On the order of the reductions of algebraic numbers

Pietro Sgobba

j.w. Antonella Perucca

University of Luxembourg

6 February 2020

The multiplicative order of (2 mod p)

p odd prime	3	5	7	11	13	17	19	23	29	31	37
ord(2 mod p)	2	4	3	10	12	8	18	11	28	5	36

41	43	47	53	59	61	67	71	73	79	83	89	97	...
20	14	23	52	58	60	66	35	9	39	82	11	48	...

The multiplicative order of $(2 \bmod p)$

p odd prime	3	5	7	11	13	17	19	23	29	31	37
$\mathrm{ord}(2 \bmod p)$	2	4	3	10	12	8	18	11	28	5	36

41	43	47	53	59	61	67	71	73	79	83	89	97	...
20	14	23	52	58	60	66	35	9	39	82	11	48	...

$$\mathrm{ord}(2 \bmod p) \neq 6 \qquad 2^6 - 1 = 3^2 \times 7$$

The multiplicative order of (2 mod p)

p odd prime	3	5	7	11	13	17	19	23	29	31	37
ord(2 mod p)	2	4	3	10	12	8	18	11	28	5	36

41	43	47	53	59	61	67	71	73	79	83	89	97	...
20	14	23	52	58	60	66	35	9	39	82	11	48	...

$$\mathrm{ord}(2 \bmod p) \neq 6 \qquad 2^6 - 1 = 3^2 \times 7$$

- Artin's Conjecture on primitive roots (1927): Are there infinitely many primes p such that $\mathrm{ord}(2 \bmod p) = p - 1$?

The multiplicative order of $(2 \bmod p)$

p odd prime	3	5	7	11	13	17	19	23	29	31	37
$\mathrm{ord}(2 \bmod p)$	2	4	3	10	12	8	18	11	28	5	36

41	43	47	53	59	61	67	71	73	79	83	89	97	...
20	14	23	52	58	60	66	35	9	39	82	11	48	...

$$\mathrm{ord}(2 \bmod p) \neq 6 \qquad 2^6 - 1 = 3^2 \times 7$$

- Artin's Conjecture on primitive roots (1927): Are there infinitely many primes p such that $\mathrm{ord}(2 \bmod p) = p - 1$?
- The density of primes p for which $\mathrm{ord}(2 \bmod p)$ is odd is $\frac{7}{24}$.
- Are there infinitely many primes p such that e.g. $\mathrm{ord}(2 \bmod p) \equiv 1 \bmod 3$?

Reductions for number fields

Let K be a number field.
Let $G \subseteq K^\times$ torsion-free subgroup of finite rank r.

For all but finitely many primes $\mathfrak{p}$ of K the reduction $G \bmod \mathfrak{p}$

- is a cyclic subgroup of $k_\mathfrak{p}^\times = (O_K/\mathfrak{p}O_K)^\times$
- has a multiplicative order $\mathrm{ord}_\mathfrak{p}(G) = \#(G \bmod \mathfrak{p})$
- satisfies

$$\mathrm{ord}_\mathfrak{p}(G) \mid \# k_\mathfrak{p}^\times = N(\mathfrak{p}) - 1$$

Reductions for number fields

Let K be a number field.
Let $G \subseteq K^\times$ torsion-free subgroup of finite rank r.

For all but finitely many primes $\mathfrak{p}$ of K the reduction G mod $\mathfrak{p}$

- is a cyclic subgroup of $k_\mathfrak{p}^\times = (O_K/\mathfrak{p}O_K)^\times$
- has a multiplicative order $\mathrm{ord}_\mathfrak{p}(G) = \#(G \bmod \mathfrak{p})$
- satisfies

$$\mathrm{ord}_\mathfrak{p}(G) \mid \#k_\mathfrak{p}^\times = N(\mathfrak{p}) - 1$$

Questions: Are there infinitely many primes $\mathfrak{p}$ for which

$$\mathrm{ord}_\mathfrak{p}(G) \equiv a \bmod d$$

for some fixed integers a, d? Does the density exist?

Theorem

$$\mathcal{P} := \{\mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d\}$$

Theorem

Assuming (GRH), the number of primes in $\mathcal{P}$ with norm up to x is

$$\mathcal{P}(x) = \frac{x}{\log x} \sum_{n,t \geqslant 1} \frac{\mu(n)c(n,t)}{[K(\zeta_{\mathrm{lcm}(dt,nt)}, \sqrt[nt]{G}) : K]} + O\left(\frac{x}{\log^{3/2} x}\right),$$

where $c(n,t) \in \{0,1\}$, with $c(n,t) = 1$ if and only if

- $\gcd(1+at, d) = 1$
- $\gcd(d, n) \mid a$
- *the element of* $\mathrm{Gal}(\mathbb{Q}(\zeta_{dt})/\mathbb{Q})$ *which maps* ζ_{dt} *to* ζ_{dt}^{1+at} *is the identity on* $\mathbb{Q}(\zeta_{dt}) \cap K(\zeta_{nt}, \sqrt[nt]{G})$

Ziegler, 2006: case of rank 1

Bounded failure of maximality of Kummer degrees:

Theorem

There is an integer $C \geqslant 1$, which depends only on K and G, such that for all $n, m \geqslant 1$ with $n \mid m$ the ratio

$$\frac{n^r}{[K(\zeta_m, \sqrt[n]{G}) : K(\zeta_m)]} \quad \textit{divides} \quad C\,.$$

Direct proof by Perucca, S. (2018)

Properties of the density

Denote the natural density of $\mathcal{P} = \{\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(G) \equiv a \bmod d\}$ by

$$\mathrm{dens}_K(G, a \bmod d) = \sum_{n,t \geqslant 1} \frac{\mu(n)c(n,t)}{[K(\zeta_{\mathrm{lcm}(dt,nt)}, \sqrt[nt]{G}) : K]}$$

We investigate whether this density is

- positive
- a rational number
- computable

The prime power case, $d = \ell^e$

Let ℓ be a prime number and $e \geqslant 1$.

Proposition (Debry, Perucca, 2016)

Given an integer $x \geqslant 0$ we have that

$$\mathrm{dens}_K(\{\mathfrak{p} : v_\ell(\mathrm{ord}_\mathfrak{p}(G)) = x\})$$

is a positive computable rational number.

The prime power case, $d = \ell^e$

Let ℓ be a prime number and $e \geqslant 1$.

Proposition (Debry, Perucca, 2016)

Given an integer $x \geqslant 0$ we have that

$$\mathrm{dens}_K(\{\mathfrak{p} : v_\ell(\mathrm{ord}_\mathfrak{p}(G)) = x\})$$

is a positive computable rational number.

Theorem

Assume (GRH). Suppose that $\zeta_\ell \in K$ if ℓ is odd, or that $\zeta_4 \in K$ if $\ell = 2$. Then

$$\mathrm{dens}_K(G, a \bmod \ell^e)$$

depends on a only through its ℓ-adic valuation, and it is a computable positive rational number.

Uniformity and positivity

Taking ℓ odd and $\ell \mid a$, if $\mathfrak{p}$ is a prime of K of degree 1 and unramified in $K(\zeta_\ell)$ and such that $\mathrm{ord}_\mathfrak{p}(G) \equiv a \bmod \ell^e$, then it splits completely in $K(\zeta_\ell)$

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \frac{1}{[K(\zeta_\ell) : K]} \cdot \mathrm{dens}_{K(\zeta_\ell)}(G, a \bmod \ell^e)$$

Uniformity and positivity

Taking ℓ odd and $\ell \mid a$, if $\mathfrak{p}$ is a prime of K of degree 1 and unramified in $K(\zeta_\ell)$ and such that $\mathrm{ord}_\mathfrak{p}(G) \equiv a \bmod \ell^e$, then it splits completely in $K(\zeta_\ell)$

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \frac{1}{[K(\zeta_\ell) : K]} \cdot \mathrm{dens}_{K(\zeta_\ell)}(G, a \bmod \ell^e)$$

Corollary

Assume (GRH). Suppose that $\ell \mid a$ if ℓ is odd, and that $4 \mid a$ (and $e \geqslant 2$) if $\ell = 2$. Then the density $\mathrm{dens}_K(G, a \bmod \ell^e)$ depends on a only through its ℓ-adic valuation, and it is a computable positive rational number.

Uniformity and positivity

Taking ℓ odd and $\ell \mid a$, if $\mathfrak{p}$ is a prime of K of degree 1 and unramified in $K(\zeta_\ell)$ and such that $\operatorname{ord}_{\mathfrak{p}}(G) \equiv a \bmod \ell^e$, then it splits completely in $K(\zeta_\ell)$

$$\operatorname{dens}_K(G, a \bmod \ell^e) = \frac{1}{[K(\zeta_\ell) : K]} \cdot \operatorname{dens}_{K(\zeta_\ell)}(G, a \bmod \ell^e)$$

Corollary

Assume (GRH). Suppose that $\ell \mid a$ if ℓ is odd, and that $4 \mid a$ (and $e \geqslant 2$) if $\ell = 2$. Then the density $\operatorname{dens}_K(G, a \bmod \ell^e)$ depends on a only through its ℓ-adic valuation, and it is a computable positive rational number.

Corollary

Assume (GRH). The density $\operatorname{dens}_K(G, a \bmod \ell^e)$ is positive.

The composite case

It is known unconditionally that $\text{dens}_K(G, 0 \bmod d)$ is a positive computable rational number.

The composite case

It is known unconditionally that $\mathrm{dens}_K(G, 0 \bmod d)$ is a positive computable rational number.

Theorem

Assume (GRH). Suppose that $\zeta_\ell \in K$ for all $\ell \mid d$, and $\zeta_4 \in K$ if d is even. Then for a coprime to d

$$\mathrm{dens}_K(G, a \bmod d)$$

is a computable positive rational number which does not depend on a.

The composite case

It is known unconditionally that $\mathrm{dens}_K(G, 0 \bmod d)$ is a positive computable rational number.

Theorem

Assume (GRH). Suppose that $\zeta_\ell \in K$ for all $\ell \mid d$, and $\zeta_4 \in K$ if d is even. Then for a coprime to d

$$\mathrm{dens}_K(G, a \bmod d)$$

is a computable positive rational number which does not depend on a.

Corollary

Assume (GRH). The density $\mathrm{dens}_K(G, a \bmod d)$ is positive whenever a is coprime to d.

An example

Take $G = \langle 2, 3 \rangle \leqslant \mathbb{Q}^\times$.

$a \bmod d$	$\mathrm{dens}_{\mathbb{Q}}(G, a \bmod d)$	primes up to 10^6
4 mod 16	$17/112 \approx 0.1518$	0.1522
12 mod 16	$17/112 \approx 0.1518$	0.1508
3 mod 9	$2/13 \approx 0.1538$	0.1538
6 mod 9	$2/13 \approx 0.1538$	0.1540
9 mod 27	$2/39 \approx 0.0513$	0.0513
18 mod 27	$2/39 \approx 0.0513$	0.0513
3 mod 27	$2/39 \approx 0.0513$	0.0518
6 mod 27	$2/39 \approx 0.0513$	0.0512
15 mod 27	$2/39 \approx 0.0513$	0.0513
21 mod 27	$2/39 \approx 0.0513$	0.0507

Thank you for your attention!