WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

Ray class group calculations for Fermat curves over cyclotomic fields

Rachel Davis [1] and Rachel Pries[2]

[1] University of Wisconsin-Madison Department of Mathematics

[2] Colorado State University Department of Mathematics

Introduction

Let p be an odd prime and consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$. Let X be the smooth, projective Fermat curve of exponent p given by

$$x^p + y^p = z^p.$$

Fermat's Last Theorem: If $[x : y : z] \in X(\mathbb{Q})$ then $xyz = 0$.

The genus of X is $g = \frac{(p-1)(p-2)}{2}$. Let $U \subset X$ be the open affine given by $z \neq 0$ and let $Y \subset U$ denote the $2p$ points with $xy = 0$.

The group $\mu_p \times \mu_p$ acts on X and this action stabilizes U and Y. Let ϵ_0 and ϵ_1 be the generators of $\mu_p \times \mu_p$ which act by $\epsilon_0(x, y) = (\zeta_p x, y)$ and $\epsilon_1(x, y) = (x, \zeta_p y)$. Consider the group ring $\Lambda_1 = (\mathbb{Z}/p\mathbb{Z})[\mu_p \times \mu_p]$. Let $y_i = \epsilon_i - 1$, so that $\Lambda_1 = \mathbb{Z}/p\mathbb{Z}[y_0, y_1]/\langle y_0^p, y_1^p \rangle$.

Klassen/Tzermias, Tzermias, Sall: For Fermat curve of degree $p = 5, 7$, have complete description of degree $\leq p - 1$ points.

Debarre/Klassen: For ($d \geq 8$) all but finitely many points of X of degree $d - 1$ arise by intersecting X with rational line through rational point of X.

The relative homology group $M = H_1(U, Y)$ has dimension p^2. The homology group $H_1(U)$ has dimension $(p-1)^2$. Its quotient $H_1(X)$ has dimension $2g = (p-1)(p-2)$. Let $\beta \in H_1(U, Y)$ be the path $\beta : [0, 1] \to U(\mathbb{C})$ given by $t \mapsto (\sqrt[p]{t}, \sqrt[p]{1-t})$.

Anderson The relative homology group $H_1(U, Y)$ is a free Λ_1-module of rank 1 with generator β.

Motivation

The motivation to study Galois cohomology arises from the Kummer map. Let $b = [0 : 1 : 0]$ be a base point of X. Let $\pi_1(X)$ denote the étale fundamental group of X. Consider the lower central series:

$$\pi_1(X) = [\pi]_1 \supseteq [\pi]_2 \supseteq \ldots \supseteq [\pi]_n \supseteq \ldots.$$

Let G_K be the absolute Galois group of K. For a K-rational point η of X, let γ be a path in $X(\mathbb{C})$ from b to η. The generalized Kummer map

$$\kappa : \mathrm{Jac}(X)(K) \to \mathrm{H}^1(G_K, \pi_1(X))$$

is defined by $\kappa(\eta) = [\sigma \mapsto \gamma^{-1}\sigma(\gamma)]$ for $\sigma \in G_K$. Let $G_{K,S}$ be the Galois group of the maximal p-extension of K ramified only over $S = \{\nu\}$ where $\nu = \langle 1 - \zeta_p \rangle$. The Fermat curve has good reduction away from p and κ factors through $\kappa : \mathrm{Jac}(X)(K) \to \mathrm{H}^1(G_{K,S}, H_1(X) \otimes \mathbb{Z}/p\mathbb{Z})$.

Using work of Schmidt and Wingberg, Ellenberg defines a series of obstructions to $\mathrm{Jac}(X)(K)$. Let δ_2 denote the first of these obstructions; it was also studied by Zarkhin. The map δ_2 also factors through $G_{K,S}$ and has the form

$$\delta_2 : \mathrm{H}^1(G_{K,S}, \mathrm{H}_1(X) \otimes \mathbb{Z}_p) \to \mathrm{H}^2(G_{K,S}, ([\pi]_2/[\pi]_3) \otimes \mathbb{Z}_p).$$

Ray class groups

Let L be the splitting field of $1 - (1 - x^p)^p$. Let E, the maximal elementary abelian p-extension of L unramified outside $\mathfrak{p}$, a unique prime in L above p. It suffices to consider $G = \mathrm{Gal}(E/K)$ instead of $G_{K,S}$.

Let $Q = \mathrm{Gal}(L/K)$ where Then Q is an elementary abelian p-group. For p satisfying Vandiver's conjecture, the rank of Q is $r + 1$.

Then, letting $N = \mathrm{Gal}(E/L)$, there is a short exact sequence

$$0 \to N \to G \to Q \to 0.$$

There is an element in $\mathrm{H}^2(Q, N)$ which classifies the extension and determines the isomorphism class of the group G.

Writing $d_2 : \mathrm{H}^1(N, M)^Q \to \mathrm{H}^2(Q, M)$, then there is an exact sequence

$$0 \to \mathrm{H}^1(Q, M) \to \mathrm{H}^1(G, M) \to \mathrm{Ker}(d_2) \to 0.$$

Set $p = 3$. We compute the rank of the maximal elementary abelian 3-group quotient of the ray class group $\mathrm{Cl}_{\mathfrak{p}^k}(L)$ with modulus $\mathfrak{p}^k$ for $1 \leq k \leq 28$, where $\mathfrak{p}$ is the unique prime of L above p.

The rank increases at modulus $\mathfrak{p}^k$ when k is one of the following values $m_1, \ldots, m_{10}$: 12, 15, 18, 20, 21, 23, 24, 26, 27, 28 and then stabilizes. Let N_i and G_i be the corresponding Galois groups. Thus, $G = G_{10}$ has order 3^{12}.

Galois action

The group Q acts on N_i. For example, here are (the transposes of) the matrices computed using Magma for the action of σ and τ on N_7:

$$M_{\sigma,7} = \begin{pmatrix} 1&0&1&0&1&0&1 \\ 0&1&0&0&0&2&0 \\ 0&0&1&2&0&2&2 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&1&2&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix} \text{ and } M_{\tau,7} = \begin{pmatrix} 1&0&0&1&2&1&2 \\ 0&1&0&1&0&2&1 \\ 0&0&1&0&0&1&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1. \end{pmatrix}.$$

To compute d_2, we view $\phi \in \mathrm{H}^1(N, M)^Q$ as a Q-invariant homomorphism $\phi : N \to M$ and consider 2-cocycle $\omega : Q \times Q \to N$. Then ω is equivalent to a_i, $c_{j,k}$ for $0 \leq i \leq r$ and $0 \leq j < k \leq r$.

Here, we use $a_i = \omega(\sigma^2, \sigma)$, $b_i = \omega(\tau^2, \tau)$, $c = \omega(\tau, \sigma) - \omega(\sigma, \tau)$ to find

$$a_7 = [0, 2, 0, 2, 1, 0, 2], \; b_7 = [0, 0, 0, 0, 0, 0, 2], \text{ and } c_7 = [2, 1, 2, 0, 2, 1, 0].$$

Putting together information, yields presentations for the G_i. For example,

$$G_3 = \mathrm{Group}\langle s, t, n_1, n_2, n_3 | s^9, t^3, n_1^3, n_2^3, n_3^3, (t, n_1), (t, n_2), (t, n_3), (s, n_1) = n_3, (s, n_2), (s, n_3), (n_1, n_2), (n_1, n_3), (n_2, n_3), s^3 = n_2^{-1}, (s, t) = n_1^{-1} n_2 n_3^{-1} \rangle = \mathrm{SmallGroup}(243, 13).$$

Invariant maps

A map ϕ is Q-invariant if and only if, for every $\vec{n} \in N$,

$$A_\phi(\vec{n}^\sigma) = B_\sigma \cdot A_\phi(\vec{n}), \; A_\phi(\vec{n}^\tau) = B_\tau \cdot A_\phi(\vec{n}).$$

To find the Q-invariant homomorphisms, we set

$$A_{\sigma,10} = M_{\sigma,10} \otimes I_9 - I_{10} \otimes B_\sigma^t, \; A_{\tau,10} = M_{\tau,10} \otimes I_9 - I_{10} \otimes B_\tau^t.$$

Then ϕ is Q-invariant if and only if $A_\phi \in \mathrm{Ker}(A_{\sigma,10}) \cap \mathrm{Ker}(A_{\tau,10})$.

- Then $\mathrm{H}^1(N, M)^Q = \mathrm{H}^1(N_7, M)^Q$ and $\dim_{\mathbb{F}_p}(\mathrm{H}^1(N_7, M)^Q) = 18$.
- There is a basis $\xi_1, \ldots, \xi_7$ for N_7 (also the images of $\{\xi_1, \ldots, \xi_i\}$ in N_i are a basis for N_i for $1 \leq i \leq 7$), such that $\mathrm{H}^1(N_7, M)^Q$ is spanned by the image of the 10-dimensional space $\mathrm{Hom}(N_2, M^Q)$ and the 8 maps $A_{11}, \ldots, A_{18}$ (all basis elements ξ_i not listed map to 0):
$$\begin{array}{llll}
A_{11} : \xi_1 \mapsto y_1 & \xi_4 \mapsto y_0 y_1^2 + y_0^2 y_1^2 & \xi_5 \mapsto y_0 y_1^2 & \xi_7 \mapsto -y_0 y_1^2 - y_0^2 y_1^2 \\
A_{12} : \xi_1 \mapsto y_0 & \xi_4 \mapsto y_0^2 y_1 + y_0^2 y_1^2 & \xi_5 \mapsto y_0^2 y_1 & \xi_7 \mapsto -y_0 y_1^2 - y_0^2 y_1^2 \\
A_{13} : \xi_1 \mapsto y_0 y_1 & \xi_4 \mapsto y_0^2 y_1^2 & \xi_5 \mapsto y_0^2 y_1^2 & \xi_7 \mapsto -y_0^2 y_1^2 \\
A_{14} : \xi_3 \mapsto y_1^2 & \xi_4 \mapsto -y_1^2 & \xi_5 \mapsto y_1^2 & \xi_7 \mapsto y_1^2 \\
A_{15} : \xi_3 \mapsto y_0 y_1^2 & \xi_4 \mapsto -y_0 y_1^2 & \xi_5 \mapsto y_0 y_1^2 & \xi_7 \mapsto y_0 y_1^2 \\
A_{16} : \xi_3 \mapsto y_0^2 & \xi_4 \mapsto -y_0^2 & \xi_5 \mapsto y_0^2 & \xi_7 \mapsto y_0^2 \\
A_{17} : \xi_3 \mapsto y_0^2 y_1 & \xi_4 \mapsto -y_0^2 y_1 & \xi_5 \mapsto y_0^2 y_1 & \xi_7 \mapsto y_0^2 y_1 \\
A_{18} : \xi_3 \mapsto y_0^2 y_1^2 & \xi_4 \mapsto -y_0^2 y_1^2 & \xi_5 \mapsto y_0^2 y_1^2 & \xi_7 \mapsto y_0^2 y_1^2
\end{array}$$

Theorem [DPSW] The map $\phi \in \ker(d_2)$ if and only if there exist $m_0, \ldots m_r \in M$ such that $\phi(a_i) = -N_{\tau_i} m_i$ for $0 \leq i \leq r$ and $\phi(c_{j,k}) = (1 - \tau_k)m_j - (1 - \tau_j)m_k$ for $0 \leq j < k \leq r$.

Theorem [D.-Pries] The set $\{A_2, A_4, A_5, A_{10}, A_{13} + A_{18}\}$ is a basis for $\ker(d_2)$ when $p = 3$ and $M = \mathrm{H}_1(U; Y)$. Thus, $\dim \ker(d_2) = 5$ and $\dim H^1(G, M) = 14$ in this case.

Rank of N

Gras and Maire suggested p-rationality results, which imply the following:

Proposition. *If p is a regular prime then there is a unique prime $\mathfrak{p}$ of L above p and $\mathrm{rk}_p(N) = 1 + d/2$, where $d = p^{\frac{p+1}{2}}(p-1)$.*

For $p = 5$, $d = \deg(L/\mathbb{Q}) = \frac{p-1}{2} p^{\frac{p+1}{2}} = 500$. Directly computing even just the class number of L does not finish in a week. We know that $\mathrm{rk}_p \mathrm{Gal}(E/L) = 1 + d/2 = 251$, so $|\mathrm{Gal}(E/K)| = 5^{254}$. The hope is to be able to compute the quotient the action of Galois on local units to find the action of Q on N and ω.

Acknowledgements

This poster is based on joint work with Rachel Pries "Cohomology groups of Fermat curves via ray class fields of cyclotomic fields" (https://arxiv.org/abs/1806.08352) and a joint project with Pries, Stojanoska (University of Illinois at Urbana-Champaign), and Wickelgren (Georgia Institute of Technology). Thank you to the organizers of ANTS XIII.