On the order modulo p of an algebraic number (for p large enough)

Georges Gras

ON THE ORDER MODULO p OF AN ALGEBRAIC NUMBER (FOR p LARGE ENOUGH)

GEORGES GRAS

ABSTRACT. Let $K/\mathbb{Q}$ be Galois of degree n, of Galois group G, and let $\eta \in K^\times$ be given such that $\langle\eta\rangle_G \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$. For p unramified in $K/\mathbb{Q}$ and prime to η, denote by n_p the residue degree of p, by g_p the number of prime ideals $\mathfrak{p} \mid p$ then by $o_\mathfrak{p}(\eta)$ and $o_p(\eta)$ the orders of η modulo $\mathfrak{p}$ and p, respectively.
In a first part, using Frobenius automorphisms, we show that for all p large enough, some explicit divisors of $p^{n_p}-1$ cannot realize $o_\mathfrak{p}(\eta)$ (Thms. 2.1, 4.1).
In a second part, we obtain that for all p large enough such that $n_p > 1$ we have $\text{Prob}(o_p(\eta) < p) \leq \frac{1}{p^{g_p\,(n_p-1)-\varepsilon}}$, where $\varepsilon = O\big(\frac{1}{\log_2(p)}\big)$ (Thm. 6.1).
Thus, under the heuristic of Borel–Cantelli this yields $o_p(\eta) > p$ for all p large enough such that $g_p(n_p-1) \geq 2$, which covers the particular cases of cubic fields with $n_p = 3$ and quartic fields with $n_p = 2$, but not the quadratic fields with $n_p = 2$; in this case, the natural conjecture is, on the contrary, that $o_p(\eta) < p$ for infinitely many inert p (Conj. 8.1).

November 5, 2015

1. Frobenius automorphisms

1.1. **Generalities.** Let $K/\mathbb{Q}$ be Galois of degree n and of Galois group G. We denote by h a possible residue degree, that is a divisor of n for which there exists a cyclic subgroup H of G of order h. One knows that, for any generator s of H, there exist infinitely many prime numbers p, unramified in $K/\mathbb{Q}$, such that s is the Frobenius automorphism of a prime ideal $\mathfrak{p} \mid p$ in $K/\mathbb{Q}$.

The number h dividing n takes a finite number of values and we fix such an integer h. We shall see that the results (especially the Theorem 2.1) only depend of h and not of the choice of H of order h nor of s generating H.

1.2. **Orders modulo $\mathfrak{p}$ and modulo p.** Let $\eta \in K^\times$. In the sequel we shall assume that the $\mathbb{Z}[G]$-module $\langle\eta\rangle_G$ generated by η is of $\mathbb{Z}$-rank n (i.e., $\langle\eta\rangle_G \otimes \mathbb{Q} \simeq \mathbb{Q}[G]$), but this is not needed for the following definition.

Definition 1.1. Let p be a prime number, prime to η, and let $\mathfrak{p}$ be a prime ideal of K dividing p. We call order of η modulo $\mathfrak{p}$ (denoted $o_\mathfrak{p}(\eta)$) the least nonzero integer k such that $\eta^k \equiv 1 \pmod{\mathfrak{p}}$. We call order of η modulo p (denoted $o_p(\eta)$) the least nonzero integer k such that $\eta^k \equiv 1 \pmod{p}$. We have $o_p(\eta) = \text{l.c.m.}\,(o_\mathfrak{p}(\eta),\ \mathfrak{p} \mid p)$.

We consider, for any prime p of residue degree $n_p = h$, the characteristic property of the Frobenius automorphism $s_\mathfrak{p}$, of $\mathfrak{p} \mid p$, which implies (cf. [Wa], Appendix, § 3, or [Gr3], Section II.1.1.5, Definition II.1.2.1.2, Remark II.3.1.3.1):

$$\eta^{s_\mathfrak{p}} \equiv \eta^p \pmod{\mathfrak{p}}.$$

Let $H := \langle s_\mathfrak{p}\rangle$ be the decomposition group of $\mathfrak{p}$ and let $\sigma \in G/H$ (or a representative in G); the Frobenius automorphism $s_\mathfrak{p}^\sigma$ of $\mathfrak{p}^\sigma$ is $\sigma.s_\mathfrak{p}.\sigma^{-1}$ and we get $\eta^{s_\mathfrak{p}^\sigma} \equiv \eta^p \pmod{\mathfrak{p}^\sigma}$. So, if $s_\mathfrak{p}$ and σ commute this yields to $\eta^{s_\mathfrak{p}} \equiv \eta^p \pmod{\mathfrak{p}^\sigma}$.

1991 *Mathematics Subject Classification.* Primary 11R04 ; Secondary 11R11, 11R16 .
Key words and phrases. algebraic numbers; order modulo a prime; Frobenius automorphisms.

In other words, we have $\eta^{s_{\mathfrak p}} \equiv \eta^p \pmod{\prod_{\sigma\in G/H,\, \sigma.s_{\mathfrak p}=s_{\mathfrak p}.\sigma} \mathfrak p^\sigma}$. In the Abelian case, we get $\eta^{s_{\mathfrak p}} \equiv \eta^p \pmod p$ independently on the choice of $\mathfrak p \mid p$.

Lemma 1.2. *Let $\eta \in K^\times$ be such that $\langle \eta\rangle_G$ is of $\mathbb Z$-rank n and let $\mu(K)$ be the group of roots of unity contained in K. Let $s \in G$, s of order h, and let $f(X) \in \mathbb Z[X]$ be a given polynomial such that $f(s) \neq 0$ in $\mathbb Z[G]$.*
Then, for all large enough prime number p such that $s = s_{\mathfrak p}$ for $\mathfrak p \mid p$, whatever $\zeta \in \mu(K)$ we have $\eta^{f(p)} \not\equiv \zeta \pmod{\mathfrak p}$.
Hence, if $d = \text{g.c.d.}\,(p^h-1, f(p))$, whatever $\zeta \in \mu(K)$ we have $\eta^d \not\equiv \zeta \pmod{\mathfrak p}$.

Proof. We have $\eta^{f(p)} \equiv \eta^{f(s)} \pmod{\mathfrak p}$; thus, if $\eta^{f(p)} \equiv \zeta \pmod{\mathfrak p}$ for some ζ, this yields to $\eta^{f(s)} - \zeta \equiv 0 \pmod{\mathfrak p}$ giving $\mathrm N_{K/\mathbb Q}(\eta^{f(s)} - \zeta) \equiv 0 \pmod p$ by the norm in $K/\mathbb Q$. Since $\langle\eta\rangle_G$ is of $\mathbb Z$-rank n and $f(s) \neq 0$, we have $\eta^{f(s)} \notin \mu(K)$; then $\mathrm N_{K/\mathbb Q}(\eta^{f(s)} - \zeta)$ is a nonzero rational constant depending only on η, $f(s)$, ζ, and the proof follows with explicit possible exceptions p in finite number. □

If for instance $K/\mathbb Q$ is Abelian, the congruence is equivalent to $\eta^{f(s)} - \zeta \not\equiv 0 \pmod p$, giving a much stronger condition for a contradiction.

If s is of order h, any nonzero element of $\mathbb Z[G]$ can be writen $f(s)$ where f is a polynomial of degree $< h$ (e.g. if $h = 1$, then $f \in \mathbb Z \setminus \{0\}$). Of course, an interesting application of the Lemma, independently of p, is for instance that $f(X) \mid X^h - 1$ in $\mathbb Z[X]$.

2. Consequences for the values of $o_{\mathfrak p}(\eta)$

We have the factorization $p^h - 1 = \prod_{\delta\mid h} \Phi_\delta(p)$, where $\Phi_\delta(X)$ is the δth cyclotomic polynomial (see [Wa], Ch. 2). So we can consider the particular divisors $\prod_{\delta\in I} \Phi_\delta(p)$, where I is any strict subset of the set of divisors of h. Of course, it will be sufficient to restric ourselves to *maximal* subsets I, which gives the divisors $D_{h,\delta}(p) := \dfrac{p^h-1}{\Phi_\delta(p)}$, $\delta \mid h$. For instance, if $h = 6$, we get the set:

$$\{\, p^5+p^4+p^3+p^2+p+1,\ p^5-p^4+p^3-p^2+p-1,\ p^4-p^3+p-1,\ p^4+p^3-p-1\}.$$

giving the complete set of divisors:

$$\{\,1, p-1, p+1, p^2-1, p^2-p+1, p^3-2\,p^2+2\,p-1, p^3+1, p^4-p^3+p-1, p^2+p+1, p^3-1,$$
$$p^3+2\,p^2+2\,p+1, p^4+p^3-p-1, p^4+p^2+1, p^5-p^4+p^3-p^2+p-1, p^5+p^4+p^3+p^2+p+1\}.$$

Theorem 2.1. *Let $K/\mathbb Q$ be Galois of degree n and of Galois group G. Let $h \mid n$ be a possible residue degree in $K/\mathbb Q$. Let $\mu(K)$ be the group of roots of unity contained in K. Let $\eta \in K^\times$ be such that the $\mathbb Z[G]$-module generated by η is of $\mathbb Z$-rank n.*
Then for all large enough prime number p with residue degree h and for any $\mathfrak p \mid p$, the least integer $k \geq 1$ for which there exists $\zeta \in \mu(K)$ such that $\eta^k \equiv \zeta \pmod{\mathfrak p}$ is a divisor of $p^h - 1$ and cannot divide any of the integers $D_{h,\delta}(p) := \dfrac{p^h-1}{\Phi_\delta(p)}$, $\delta \mid h$, where Φ_δ is the δth cyclotomic polynomial.
Hence, $o_{\mathfrak p}(\eta)$ and $o_p(\eta)$ do not divide any of the $D_{h,\delta}(p)$ (cf. Definition 1.1).

Proof. Let $k' = \text{g.c.d.}\,(k, p^h-1)$. Then we have $k' = \lambda\, k + \mu\,(p^h-1)$, $\lambda, \mu \in \mathbb Z$, and $\eta^{k'} \equiv \eta^{\lambda\, k} \equiv \zeta^\lambda \pmod{\mathfrak p}$; so $k' = k \mid p^h - 1$.

Suppose that k divides some $D_{h,\delta}(p) = \dfrac{p^h-1}{\Phi_\delta(p)} = \displaystyle\prod_{\delta'\mid h,\ \delta'\neq\delta} \Phi_{\delta'}(p)$. Let s be the Frobenius automorphism of $\mathfrak p$ and $H = \langle s\rangle$ its decomposition group. Thus $\eta^k \equiv \zeta \pmod{\mathfrak p}$ yields to $\eta^{D_{h,\delta}(p)} \equiv \zeta' \pmod{\mathfrak p}$, $\zeta' \in \mu(K)$, giving

$$\eta^{D_{h,\delta}(p)} \equiv \eta^{D_{h,\delta}(s)} \equiv \zeta' \pmod{\mathfrak p}.$$

From $\mathbb{Z}[H] \simeq \mathbb{Z}[X]/(X^h-1)$, we get $D_{h,\delta}(s) = \prod_{\delta' \mid h,\, \delta' \neq \delta} \Phi_{\delta'}(s) \neq 0$ in $\mathbb{Z}[G]$ since $D_{h,\delta}(X) \notin (X^h-1)\,\mathbb{Z}[X]$; the $D_{h,\delta}(X) \in \mathbb{Z}[X]$ being independent of p, the Lemma 1.2 gives a contradiction for all p large enough with residue degree $n_p = h$. □

This result is the generalization of particular cases used in [Gr1] for $h = 2$. For instance, in the above case $h = 6$ and p large enough (with $n_p = 6$), the orders $o_{\mathfrak{p}}(\eta)$ are divisors of p^6-1 which are not divisors of the integers in the set:

$\{\, p^5+p^4+p^3+p^2+p+1,\ p^5-p^4+p^3-p^2+p-1,\ p^4-p^3+p-1,\ p^4+p^3-p-1\}$.

For $p = 1093$, only 76 divisors are possible among the 384 divisors of p^6-1.

The case $h = 1$ (p totally split in $K/\mathbb{Q}$) gives the poor information $o_{\mathfrak{p}}(\eta) > 1$ equivalent to $\eta \not\equiv 1 \pmod{\mathfrak{p}}$ which is obvious for p large enough.

The case $h = \ell$ (a prime) implies that $o_{\mathfrak{p}}(\eta)$ is not a divisor of $p-1$ nor a divisor of $p^{\ell-1}+\cdots+p+1$ for p large enough; this means that $o_{\mathfrak{p}}(\eta) = d_1 d_2$ with $d_1 \mid p-1$, $d_1 \neq 1$, $d_2 \mid p^{\ell-1}+\cdots+p+1$, $d_2 \neq 1$ (taking care of the fact that when $p \equiv 1 \pmod{\ell}$, we have g.c.d. $(p-1, p^{\ell-1}+\cdots+p+1) = \ell$).

The expression *"for all large enough prime p of residue degree h"* in the theorem is effective and only depends, numerically, of h and the conjugates of η.

Remark 2.2. It is clear that if, for instance, $r \in \mathbb{N}$ is a small nonzero integer, the Theorem 2.1 implies that for all large enough prime p with residue degree h and for any $\mathfrak{p} \mid p$, the least integer $k \geq 1$ for which there exists $\zeta \in \mu(K)$ such that $\eta^k \equiv \zeta \pmod{\mathfrak{p}}$ cannot divide any of the integers $r.\,D_{h,\delta}(p)$, $\delta \mid h$ (indeed, η^r is still "small" in an Archimedean point of view).

So the "probabilities" of $o_{\mathfrak{p}}(\eta) \mid r.\,D_{h,\delta}(p)$ increase (from 0) if the factor r (such that $r \mid \Phi_\delta(p)$) increases (from $r = 1$). In the example $h = \ell$, where $o_{\mathfrak{p}}(\eta) = d_1 d_2$, $d_1 \mid p-1$, $d_2 \mid p^{\ell-1}+\cdots+p+1$, we have $d_1, d_2 \to \infty$ when $p \to \infty$.

3. A numerical example

Let K be the cyclic cubic field of conductor 7 defined, from a primitive 7th root of unity ζ_7, via $x = \zeta_7 + \zeta_7^{-1}$, by the polynomial X^3+X^2-2X-1.

Let $\eta = 8x+5$ of norm -203; then for $p < 200$, inert in K, we obtain the exceptional example $o_{17}(\eta) = 307 = p^2+p+1$ and no other when p increases; we get some illustrations with a small $r > 1$ ($p = 101$, $r = 2$, with $o_p(\eta) = r.\,(p^2+p+1)$), according to the following numerical results (note that when $p \equiv 1 \pmod 3$, we have $o_p(\eta) = \frac{1}{3} \times$ g.c.d. $(o_p(\eta), p-1) \times$ g.c.d. $(o_p(\eta), p^2+p+1)$):

(i) $p \equiv 2 \pmod 7$:

p	g.c.d. $(o_p(\eta), p-1)$	g.c.d. $(o_p(\eta), p^2+p+1)$
23	11	553
37	36	201
79	78	6321
107	53	11557
149	37	22351
163	54	26733
191	190	36673

(ii) $p \equiv 3 \pmod 7$:

p	g.c.d. $(o_p(\eta), p-1)$	g.c.d. $(o_p(\eta), p^2+p+1)$
17 *	1	307
31	15	993
59	58	3541
73	9	5403
101 **	2	10303
157	26	8269
199	198	39801

(iii) $p \equiv 4 \pmod 7$:

p	g.c.d. $(o_p(\eta), p-1)$	g.c.d. $(o_p(\eta), p^2+p+1)$
11	10	133
53	26	2863
67	33	4557
109	27	11991
137	136	18907
151	75	22953
179	89	32221
193	192	37443

(iv) $p \equiv 5 \pmod 7$:

p	g.c.d. $(o_p(\eta), p-1)$	g.c.d. $(o_p(\eta), p^2+p+1)$
19	9	381
47	23	2257
61	10	1261
89	11	8011
103	102	10713
131	65	17293
173	172	30103

4. A lower bound for $o_p(\eta)$

When η is fixed in $K^\times$, very small orders are impossible as $p \to \infty$ because of the following theorem giving Archimedean constraints; in this result none hypothesis is done on the rank of the $\mathbb{Z}[G]$-module generated by η nor on the field K itself.

Theorem 4.1. *Let $\mu(K)$ be the group of roots of unity of K. Let $\eta \in K^\times \setminus \mu(K)$. Let $\nu \in \mathbb{N} \setminus p\,\mathbb{N}$ be such that $\nu\,\eta \in Z_K$ (the ring of integers of K).*
Then, for any p prime to η, the congruence $\eta^k \equiv \zeta \pmod p$, $\zeta \in \mu(K)$, $k \geq 1$, implies $k \geq \dfrac{\log(p)-\log(2)}{\max\big(\log(c_0(\eta))+\log(\nu), \log(\nu)\big)}$, where $c_0(\eta) = \max_{\sigma\in G}(|\eta^\sigma|)$.
If $\eta \in Z_K$ (i.e., $\nu = 1$), then $k \geq \dfrac{\log(p-1)}{\log(c_0(\eta))}$.
In other words, if $Z_{K,(p)}$ is the ring of p-integers of K, the order of the image of η in $Z_{K,(p)}/\mu(K)\,.\,(1+p\,Z_{K,(p)})$, as well as $o_p(\eta)$, satisfies the above inequalities.

Proof. Put $\eta = \frac{\theta}{\nu}$, with $\theta \in Z_K$. The congruence is equivalent to $\theta^k = \zeta\,\nu^k + \Lambda\,p$, where $\Lambda \in Z_K \setminus \{0\}$ (because $\eta \notin \mu(K)$). Taking a suitable conjugate of θ, we can suppose $|\Lambda| \geq 1$. Thus $|\Lambda|\,p = |\theta^k - \zeta\,\nu^k| \leq |\theta|^k + \nu^k$ giving $|\theta|^k + \nu^k \geq p$; so, taking a conjugate θ_0 such that $|\theta_0| = \max_{\sigma\in G}(|\theta^\sigma|)$, we have $|\theta_0|^k + \nu^k \geq p$, with $|\theta_0| > 1$ since $\theta \in Z_K \setminus \mu(K)$.

(i) If $\nu \geq 2$, then $p \leq |\theta_0|^k + \nu^k \leq 2\max(|\theta_0|^k, \nu^k)$ and we obtain the result.

(ii) The case $\nu = 1$, used in [Gr1], Lemme 6.2, gives $|\theta_0|^k \geq p-1$, hence the better upper bound $k \geq \frac{\log(p-1)}{\log(c_0(\eta))}$ since $|\theta_0| = c_0(\eta) > 1$. □

Under the assumptions of Theorem 2.1 we have the following result.

Corollary 4.2. *Suppose that $\eta \in Z_K$; let p be of residue degree $h > 1$ such that $o_p(\eta) = r\,.\,d$, $d \mid D_{\delta,h}(p)$, $r \mid \Phi_\delta(p)$ (cf. Remark 2.2). Then $r \geq \dfrac{\log(p-1)}{\log(c_0(\eta^{D_{\delta,h}(s)}))}$, where s generates a decomposition group of p.*

5. Densities–Probabilities for $o_{\mathfrak{p}}(\eta)$ and $o_p(\eta)$

In this section, we examine some probabilistic aspects concerning the orders modulo $\mathfrak{p} \mid p$ of an algebraic number $\eta \in K^\times$. For any prime number p unramified in $K/\mathbb{Q}$ we recall that g_p is the number of prime ideals $\mathfrak{p} \mid p$ and n_p the common residue degree of these ideals. Let Z_K be the ring of integers of K; the residue fields $F_{\mathfrak{p}} = Z_K/\mathfrak{p}$ are isomorphic to $\mathbb{F}_{p^{n_p}}$.

5.1. **Densities.** It is assumed in this section that $\eta \in K^\times$ is a variable modulo p, prime to the given p (i.e., $\eta \in (\mathbb{Z}_{K,(p)}/p\,\mathbb{Z}_{K,(p)})^\times$). For each prime ideal $\mathfrak{p} \mid p$, let $\eta_\mathfrak{p} \in F_\mathfrak{p}^\times$ be the residue image of η. The density of such numbers η, whose diagonal image is given in $\prod_{\mathfrak{p}\mid p} F_\mathfrak{p}^\times$, is $\frac{1}{(p^{n_p}-1)^{g_p}}$ because the map: $\eta \pmod p \mapsto (\eta_\mathfrak{p})_{\mathfrak{p}\mid p}$ yields to an isomorphism (chinese remainder theorem) and, in some sense, the g_p conditions on the $\eta_\mathfrak{p}$, $\mathfrak{p} \mid p$, are independent as η varies (the notion of density is purely algebraic). Thus the orders $o_\mathfrak{p}(\eta)$ and $o_p(\eta)$ have obvious densities (see § 5.4).

5.2. **Probabilities and Independence.** We shall speak of probability when, on the contrary, $\eta \in K^\times$ is fixed and $p \to \infty$ is the variable; but to avoid trivial cases (as $\eta \in \mathbb{Q}^\times$ for which $o_p(\eta) \mid p-1$), we must make some hypothesis on η so that $o_p(\eta)$ can have any *possible* value dividing $p^{n_p}-1$ (see Theorem 2.1, Remark 2.2 and Theorem 4.1).

Let H be the decomposition group of a prime ideal $\mathfrak{p} \mid p$, p unramified in $K/\mathbb{Q}$. Considering $F_\mathfrak{p}^\times$ as a H-module (H is generated by the global Frobenius $s = s_\mathfrak{p}$ which makes sense in $F_\mathfrak{p}/\mathbb{F}_p$), $\prod_{\mathfrak{p}\mid p} F_\mathfrak{p}^\times$ is the induced representation and we get $\prod_{\mathfrak{p}\mid p} F_\mathfrak{p}^\times = \bigoplus_{\sigma\in G/H} \sigma F_\mathfrak{p}^\times$ where $\sigma F_\mathfrak{p}^\times = F_{\mathfrak{p}^\sigma}$ for all $\sigma \in G/H$.
In the same way, the representation $\langle\eta\rangle_G$ can be written $\langle\eta\rangle_G = \sum_{\sigma\in G/H} \sigma\langle\eta\rangle_H$, where $\langle\eta\rangle_H$ is the multiplicative $\mathbb{Z}[H]$-module generated by η. So, for natural congruential reasons, independently of p, concerning the map $\eta \pmod p \mapsto (\eta_\mathfrak{p})_{\mathfrak{p}\mid p}$, the representation $\langle\eta\rangle_G$ must be induced by the H-representation $\langle\eta\rangle_H$, i.e., we must have $\langle\eta\rangle_G = \bigoplus_{\sigma\in G/H} \sigma\langle\eta\rangle_H$ (otherwise, any $\mathbb{Z}$-relation between the conjugates of η gives non-independant variables $\eta_\mathfrak{p}$ in a probabilistic point of view). Since any cyclic subgroup H of G is realizable as a decomposition group when p varies, the above must work for any H; taking $H = 1$, ve get that $\langle\eta\rangle_G$ is of $\mathbb{Z}$-rank n, giving the following heuristic.

Heuristic 5.1. *Let $K/\mathbb{Q}$ be Galois of degree n and of Galois group G. Consider $\eta \in K^\times$ and, for any prime number p unramified in $K/\mathbb{Q}$ and prime to η, let $(\eta_\mathfrak{p})_{\mathfrak{p}\mid p}$ be the diagonal image of η in $\prod_{\mathfrak{p}\mid p} F_\mathfrak{p}^\times$. The components $\eta_\mathfrak{p}$ are independent as p varies (in the meaning that for given $a_\mathfrak{p} \in F_\mathfrak{p}^\times$, $\mathrm{Prob}(\eta_\mathfrak{p} = a_\mathfrak{p},\ \forall \mathfrak{p} \mid p) = \prod_{\mathfrak{p}\mid p} \mathrm{Prob}(\eta_\mathfrak{p} = a_\mathfrak{p})$) if and only if η generates a $\mathbb{Z}[G]$-module of $\mathbb{Z}$-rank n.*

5.3. **Remarks and examples.** We suppose that η generates a $\mathbb{Z}[G]$-module of $\mathbb{Z}$-rank n, which has trivial consequences:

(i) This implies that η is not in a strict subfield L of K; otherwise, if H is a non-trivial cyclic subgroup of G such that $L \subseteq K^H$, for any unramified prime p such that H is the decomposition group of $\mathfrak{p} \mid p$ with Frobenius s (of order h), the order of $\eta \pmod\mathfrak{p}$ is not a random divisor of p^h-1 but a divisor of $p-1$, the residue field of K^H at $\mathfrak{p}$ being $\mathbb{F}_p$ for infinitely many primes p.

(ii) In the same way, η cannot be an element of $K^\times$ of relative norm 1 because of the relation $\mathrm{N}_{K/K^H}(\eta) = 1$ giving $\eta^{p^{h-1}+\cdots+p+1} \equiv 1 \pmod\mathfrak{p}$. For instance, for the unit $\eta = 2\sqrt{2}+3$ and any p inert in $\mathbb{Q}(\sqrt{2})$, we obtain $\eta^{p+1} \equiv 1 \pmod p$ (i.e., $o_p(\eta) \mid p+1$), giving infinitely many primes p such that $o_p(\eta) < p$:

$(p, o_p(\eta))$ = (29,10), (59,20), (179,36), (197,18), (227,76), (229,46), (251,84),(269,30), (293,98), (379,76), (389,78), (419,140), (443,148), ...

(iii) Let $K = \mathbb{Q}(j, \sqrt[3]{2})$, where j is a primitive 3th root of unity, and let $\eta = \sqrt[3]{2}-1$ (a unit of $\mathbb{Q}(\sqrt[3]{2})$); for the same reason with $H = \mathrm{Gal}(K/\mathbb{Q}(j))$, from $\eta^{s^2+s+1} = 1$,

we get, for any prime p inert in $K/\mathbb{Q}(j)$, $\eta^{p^2+p+1} \equiv 1 \pmod p$ (for $p=7$, η is of order 19 modulo p and we have infinitely many p such that $o_p(\eta) \mid p^2+p+1$).

In such a non-Abelian case, some relations of dependence can also occur on a specific component $F_{\mathfrak{p}}^{\times}$, $\mathfrak{p} \mid p$. Since $\eta = \sqrt[3]{2}-1 \in \mathbb{Q}(\sqrt[3]{2})$, for any prime p inert in $K/\mathbb{Q}(\sqrt[3]{2})$ (in which case, p splits in $K/\mathbb{Q}(j)$), there exists a rational a such that $\sqrt[3]{2} \equiv a \pmod{\mathfrak{p}}$, $\sqrt[3]{2} \equiv a\,j^2 \pmod{\mathfrak{p}^s}$, $\sqrt[3]{2} \equiv a\,j \pmod{\mathfrak{p}^{s^2}}$. So $\eta \equiv a-1 \pmod{\mathfrak{p}}$ is of order a divisor of $p-1$ modulo $\mathfrak{p}$, but not necessarily modulo p: for $p=5$ we have $\sqrt[3]{2} \equiv 3 \pmod{\mathfrak{p}}$, $\sqrt[3]{2} \equiv 3j^2 \pmod{\mathfrak{p}^s}$, $\sqrt[3]{2} \equiv 3j \pmod{\mathfrak{p}^{s^2}}$. Then $\eta \equiv 2 \pmod{\mathfrak{p}}$ is of order 4 modulo $\mathfrak{p}$, but $\eta \equiv 3j^2-1 \pmod{\mathfrak{p}^s}$ is of order 8 modulo $\mathfrak{p}^s$. So the order of η modulo 5 is 8 but we have some constraints on the $\eta_{\mathfrak{p}}$.

5.4. **Probabilities for the order of η modulo p.** Now we suppose that the $\mathbb{Z}[G]$-module generated by η is of $\mathbb{Z}$-rank n.

Remarks 5.2. (i) Using the Theorem 2.1 we know that for $p \to \infty$ with $n_p > 1$, $o_p(\eta) \nmid D_{n_p,\delta}(p)$, $\forall\, \delta \mid n_p$; in particular, $o_p(\eta) \nmid p-1$. For this, the hypothesis on the $\mathbb{Z}$-rank of $\langle \eta \rangle_G$ is fundamental. In other words, the probability of some orders is zero. So the "standard" probabilities used in the sequel will give majorations of the true probabilities. This is strengthened by the Remark 2.2.

(ii) Moreover, the Theorem 4.1 gives obstructions for very small orders, the defect of probabilities being less than $O(\log(p))$, to be distributed among all orders. Thus, this favors large orders, which goes in the good direction because we shall study probabilities of orders $o_p(\eta)$ less than p when $n_p \geq 2$.

In a first approach, we can neglect these aspects and give some results in an heuristic point of view corresponding to the case where η is considered as a variable (so that probabilities coincide with densities) and we use the heuristic that when η is fixed once for all, probabilities are much lower than densities as $p \to \infty$.

If $D \mid p^{n_p}-1$, $o_p(\eta) \mid D$ is equivalent to $\eta_{\mathfrak{p}}^D = 1$ for all $\mathfrak{p} \mid p$. So we obtain, for any $D \mid p^{n_p}-1$, $\mathrm{Prob}\big(o_p(\eta) = D\big) \leq \mathrm{Prob}\big(o_p(\eta) \mid D\big) = \prod_{\mathfrak{p} \mid p} \mathrm{Prob}\big(\eta_{\mathfrak{p}}^D = 1\big)$. Since $F_{\mathfrak{p}}^{\times}$ is cyclic of order $p^{n_p}-1$, we get $\mathrm{Prob}\big(\eta_{\mathfrak{p}}^D = 1\big) = \dfrac{D}{p^{n_p}-1}$ and we get, for any $D \mid p^{n_p}-1$, $\mathrm{Prob}\big(o_p(\eta) = D\big) \leq \Big(\dfrac{D}{p^{n_p}-1}\Big)^{g_p}$. If $g_p = 1$, we can replace this inequality by $\mathrm{Prob}\big(o_p(\eta) = D\big) \leq \dfrac{\phi(D)}{p^{n_p}-1}$, where ϕ is the Euler function. When $g_p > 1$, the exact expression is more complicate since $o_p(\eta) = D$ if and only if $o_p(\eta_{\mathfrak{p}_0}) = D$ for at least one prime ideal $\mathfrak{p}_0 \mid p$ and $o_p(\eta_{\mathfrak{p}}) \mid D$ for all $\mathfrak{p} \mid p$, $\mathfrak{p} \neq \mathfrak{p}_0$, but we shall see that we do not need it since we use rough majorations.

6. Probabilities of orders $o_p(\eta) < p$

Suppose p large enough, non totally split in $K/\mathbb{Q}$. In [Gr1], the number η is a fixed *integer* of $K^{\times}$ and we have to consider the set

$$I_p(\eta) := \big\{[\eta]_p, \ldots, [\eta^k]_p, , \ldots, [\eta^{p-1}]_p\big\},$$

where $[\,.\,]_p$ denotes a suitable residue modulo $p\,Z_K$.

We need that $I_p(\eta)$ be a set with $p-1$ elements, to obtain valuable statistical results on the "local regulators $\Delta_p^{\theta}(z)$", $z \in I_p(\eta)$; this is equivalent to $\eta^k \not\equiv 1 \pmod p$ for all $k = 1, \ldots, p-1$, hence to $o_p(\eta) > p$ (cf. Definition 1.1).

So we are mainely interested by the computation of $\mathrm{Prob}\big(o_p(\eta) < p\big)$ and we intend to give an upper bound for this probability when $n_p > 1$. As we know from Theorem 2.1, $o_p(\eta) \nmid p-1$ for $p \to \infty$, but $o_p(\eta) < p$ remains possible for small p (e.g. $\eta = 5+\sqrt{-1}$ for which $p=19$ is inert in $\mathbb{Q}(\sqrt{-1})$ and $o_{19}(\eta) = 3 \times 5$).

We suppose $K \neq \mathbb{Q}$ and $n_p > 1$. We observe that n_p takes a finite number of values as p varies (e.g. $n_p \in \{2,3\}$ if $G \simeq D_6$).

Let $\mathcal{D}_p := \{D \mid p^{n_p}-1, D<p,\ D \nmid D_{n_p,\delta}(p),\ \forall\, \delta \mid n_p\}$; then we have for all p large enough:

$$\mathrm{Prob}\big(o_p(\eta)<p\big)=\mathrm{Prob}\big(o_p(\eta)\in\mathcal{D}_p\big)\leq \sum_{D\in\mathcal{D}_p}\Big(\frac{D}{p^{n_p}-1}\Big)^{g_p}=\frac{1}{(p^{n_p}-1)^{g_p}}\sum_{D\in\mathcal{D}_p}D^{g_p}.$$

A trivial upper bound for $\displaystyle\sum_{D\in\mathcal{D}_p}D^{g_p}$ is $\displaystyle\sum_{k=1}^{p-1}k^{g_p}=O(1)p^{g_p+1}$, giving the inequality $\mathrm{Prob}\big(o_p(\eta)<p\big)\leq\frac{O(1)}{p^{g_p(n_p-1)-1}}$ for which the application of the Borel–Cantelli heuristic supposes $g_p(n_p-1)\geq 3$, giving possible obstructions for quadratic or cubic fields with p inert, and quartic fields with $n_p=2$. But we can remove the obstructions concerning the cubic and quartic cases by giving a best upper bound using an analytic argument suggested by G. Tenenbaum.

Theorem 6.1. *Let $K/\mathbb{Q}$ be Galois of degree n and of Galois group G, and let $\eta\in K^\times$ be such that the $\mathbb{Z}[G]$-module generated by η is of $\mathbb{Z}$-rank n. For any prime p, let g_p be the number of prime ideals $\mathfrak{p}\mid p$ and let n_p be the residue degree of p in $K/\mathbb{Q}$. Then, for all large enough unramified p, such that $n_p>1$, we get $\mathrm{Prob}(o_p(\eta)<p)\leq\frac{1}{p^{g_p(n_p-1)-\varepsilon}}$, where $\varepsilon=O\big(\frac{1}{\log_2(p)}\big)$.*

Proof. Let $S_p:=\displaystyle\sum_{D\in\mathcal{D}_p}D^{g_p}$; under the sole conditions $D\mid p^{n_p}-1$, $D<p$, we have $S_p<\displaystyle\sum_{D\mid p^{n_p}-1}\Big(\frac{p}{D}\Big)^{g_p}D^{g_p}=p^{g_p}\times\tau(p^{n_p}-1)$, where $\tau(m)$ denotes the number of divisors of the integer m. From [T], Theorem I.5.4, we have for all $c>\log(2)$ and for all m large enough, $\tau(m)\leq m^{\frac{c}{\log_2(m)}}$, where $\log_2=\log\circ\log$. Taking $c=1$ and $m=p^{n_p}-1<p^{n_p}$, this yields $S_p<p^{g_p+n_p\,\frac{1}{\log_2(p^{n_p}-1)}}$ for all p large enough. Thus,

$$\begin{aligned}\mathrm{Prob}(o_p(\eta)<p)&\leq\frac{S_p}{(p^{n_p}-1)^{g_p}}\leq\frac{1}{(p^{n_p}-1)^{g_p}\times p^{-g_p-n_p/\log_2(p^{n_p}-1)}}\\&=\frac{1}{p^{g_p(n_p-1)-O\left(\frac{1}{\log_2(p)}\right)}}.\end{aligned}$$

□

To apply the Borel–Cantelli heuristic to obtain the finiteness of primes p such that $o_p(\eta)<p$, we must have $g_p(n_p-1)>\varepsilon+1$, hence $g_p(n_p-1)\geq 2$. Otherwise, if $g_p(n_p-1)\leq 1$, we get $g_p=1$ & $n_p=2$. So this is not sufficient to conclude for quadratic fields with p inert since in this case, $\mathrm{Prob}(o_p(\eta)<p)\leq\frac{1}{p^{1-\varepsilon}}$ with $\varepsilon=O\big(\frac{1}{\log_2(p)}\big)$.

Remarks 6.2. (i) We can replace the condition $\mathrm{Prob}\big(o_p(\eta)<p\big)$ by the condition $\mathrm{Prob}\big(o_p(\eta)<p^\kappa\big)$ for any real κ such that $1\leq\kappa<n_p-\frac{1}{g_p}$, in which case the Borel–Cantelli heuristic still applies and may have some interest for large n_p; for instance, if $K=\mathbb{Q}_r$ is the subfield of degree ℓ^r, $r\geq 1$, of the cyclotomic $\mathbb{Z}_\ell$-extension (ℓ a prime), and if we take primes p totally inert in $K/\mathbb{Q}$, then the result applies with $\kappa=\ell^r-2$ (if $\ell^r\neq 2$) for η as usual.

(ii) In the case of quadratic fields, we have to estimate $\frac{1}{p^2-1}\displaystyle\sum_{D\in\mathcal{D}_p}\phi(D)$ and a numerical experimentation with the following PARI program (see [P]) shows that the number of such divisors $D\in\mathcal{D}_p$ is conjecturally larger than $\frac{1}{3}\log_2(p)$ (we have no counterexamples for $7<p\leq 10^8$); but there are much solutions p (probably infinitely many) for which this number of divisors is less than $2\log_2(p)$.

```
{B = 10^8; p = 1; while(p < B, p = nextprime(p + 2); D = divisors(p^2 − 1);
d = 0; k = 0; N = 0; while(d < p − 1, k = k + 1; d = component(D, k);
if(Mod(p − 1, d)! = 0&Mod(p + 1, d)! = 0, N = N + 1));
Z = N − 1/3 ∗ log(log(p)); if(Z < 0, print(p, "", N)))}
```

We shall return more precisely to the quadratic case in § 8.4. We can state:

Conjecture 6.3. *Let $K/\mathbb{Q}$ be Galois of degree $n \geq 3$ and of Galois group G. Let $\eta \in K^\times$ be such that the $\mathbb{Z}[G]$-module generated by η is of $\mathbb{Z}$-rank n. For any prime p, prime to η, we denote by $o_p(\eta)$ the order of η modulo p.*
Then $o_p(\eta) > p$ for all unramified prime p, non totally split in $K/\mathbb{Q}$, except a finite number.

7. NUMERICAL EVIDENCES FOR THE ABOVE CONJECTURE

This section is independent of any $\eta \in K^\times$ but only depends on given parameters (n_p, g_p). For $n_p \geq 2$, we explicitely compute $S_p := \sum_{D \in \mathcal{D}_p} D^{g_p}$ and the upper bound $\frac{S_p}{(p^{n_p}-1)^{g_p}}$ of $\mathrm{Prob}\big(o_p(\eta) < p\big)$, using the program described below.

7.1. **General program about the divisors $D \in \mathcal{D}_p$.** It is sufficient to precise $n_p > 1$, g_p and the interval $[b, B]$ of primes p. The program gives the least value $C_b^B =: C$ of $C(p)$, when p varies in $[b, B]$, where we put $\frac{S_p}{(p^{n_p}-1)^{g_p}} =: \frac{1}{p^{C(p)}}$. The favourable cases for the Borel–Cantelli principle are those with $C_b^B > 1$, but the inequalities $C_b^B \geq C_b^\infty := \mathrm{Inf}_{p \in [b,\infty]} C(p)$, do not mean that the Borel–Cantelli principle applies since we ignore if $C_b^\infty > 1$ or not for b large enough, since C_b^∞ is an increasing function of b.

In the applications given below, n_p is a prime number (for which $D_{\delta,n_p}(p) \in \{p-1,\, p^{n_p-1} + \cdots + p + 1\}$); for more general values, one must first compute the set $\mathcal{D}_p$ as defined in the Theorem 2.1.

```
{B = 10^7; b = 10^6; gp = 1; np = 2; CC = gp ∗ (np − 1) + 1; p = b;
while(p < B, p = nextprime(p + 2); S = 0.0; M = p^np − 1;
D = divisors(M); d = 0; k = 0; while(d < p − 1, k = k + 1; d = component(D, k);
if(Mod(p − 1, d)! = 0&Mod(M/(p − 1), d)! = 0, S = S + d^gp));
C = (gp ∗ log(M) − log(S))/log(p); if(C < CC, CC = C)); print(CC)}
```

The initial value $CC := g_p\,(n_p - 1) + 1 \geq 2$ is an obvious upper bound for C_b^B.

7.2. **Application to quadratic fields with $n_p = 2$.** We have $g_p = 1$, $n_p = 2$. We obtain $C \approx 0.56402...$ for $10^6 \leq p \leq 10^7$, and we obtain $C \approx 0.58341...$ for $10^7 \leq p \leq 10^8$.

For larger primes p it seems that the constant C stabilizes.

If we replace D by $\phi(D)$ the result is a bit better (e.g. $C \approx 0.64766...$ instead of $0.56402...$ for $10^6 \leq p \leq 10^7$).

These results are coherent with the conclusions that we shall give in § 8.4.

7.3. **Application to cyclic cubic fields with $n_p = 3$.** We use the program with $g_p = 1$, $n_p = 3$. For instance, for $10^6 \leq p \leq 10^7$, we get $C \approx 1.5652... > 1$ as expected from Theorem 6.1.

7.4. **Application to quartic fields with $n_p = 2$.** For $g_p = 2$, $n_p = 2$, and $10^6 \leq p \leq 10^7$, we get $C = 1.6103....$

Of course, for $n_p = 4$ we get the larger constant $C = 2.4596....$ But if $n_p = 4$ we can test the similar stronger condition $\mathrm{Prob}\big(o_p(\eta) < p^2\big)$ for which one finds $C = 1.28442...$, giving the conjectural finiteness of totally inert primes p such that $o_p(\eta) < p^2$.

8. Numerical examples with fixed η and $p \to \infty$

The above computations are of a density nature and the upper bound $\frac{1}{p^C}$ is much higher than the true probability. So we intend to take a fixed $\eta \in K^\times$, restrict ourselves to primes p with suitable parameter n_p, and to compute the order of η modulo p to find the solutions p of $o_p(\eta) < p$.

The programs verify that η generates a $\mathbb{Z}[G]$-module of rank n. In the studied cases, $K/\mathbb{Q}$ is Abelian ($G = C_2$, C_3, C_4, $C_2 \times C_2$) and this condition is equivalent to $\eta^e \neq 1$ in $\langle\eta\rangle_G \otimes \mathbb{Q}$, for all rational idempotent e of $\mathbb{Q}[G]$.

8.1. **Cubic cyclic fields.** We then consider the following program with the polynomial $P = X^3 + X^2 - 2\,X - 1$ (see data in Section 3). Put $\eta = ax^2 + bx + c$; then a is fixed and b, c vary in $[-10, 10]$ and p in $[3, 10^4]$:

$\{P = x^3 + x^2 - 2 * x - 1; x0 = Mod(x, P); x1 = -x0^2 - x0 + 1; x2 = x0^2 - 2;$
$a = 1; for(b = -10, 10, for(c = -10, 10,$
$Eta0 = a * x0^2 + b * x0 + c; Eta1 = a * x1^2 + b * x1 + c; Eta2 = a * x2^2 + b * x2 + c;$
$N = norm(Eta0); R1 = Eta0 * Eta1 * Eta2; R2 = Eta0^2 * Eta1^{-1} * Eta2^{-1};$
$if(R1! = 1 \& R2! = 1 \& R1! = -1 \& R2! = -1,$
$p = 1; while(p < 10^4, p = nextprime(p + 2); if(Mod(N, p)! = Mod(0, p),$
$T = Mod(p, 7)^2; if(T! = 1, P1 = P + Mod(0, p);$
$A = Mod(a, p); B = Mod(b, p); C = Mod(c, p); X = Mod(A * x^2 + B * x + C, P1); Y = 1;$
$for(k = 1, p - 1, Y = Y * X; if(component(Y, 2) == 1,$
$print(a, "", b, "", c, "", p, "", k); k = p - 1)))))))\}$

We obtain no solutions except the following triples (where $\eta^k \equiv 1 \pmod p$; the eventual multiples of k are not written):

$(a, b, c, p, o_p(\eta)) = (1, -7, 7, 137, 56),\ (1, -3, 3, 37, 28),\ (1, 4, 8, 47, 37),\ (1, 6, -10, 31, 18).$

We have here an example ($\eta = x^2 + 4x + 8$, $p = 47$) where $o_p(\eta) = 37$ divides $p^2 + p + 1 = 37 \times 61$; this can be possible because p is too small regarding $\eta^{s^2+s+1} = 1 + 8\,p = 377$ (see Lemma 1.2).

8.2. **Quartic cyclic or biquadratic fields.** We consider the quartic cyclic field K defined by the polynomial $P = X^4 - X^3 - 6X^2 + X + 1$ of discriminant 34^2. The quadratic subfield of K is $k = \mathbb{Q}(\sqrt{17})$ and $K = k\Big(\sqrt{\frac{17+\sqrt{17}}{2}}\Big)$. The program is analogous to the previous one with $n_p = 2$. Put $\eta = ax^3 + bx^2 + cx + d$; then b, c, d vary in $[-10, 10]$, and p in $[3, 10^4]$:

$\{P = x^4 - x^3 - 6 * x^2 + x + 1; x0 = Mod(x, P); x1 = -1/2 * x0^3 + 3 * x0 + 3/2;$
$x2 = x0^3 - x0^2 - 6 * x0 + 1; x3 = -1/2 * x0^3 + x0^2 + 2 * x0 - 3/2;$
$a = 1; for(b = -10, 10, for(c = -10, 10, for(d = -10, 10,$
$Eta0 = a * x0^3 + b * x0^2 + c * x0 + d; Eta1 = a * x1^3 + b * x1^2 + c * x1 + d;$
$Eta2 = a * x2^3 + b * x2^2 + c * x2 + d; Eta3 = a * x3^3 + b * x3^2 + c * x3 + d;$
$N = norm(Eta0);$
$R1 = Eta0 * Eta1 * Eta2 * Eta3; R2 = Eta0 * Eta2^{-1}; R3 = Eta0 * Eta1^{-1} * Eta2 * Eta3^{-1};$
$if(R1! = 1 \& R2! = 1 \& R3! = 1 \& R1! = -1 \& R2! = -1 \& R3! = -1,$
$p = 1; while(p < 10^4, p = nextprime(p + 2);$
$if(Mod(N, p)! = Mod(0, p),$
$if(issquare(Mod(p, 17)) == 1, u = sqrt(Mod(17, p)); v = (17 + u)/2;$
$if(issquare(v) == 0, P1 = P + Mod(0, p); A = Mod(a, p); B = Mod(b, p);$
$C = Mod(c, p); D = Mod(d, p); X = Mod(A * x^3 + B * x^2 + C * x + D, P1); Y = 1;$
$for(k = 1, p - 1, Y = Y * X; if(component(Y, 2) == 1,$
$print(a, "", b, "", c, "", d, "", p, "", k); k = p - 1))))))))))\}$

We obtain no solutions except the following ones (where $\eta^k \equiv 1 \pmod p$ and where we consider only a representative of η modulo p and $k = o_p(\eta)$):

$(a, b, c, d, p, o_p(\eta)) = (1, -10, 2, -10, 19, 12),\ (1, -9, 6, 9, 43, 33),\ (1, -8, 7, 7, 461, 276),$
$(1, -3, 0, -6, 223, 64),\ (1, -1, -6, -10, 229, 184),\ (1, -1, 3, -2, 59, 40),$

$(1,3,-8,6,53,9)$, $(1,3,-5,10,83,21)$, $(1,9,-7,5,43,22)$.

For the last three cases, the order divides $p+1$ for the same reason as above.

Then we have the more exceptional solution $(1,-4,1,8,1549,1395)$ where $1395 = 9\times 5\times 31$ with $9 \mid p-1$ and $5\times 31 \mid p+1$.

8.3. **Quadratic fields.** We consider the field K defined by the polynomial $P = X^2-3$ and the following program with $\eta = a\sqrt{3}+b$, $b\in[-10,10]$:

$\{P=x^2-3; x0=Mod(x,P); x1=-x0; a=1; for(b=-10,10,$
$Eta0=a*x0+b; Eta1=a*x1+b; N=norm(Eta0);$
$R1=Eta0*Eta1; R2=Eta0*Eta1^{-1}; if(R1!=1\&R2!=1\&R1!=-1\&R2!=-1,$
$p=10^4; while(p<10^5, p=nextprime(p+2); if(Mod(N,p)!=Mod(0,p),$
$T=Mod(3,p); if(issquare(T)==0, P1=P+Mod(0,p);$
$A=Mod(a,p); B=Mod(b,p); X=Mod(A*x+B,P1); Y=1; for(k=1,p-1, Y=Y*X;$
$if(component(Y,2)==1, print(a,"",b,"",p,"",k); k=p-1)))))))\}$

For small primes p we obtain the following solutions (there are solutions $o_p(\eta)\mid p-1$ or $o_p(\eta)\mid p+1$ since p is small regarding η):

$(a,\ b,\ p,\ o_p(\eta)) = (1,-9,41,15)$, $(1,-9,1301,403)$, $(1,-8,5,3)$, $(1,-7,29,24)$, $(1,-7,103,39)$,
$(1,-7,727,143)$, $(1,-4,701,675)$, $(1,3,43,33)$, $(1,6,1123,843)$, $(1,7,29,24)$, $(1,7,103,78)$,
$(1,7,727,286)$, $(1,9,41,30)$, $(1,9,89,55)$, $(1,9,1301,806)$, $(1,9,6163,4623)$,$(1,10,79,65)$,
$(1,10,101,75)$, $(1,10,967,847)$.

For $10^4\le p\le 10^5$ we get the following solutions:

$(a,\ b,\ p,\ o_p(\eta)) = (1,-10,20359,13234)$, $(1,-10,90149,72700)$, $(1,-9,29501,6705)$,
$(1,-8,10711,2210)$, $(1,-5,86969,81172)$, $(1,-4,30941,25785)$, $(1,5,86969,81172)$,
$(1,8,10711,1105)$, $(1,9,29501,13410)$, $(1,10,20359,6617)$, $(1,10,90149,72700)$.

It is clear that the Conjecture 6.3 is likely for degrees $n>2$. The question arises for quadratic fields with $n_p=2$. We give here some supplementary computations.

(i) For instance, if we fix $\eta = 5\sqrt{3}+2$ and take large primes, inert in $\mathbb{Q}(\sqrt{3})$, the following simplified program:

$\{m=3; a=5; b=2; p=1; while(p<5*10^7, p=nextprime(p+2); T=Mod(p,12);$
$if(T!=1\&T!=11, A=Mod(a,p); B=Mod(b,p); Y1=0; Y2=1;$
$for(k=1,p-1, Z=B*Y1+A*Y2; Y2=B*Y2+m*A*Y1; Y1=Z;$
$if(Y1==0\&Y2==1, print(p,"",k); k=p-1))))\}$

gives the few solutions (up to $p\le 5\times 10^7$):

$(p, o_p(\eta)) = (5,4)$, $(29,21)$, $(1063,944)$, $(32707,23384)$, $(90401,68930)$.

(ii) For $\eta = 7\sqrt{3}+3$ we obtain the solutions (up to $p\le 5\times 10^7$):

$(p, o_p(\eta)) = (7,6)$, $(29,21)$, $(137,92)$, $(7498769,5927335)$, $(39208553,31070928)$.

The presence of the common solution $(29,21)$ shows that the pairs $(o_p(\eta),p)$ such that $o_p(\eta)\mid p^2-1$ & $o_p(\eta)<p$ give many solutions when η varies. Moreover, the presence of large solutions as $(39208553,31070928)$ is a bad indication for finiteness.

(iii) Consider $K=\mathbb{Q}(\sqrt{-1})$ with $p\equiv 3 \pmod 4$ up to $p\le 5\times 10^7$.

For $a=1$, $b=4$ ($\mathrm{N}(\eta)=17$), we obtain the solution $(p, o_p(\eta)) = (49139,19593)$.

For $a=1$, $b=2$ ($\mathrm{N}(\eta)=5$), we obtain no solutions up to $p\le 5\times 10^7$.

For $a=3$, $b=11$ ($\mathrm{N}(\eta)=130$), we obtain the solutions $(p, o_p(\eta)) = (3,2)$, $(43,11)$, $(131,24)$, $(811,174)$, $(911,133)$, $(5743,3168)$, $(2378711,1486695)$.

Although this looks like the case of Fermat quotients for wich a specific heuristic is used in [Gr2], it seems that we observe more systematic large solutions in the quadratic case with p inert, and, contrary to the Fermat case, we have possibly infinitely many solutions. This should be because the problem is of a different nature and is connected with primitive roots problem in number fields (see [Mo]).

So we shall try in the next subsection to give some insights in the opposite direction for quadratic fields (infiniteness of inert primes p such that $o_p(\eta) < p$).

8.4. **Analysis of the quadratic case.** From the formula $\text{Prob}\big(o_p(\eta) < p\big) < \frac{1}{p^2-1}\sum_{D\in\mathcal{D}_p}\phi(D)$ of Remark 6.2 (ii), we study the right member of the inequality

$$(p+1)\times \text{Prob}(o_p(\eta)<p) < \frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D);$$

from numerical experimentations, we can state, independently of any quadratic field K and $\eta\in K^\times$:

Conjecture 8.1. *Let $\mathcal{D}_p$ be the set of divisors D of p^2-1 such that $D<p$, $D\nmid p-1$, $D\nmid p+1$ (see Theorem 2.1). We have the inequalities:*

$$\frac{1}{3} \le \frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D) < O(1)\,p^{\log_2(p)/\log(p)},\quad p\to\infty.$$

The majoration $\frac{1}{p^2-1}\sum_{D\in\mathcal{D}_p}\phi(D) < \frac{O(1)}{p^{1-\log_2(p)/\log(p)}}$ (if exact) is an improvement of the upper bound $\frac{1}{p^{1-\varepsilon}}$ (for $\varepsilon = O\big(\frac{1}{\log_2(p)}\big)$) of the Theorem 6.1, but the sets of divisors are not the same and this information is only experimental.

On the contrary, the lower bound seems exact, except very few cases, and (if so) proves the infiniteness of inert primes p such that $o_p(\eta)<p$ (with $o_p(\eta)\nmid p-1$ and $o_p(\eta)\nmid p+1$) for fixed $\eta\in K^\times$ (such that η^{1+s} and η^{1-s} are distinct from roots of unity), for any quadratic field K.

For $p\in\{2,3,5,7,17\}$, we get the strict inequality $\frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D)<\frac{1}{3}$ and we have no other examples up to 10^8. Then for $p\in\{13,\ 37,\ 73,\ 193,\ 1153,\ 2593,\ 2917,\ 1492993,\ 1990657,\ 5308417,\ 28311553\}$, we have the equality $\frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D)=\frac{1}{3}$; in all these examples we have $p=1+2^u\times 3^v$, $u\ge 0$, $v\ge 0$, but the reciprocal is not exact (e.g., $p=19$ and $\mathcal{D}_p=\{8,12,15\}$).

It is not difficult to see that $\frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D)\approx\frac{1}{3}$ as soon as p is a "quasi Sophie Germain prime". We call quasi Sophie Germain a prime p such that $p^2-1=2^e\times q\,\ell$, $e\ge 3$, where q and ℓ are odd prime numbers.

Up to 10^7, we find only the quasi Sophie Germain primes $p=11$, 13, 17, 23, 31, 47, 193, 257, 383. Indeed, if for instance $p-1=2q$ and $p+1=2^{e-1}\ell$, this yields $q=-1+2^{e-2}\ell$ and $p=1+2q$; if $p-1=2^{e-1}q$ and $p+1=2\ell$, this yields $\ell=2^{e-2}q+1$ and $p=-1+2\ell$. Perhaps there are no other solutions.

With the following program

$\{b=10^{36}+123456789101112131415161718 19;\ B=b+10^3;\ p=b;$
$while(p<B, p=nextprime(p+2);\ S=0.0;\ M=p^2-1;\ L=1-log(log(p))/log(p);$
$D=divisors(p^2-1);\ d=0;\ k=0;\ while(d<p-1, k=k+1;\ d=component(D,k);$
$if(Mod(p-1,d)!=0 \& Mod(p+1,d)!=0, S=S+eulerphi(d)));$
$Pr=S/M;\ V1=S/(p-1)-1/3;\ V2=Pr*p^L;\ print(p,"",V1,"",Pr,"",V2))\}$

we obtain, for the inequalities $\frac{1}{3}\le\frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D)<O(1)\,p^{\log_2(p)/\log(p)}$, the following numerical data, first for small prime numbers, then for larger ones, where

- $\text{Proba} := \frac{1}{p^2-1}\sum_{D\in\mathcal{D}_p}\phi(D)$,
- $V_1 := (p+1)\times\text{Proba}-\frac{1}{3} = \frac{1}{p-1}\sum_{D\in\mathcal{D}_p}\phi(D)-\frac{1}{3}$,
- $V_2 := (p+1)\times\text{Proba}\times p^{1-\log_2(p)/\log(p)}$ giving a minoration of the possible $O(1)$ of the right member:

prime number p	V_1	Proba	V_2
112757	1.1437	1.31×10^{-5}	0.1269
112759	1.6679	1.77×10^{-5}	0.1720
112771	14.9499	1.35×10^{-4}	1.3137
112787	0.0538	3.43×10^{-6}	0.0332
112799	11.2873	1.03×10^{-4}	0.9989
112807	2.2715	2.31×10^{-5}	0.2239
112831	3.5941	3.48×10^{-5}	0.3376
112843	0.7225	9.35×10^{-6}	0.0907
112859	12.7989	1.16×10^{-4}	1.1288

prime number p	V_1	Proba	V_2
10000000123456789101112131415161723 23	10.4454	1.08×10^{-35}	0.1300
10000000123456789101112131415161724 39	110.0698	1.10×10^{-34}	1.3318
10000000123456789101112131415161724 57	0.0054	3.39×10^{-37}	0.0040
10000000123456789101112131415161725 51	112.7791	1.13×10^{-34}	1.3645
10000000123456789101112131415161726 31	19.9470	2.02×10^{-35}	0.2446
10000000123456789101112131415161726 43	0.6552	9.88×10^{-37}	0.0119
10000000123456789101112131415161726 61	16.5501	1.69×10^{-35}	0.2036
10000000123456789101112131415161727 19	67.9646	6.83×10^{-35}	0.8239
10000000123456789101112131415161727 61	185.5954	1.86×10^{-34}	2.2430

(i) For $p = 10000000123456789101112131415161724 57$, we have:

$p - 1 = 2^3 \times 3^2 \times 389 \times 62528362319 \times 571006238831466292903$,

$p + 1 = 2 \times 8131511 \times 614891877011344453762168643 39$.

(ii) We get the most spectacular case $p = 101234567891234567891258 87$, where the difference between $\dfrac{1}{3\,(p+1)}$ and the probability is $5.064... \times 10^{-23}$; then the upper bound is $V_2 = 0.00579$. For this prime we have the factorizations:

$p-1 = 2\times 5061728394561728394562943$, $p+1 = 2^8\times 3\times 13181584360837834360841$.

(iii) For $p = 504202701918008951235073$, where $V_1 = 0$, we have the factorizations $p - 1 = 1 + 2^9 \times 3^{44}$, $p + 1 = 2 \times 252101350959004475617537$.

References

[Gr1] G. Gras, *Les θ-régulateurs locaux d'un nombre algébrique – Conjectures p-adiques*, Canadian Journal of Mathematics, to appear (2016). http://dx.doi.org/10.4153/CJM-2015-026-3

[Gr2] G. Gras, *Étude probabiliste des quotients de Fermat*, Functiones et Approximatio, Commentarii Mathematici 2016 (to appear). https://www.dropbox.com/sh/64q8ezazl6b4z7d/AABhBL3Fvnf_YNTHV0GzhR8ma?dl=0

[Gr3] G. Gras, *Class Field Theory: from theory to practice*, SMM, Springer-Verlag 2003; second corrected printing 2005.

[Mo] P. Moree, *Artin's Primitive Root Conjecture - A Survey*, In: The John Selfridge Memorial Volume, Integers, Vol. 12A, 13 (2012), 1305–1416. http://www.integers-ejcnt.org/vol12a.html

[P] K. Belabas and al., *Pari/gp, Version 2.5.3*, Laboratoire A2X, Université de Bordeaux I. http://sagemath.org/

[T] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 3^e édition revue et augmentée, Coll. Échelles, Belin 2008.

[Wa] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

Villa la Gardette, chemin Château Gagnière, F–38520 Le Bourg d'Oisans.

E-mail address: g.mn.gras@wanadoo.fr http://www.researchgate.net/profile/Georges_Gras