbb{Z}).$$

2.4 Higher K-groups

We may now give (one of) Quillen's definition's of the higher K-groups of R:

Definition 2 *For each* $m \geq 1$*, set* $K_m(R) := \pi_m(\mathrm{BGL}(R)^+)$*.*

We note that in particular $K_m(R)$ is an abelian group for $m \geq 0$.

2.5 K-theory of rings of integers

Let F be a number field, and let $\mathcal{O}_F$ denote the ring of integers of F. The next theorem shows that one might expect that the higher K-groups of $\mathcal{O}_F$ should contain much interesting information about F:

Theorem 6 *1. $K_0(\mathcal{O}_F) = \mathbb{Z} \oplus Cl(F)$, where $Cl(F)$ denote the class group of F.*

2. $K_1(\mathcal{O}_F) = \mathcal{O}_F^\times$, the group of units of $\mathcal{O}_F$.

Quillen had shown that, in general, the abelian groups $K_m(\mathcal{O}_F)$ are finitely generated. Their ranks were subsequently computed by Borel [1]:

Theorem 7 *(Borel) Let r_1 (respectively r_2) denote the number of embeddings of K into $\mathbb{R}$ (respectively $\mathbb{C}$). Then the ranks of $K_m(\mathcal{O}_F)$ are as follows:*

$$\mathrm{rk}(K_0(\mathcal{O}_F)) = 1, \quad \mathrm{rk}(K_1(\mathcal{O}_F)) = r_1 + r_2 - 1 \quad \text{and}$$

$$\mathrm{rk}(K_m(\mathcal{O}_F)) = \begin{cases} r_1 + r_2 & \text{if } m = 4i+1 > 1, \\ r_2 & \text{if } m = 4i+3 > 1, \\ 0 & \text{if } m = 2i. \end{cases}$$

On the other hand, almost nothing is known about the torsion subgroups of $K_m(\mathcal{O}_F)$. The following theorems summarizes our current state of ignorance when $F = \mathbb{Q}$.

Theorem 8 *The K-theory of $\mathbb{Z}$ computed to date is: $K_0(\mathbb{Z}) = \mathbb{Z}$, $K_1(\mathbb{Z}) = \mathbb{Z}/2$, $K_2(\mathbb{Z}) = \mathbb{Z}/2$, $K_3(\mathbb{Z}) = \mathbb{Z}/48$, and $K_4(\mathbb{Z}) = 0$.*

2.6 The Hurewicz map

For computational purposes, we will need the Hurewicz maps ($m \geq 1$)

$$\text{Hurewicz} : \pi_m(X) \to \mathrm{H}_m(X, \mathbb{Z}),$$

which are homomorphisms from the homotopy groups of a CW-complex X, to the homology groups of X. Roughly, they are defined as follows (see Appendix A of [7] for further details). A typical element $[f]$ of $\pi_m(X)$ is a homotopy class of a continuous map $f : S_m \to X$, where S_m is the m-dimensional sphere. We have an induced map

$$\mathrm{H}_m(f) : \mathrm{H}_m(S_m, \mathbb{Z}) \to \mathrm{H}_m(X, \mathbb{Z}),$$

and we set $\mathrm{Hurewicz}([f]) = \mathrm{H}_m(f)(\omega)$ where ω is the standard generator (corresponding to a choice of orientation) of $\mathrm{H}_m(S_m, \mathbb{Z}) = \mathbb{Z}$.

It is not true in general that the Hurewicz maps are isomorphisms, though this does hold for $m \geq 2$ when X is $(m-1)$-connected, that is, when $\pi_j(X) = 0$ for $j \leq m-1$. When $m = 1$, and X is 0-connected, that is when X is connected, the kernel of the Hurewicz map is just the commutator subgroup of $\pi_1(X)$, and in this case the Hurewicz map gives an explicit isomorphism $\pi_1(X)^{\mathrm{ab}} = \mathrm{H}_1(X, \mathbb{Z})$.

In our situation the Hurewicz map is a homomorphism (cf. Theorem 5):

$$\mathrm{Hurewicz} : K_m(\mathcal{O}_F) = \pi_m(\mathrm{BGL}(\mathcal{O}_F)^+) \to \mathrm{H}_m(\mathrm{GL}(\mathcal{O}_F), \mathbb{Z}).$$

This map is not injective[7], but when $F = \mathbb{Q}$ we have the following (see the remarks in Section 2.5 of [6] and the references there):

Proposition 1 *The kernel of*

$$\mathrm{Hurewicz} : K_m(\mathbb{Z}) \to \mathrm{H}_m(\mathrm{GL}(\mathbb{Z}), \mathbb{Z})$$

is a finite abelian group, with non-zero p-primary components only for p smaller than the integral part of $(m+1)/2$.

3 The Chern map

We now show how the map (2) is constructed. Unfortunately, we will have to be somewhat brief since we ourselves do not understand some of the details.

Let X be a scheme over $\mathbb{Z}[\frac{1}{p}]$, and let

$$\mathrm{H}^k_{\mathrm{et}}(X, \mathbb{Z}_p(n)) \tag{3}$$

[7] Srinivas has remarked that the kernel of the Hurewicz map for $\mathrm{BGL}(R)^+$ is always a torsion group. In fact it is a theorem of Milnor and Moore that the kernel of Hurewicz is torsion when X is an H-space. We refer the reader to Appendix A of [7] for the definition and properties of H-spaces.

denote the étale cohomology groups of X with coefficients in the n^{th} Tate twist of the group of p-adic integers.

Let us explain what we mean by this in the situation that matters to us, namely when $X = \mathrm{Spec}(\mathbb{Z}[1/p])$. We need some notation. Let $\mathbb{Q}^{p,\infty}$ denote the maximal extension of $\mathbb{Q}$ unramified outside p and ∞. Let ϵ denote the cyclotomic character

$$\epsilon : \mathrm{Gal}(\mathbb{Q}^{p,\infty}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times \subset \mathbb{Z}_p.$$

Then $\mathbb{Z}_p(n)$ is the $\mathrm{Gal}(\mathbb{Q}^{p,\infty}/\mathbb{Q})$-module $\mathbb{Z}_p$ with action:

$$g \cdot a = \epsilon(g)^n a,$$

where $g \in \mathrm{Gal}(\mathbb{Q}^{p,\infty}/\mathbb{Q})$ and $a \in \mathbb{Z}_p$. Then, when $X = \mathbb{Z}[1/p]$, the group (3) above is nothing but the continuous Galois cohomology group

$$\mathrm{H}^k(\mathrm{Gal}(\mathbb{Q}^{p,\infty}/\mathbb{Q}), \mathbb{Z}_p(n)).$$

One may also speak of the K-theory of the scheme X. The exact definition[8] does not concern us here, since when $X = \mathrm{Spec}(R)$ is affine (as a scheme over $\mathrm{Spec}(\mathbb{Z}[1/p])$, then $K_m(X) = K_m(R)$. There is also the notion of the étale K-groups, $K_m^{\text{et}}(X)$, of X, whose definition I don't know. However, I do know that these are $\mathbb{Z}_p$-modules which come equipped with maps

$$K_m(X) \otimes \mathbb{Z}_p \to K_m^{\text{et}}(X). \tag{4}$$

Finally Dwyer and Friedlander have shown that these gadgets are connected by an Atiyah-Hirzebruch type[9] spectral sequence:

$$E_2^{rs} = \mathrm{H}^r_{\text{et}}(X, \mathbb{Z}_p(-s/2)) \Longrightarrow K^{\text{et}}_{-r-s}(X),$$

or re-indexing (set $r = k$, and $s = -2n$)

$$E_2^{kn} = \mathrm{H}^k_{\text{et}}(X, \mathbb{Z}_p(n)) \Longrightarrow K^{\text{et}}_{2n-k}(X).$$

We now have the following

[8] See Chapters 3 and 4 of [7] if you are interested in the definition!

[9] The name is because it is the exact analog of Atiyah-Hirzebruch spectral sequence connecting the singular homology of a space X with the topological K-theory of X.

Theorem 9 *Say $X = \mathbb{Z}[1/p]$. Assume that $n > 0$ and p is odd. Then*

$$\mathrm{H}^k_{\text{et}}(X, \mathbb{Z}_p(n)) = 0,$$

unless $k = 1$ or 2.

Now set $m = 2n-k$. Then Theorem 9 shows that when $X = \mathrm{Spec}(\mathbb{Z}[1/p])$, the spectral sequence above degenerates, and so there are surjective maps:

$$K^{\text{et}}_m(X) \twoheadrightarrow \mathrm{H}^k_{\text{et}}(X, \mathbb{Z}_p(n)), \tag{5}$$

for $m = 2n-1$ or $2n-2$.

We are interested in the case when $k = 2$, and $n > 1$ is odd. In this case $m = 2n-2$, and in particular m is even. By Theorem 7, we see that $K_m(\mathbb{Z})$ is a finite abelian group. Also we have the following (see Section 1 of [2]):

Proposition 2 *Let $X = \mathrm{Spec}(\mathbb{Z}[1/p])$. Suppose $n > 1$ is odd. Then*

$$\mathrm{H}^2_{\text{et}}(X, \mathbb{Z}_p(n)) \otimes \mathbb{Z}/p = A_{p-n}.$$

Combining the natural maps

$$K_{2n-2}(\mathbb{Z}) \to K_{2n-2}(\mathbb{Z}[1/p]) \to K_{2n-2}(\mathbb{Z}[1/p]) \otimes \mathbb{Z}_p$$

with the maps (4), (5), and the above proposition, we get a map

$$K_{2n-2}(\mathbb{Z}) \otimes \mathbb{Z}/p \to A_{p-n}.$$

It is (apparently) a fact (due to Soulé and Dwyer-Friedlander) that this map is surjective, and this is the map (2) that we have called the Chern map in the Introduction.

4 Voronoi's reduction theory

Fix $N \geq 2$. Let V_N denote the space of $N \times N$ real symmetric matrices.

Recall that a symmetric matrix A is called *positive semi-definite* if $vAv^t \geq 0$, for all v, and is called *positive definite* if in addition $vAv^t = 0 \iff v = 0$. Let P_N denote the subset of V_N of all positive definite symmetric matrices.

Note that $\mathbb{R}_+^\times$ acts on V_N by scalar multiplication. Set $X_N = P_N/\mathbb{R}_+^\times$. Then $X_N = SL_N(\mathbb{R})/SO_N(\mathbb{R})$ is the symmetric space for $SL_N(\mathbb{R})$.

Let P_N^* denote the subset of V_N of all symmetric positive semi-definite matrices, with rational null-space (that is $\ker(A)$ is spanned by vectors in $\mathbb{Q}^N$). Set $X_N^* = P_N^*/\mathbb{R}_+^\times$. We have the following commutative diagram of spaces:

$$\begin{tikzcd}
P_N \arrow[r, phantom, "\subset"] \arrow[d] & P_N^* \arrow[d, "\pi"] \\
X_N \arrow[r, phantom, "\subset"] & X_N^*,
\end{tikzcd}$$

where π denotes the projection map.

Now $SL_N(\mathbb{Z})$ acts on P_N^* as follows:

$$g \cdot A = gAg^t,$$

where $g \in SL_N(\mathbb{Z})$ and $A \in P_N^*$. P_N is clearly preserved under this action. Set $Y_N = X_N/SL_N(\mathbb{Z})$ and $Y_N^* = X_N^*/SL_N(\mathbb{Z})$.

Definition 3 *Let $A \in P_N$. Set*

$$\begin{aligned}
\mu(A) &:= \min\{vAv^t \mid v \in \mathbb{Z}^N \subset \mathbb{R}^N\}, \\
m(A) &:= \{v \in \mathbb{Z}^N \setminus 0 \mid vAv^t = \mu(A)\}.
\end{aligned}$$

Definition 4 *Let $A \in P_N$. Then say A is* perfect *if $\mu(A) = 1$, and if whenever $B \in P_N$ with $\mu(B) = 1$ and $m(A) = m(B)$, then $B = A$.*

Note that each element $v \in \mathbb{Z}^N \setminus 0$ determines an element $\hat{v} = v^t v \in P_N^*$.

Definition 5 *Given any finite subset $B \subset \mathbb{Z}^N \setminus 0$, the* convex hull of B *is the set $\pi\left(\{\sum_j \lambda_j \hat{v}_j \mid v_j \in B, \lambda_j \geq 0\}\right)$.*

When A is perfect, let $\sigma(A)$ denote the convex hull of $m(A)$. We may now state the main theorem of Voronoi reduction theory:

Theorem 10 *(Voronoi)*

1. *Up to conjugation by $SL_N(\mathbb{Z})$, there are only finitely many perfect forms.*

2. *The cells $\sigma(A)$ and their intersections, as A varies through the set of perfect forms, gives a cell decomposition of X_N^*, invariant under $SL_N(\mathbb{Z})$.*

The above theorem says that the space $Y_N^* = X_N^*/\mathrm{SL}_N(\mathbb{Z})$ is a finite CW-complex. Soulé has computed explicit upper bounds for the number of cells of a fixed dimension, and the number of faces of such cells:

Proposition 3 *There exist explicit constants $c(k, N)$ and $f(k, N)$ such that*

1. *The number of $SL_N(\mathbb{Z})$-conjugacy classes of k-dimensional cells in the Voronoi cell decomposition of X_N^* is bounded by $c(k, N)$, and,*

2. *Any k-dimensional cell has at most $f(k, N)$ faces.*

Proof: The proof is easy: we refer the reader to Propositions 1 and 2 of [6] for details.

5 A key Lemma

The following simple lemma (it is a good exercise to try and prove it for yourself) is really at the heart of the whole proof:

Lemma 1 *Let $\phi : \mathbb{Z}^a \to \mathbb{Z}^b$ be a $\mathbb{Z}$-linear map. Let $Q = \mathrm{coker}(\phi)$. Let $\{e_i \mid 1 \leq i \leq a\}$ denote the standard basis of $\mathbb{Z}^a$, and let $I \subset \{1, \ldots, a\}$ be such that $\{\phi(e_i) \mid i \in I\}$ is a basis for $\mathrm{image}(\phi) \otimes \mathbb{R}$. Then*

$$\mathrm{card}(Q_{\mathrm{tors}}) \leq \prod_{i \in I} ||\phi(e_i)||.$$

Now let X be a finite CW-complex. Let $(C_.(X), \partial_.)$ denote its cellular chain complex. Recall that $C_k(X)$ is a free $\mathbb{Z}$-module of finite rank, with basis, say, Σ_k, and that there are boundary maps

$$\partial_{k+1} : C_{k+1}(X) \to C_k(X). \tag{6}$$

Suppose that

$$\partial_{k+1}(\sigma) = \sum_{\sigma' \in \Sigma_k} n_{\sigma\sigma'}\, \sigma',$$

for $\sigma \in \Sigma_{k+1}$. Set

$$\begin{aligned} a(k) &= \min\left(\operatorname{card}(\Sigma_{k+1}), \operatorname{card}(\Sigma_k)\right), \\ b(k) &= \max\left(1, \max_{\sigma \in \Sigma_{k+1}} \left(\sum_{\sigma' \in \Sigma_k} n_{\sigma\sigma'}^2\right)^{1/2}\right). \end{aligned}$$

The following corollary follows immediately from Lemma 1:

Corollary 1 *(Gabber) We have*

$$\operatorname{card}(\mathrm{H}_k(C., \partial.)_{\mathrm{tors}}) \leq b(k)^{a(k)}.$$

Proof: Note that

$$\mathrm{H}_k(C., \partial.) = \frac{\ker(\partial_k)}{\operatorname{image}(\partial_{k+1})} \subset Q = \operatorname{coker}(\partial_{k+1}).$$

Also $||\partial_{k+1}(\sigma)|| \leq b(k)$. Thus

$$\operatorname{card}(\mathrm{H}_k(C., \partial.)_{\mathrm{tors}}) \leq \operatorname{card}(Q_{\mathrm{tors}}) \leq b(k)^{a(k)}.$$

Let us apply this corollary in our situation: namely when $X = Y_N^*$. We choose our basis set Σ_k to be a set of representatives of the conjugacy classes of k-dimensional cells in the Voronoi cell decomposition. Note that if $\sigma \in \Sigma_{k+1}$, the absolute values $|n_{\sigma\sigma'}|$ of the integers appearing in (6) above are at most the number of faces τ of σ which are conjugate to σ'. So

$$\left(\sum_{\sigma' \in \Sigma_k} n_{\sigma\sigma'}^2\right)^{1/2} \leq \sum_{\sigma' \in \Sigma_k} |n_{\sigma\sigma'}| \leq f(k+1, N),$$

by Proposition 3. The same proposition shows that

$$\operatorname{card}(\Sigma_k) \leq c(k, N).$$

Consequently, in our situation, we may rephrase Corollary 1 as:

Corollary 2 *We have*

$$\operatorname{card}(\mathrm{H}_k(Y_N^*, \mathbb{Z})_{\mathrm{tors}}) \leq f(k+1, N)^{c(k+1, N)}.$$

6 Proof of Theorem 4

In this section, we tie together the previous sections and give a sketch of the proof of Theorem 4.

Let p be an odd prime, and let $n > 1$ be odd. Recall that the map (2)

$$K_{2n-2}(\mathbb{Z}) \otimes \mathbb{Z}/p \to A_{p-n}$$

is surjective, and that, moreover, the abelian group $K_{2n-2}(\mathbb{Z})$ is finite. We would therefore like to get a bound for the torsion in $K_{2n-2}(\mathbb{Z})$.

The Hurewicz map (see Section 2.6)

$$\text{Hurewicz} : K_m(\mathbb{Z}) \to \mathrm{H}_m(\mathrm{GL}(\mathbb{Z}), \mathbb{Z}).$$

converts our task into a question of computing homology groups (easy), rather than computing homotopy groups (more difficult). Indeed modulo 'small primes' (cf. Proposition 1 above), which we can ignore, the Hurewicz map is in fact injective.

Moreover, it is a fact that the homology groups of $\mathrm{GL}(\mathbb{Z})$ are 'stable' (see the references in Section 2.5 of [6]). Thus we have:

$$\mathrm{H}_m(\mathrm{GL}(\mathbb{Z}), \mathbb{Z}) = \mathrm{H}_m(\mathrm{GL}_N(\mathbb{Z}), \mathbb{Z}),$$

for N large, in fact for $N \geq 2m + 1$.

On the other hand there is an exact sequence

$$1 \longrightarrow \mathrm{SL}_N(\mathbb{Z}) \longrightarrow \mathrm{GL}_N(\mathbb{Z}) \xrightarrow{\det} \{\pm 1\} \to 1,$$

and so a simple application of the Hochschild-Serre spectral sequence shows that up to a power of 2 (which again we can ignore) we have

$$\mathrm{card}(\mathrm{H}_m(\mathrm{GL}_N(\mathbb{Z}), \mathbb{Z})) = \mathrm{card}(\mathrm{H}_m(\mathrm{SL}_N(\mathbb{Z}), \mathbb{Z})).$$

Now, modulo some more small primes, we have

$$\mathrm{card}(\mathrm{H}_m(\mathrm{SL}_N(\mathbb{Z}), \mathbb{Z})) = \mathrm{card}(\mathrm{H}_m(Y_N, \mathbb{Z})). \tag{7}$$

This would have been an exact equality, except for the fact that $\mathrm{SL}_N(\mathbb{Z})$ has some elements of finite order. By passing to a torsion-free normal subgroup Γ of $\mathrm{SL}_N(\mathbb{Z})$ of finite index (divisible by exactly the primes which divide the cardinalities of the elements of finite order in $\mathrm{SL}_N(\mathbb{Z})$), and noting that the analog of (7) holds for Γ, we may deduce (7) itself, by 'taking invariants'.

But, by Corollary 2 we have

$$\mathrm{card}(\mathrm{H}_m(Y_N^*, \mathbb{Z})_{\mathrm{tors}}) \leq f(m+1, N)^{c(m+1,N)}.$$

Now a technical argument (see [6], proof of Theorem 1) allows us to deduce that the cardinality of the homology of the non-compact space $Y_N \subset Y_N^*$ may also be bounded explicitly. Thus there is a constant $A(m, N)$, related to $f(m+1, N)^{c(m+1,N)}$, such that

$$\mathrm{card}(\mathrm{H}_m(Y_N, \mathbb{Z})) \leq A(m, N).$$

An explicit computation of $A(m, N)$ for $N = 2m+1$ and $m = 2n-2$ (see [6], Lemma 2)) shows that if p is large compared to n, namely $p > \exp(n^{224n^4})$, then $p \not| \,\mathrm{card}(\mathrm{H}_m(Y_N, \mathbb{Z}))$. By the remarks above, and the surjectivity of the map (2), we have:

$$A_{p-n} = 0,$$

for such p. This 'finishes' the proof of Theorem 4.

References

[1] A. Borel. Stable real cohomology of arithmetic groups. *Ann. Scient. Ec. Norm. Sup.*, 7:235–272, 1974.

[2] M. Kurihara. Some remarks on conjectures about cyclotomic fields and K-groups of Z. *Compositio Math.*, 81:223–236, 1992.

[3] B. Mazur and A. Wiles. Class fields of abelian extensions of Q. *Invent. Math*, 76:179–330, 1984.

[4] J. Rosenberg. *Algebraic K-Theory and Its Applications, GTM, 147.* Springer-Verlag, Berlin-New York, 1994.

[5] K. Rubin. *Appendix to Cyclotomic fields I and II, by Serge Lang, GTM, 121.* Springer-Verlag, Berlin-New York, 1990.

[6] C. Soulé. Perfect forms and Vandiver's conjecture. *Preprint, http://www.math.uiuc.edu/K-theory*, 1998.

[7] V. Srinivas. *Algebraic K-theory, Second Edition, Progress in Mathematics, 90.* Birkhäuser, 1993.

[8] L. Washington. *Introduction to cyclotomic fields, Second edition.* Springer-Verlag, Berlin-New York, 1996.