Like a bird on the wire,
Like a drunk in a midnight choir
I have tried in my way to be free[1].

To Stephen Smale, at his 80 - *th birthday*

TURNING WASHINGTON'S HEURISTICS IN FAVOR OF VANDIVER'S CONJECTURE

PREDA MIHĂILESCU

ABSTRACT. A famous conjecture bearing the name of Vandiver states that $h_p^+ = 1$ in the p - cyclotomic extension of $\mathbb{Q}$. Heuristics arguments of Washington, which have been briefly exposed in [La], p. 261 and [Wa], p. 158 suggest that the Vandiver conjecture should be false, if certain conditions of statistical independence are fulfilled. In this note we assume that Greenberg's conjecture is true for the $p-$th cyclotomic extensions and prove an elementary consequence of the assumption that Vandiver's conjecture fails for a certain value of p: the result indicates that there are deep correlations between this fact and the defect $\lambda^- i(p)$, where $i(p)$ is like usual the irregularity index of p, i.e. the number of Bernoulli numbers $B_{2k} \equiv 0 \bmod p, 1 < k < (p-1)/2$. As a consequence, if one combines the various assumptions in Washington's heuristics, these turn, on base of the present result, into an argument in favor of the Vandiver's conjecture.

1. Introduction

Let p be an odd prime and $\mathbb{K} = \mathbb{Q}[\zeta]$ be the $p-$th cyclotomic field and $G =$ Gal $(\mathbb{K}/\mathbb{Q})$. If X is a finite abelian group, we denote by X_p its p - Sylow group; let $A = \mathcal{C}(\mathbb{K})_p$, the p - Sylow subgroup of the class group $\mathcal{C}(\mathbb{K})$ and h^+, h^- the sizes of A^+ respectively A^-. In a letter to Kronecker from 1857, Kummer refers to $p \nmid h^+$ as a *noch zu beweisender Satz*, a theorem yet to prove (see also [Wa], p. 158). The fact was stated later as a conjecture by Vandiver.

In [La], p. 261 Washington gives an heuristic argument which suggests that there might be an asymptotic amount of $O(\log\log(N))$ of primes $p \leq N$ for which $\lambda(A_\infty^-) = i(p) + 1$, where $i(p)$ is the irregularity index of p, i.e. the number of Bernoulli numbers $B_{2k}, 1 < k < (p-1)/2$

[1] Leonard Cohen: *Bird on the wire.*

Date: Version 2.0 September 8, 2010.

that vanish modulo p. In [Wa], p.158, Washington starts with a naive argument, on base of which the cyclotomic unit $\eta_{2k} := e_{2k}(1-\zeta)^{\sigma-1}$ (see below for the definition of the idempotents $e_j \in \mathbb{F}_p[G]$) may be a $p-$th power with probability $1/p$: this yields a probability of more than one half, for the failure of Vandiver's conjecture, so the argument is obviously too crude. Washington considers then that the probabilities that a Bernoulli number vanishes modulo p and the one that the corresponding cyclotomic unit η_{2k} is a p-power are independent: this heuristic leads to a frequence of $O(\log\log(n))$ primes $p < n$ for which the conjecture fails. As a consequence, various specialists in the field expect that the conjecture should not always hold. Our result in this note, shows that if Vandiver's conjecture fails, then one has the additional condition $\lambda^- > i(p)$. If one considers this condition also as statistically independent (!) from the two conditions in Washington's heuristiscs, then the same argument suggest that there may be $O(1)$ primes $p < n$ for which Vandiver's conjecture fails, thus possibly none. *Therefore the elementary result in this note may be understood as one that turns Washington's heuristics into an argument in favor of Vandiver's conjecture.*

In this paper we prove an elementary fact, which implies that the failure of Vandiver's conjecture has an impact on the value of λ, and thus two events which were supposed to be uncorrelated in the heuristic approach: namely $h_p^+ \neq 0$ and $\lambda^- > i(p)$ are not independent. No direct consequence can be drawn as to the truth of the Kummer - Vandiver conjecture; however we have an explicite theorem which indicates an unknown dependence, and also a method of investigation which may be extended for the purpose of investigating more possible consequences of the assumption that the Kummer-Vandiver conjecture is false.

The result of this paper is the following:

Theorem 1. *Let p be an odd prime with irregularity index $i(p) = 1$. If $h_p^+ > 1$, then $\lambda^- \geq 2$.*

Since $\lambda^- > 1$ is an implication of $h_p^+ > 1$, the two events cannot be considered as independent events, each one with probability $1/p$. But this implication can also suggest that the probability that η_{2k} is a $p-$th power has rather the probability $1/p^2$ than $1/p$, since it implies the vanishing of a higher order Bernoulli number. Either way, we consider that our elementary result should suggest that it is worthwhile to consider that Vandiver's conjecture might be true, and pursue the investigation for the reasons why this may be the case. For this purpose, the central idea of our proof can be extended, with additional detail, to the general case, and this shall be done in a subsequent paper.

Note that we restrict our analysis, for simplicity, to the case of irregularity index 1. However, this is the critical case in Washington's heuristics, and if the assumption of "statistical independence" is close to reality[1], then the probability of failure of the conjecture for higher values of $i(p)$ can only be smaller, so the argument stays valid.

2. Proof of the Theorem

We let $\mathbb{K} = \mathbb{Q}[\zeta]$ be the $p-$th cyclotomic extension and $\mathbb{K}_n = \mathbb{K}[\zeta^{1/p^n}], n \geq 1$, the p^n-th extension. The galois groups are

$$\begin{array}{rcl} G = \text{ Gal } (\mathbb{K}/\mathbb{Q}) & = & \{\sigma_a \ : \ a = 1, 2, \ldots p-1, \ \zeta \mapsto \zeta^a\} \cong (\mathbb{Z}/p \cdot \mathbb{Z})^*, \\ G_n = \text{ Gal } (\mathbb{K}_n/\mathbb{Q}) & = & G \times \langle \tau \rangle, \quad \tau(\zeta_{p^n}) = \zeta_{p^n}^{1+p}, \end{array}$$

so τ generates Gal $(\mathbb{K}_n/\mathbb{K})$, in particular. If $g \in \mathbb{F}_p$ is a generator of $(\mathbb{Z}/p \cdot \mathbb{Z})^*$, then $\sigma = \sigma_g$ generates G multiplicatively. We write $\jmath \in G$ for complex multiplication. For $\sigma \in G$ and $R \in \{\mathbb{F}_p, \mathbb{Z}_p, \mathbb{Z}/(p^m \cdot \mathbb{Z})\}$ we let $\varpi(\sigma) \in R$ be the value of the Theichmüller character on σ; for $R = \mathbb{F}_p$ we may also write $\hat{\sigma}$ for this values. The orthogonal idempotents $e_k \in R[G]$ are

$$e_k = \frac{1}{p-1} \sum_{a=1}^{p-1} \varpi^k(\sigma_a) \cdot \sigma_a^{-1}.$$

If X is a finite abelian p - group on which G acts, then $e_k(\mathbb{Z}_p)$ acts via its approximants to the p^m-th order; we shall not introduce additional notations for these approximants. A fortiori, complex conjugation acts on X splitting it in the canonical plus and minus parts: $X = X^+ \oplus X^-$, with $X^+ = X^{1+\jmath}, X^- = X^{1-\jmath}$. The units of $\mathbb{K}$ and $\mathbb{K}_n$ are denoted by E, E_n and the cyclotomic units by C, C_n. The Iwasawa invariants λ, λ^- are related to the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{K}_\infty = \cup_n \mathbb{K}_n$ and $A_n = (\mathcal{C}(\mathbb{K}_n))_p$ are the p-parts of the ideal class groups of $\mathbb{K}_n$. They form a projective sequence with respect to the relative norms $N_{m,n} = \mathbf{N}_{\mathbb{K}_m/\mathbb{K}_n}, m > n \geq 1$ and $\mathbf{A} = \varprojlim_n A_n$. We also write A for A_1. We shall write for simplicity $A(\mathbb{L}) = (\mathcal{C}(\mathbb{L}))_p$ for the p-part of the class group of an arbitrary number field $\mathbb{L}$, so $A = A(\mathbb{K})$, etc.

We fix now an odd prime p such that

1. Greenberg's conjecture holds for p, so A^+ is finite and $\lambda^+ = 0$.
2. Vandiver's conjecture fails for p.

[1] Washington mentions explicitly that this is the crucial and critical in the various heuristics of this kind.

3. There is a unique irregular index $2k$ such that $A_{p-2k} = \varepsilon_{p-2k} A \neq \{1\}$. Additionally $A_{2k} \neq \{1\}$, as a consequence of 2.

Under these premises, we show that $\mathbb{Z}_p$-rk$(\varepsilon_{p-2k}\mathbf{A} > 1$, which is the statement of the theorem. We prove the statement by contraposition, so we assume that $\mathbb{Z}_p$-rk$(\varepsilon_{p-2k}\mathbf{A}) = 1$. Since there is a unique irregular index, the minimal polynomial of $\mathbf{A}$ is linear. Let $\mathbb{H}_n/\mathbb{K}_n$ be the maximal p-abelian unramified extensions. They split in plus and minus parts according to $A_n = A_n^+ \oplus A_n^-$ and our assumption implies that $\mathbb{H}_n^+/\mathbb{K}_n$ are cyclic extensions of degree

$$d_n := [\mathbb{H}_n^+ : \mathbb{K}_n] = |A_n^+|.$$

We may also consider $\mathbb{H}_n^+$ as the compositum of $\mathbb{K}_n$ with the full p-part of the Hilbert class field of $\mathbb{K}_n^+ \subset \mathbb{K}_n$, the maximal reals subextension of $\mathbb{K}_n$: thus $\mathbb{H}_n^+$ is a canonical subfield, corresponding by the Artin map to A_n^+. It follows that $\mathbb{H}_n^+/\mathbb{K}_n^+$ is an abelian extension, and thus $\mathbb{H}_n^+$ is a CM field (see also [Wa], Lemma 9.2 for a detailed proof). There is a canonic construction of radicals from A_n^-, such that $\mathbb{H}_n \cdot \mathbb{K}_m \subset \mathbb{K}_m[(A_m^-)^{1/p^m}]$ for sufficiently large m. As a consequence of Greenberg's conjecture holding for $\mathbb{K}$, there is an $n_0 \geq 1$ such that $|A_n^+| = |A_{n_0}^+|$ for all $n \geq n_0$ and for such n, let $a_n \in A_n^-$ generated this cyclic group. Let $\mathfrak{Q} \in a_n$ and $\alpha_0 \in \mathbb{K}_n^\times$ with $(\alpha_0) = \mathfrak{Q}^{\text{ord }(a_n)}$; there is an $\alpha = \eta \cdot \alpha_0^{1-\jmath}, \eta \in \mu_{p^n}$ which is well defined up to roots of unity, such that $\mathbb{H}_n^+ \subset \mathbb{K}_n[\alpha^{1/p^n}]$. The radical B_n of $\mathbb{H}_n^+$ is then the multiplicative group generated by α and $(\mathbb{K}_n^\times)^{d_n}$.

Since $\mathbb{H}_n^+/K_n$ is cyclic, a folklore result, which we prove for completeness in Lemma 2 of the Appendix below, implies that

$$A(\mathbb{H}_n^+) = (\mathcal{C}(\mathbb{H}_n^+))_p = \{1\}. \tag{1}$$

A classical result, proved by Iwasawa [Iw] in a general cohomological language, states that for an arbitrary galois extension $\mathbb{L}/\mathbb{F}$ of finite number fields, there is a canonical isomorphism

$$H^1(\text{ Gal }(\mathbb{L}/\mathbb{F}), E(\mathbb{L})) \cong \mathcal{A}(\mathbb{L}), \tag{2}$$

where $\mathcal{A}(\mathbb{F})$ are Hilbert's *ambig* ideals, i.e. the ideals of $\mathbb{L}$ which are invariant under Gal $(\mathbb{L}/\mathbb{F})$, factored by the principal ideals of $\mathbb{F}$. These can be either totally ramified ideals or ideals from $\mathbb{F}$ that capitulate completely (become principal) in $\mathbb{L}$. We shall in the sequel often consider the homology groups H^0, H^1 for the unit groups. We can then write, for simplicity

$$H^i(\mathbb{L}/\mathbb{F}) := H^i(\text{ Gal }(\mathbb{L}/\mathbb{F}), E(\mathbb{L})) \quad \text{for} \quad i = 0, 1.$$

The isomorphism above restricts also to one of p-parts of the respective groups; furthermore, complex conjugation also induces canonical isomorphisms of the plus and minus parts of H^i. The extensions $\mathbb{H}_n^+/\mathbb{K}_n$ being cyclic of degree d_n, the Herbrand quotient is d_n and thus

$$H^1(\mathbb{H}_n^+/\mathbb{K}_n) = d_n \cdot H^0(\mathbb{H}_n^+/\mathbb{K}_n).$$

We claim that $(H^0(\mathbb{H}_n^+/\mathbb{K}_n))^+ = \{1\}$. Indeed, the ambig ideals in an unramified extension are capitulated ideals. In our case, since $d_n = |A_n^+|$ by definition, we have exactly $|\mathcal{A}(\mathbb{H}_n^+)| = d_n^2$. This follows from the fact that the plus part capitulates completely, while the minus part is cyclic too and generates the radical of the extension. Consequently $\mathfrak{Q}^{\mathrm{ord}\ (a_n)/d_n}$ becomes principal in $\mathbb{H}_n^+$, which confirms that

$$|\mathcal{A}(\mathbb{H}_n^+)| = d_n^2 \quad \text{ and } |\mathcal{A}(\mathbb{H}_n^+)|^- = |\mathcal{A}(\mathbb{H}_n^+)|^+ = d_n.$$

Therefore, $|H^0(\mathbb{H}_n^+/\mathbb{K}_n)| = d_n$. The roots of unity $\zeta_{p^n} \not\in \mathbf{N}_{\mathbb{H}_n^+/\mathbb{K}_n}(E(\mathbb{H}_n^+))$: indeed, if $\zeta_{p^m} = N(\delta)$ for $\delta \in E(\mathbb{H}_n^+)$ and $m \leq n$, then $\varepsilon = \delta/\overline{\delta}$ is well defined in the CM field $\mathbb{H}_n^+$ and it is a root of unity, by Dedekind's unit Theorem – so $\varepsilon \in \mathbb{K}_n$. Moreover, we have $\mathbf{N}_{\mathbb{H}_n^+/\mathbb{K}_n}(\varepsilon) = \varepsilon^{d_n} = \zeta_{p^m}^2$. Since p is odd, it follows that $\mu_{p^n}/\mu_{p^n/d_n} \subset H^0(\mathbb{H}_n^+/\mathbb{K}_n)$; by comparing orders of the groups, we conclude that

$$H^0(\mathbb{H}_n^+/\mathbb{K}_n) = \mu_{p^n}/\mu_{(p^n/d_n)} = \left(H^0(\mathbb{H}_n^+/\mathbb{K}_n)\right)^- .$$

We have proved:

Lemma 1. *Notations being like above,*

$$\left(H^0(\mathbb{H}_n^+/\mathbb{K}_n)\right)^+ = \{1\}.$$

In particular

$$\mathbf{N}_{\mathbb{H}_n^+/\mathbb{K}_n}(E^+(\mathbb{H}_n^+)) = E^+(\mathbb{K}_n), \tag{3}$$

where for a CM field $\mathbb{F}$ *we write* $E^+(\mathbb{F}) = \{e \cdot \overline{e} : e \in E(\mathbb{F})\}$.

In our case, E^+ are the real units and the units of $\mathbb{K}_n^+$, resp. $\mathbb{H}(\mathbb{K}_n^+) \subset \mathbb{H}_n^+$; the prime p is odd and we are interested in p-parts, so the implicit exponent 2 in the above definition has no further consequences: the norm is surjective on the real units in our class field. Then $\mathbb{H}_{n+1}^+ = \mathbb{K}_{n+1} \cdot \mathbb{H}_n^+$ and we have a commutative diagram of fields. By computing $H^0(\mathbb{H}_{n+1}^+/\mathbb{K}_n)$ in two ways, over the intermediate field $\mathbb{K}_{n+1}$ and respectively over $\mathbb{H}_n^+$, we obtain from (3) that

$$\left(H^0(\mathbb{K}_{n+1}/\mathbb{K}_n)\right)^+ = \left(H^0(\mathbb{H}_{n+1}^+/\mathbb{H}_n^+)\right)^+ . \tag{4}$$

The core observation of this proof is

Proposition 1. *Let* $\lambda_n = 1 - \zeta_{p^n}$*. Then the ramified prime* $\wp_n = (\lambda_n) \subset \mathbb{K}_n$ *above* p *splits totally in* $\mathbb{H}_n^+$ *in* p*-principal ideals. Moreover, if* $\nu \in$ *Gal* $(\mathbb{H}_n^+/\mathbb{K}_n)$ *is a generator of this cyclic group, then there is a prime* $\pi_n \in \mathbb{H}_n^+$ *with* $\mathbf{N}_{\mathbb{H}_n^+/\mathbb{K}_n}(\pi_n) = \lambda_n$*.*

Proof. Since $\wp_n = (\lambda_n)$ is principal, the Principal Ideal Theorem implies that it splits completely in the unramified extension $\mathbb{H}_n^+/\mathbb{K}_n$ and since $A(\mathbb{H}_n^+) = \{1\}$ by (2), the primes above $\wp_n$ are p-principal. Let $E'(\mathbb{F})$ denote the p-units of the number field $\mathbb{F}$, i.e. the units of the smallest ring containing $E(\mathbb{K})$ and in which all the primes above p are invertible. In particular $E'_n = E_n[1/\lambda_n]$; it is customary to denote by A'_n the p-part of the ideal class group of the p-integers. Since $\mathbb{H}_n^+/\mathbb{K}_n$ splits the prime above p and $A_n^+ = (A'_n)^+$ and $H^0($ Gal $(\mathbb{H}_n^+/\mathbb{K}_n), E'(\mathbb{H}_n^+)) = H^0(\mathbb{H}_n^+/\mathbb{K}_n)$. In particular, the norm $\mathbf{N}_{\mathbb{H}_n^+/\mathbb{K}_n} : E'(\mathbb{H}_n^+) \to E'(\mathbb{K}_n)$ is surjective, so there is a prime $\pi_n \in \mathbb{H}_n^+$ mapping on λ_n.

The proof of this proposition is made particularly simple by the use of (2). However, a more involved proof shows that the facts hold in more generality and the primes above λ are principal in any subfield of the Hilbert class field $\mathbb{H}_n$. □

As a consequence of the proposition, we see that $\mathcal{A}(\mathbb{H}_n^+) = \{1\}$. Indeed, by Lemma 2, the class group $A(\mathbb{H}_n^+) = \{1\}$, and the only primes that ramify in $\mathbb{H}_{n+1}^+/\mathbb{H}_n^+$ lay above p, so they are principal by Lemma 1. There are consequently no real ambig ideals in $\mathbb{H}_n^+$. On the other hand, for n such that $|A_n^+| = |A_{n+1}^+|$, the capitulation kernel $P_n :=$ Ker $(\iota_{n,n+1} : A_n^+ \to A_{n+1}^+$ is an $\mathbb{F}_p$-space of dimension $d = p -$ rank $(\mathbf{A}^+) = p -$ rank $(A_n) = 1$. We obtain a contradiction with (4), which shows that if $i(p) = 1$, then either $\mathbb{Z}_p$-rk$(A^-) > 1$ or $h_p^+ = 1$. This completes the proof of the Theorem.

3. Appendix

For the sake of completeness, we give a proof of the following

Lemma 2. *Let* $\mathbb{K}$ *be a number field and* A *be the* p *- part of its class group, while* $\mathbb{H}$ *is the* p *- part of its Hilbert class group. If* A *is cyclic, then* $A(\mathbb{H}) := \mathcal{C}(\mathbb{H})_p = \{1\}$*.*

Proof. Since A is cyclic, Gal $(\mathbb{H}/\mathbb{K}) \cong A$ is a cyclic group and the ideals of a generating class $a \in A$ are inert and become principal in $\mathbb{H}$. Let $\sigma = \varphi(a) \in$ Gal $(\mathbb{H}/\mathbb{K})$ be a generator and $s = \sigma - 1$. Suppose that $b \in A(\mathbb{H}) \setminus A(\mathbb{H})^{(s,p)}$ is a non trivial class and let $\mathfrak{Q} \in b$ be an ideal above a rational prime $\mathfrak{q} \subset \mathbb{K}$, which splits completely in $\mathbb{H}/\mathbb{K}$: such a prime must exist, by Tchebotarew's Theorem. If $b' = [\mathfrak{q}]$, then the order of b' must be a power of p, since this holds for $\mathfrak{Q}$; thus $b' \in A(\mathbb{K}) = \langle a \rangle$. But we have seen that the ideals from a capitulate in $\mathbb{H}$, so $b = 1$, in contradiction with our choice. Therefore $b' = 1$ and thus $\mathbf{N}_{\mathbb{H}/\mathbb{K}}(b) = 1$. Furtwängler's Hilbert 90 Theorem for ideal class groups in cyclic extensions [Fu] says that Ker $(\mathbf{N} : A(\mathbb{H}) \to A(\mathbb{K})) \subset A(\mathbb{H})^s$, and this implies that $b \in A(\mathbb{H})^s$, which contradicts the choice of b and completes the proof. □

References

[Fu] P. Furtwängler: *Über die Reziprozitätsgesetze zwischen l-ten Potenzresten in algebraischen Zahlkörpern, wenn l eine ungerade Primzahl bedeutet*, (German) Math. Ann. **58**, 1-50 (1904).

[Hi] David Hilbert: *The Theory of Algebraic Numbers (Zahlbericht)*, Translated by Iain Adamson, Edited by Iain Adamson, Franz Lemmermayer and Norbert Schappacher; Springer (1998).

[La] S. Lang: *Cyclotomic fields I and II*, First Edition, Springer (1978,80)

[Iw] K. Iwasawa: *A note on the group of units of an algebraic number fields*, Journal de Math. Pures et Appl. **35/121** (1956), pp. 189-192.

[Wa] Lawrence Washington: *Introduction to cyclotomic fields*, Springer, Graduate Texts in Mathematics **83**, 2-nd edition (1996).

(P. Mihăilescu) Mathematisches Institut der Universität Göttingen
E-mail address, P. Mihăilescu: preda@uni-math.gwdg.de