Enumerative arithmetic
Pagano, C.

Author: Pagano, C.
Title: Enumerative arithmetic
Issue Date: 2018-12-05

Stellingen

Stellingen

1

Let p be a prime number and let K be a field with $\mathrm{char}(K) = p$. Let $\Gamma \subseteq K^* \times K^*$ be a finitely generated subgroup. Denote by $r := \dim_{\mathbb{Q}}(\Gamma \otimes_{\mathbb{Z}} \mathbb{Q})$. Then

$$\#\{(x, y) \in \Gamma - \Gamma^p : x + y = 1\} \leq 31 \cdot 19^r.$$

2

Let p be an odd prime number and denote by ζ_p an element of $\mathbb{Q}_p^{\mathrm{sep}}$ having multiplicative order equal to p. Let d be in $p\mathbb{Z}_{\geq 1}$. For each $h \in \{1, ..., d-1\}$ we say that a polynomial $g(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$ in $\mathbb{Q}_p(\zeta_p)[x]$ is *h-Eisenstein* if $a_i \in (1-\zeta_p)\mathbb{Z}_p[\zeta_p]$ for each $i \in \{0, ..., d-1\}$ and $a_i \in (1-\zeta_p)\mathbb{Z}_p[\zeta_p] - (1-\zeta_p)^2\mathbb{Z}_p[\zeta_p]$ if and only if $i \in \{0, h\}$.

Let k, j be in $\{1, ..., d-1\}$ with $\gcd(p, kj) = 1$, and let $r_1(x), r_2(x)$ be respectively k- and j-Eisenstein polynomials of degree d. Then one has $k = j$ if and only if there is a group isomorphism $\varphi : (\frac{\mathbb{Z}_p[\zeta_p][x_1]}{r_1(x_1)})^* \to (\frac{\mathbb{Z}_p[\zeta_p][x_2]}{r_2(x_2)})^*$ such that

$$\varphi(1 + x_1^n \frac{\mathbb{Z}_p[\zeta_p][x_1]}{r_1(x_1)}) = 1 + x_2^n \frac{\mathbb{Z}_p[\zeta_p][x_2]}{r_2(x_2)},$$

for every positive integer n.

3

For a number field K and a positive integer c, we denote by $\mathrm{Cl}(K)$ the class group of K and by $\mathrm{Cl}(K, c)$ the ray class group of conductor c of K.

Let l be a prime number congruent to 3 modulo 8. Let $\mathcal{P}$ be the set of imaginary quadratic number fields K such that $\mathrm{disc}(K)$ is congruent to 1 modulo 4, $2\mathrm{Cl}(K)[2^\infty]$ is a cyclic non-trivial group and l is inert in K. Let $\mathcal{P}_0$ be the set of $K \in \mathcal{P}$ such that $\mathrm{Cl}(K, l)[2^\infty] \simeq_{\mathrm{ab.gr.}} \mathbb{Z}/4\mathbb{Z} \oplus \mathrm{Cl}(K)[2^\infty]$. We have that

$$\lim_{X \to \infty} \frac{\#\{K \in \mathcal{P}_0 : |\mathrm{disc}(K)| < X\}}{\#\{K \in \mathcal{P} : |\mathrm{disc}(K)| < X\}} = \frac{1}{2}.$$

Moreover, if $K \in \mathcal{P} - \mathcal{P}_0$ then $2\mathrm{Cl}(K, l)[2^\infty]$ is also cyclic with $\#2\mathrm{Cl}(K, l)[2^\infty] = 2 \cdot \#2\mathrm{Cl}(K)[2^\infty]$.

4

Let G be a topological group and H a normal subgroup of G. A *set of topological normal generators* of H in G is a subset X of H such that $\{gxg^{-1} : x \in X, g \in G\}$ is a set of topological generators of H.

Let p be a prime number and suppose that G is a pro-p group. Let moreover r be a positive integer. Then the group G is isomorphic to $\mathbb{Z}_p^r$ if and only if for every open normal subgroup N of G, a set of topological normal generators of N in G of smallest possible size has cardinality r.

5

Let L/K be a finite Galois extension of fields, with $\mathrm{Gal}(L/K)$ being an elementary abelian 2-group and with $\mathrm{char}(K) \neq 2$. Denote by $\mathbb{F}_2[\mathrm{Gal}(L/K)]$ the group ring of $\mathrm{Gal}(L/K)$ with coefficients in $\mathbb{F}_2$; this is a local Gorenstein $\mathbb{F}_2$-algebra. For an element $\alpha \in L^*$ denote by $\tilde{L}_{\sqrt{\alpha}}$ the normal closure of $L(\sqrt{\alpha})$ over K. Then the element $N_{L/K}(\alpha)$ is not in L^{*2} if and only if

$$\mathrm{Gal}(\tilde{L}_{\sqrt{\alpha}}/K) \simeq_{\mathrm{grp.}} \mathbb{F}_2[\mathrm{Gal}(L/K)] \rtimes \mathrm{Gal}(L/K),$$

where the implicit action in the semidirect product is given by the regular representation.

6

Let r be a positive integer and p a prime number. Let A be a free module over the ring $\mathbb{Z}/p^{r+1}\mathbb{Z}$ and G be a subgroup of $\mathrm{Aut}_{\mathrm{gr}}(A)$. Suppose that $p-1 > \mathrm{rk}_{\mathbb{Z}/p^{r+1}\mathbb{Z}}(A)$ and that A^G admits a cyclic direct summand of size p^r. Then there exists a cyclic subgroup H_0 of G such that A^{H_0} admits a cyclic direct summand of size p^r.

7

Let p be a prime number. Let $G := (\mathbb{Z}/p\mathbb{Z})^2$. Then there is a $\mathbb{Z}/p^2\mathbb{Z}[G]$-module A, free of rank $p(p+1)$ as a $\mathbb{Z}/p^2\mathbb{Z}$-module, such that A^G admits a cyclic direct summand of size p, but A^H doesn't for any proper subgroup H of G.

For a commutative ring R and for an R-module N, the *annihilator* of N is the set $\mathrm{Ann}_R(N) := \{x \in R : \forall n \in N, xn = 0\}$; it is an ideal of R. An R-module N is said to be *faithful* if $\mathrm{Ann}_R(N) = 0$.

8

Let R be a commutative ring, M a faithful R-module and J an ideal of R. Then $M/\mathrm{Ann}_R(J)M$ is a faithful $R/\mathrm{Ann}_R(J)$-module.

9

Let k be a field and A a commutative k-algebra such that $\dim_k(A) < \infty$. Suppose A has a unique maximal ideal m_A, and that $\dim_k(A/m_A) = 1$. Let M be a faithful A-module. Then

$$\dim_k(M) \geq 2\sqrt{\dim_k(A) - 1}.$$