

AN OVERKILL PROOF OF THE INFINITUDE OF PRIMES

NIKLAS ARPPE

ABSTRACT. We deduce the infinitude of the primes from the Lichtenbaum conjecture for $\mathbf{Q}$ at all primes. Our proof rests on the norm residue isomorphism of Voevodsky–Rost, the main conjecture of Iwasawa theory proved by Mazur–Wiles, and the work of Rognes–Weibel relating the algebraic K -theory of rings of integers to étale cohomology.

1. INTRODUCTION

Let us begin by recalling Euclid’s theorem and providing an overview of our proof.

Theorem 1.1 (Euclid). — *There are infinitely many primes.*

The idea of our proof is as follows. If there were only finitely many primes, we could choose an integer k with $p - 1 \mid 2k$ for all primes p . For such an integer k , a simple Galois cohomology computation shows that the K -group $K_{4k-2}(\mathbf{Z})$ has no odd torsion. Moreover, the computation of the 2-primary algebraic K -theory of $\mathbf{Z}$ shows that its 2-torsion is at most $\mathbf{Z}/2\mathbf{Z}$. Denoting by ζ the Riemann ζ -function, Lichtenbaum’s conjecture for $\mathbf{Q}$ then implies that $|\zeta(1 - 2k)|$ is bounded. But $|\zeta(1 - 2k)|$ is known to grow faster than any exponential in k .

1.1. Notation and conventions. We fix an algebraic closure $\mathbf{Q} \subseteq \overline{\mathbf{Q}}$. For a finite set S of places of $\mathbf{Q}$ containing ∞ , we write $\mathbf{Q}_S \subseteq \overline{\mathbf{Q}}$ for the maximal extension of $\mathbf{Q}$ unramified outside of S and $G_{\mathbf{Q},S} := \text{Gal}(\mathbf{Q}_S/\mathbf{Q})$. We will only use this for $S = \{p, \infty\}$ with p a prime. Moreover, for a prime p and an abelian group A , we write $A\{p\}$ for its p -primary part; when A is finite, this is isomorphic to $A \otimes \mathbf{Z}_p$.

1.2. Author’s comment. The idea for writing this short note came to me while preparing my talk on the algebraic K -theory of finite fields for the Kan seminar at the University of Bonn. I got curious about what was known about the K -theory of $\mathbf{Z}$, and started reading up on the Lichtenbaum and Quillen–Lichtenbaum conjectures in detail. I had also been wanting to write an overkill proof of a simple statement for fun, and now the pieces happened to align suitably.

There may well be some circularity in the argument, and hence this note should not be taken seriously. I have not checked this in detail. It is simply meant to provide an amusing “proof” of a classical statement.

2. PRELIMINARIES

We start by recalling the heavy machinery that will be used in the proof. As none of the results will be proven here in detail, we have instead made an effort to make some historical remarks.

Theorem 2.1. — *For $k \geq 1$, the groups $K_{4k-2}(\mathbf{Z})$ and $K_{4k-1}(\mathbf{Z})$ are finite.*

Date: October 25, 2026.

Proof. This is [Wei05, Theorem 6]. Note that for the odd case, $\mathbf{Q}$ is totally real and $4k - 1 \equiv 3 \pmod{4}$, so *loc. cit.* shows that $\text{rank } K_{4k-1}(\mathbf{Z}) = 0$, i.e., the group is finite. The finite generation is originally due to Quillen [Qui73], and the ranks were computed by Borel [Bor74]. $\square$

Theorem 2.2 (Quillen–Lichtenbaum conjecture at odd primes). — *Let p be an odd prime and $j \geq 2$. Then there is a natural isomorphism*

$$K_{2j-2}(\mathbf{Z}) \otimes \mathbf{Z}_p \cong H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(j)).$$

Proof. This is [Wei05, Theorem 70]. The proof there rests on [RW00] and on the norm residue isomorphism of Voevodsky–Rost (also known as the Bloch–Kato conjecture) [Voe11], relating Milnor K -theory to étale cohomology. $\square$

Theorem 2.3 (Lichtenbaum’s conjecture for odd primes). — *Let $k \geq 1$, and let p be an odd prime. Then*

$$v_p(\zeta(1 - 2k)) = v_p(\#K_{4k-2}(\mathbf{Z})) - v_p(\#K_{4k-1}(\mathbf{Z})).$$

Proof. By [Wei05, Remark 25], the denominator of $\zeta(1 - 2k)$ is $\frac{1}{2}w_{2k}(\mathbf{Q})$, where we write

$$w_{2k}(\mathbf{Q}) = \prod_{\ell \text{ prime}} w_{2k}^{(\ell)}(\mathbf{Q}),$$

with $w_{2k}^{(\ell)}(\mathbf{Q}) = \max_{\nu} \{\ell^{\nu} : \text{Gal}(\mathbf{Q}(\mu_{\ell^{\nu}})/\mathbf{Q}) \text{ has exponent dividing } 2k\}$. We note that this is indeed a finite number for all local and global fields. Now, by [Wei05, Example 44], the Main Conjecture of Iwasawa theory,¹ proved by Mazur–Wiles [MW84], implies that the order of $H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(2k))$ is the p -primary part of the numerator of $\zeta(1 - 2k)$. By Theorem 2.2, this is the order of $K_{4k-2}(\mathbf{Z})\{p\}$.

Finally, we apply [Wei05, Theorem 70] to see that

$$K_{4k-1}(\mathbf{Z})\{p\} \cong \mathbf{Z}/w_{2k}^{(p)}(\mathbf{Q})$$

as $\mathbf{Q}$ is totally real, which implies that

$$v_p(\#K_{4k-1}(\mathbf{Z})) = v_p(w_{2k}^{(p)}(\mathbf{Q})) = v_p(w_{2k}(\mathbf{Q})).$$

Combining the above yields the claim. $\square$

Theorem 2.4 (Lichtenbaum’s conjecture, 2-primary part). — *For $k \geq 1$, we have*

$$v_2(\zeta(1 - 2k)) = 1 + v_2(\#K_{4k-2}(\mathbf{Z})) - v_2(\#K_{4k-1}(\mathbf{Z})).$$

Proof. We begin by noting that we have

$$v_2(\zeta(1 - 2k)) = 1 + v_2(\#K_{4k-2}(\mathbf{Z}[1/2])\{2\}) - v_2(\#K_{4k-1}(\mathbf{Z}[1/2])\{2\})$$

by [RW00, Theorem 0.2]. This again uses some input from Iwasawa theory, namely Wiles’ theorem [Wil90]; see also Kolster’s appendix to [RW00]. It remains to identify factors on the right-hand side. For this, it will suffice to show that there are isomorphisms

$$K_n(\mathbf{Z}[1/2])\{2\} \cong K_n(\mathbf{Z})\{2\}$$

for all $n \geq 2$. To this end, consider Quillen’s localization sequence

$$\cdots \longrightarrow K_n(\mathbf{F}_2) \longrightarrow K_n(\mathbf{Z}) \longrightarrow K_n(\mathbf{Z}[1/2]) \longrightarrow K_{n-1}(\mathbf{F}_2) \longrightarrow \cdots$$

Quillen’s computation of the K -theory of finite fields [Qui72] shows that $K_{2j-1}(\mathbf{F}_2) \cong \mathbf{Z}/(2^j - 1)$ and $K_{2j}(\mathbf{F}_2) = 0$ for $j \geq 1$. Thus $K_n(\mathbf{F}_2)$ is a finite group of odd order for all

¹This requires p to be odd.

$n \geq 1$. Localizing the long exact sequence above at the prime 2 (which kills the $\mathbf{F}_2$ -terms) and passing to torsion subgroups then shows that we obtain the desired isomorphism

$$K_n(\mathbf{Z}[1/2])\{2\} \cong (K_n(\mathbf{Z}[1/2])_{(2)})_{\text{tors}} \cong (K_n(\mathbf{Z})_{(2)})_{\text{tors}} \cong K_n(\mathbf{Z})\{2\}.$$

□

Theorem 2.5. — *Let $k \geq 1$. Then*

$$K_{4k-2}(\mathbf{Z})\{2\} \cong \begin{cases} \mathbf{Z}/2\mathbf{Z} & \text{if } k \text{ is odd} \\ 0 & \text{if } k \text{ is even.} \end{cases}$$

Proof. This is part of [Wei97, Theorem 1], but let us deduce from the actual statement in *loc. cit.* If k is odd, then $4k \equiv 4 \pmod{8}$ and thus $4k - 2 \equiv 2 \pmod{8}$. Similarly, if k is even, then $4k \equiv 0 \pmod{8}$ and so $4k - 2 \equiv 6 \pmod{8}$. It thus suffices to read off Weibel's results for $K_{8n+2}(\mathbf{Z})$ and $K_{8n+6}(\mathbf{Z})$. Taking the 2-primary part kills off any finite group of odd order, yielding our desired result. □

Having now stated the big results, we further deduce some estimates on the growth of the Riemann ζ -function.

Lemma 2.6. — *For every $k \geq 1$, we have*

$$|\zeta(1 - 2k)| = \frac{2(2k - 1)!\zeta(2k)}{(2\pi)^{2k}} \geq \frac{2(2k - 1)!}{(2\pi)^{2k}}.$$

In particular, $|\zeta(1 - 2k)| \rightarrow \infty$ as $k \rightarrow \infty$.

Proof. The first equality is just the functional equation, where the absolute value removes the sign $(-1)^k$ appearing. For the inequality, we simply note that $\zeta(2k) = \sum_{n \geq 1} n^{-2k}$ is a convergent sum of positive terms with first term 1, hence $\zeta(2k) \geq 1$. The fact that the right-hand side of the inequality diverges is an exercise in elementary analysis. □

Lemma 2.7. — *For every $k \geq 1$, we have $v_2(\zeta(1 - 2k)) \leq 2$.*

Proof. By Theorem 2.1, the groups $K_{4k-2}(\mathbf{Z})$ and $K_{4k-1}(\mathbf{Z})$ are finite, so Theorem 2.4 and Theorem 2.5 give

$$\begin{aligned} v_2(\zeta(1 - 2k)) &= 1 + v_2(\#K_{4k-2}(\mathbf{Z})) - v_2(\#K_{4k-1}(\mathbf{Z})) \\ &\leq 1 + v_2(\#K_{4k-2}(\mathbf{Z})) \\ &\leq 1 + 1 = 2. \end{aligned}$$

□

Remark 2.8. — The bound in Lemma 2.7 is far from sharp. However, we only need a uniform one, so we have chosen a simple one that follows easily from our previous results.

3. THE ÉTALE VANISHING

Our final ingredient is a vanishing result for some étale cohomology groups. This computation will take place on the Galois cohomology side, so let us recall how these two compare. This is also where we will have to put in the most amount of effort.

Proposition 3.1. — *Let p be a prime, $S = \{p, \infty\}$, and let M be a finite $G_{\mathbf{Q}, S}$ -module of p -power order, which we view as a locally constant étale sheaf on $\text{Spec } \mathbf{Z}[1/p]$. Then, for all $j \geq 0$, there are natural isomorphisms*

$$H_{\text{ét}}^j(\text{Spec } \mathbf{Z}[1/p], M) \cong H^j(G_{\mathbf{Q}, S}, M).$$

Moreover, these groups are finite.

Proof. The isomorphism is [Mil06, Proposition II.2.9], and the finiteness claim [Mil06, Corollary I.4.15]. $\square$

Proposition 3.2. — *Let p be an odd prime, and let $j \geq 0$ be an integer with $p - 1 \mid j$. Then*

$$H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(j)) = 0.$$

Proof. Put $S = \{p, \infty\}$. The short exact sequences of étale sheaves

$$0 \longrightarrow \mathbf{Z}/p^n(j) \xrightarrow{p} \mathbf{Z}/p^{n+1}(j) \longrightarrow \mathbf{Z}/p(j) \longrightarrow 0$$

give exact sequences

$$H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}/p^n(j)) \xrightarrow{p} H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}/p^{n+1}(j)) \longrightarrow H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}/p(j))$$

for all n . As all the groups involved are finite by Proposition 3.1, taking the limit is exact, and hence we obtain an injection

$$H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(j))/p \hookrightarrow H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}/p(j)) \cong H^2(G_{\mathbf{Q},S}, \mathbf{Z}/p(j)).$$

Let us first argue why it will be enough to show that the right-hand side vanishes. If this were the case, then we would have

$$pH_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(j)) = H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(j)).$$

By induction, $p^n H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(j)) = H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(j))$ for all $n \geq 1$. This shows that all of the projection maps in the inverse system are zero, showing that also $H_{\text{ét}}^2(\text{Spec } \mathbf{Z}[1/p], \mathbf{Z}_p(j))$ must vanish.

It therefore remains to show that $H^2(G_{\mathbf{Q},S}, \mathbf{Z}/p(j)) = 0$. The Galois module $\mathbf{Z}/p(j) = \mu_p^{\otimes j}$ is given by the character χ^j , where $\chi: G_{\mathbf{Q},S} \longrightarrow (\mathbf{Z}/p)^\times$ is the mod p cyclotomic character. As $(\mathbf{Z}/p)^\times$ has order $p - 1$ and $p - 1 \mid j$ by assumption, the character χ^j is trivial. Hence $\mathbf{Z}/p(j) \cong \mathbf{Z}/p$ with trivial action, and we must show $H^2(G_{\mathbf{Q},S}, \mathbf{Z}/p) = 0$.

Write $h^j = \dim_{\mathbf{F}_p} H^j(G_{\mathbf{Q},S}, \mathbf{Z}/p)$. Recall Tate's global Euler characteristic formula [Mil06, Theorem I.5.1], which might take some decyphering. Since $\mathbf{Q}$ has a single archimedean place, which is real, the formula reads

$$\frac{p^{h^0} p^{h^2}}{p^{h^1}} = \frac{\#H^0(\text{Gal}(\mathbf{C}/\mathbf{R}), \mathbf{Z}/p)}{|\#\mathbf{Z}/p|_\infty} = \frac{p}{p} = 1.$$

Since $G_{\mathbf{Q},S}$ acts trivially on $\mathbf{Z}/p$, we have

$$H^0(G_{\mathbf{Q},S}, \mathbf{Z}/p) = (\mathbf{Z}/p)^{G_{\mathbf{Q},S}} = \mathbf{Z}/p,$$

so $h^0 = 1$. By the triviality of the action we also have

$$H^1(G_{\mathbf{Q},S}, \mathbf{Z}/p) = \text{Hom}_{\text{cts}}(G_{\mathbf{Q},S}, \mathbf{Z}/p) = \text{Hom}_{\text{cts}}(G_{\mathbf{Q},S}^{\text{ab}}, \mathbf{Z}/p),$$

where $G_{\mathbf{Q},S}^{\text{ab}}$ is the Galois group of the maximal abelian extension of $\mathbf{Q}$ unramified outside S . By the Kronecker–Weber theorem, every finite abelian extension of $\mathbf{Q}$ is contained in a cyclotomic field $\mathbf{Q}(\mu_m)$, and the maximal one unramified outside of S is $\mathbf{Q}(\mu_{p^\infty})$. Therefore

$$G_{\mathbf{Q},S}^{\text{ab}} \cong \text{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \cong \varprojlim_k (\mathbf{Z}/p^k \mathbf{Z})^\times = \mathbf{Z}_p^\times \cong \mathbf{Z}/(p-1) \times \mathbf{Z}_p,$$

where the last isomorphism uses that p is odd. Since $p \nmid p-1$, we have $\text{Hom}(\mathbf{Z}/(p-1), \mathbf{Z}/p) = 0$, and $\text{Hom}_{\text{cts}}(\mathbf{Z}_p, \mathbf{Z}/p) \cong \mathbf{Z}/p$. Thus $h^1 = 1$, hence $h^2 = h^1 - h^0 = 0$, which finishes the proof. $\square$

Corollary 3.3. — *Let p be an odd prime, and let $k \geq 1$ be an integer with $p - 1 \mid 2k$. Then $K_{4k-2}(\mathbf{Z}) \otimes \mathbf{Z}_p = 0$. In other words, $K_{4k-2}(\mathbf{Z})$ is p -torsion-free.*

Proof. Apply Theorem 2.2 with $j = 2k$ and Proposition 3.2. $\square$

4. PROOF OF THE THEOREM

Putting together all the ingredients from the previous section, we are now ready to prove our main theorem.

Proof of Theorem 1.1. Suppose towards a contradiction that the set P of all primes is finite. Put $l = \text{lcm}\{p - 1 : p \in P\}$. Let $m \geq 1$ and put $k = ml$. Then $p - 1 \mid 2k$ for all $p \in P$.

Let p be an odd prime, so that $v_p(\#K_{4k-2}(\mathbf{Z})) = 0$ by Corollary 3.3. Theorem 2.1 ensures that the relevant K -groups are finite, whence Theorem 2.3 yields

$$v_p(\zeta(1 - 2k)) = -v_p(\#K_{4k-1}(\mathbf{Z})) \leq 0.$$

In particular, this shows that $p^{v_p(\zeta(1-2k))} \leq 1$ for each odd prime p . Combining this with Lemma 2.7 and unique factorization of $\zeta(1 - 2k)$, we get

$$|\zeta(1 - 2k)| = \prod_{p \in P} p^{v_p(\zeta(1-2k))} \leq 2^{v_2(\zeta(1-2k))} \leq 4.$$

This holds for any $k = ml$ with $m \geq 1$ arbitrary. Letting $m \rightarrow \infty$ contradicts Lemma 2.6, finishing the proof. $\square$

REFERENCES

- [Bor74] Armand Borel. *Stable real cohomology of arithmetic groups*. Ann. Sci. École Norm. Sup. (4) 7.2 (1974), pp. 235–272.
- [Mil06] James S. Milne. *Arithmetic duality theorems*. 2nd ed. Charleston, SC: BookSurge, LLC, 2006.
- [MW84] Barry Mazur and Andrew Wiles. *Class fields of abelian extensions of $\mathbf{Q}$* . Invent. Math. 76 (1984), pp. 179–330.
- [Qui72] Daniel Quillen. *On the Cohomology and K-Theory of the General Linear Groups Over a Finite Field*. Annals of Mathematics 96.3 (1972), pp. 552–586.
- [Qui73] Daniel Quillen. “Finite generation of the groups K_i of rings of algebraic integers”. Vol. 341. Lecture Notes in Math. Berlin: Springer, 1973, pp. 179–198.
- [RW00] John Rognes and Charles Weibel. *Two-primary algebraic K-theory of rings of integers in number fields*. J. Amer. Math. Soc. 13.1 (2000). With an appendix by Manfred Kolster, pp. 1–54.
- [Voe11] Vladimir Voevodsky. *On motivic cohomology with $\mathbf{Z}/l$ -coefficients*. Annals of Mathematics 174.1 (2011), pp. 401–438.
- [Wei05] Charles Weibel. “Algebraic K-theory of rings of integers in local and global fields”. *Handbook of K-theory. Vol. 1*. Ed. by Eric M. Friedlander and Daniel R. Grayson. Berlin: Springer, 2005, pp. 139–190. URL: <https://sites.math.rutgers.edu/~weibel/archive/papers-dir/KZsurvey-published.pdf>.
- [Wei97] Charles Weibel. *The 2-torsion in the K-theory of the integers*. C. R. Acad. Sci. Paris Sér. I Math. 324 (1997), pp. 615–620.

- [Wil90] Andrew Wiles. *The Iwasawa conjecture for totally real fields*. Ann. of Math. (2) 131 (1990), pp. 493–540.