Math. Res. Lett. **14** (2007), *no.* 4, 691–701

GONALITY OF MODULAR CURVES IN CHARACTERISTIC p

Bjorn Poonen

Abstract. Let k be an algebraically closed field of characteristic p. Let $X(p^e;N)$ be the curve parameterizing elliptic curves with full level N structure (where $p \nmid N$) and full level p^e Igusa structure. By modular curve, we mean a quotient of any $X(p^e;N)$ by any subgroup of $\left((\mathbb{Z}/p^e\mathbb{Z})^\times \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right)/\{\pm 1\}$. We prove that in any sequence of distinct modular curves over k, the k-gonality tends to infinity. This extends earlier work, in which the result was proved for particular sequences of modular curves, such as $X_0(N)$ for $p \nmid N$. As an application, we prove the function field analogue of a uniform boundedness conjecture for the image of Galois on torsion of elliptic curves.

1. Introduction

1.1. Gonality. The gonality $\gamma_k(X)$ of a curve[1] X over a field k is the smallest possible degree of a dominant rational map $X \dashrightarrow \mathbb{P}^1_k$. For any field extension L of k, we define also the L-gonality $\gamma_L(X)$ of X as the gonality of $X_L := X \times_k L$. General facts about gonality (mostly well-known) are gathered in Proposition A.1 in the appendix.

1.2. Modular curves. Our goal is to obtain lower bounds on the gonality of modular curves. By Proposition A.1(ii), it suffices to consider $k = \mathbb{C}$ and $k = \overline{\mathbb{F}}_p$ (an algebraic closure of $\mathbb{F}_p$) for each prime p.

Suppose N is a positive integer not divisible by the characteristic of k. Choose a primitive N-th root of unity ζ. Let $X(N)$ be the smooth projective model of the (possibly coarse) moduli space parameterizing triples (E,P,Q) where $P,Q \in E$ are a basis for $E[N]$ with Weil pairing $e_N(P,Q) = \zeta$. For $k = \mathbb{C}$, we can describe $X(N)(\mathbb{C})$ alternatively as the quotient of an extended upper half plane by a finite-index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. More generally, any congruence subgroup $G \le \mathrm{PSL}_2(\mathbb{Z})$ gives rise to a curve X_G over $\mathbb{C}$. Abramovich proved:

Theorem 1.1 ([Abr96])**.** *Let* $D = (\mathrm{PSL}_2(\mathbb{Z}) : G)$*. Then* $\gamma_{\mathbb{C}}(X_G) \ge \frac{7}{800}D$*.*

Remark 1.2. As mentioned in [Abr96], combining Theorem 1.1 with the genus bound $g - 1 \le D/12$ [Shi94, Proposition 1.40] yields

$$\gamma_{\mathbb{C}}(X_G) \ge \frac{21}{200}(g-1).$$

The proof of Theorem 1.1 makes use of a lower bound on the leading nontrivial eigenvalue of the noneuclidean Laplacian; this bound has been improved since 1996, so the constants 7/800 and 21/200 can be improved too. See also [BGJGP05, §4.3] for some further results.

Received by the editors April 8, 2006.

2000 *Mathematics Subject Classification.* Primary 14G35; Secondary 14H51, 11G18.

Key words and phrases. gonality, modular curve, Igusa curve, image of Galois.

[1]All our curves are assumed to be geometrically integral.

In characteristic p, one has other kinds of modular curves, involving level structure where p divides the level. If $q = p^e$ for some $e \in \mathbb{Z}_{\geq 1}$, the Igusa curve of level q is the smooth projective model $\mathrm{Ig}(q)$ of the curve over $\overline{\mathbb{F}}_p$ parameterizing pairs (E, R) where E is an ordinary elliptic curve, and R is a generator of the kernel of the degree-q Verschiebung isogeny $V_q\colon E^{(q)} \to E$, where $E^{(q)}$ is the elliptic curve obtained by raising all the coefficients of a model of E to the q-th power. Given N not divisible by p, and $e \in \mathbb{Z}_{\geq 1}$, we can define also a hybrid modular curve $X(p^e; N)$ over $\overline{\mathbb{F}}_p$ parameterizing (E, R, P, Q), with R generating $\ker V_q$ and $P, Q \in E[N]$ as above.

The group $G_{p^e N} := (\mathbb{Z}/p^e\mathbb{Z})^\times \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $X(p^e; N)$. The kernel of the action is $\{\pm 1\}$ embedded diagonally in $G_{p^e N}$. For any subgroup $G \leq G_{p^e N}$ containing $\{\pm 1\}$, let X_G be the smooth projective model of the quotient $X(p^e; N)/G$. The $G_{p^e N}$ form an inverse system with inverse limit

$$S := \mathbb{Z}_p^\times \times \prod_{\text{prime } \ell \neq p} \mathrm{SL}_2(\mathbb{Z}_\ell).$$

The inverse image of G under $S \twoheadrightarrow G_{p^e N}$ is an open subgroup of the profinite group S, and every open subgroup of S containing $\{\pm 1\}$ arises this way for some $p^e N$. Thus we may define X_G for any open subgroup G of S containing $\{\pm 1\}$.

It seems likely that there is a constant $c > 0$ independent of p and G such that $\gamma_{\overline{\mathbb{F}}_p}(X_G) \geq c(S : G)$. We are unable to prove such a linear lower bound, even for fixed p, but we can show that the gonality goes to infinity for fixed p. Here is our main theorem:

Theorem 1.3. *Fix a prime p. Let $G_1, G_2, \ldots$ be a sequence of distinct open subgroups of S containing $\{\pm 1\}$. Then $\gamma_{\overline{\mathbb{F}}_p}(X_{G_i}) \to \infty$ as $i \to \infty$.*

1.3. Outline of proof of main theorem. Many of the ideas used in the proof of Theorem 1.3 are due to earlier authors, though we consider a broader class of modular curves than had been treated earlier. Section 2 proves Theorem 2.5, an inequality in the direction opposite to Proposition A.1(i): the ideas used here and their application to the classical modular curves $X_0(N)$ can be found in [HS91], [NS96], and [Bak99, Chapter 3]. Theorem 2.5 reduces the problem to finding lower bounds on gonality over *finite* fields, and these can be obtained by counting in the spirit of [Ogg74], which among other things determined the N for which $X_0(N)$ is hyperelliptic. In Section 3 we find that, as in [Ogg74], modular curves of level prime to p have too many supersingular points over $\mathbb{F}_{p^2}$ to have small gonality. In Section 4 we cite results of Schweizer [Sch05], who obtained lower bounds on the $\overline{\mathbb{F}}_p$-gonality of Igusa curves directly from the geometry of the curves, instead of first getting lower bounds on $\mathbb{F}_p$-gonality by counting $\mathbb{F}_p$-points. Section 5 uses Goursat's lemma to study the subgroups of S, so that the prime-to-p and p-power cases can be combined to prove the general case of Theorem 1.3 in Section 6.

1.4. Application to the image of Galois. One application of results like Theorem 1.3, noted already by many other authors, is to the function field analogue of the strong uniform boundedness theorem for elliptic curves. By the work of Mazur, Kamienny, and Merel [Mer96], for every $d \in \mathbb{Z}_{\geq 1}$, there exists a constant N_d such that for any number field K with $[K : \mathbb{Q}] \leq d$ and for any elliptic curve E over K, the torsion subgroup $E(K)_{\mathrm{tors}}$ of the finitely generated abelian group $E(K)$ satisfies

$\#E(K)_{\mathrm{tors}} \leq N_d$. In the function field case, we can prove a stronger result, one which bounds the index of the image of Galois acting on torsion. If E is an ordinary elliptic curve over a field K of characteristic $p \geq 0$, and K^s is a separable closure of K, there exists a homomorphism

$$\rho_E \colon \mathrm{Gal}(K^s/K) \to \mathbb{Z}_p^\times \times \prod_{\ell \neq p} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

describing the Galois action on $\varprojlim \ker\left(V_{p^e} \colon E^{(p^e)} \to E\right)$ and the ℓ-adic Tate modules of E. (Of course, if $\mathrm{char}\, K = 0$, there is no $\mathbb{Z}_p^\times$ factor.)

Theorem 1.4. *Given $p \geq 0$ and $d \in \mathbb{Z}_{\geq 1}$, there exists a constant $N_{p,d}$ such that for any field k of characteristic p, any field K of degree $\leq d$ over $k(t)$, and any elliptic curve E over K with $j(E)$ not algebraic over k, the index $(S : \rho_E(\mathrm{Gal}(K^s/K)) \cap S)$ is at most $N_{p,d}$.*

Remark 1.5. Cojocaru and Hall [CH05, Theorem 1.1] give an explicit upper bound on the set of primes $\ell \neq \mathrm{char}\, k$ for which the image of ρ_E in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ does not contain $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$; their bound depends on the genus and not only on the gonality of the function field K.

Remark 1.6. In Theorem 1.4, we cannot hope to bound the index of $\rho_E(\mathrm{Gal}(K^s/K))$ in $\mathbb{Z}_p^\times \times \prod_{\ell \neq p} \mathrm{GL}_2(\mathbb{Z}_\ell)$ (i.e., with GL_2 instead of the SL_2 in the definition of S), since the determinant of the image in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ gives the action of $\mathrm{Gal}(K^s/K)$ on roots of unity, and this is trivial if k is algebraically closed, for example.

Theorem 1.4 will be deduced from Theorem 1.3 in Section 7.

2. Change in gonality under extension of the ground field

In this section we give an exposition of the "tower theorem" of Nguyen and Saito [NS96, Theorem 2.1], and its implication for relating gonalities of a single curve over different fields. We will reprove it as our Proposition 2.4, since [NS96] remains unpublished after 10 years, and since we can simplify the proof slightly. Throughout this section, k is a perfect field.

Proposition 2.1 (Castelnuovo-Severi inequality)**.** *Let F, F_1, F_2 be function fields of curves over k, of genera g, g_1, g_2, respectively. Suppose that $F_i \subseteq F$ for $i = 1, 2$ and the compositum of F_1 and F_2 in F equals F. Let $d_i = [F : F_i]$ for $i = 1, 2$. Then*

$$g \leq d_1 g_1 + d_2 g_2 + (d_1 - 1)(d_2 - 1).$$

Proof. See [Sti93, III.10.3]. □

Let X be a curve over k. A subfield F of $k(X)$ will be called d-controlled if there exists $e \in \mathbb{Z}_{>0}$ such that $[k(X) : F] = d/e$ and the genus of F is $\leq (e-1)^2$.

Lemma 2.2. *If F is d-controlled, and $f \in k(X)$ is a rational function of degree d, then $F(f)$ is d-controlled.*

Proof. View $F(f)$ as the compositum of F and $k(f)$ in $k(X)$. Let $a = [F(f) : F]$. Then $[k(X) : F(f)] = d/(ae)$, so $[F(f) : k(f)] = ae$. By Proposition 2.1, the genus of $F(f)$ is at most

$$a(e-1)^2 + 0 + (a-1)(ae-1) \quad = \quad (ae-1)^2 - ae(a-1)(e-1) \quad \leq \quad (ae-1)^2,$$

since $a, e \geq 1$. □

Corollary 2.3. *A subfield of $k(X)$ generated over k by one or more elements of degree d is d-controlled.*

Proof. Induction on the number of elements: the case of one element is trivial ($e = 1$), and Lemma 2.2 gives the inductive step. □

Proposition 2.4 (Tower theorem)**.** *Let X be a curve over a perfect field k. Let $L \supseteq k$ be an algebraic field extension. Let $d = \gamma_L(X)$. Then $k(X)$ has a d-controlled subfield.*

Proof. Enlarging L cannot increase $\gamma_L(X)$, so we may assume L/k is Galois. Choose $f \in L(X)$ of degree d. Let F_L be the subfield generated over L by the $\mathrm{Gal}(L/k)$-conjugates of f. By Corollary 2.3, F_L is d-controlled as a subfield of $L(X)$. The action of $\mathrm{Gal}(L/k)$ on $L(X)$ preserves F_L, and the invariant subfield $F_k := F_L^{\mathrm{Gal}(L/k)}$ satisfies $[k(X) : F_k] = [L(X) : F_L]$ and has the same genus as F_L. Thus F_k is a d-controlled subfield of $k(X)$. □

Theorem 2.5. *Let X be a curve over a perfect field k. Let $L \supseteq k$ be an algebraic field extension. Let $d = \gamma_L(X)$. Assume that $X(k) \neq \emptyset$.*

(i) *If $d \leq 2$, then $\gamma_k(X) = d$.*
(ii) *If $d > 2$, then $\gamma_k(X) \leq (d-1)^2$.*
(iii) *In any case, $\gamma_L(X) \geq \sqrt{\gamma_k(X)}$.*

Proof.

(i) If $d = 1$, then $X \simeq \mathbb{P}^1_k$, so $\gamma_k(X) = 1$. If $d = 2$, then X is elliptic or hyperelliptic; if elliptic, then $\gamma_k(X) = 2$; if hyperelliptic then the canonical map is a degree-2 map to a genus-0 curve Z over k, and $Z(k) \neq \emptyset$ so $Z \simeq \mathbb{P}^1_k$, so $\gamma_k(X) = 2$.

(ii) Now suppose $d > 2$. By Proposition 2.4 there exists $e \in \mathbb{Z}_{>0}$ and a rational map $\pi\colon X \dashrightarrow Y$ of curves over k such that $\deg \pi = d/e$ and the genus g of Y satisfies $g \leq (e-1)^2$. We have $Y(k) \neq \emptyset$. If $g = 0$, then $Y \simeq \mathbb{P}^1$, so

$$\gamma_k(X) \leq d/e \leq d < (d-1)^2.$$

If $g = 1$, then $e \geq 2$ and $\gamma_k(Y) = 2$, so

$$\gamma_k(X) \leq (d/e)\gamma_k(Y) \leq (d/2)2 = d < (d-1)^2.$$

If $g \geq 2$, then $\gamma_k(Y) \leq g$ by Proposition A.1(iv), so

$$\gamma_k(X) \leq \frac{d}{e}\gamma_k(Y) \leq \frac{d}{e}(e-1)^2.$$

For $e \in [1, d]$, the function $\frac{d}{e}(e-1)^2$ is maximized at $e = d$, and the value there is $(d-1)^2$.

(iii) This follows directly from the first two parts.

□

Remark 2.6. The hypothesis $X(k) \neq \emptyset$ is necessary: Genus-1 curves over $\mathbb{Q}$ have $\overline{\mathbb{Q}}$-gonality 2, but their $\mathbb{Q}$-gonality can be arbitrarily large.

Remark 2.7. We do not know whether the $(d-1)^2$ in Theorem 2.5(ii) can be improved.

Remark 2.8. For $N = 38, 44, 53, 61$, the modular curve $X_0(N)$ is of genus 4 and has $\mathbb{Q}$-gonality 4 and $\overline{\mathbb{Q}}$-gonality 3 [HS99, p. 136]. In particular, Theorem 2.5(ii) is best possible for $d = 3$.

3. Level prime to p

Suppose $p \nmid N$. We begin by defining a twisted form $X(N)'$ over $\mathbb{F}_{p^2}$ of $X(N)$. Let M be $(\mathbb{Z}/N\mathbb{Z})^2$ made into a $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{p^2})$-module by letting the p^2-power Frobenius automorphism act as multiplication by $-p$. There exists an isomorphism of Galois modules $\iota\colon \bigwedge^2 M \to \mu_N$; fix one. Let $X(N)'$ be the smooth projective model of the affine curve over $\mathbb{F}_{p^2}$ parameterizing pairs (E, ϕ) where E is an elliptic curve and ϕ is an isomorphism $E[N] \to M$ under which the Weil pairing corresponds to ι. Over $\overline{\mathbb{F}}_p$, $X(N)'$ becomes isomorphic to $X(N)$. The automorphisms of M as an abelian group automatically commute with the Galois action, so they induce automorphisms of $X(N)'$ defined over $\mathbb{F}_{p^2}$. Thus we get $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \leq \mathrm{Aut}\, X(N)'$. Moreover, it follows from [BGJGP05, Lemma 3.21] that all the points of $X(N)'$ corresponding to supersingular elliptic curves are defined over $\mathbb{F}_{p^2}$.

Proposition 3.1. *Let p, N, and $X(N)'$ be as above. Let G be a subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ of index D. Let X be the curve $X(N)'/G$. Then the $\mathbb{F}_{p^2}$-gonality γ of X satisfies*

$$\gamma \geq \frac{p-1}{12(p^2+1)} D.$$

Proof. This resembles the proof of [BGJGP05, Lemma 3.22]. By [BGJGP05, Lemma 3.20], the number of supersingular points on X is $\geq (p-1)D/12$, and these are images of supersingular points on $X(N)'$ so they are defined over $\mathbb{F}_{p^2}$; thus $\#X(\mathbb{F}_{p^2}) \geq (p-1)D/12$. On the other hand, $\#X(\mathbb{F}_{p^2}) \leq \gamma \#\mathbb{P}^1(\mathbb{F}_{p^2}) = \gamma(p^2+1)$. Combine the two previous sentences. □

Remark 3.2. Let g be the genus of X. One could also combine Proposition 3.1 with the bound $g - 1 < D/12$ of [Shi94, Proposition 1.40] to give a lower bound for γ in terms of g instead of D.

We now consider the $\overline{\mathbb{F}}_p$-gonality of all modular curves of level prime to p.

Corollary 3.3. *Fix p. Define $\Phi_p(D) := \sqrt{\frac{p-1}{12(p^2+1)} D}$. If G is the inverse image under $S \twoheadrightarrow \prod_{\ell \neq p} \mathrm{SL}_2(\mathbb{Z}_\ell)$ of an open subgroup of index D in $\prod_{\ell \neq p} \mathrm{SL}_2(\mathbb{Z}_\ell)$ containing $\{\pm 1\}$, then $\gamma_{\overline{\mathbb{F}}_p}(X_G) \geq \Phi_p(D)$.*

Proof. Combine Proposition 3.1 and Theorem 2.5(iii). □

Remark 3.4. One could also consider Atkin-Lehner quotients of $X_0(N)$ for N prime to p. These are generally not of the form X_G. Nevertheless, gonality bounds tending to infinity for fixed p can be obtained: first apply Proposition 3.1 to get a lower bound on $\gamma_{\mathbb{F}_{p^2}}(X_0(N))$, next use Proposition A.1(vi) to get a lower bound on the $\mathbb{F}_{p^2}$-gonality of any quotient of $X_0(N)$, and finally apply Theorem 2.5. This works since the size of the Atkin-Lehner group (some power of 2) is asymptotically small compared to the index of the congruence subgroup $\Gamma_0(N)$ in $\mathrm{PSL}_2(\mathbb{Z})$.

4. Level a power of p

The necessary lower bound on the gonality of $\mathrm{Ig}(p^e)$ has been proved already by Schweizer, in a strong form:

Theorem 4.1 ([Sch05, Lemma 1.5(d,e)])**.**

(i) *If $p \geq 7$, then $\frac{p+13}{24} \leq \gamma_{\overline{\mathbb{F}}_p}(\mathrm{Ig}(p)) \leq \frac{p-1}{6}$.*
(ii) *If $e > 1$ and $p^e \notin \{25, 9, 8, 4\}$, then $\gamma_{\overline{\mathbb{F}}_p}(\mathrm{Ig}(p^e)) = p\gamma_{\overline{\mathbb{F}}_p}(\mathrm{Ig}(p^{e-1}))$.*

In fact, [Sch05] proves many more results. The above are more than we need to deduce the following.

Corollary 4.2. *Let G be the inverse image under $S \twoheadrightarrow \mathbb{Z}_p^\times$ of an open subgroup of index D in $\mathbb{Z}_p^\times$ containing $\{\pm 1\}$. Then $\gamma_{\overline{\mathbb{F}}_p}(X_G) > D/12$.*

Proof. First suppose that $X_G = \mathrm{Ig}(p^e)$ for some prime power $p^e > 2$. Then $D = p^{e-1}(p-1)/2$. For $p^e \leq 25$, we have $D < 12$, and $\gamma_{\overline{\mathbb{F}}_p}(X_G) \geq 1 > D/12$ trivially. For $p > 25$, Theorem 4.1(i) gives

$$\gamma_{\overline{\mathbb{F}}_p}(\mathrm{Ig}(p)) \geq \frac{p+13}{24} > \frac{p-1}{24} = \frac{D}{12}.$$

For $p^e > 25$ with $e > 1$, we use induction on e, with Theorem 4.1(ii) giving the inductive step.

Any other X_G in Corollary 4.2 is a quotient of $\mathrm{Ig}(p^e)$ for some $p^e > 2$, and the inequality for X_G follows from the inequality for $\mathrm{Ig}(p^e)$, by Proposition A.1(vi). □

Remark 4.3. An alternative approach to lower bounds on the gonality of Igusa curves is to show that they have many points over certain finite fields, to deduce that the gonality over these finite fields is large, and then to apply Theorem 2.5. One can no longer use supersingular points, however, since these are totally ramified in $\mathrm{Ig}(p^e) \xrightarrow{j} \mathbb{P}^1$, and hence their number does not grow with e. Instead we could use *ordinary* points: it follows from [Pac96, Corollary 2.13] and Hurwitz class number estimates that $\#\,\mathrm{Ig}(q)(\mathbb{F}_q) \geq q^{3/2-o(1)}$ as $q \to \infty$. Or one could use cusps, as in the proof of [Sch04, Theorem 6.1], to get lower bounds on $\#\,\mathrm{Ig}(q)(\mathbb{F}_p)$, since the cusps split completely in $\mathrm{Ig}(p^e) \xrightarrow{j} \mathbb{P}^1$ [KM85, Corollary 12.7.2]. But the lower bounds on gonality obtained by these methods are weaker than the ones we took from [Sch05].

5. Group theory

Here we study the open subgroups of S. Let $S_p = \mathbb{Z}_p^\times$ and $S_{\neq p} = \prod_{\ell \neq p} \mathrm{SL}_2(\mathbb{Z}_\ell)$, so $S = S_p \times S_{\neq p}$. Given an open subgroup $G \leq S$, let G_p and $G_{\neq p}$ be the images of G in S_p and $S_{\neq p}$, respectively.

Lemma 5.1. *Let $B \in \mathbb{Z}_{>0}$. Any open subgroup H of $S_{\neq p}$ of index $\leq B$ contains*

$$\prod_{\ell \leq B!,\ \ell \neq p} \{1\} \times \prod_{\ell > B!,\ \ell \neq p} \mathrm{SL}_2(\mathbb{Z}_\ell).$$

Proof. For each $\ell \neq p$, identify $\mathrm{SL}_2(\mathbb{Z}_\ell)$ with a subgroup of $S_{\neq p}$ in the obvious way. It suffices to show that H contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$ for each $\ell > B!$ with $\ell \neq p$.

The kernel of the action of $S_{\neq p}$ on the coset space $S_{\neq p}/H$ is a normal open subgroup $N \trianglelefteq S_{\neq p}$ contained in H. Let $n := (S_{\neq p} : N)$, so $n \leq B!$. Now $\ell > B! \geq n$, so $1/n \in \mathbb{Z}_\ell$, and

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1/n \\ 0 & 1 \end{pmatrix}^n \in N,$$

where the matrices belong to $\mathrm{SL}_2(\mathbb{Z}_\ell) \leq S_{\neq p}$. Similarly $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in N$. But these two matrices generate the dense subgroup $\mathrm{SL}_2(\mathbb{Z})$ of $\mathrm{SL}_2(\mathbb{Z}_\ell)$, so $\mathrm{SL}_2(\mathbb{Z}_\ell) \leq N \leq H$. □

Lemma 5.2. *For each $B > 0$, there are at most finitely many open subgroups G of S such that $(S_p : G_p) < B$ and $(S_{\neq p} : G_{\neq p}) < B$.*

Proof. Fix B. By Lemma 5.1, it suffices to consider instead the situation in which $S_{\neq p}$ is replaced by $S_L := \prod_{\ell \in L} \mathrm{SL}_2(\mathbb{Z}_\ell)$ for a *finite* set L of primes $\neq p$: i.e., G is now an open subgroup of $S_p \times S_L$, G_L is the image of G in S_L, and we are given $(S_p : G_p) < B$ and $(S_L : G_L) < B$.

Since S_p and $S_{\neq p}$ are topologically finitely generated, there are finitely many possibilities for G_p and G_L. Goursat's Lemma [Lan02, p. 75] states that each possible G is the inverse image under

$$G_p \times G_L \twoheadrightarrow \frac{G_p}{H_p} \times \frac{G_L}{H_L}$$

of the graph of an isomorphism

$$\frac{G_p}{H_p} \to \frac{G_L}{H_L}$$

for some normal open subgroups $H_p \trianglelefteq G_p$ and $H_L \trianglelefteq G_L$. By the finite generation again, it suffices to bound $(G_p : H_p) = (G_L : H_L)$. It is bounded by the supernatural number $\gcd(\#S_p, \#S_L)$, which is finite, since S_p has a pro-p open subgroup, while S_L has an open subgroup of order prime to p. (See [Ser02, I.§1.3] for the notion of supernatural number.) □

6. The general case of Theorem 1.3

Proof of Theorem 1.3. Let $m > 0$. We will show that $\gamma_{\overline{\mathbb{F}}_q}(X_{G_i}) > m$ for all but finitely many i. Let Φ_p be as in Corollary 3.3. Choose B_0 such that $\min\{\Phi_p(B), B/12\} > m$ for all $B \geq B_0$. By Lemma 5.2, all but finitely many G_i in our sequence have either $(S_p : (G_i)_p) \geq B$ or $(S_{\neq p} : (G_i)_{\neq p}) \geq B$. For each such i, X_{G_i} dominates an X_G with

G as in Corollary 3.3 or Corollary 4.2; then $\gamma_{\overline{\mathbb{F}}_p}(X_G)$ exceeds either $\Phi_p(B)$ or $B/12$. By Proposition A.1(vii),

$$\gamma_{\overline{\mathbb{F}}_p}(X_{G_i}) \geq \gamma_{\overline{\mathbb{F}}_p}(X_G) \geq \min\{\Phi_p(B), B/12\} > m.$$

□

7. Image of Galois

Proof of Theorem 1.4. We may assume that k is algebraically closed. By Theorem 1.3, there are only finitely many subgroups $G \leq S$ containing $\{\pm 1\}$ such that $\gamma_{\overline{\mathbb{F}}_p}(X_G) \leq d$. Choose $N_{p,d}$ such that $N_{p,d} \geq 2(S : G)$ for every such G.

Let K be a field of degree $\leq d$ over $k(t)$, and let E be an elliptic curve over K with $j(E)$ not algebraic over k (i.e., not in k). Then E is ordinary. Write $K = k(C)$, where C is a curve over k with $\gamma_k(C) \leq d$. Define $H := \rho_E(\mathrm{Gal}(K^s/K))$. Since k is algebraically closed, $H \subseteq S$. We want $(S : H) \leq N_{p,d}$.

Suppose not. If $(S : H)$ is infinite, then since S/H is a profinite group, we can find a group H' with $H \leq H' \leq S$ and $N_{p,d} < (S : H') < \infty$. If $(S : H)$ is finite, let $H' = H$. In either case, let H'' be the group generated by H' and -1, so $N_{p,d}/2 < (S : H'') < \infty$. By definition of $N_{p,d}$, the group H'' does not equal any of the groups G, so $\gamma_{\overline{\mathbb{F}}_p}(X_{H''}) > d$. Equivalently, by Proposition A.1(ii), $\gamma_k(X_{H''}) > d$.

The curve $X_{H''}$ is defined as a quotient of some $X(p^e; N)$. Choosing level structure for E over K^s gives a point in $X(p^e; N)(K^s)$, and the action of $\mathrm{Gal}(K^s/K)$ moves this point within the H''-orbit, since $H \subseteq H''$, so the image point in $X_{H''}(K^s)$ is K-rational. This point in $X_{H''}(K)$ may be viewed as a rational map $C \dashrightarrow X_{H''}$, and this map is non-constant since the composition $C \dashrightarrow X_{H''} \xrightarrow{j} X(1) \simeq \mathbb{P}^1$ corresponds to $j(E) \in K - k$. Proposition A.1(vii) implies $\gamma_k(X_{H''}) \leq \gamma_k(C) \leq d$, contradicting the previous paragraph. □

Appendix A. General facts about gonality

Proposition A.1. *Let X be a curve of genus g over a field k.*

(i) *If L is a field extension of k, then $\gamma_L(X) \leq \gamma_k(X)$.*
(ii) *If k is algebraically closed, and L is a field extension of k, then $\gamma_L(X) = \gamma_k(X)$.*
(iii) *If $g > 1$, then $\gamma_k(X) \leq 2g - 2$. For each $g > 1$, there exist k and X for which equality holds.*
(iv) *If $X(k) \neq \emptyset$, then $\gamma_k(X) \leq g + 1$. If $X(k) \neq \emptyset$ and $g \geq 2$, then $\gamma_k(X) \leq g$ (and again, equality is possible for each g).*
(v) *If k is algebraically closed, then $\gamma_k(X) \leq \lfloor \frac{g+3}{2} \rfloor$. Equality holds for a general curve of genus g over k.*
(vi) *If $\pi\colon X \dashrightarrow Y$ is a dominant rational map of curves over k, then $\gamma_k(X) \leq (\deg \pi)\gamma_k(Y)$.*
(vii) *If $\pi\colon X \dashrightarrow Y$ is a dominant rational map of curves over k, then $\gamma_k(Y) \leq \gamma_k(X)$.*

Proof.

(i) Trivial.

(ii) Given a map over L, standard specialization arguments give a map over k of the same degree.

(iii) The canonical linear system $|K|$ has dimension $g-1 \geq 1$ and degree $2g-2$. So we may use a rational function whose divisor is the difference of two different canonical divisors. Equality holds for the general curve over the function field of the moduli space M_g of genus-g curves in characteristic 0, since its only line sheaves are the powers of the canonical sheaf: this was the Franchetta conjecture, proved in [Har83] and strengthened in [Mes87].

(iv) Let $P \in X(k)$. The Riemann-Roch theorem shows that $\dim |(g+1)P| \geq 1$, and that $\dim |K-(g-2)P| \geq 1$ if $g-2 \geq 0$. These linear systems have degree $g+1$ and g, respectively.

Now we prove that equality is possible, by considering the general curve $X_{g,1}$ over the function field of the moduli space $M_{g,1}$ of genus-g curves with one marked point in characteristic 0. We may assume $g \geq 3$. The Picard group of $X_{g,1}$ is generated by the canonical sheaf K and the class of the marked point P: this extension of the Franchetta conjecture can be deduced from the description of the Picard group of the moduli stack of genus-g curves with *two* marked points, in the same way that the original Franchetta conjecture is deduced in [AC87, §4]. It remains to show that $\dim |aK+bP| < 1$ whenever $a, b \in \mathbb{Z}$ are such that $\deg(aK+bP) < g$. By adding multiples of P, it suffices to consider the case $\deg(aK+bP) = g-1$. By Riemann-Roch symmetry, we may assume $a \geq 1$. If $a = 1$, we have $\dim |K-(g-1)P| = 0$ since the general point P is not a Weierstrass point. If $a > 1$, $|aK-(2a-1)(g-1)P|$ is empty by [Nee84, Theorem 4.2].

(v) These are consequences of Brill-Noether theory: see (1.1) and (1.5) of [ACGH85, Chapter V] for an exposition. The first statement is proved in arbitrary characteristic in [KL72, KL74]. The second statement is proved in characteristic 0 in [Far66, Mar67, Mar68], and can be deduced in characteristic p from the unramified case of [Oss05, Theorem 1.2], for instance.

(vi) Trivial.

(vii) (The ideas in the following argument go back at least to [New72, Theorem VII.2].) Choose $f \in k(X)$ of degree $d := \gamma_k(X)$. Let $r = \deg \pi = [k(X) : k(Y)]$. Let $P(T) \in k(Y)[T]$ be the characteristic polynomial of f viewed as an element of the field extension $k(X)$ of $k(Y)$. For some finite normal extension M of $k(Y)$, we may write $P(T) = \prod_{i=1}^{r}(T - f_i)$ for some $f_i \in M$. As a function in M, f has degree $[M : k(X)]d$. The same is true of each f_i, since they are all in the same $\mathrm{Aut}(M/k(Y))$-orbit. The polar divisor of a coefficient of P viewed in M is at most the sum of the polar divisors of the f_i, so each coefficient has degree at most $r[M : k(X)]d = [M : k(Y)]d$ as a function in M, and hence degree at most d as a function in $k(Y)$. Since f is non-constant, at least one of these coefficients is non-constant. Thus $\gamma_k(Y) \leq d$.

□

Acknowledgements

Most of all I thank Andreas Schweizer for several discussions, for suggesting references, and for pointing out that existing versions of the Castelnuovo-Severi inequality seem to require a perfect field of constants. I also thank Matt Baker, from whom I first learned the idea in [HS91] that the Castelnuovo-Severi inequality could be used to bound change in gonality under algebraic extensions. I thank Brian Osserman for pointing out that the lower bound on the geometric gonality of the general curve of genus g in characteristic p could be deduced from [Oss05]. I thank Joe Harris for suggesting the reference [AC87] and Doug Ulmer for a remark about cusps of Igusa curves, Finally I thank Alina Cojocaru, Chris Hall, Dinesh Thakur, and Doug Ulmer for asking questions that inspired this paper. This research was supported by NSF grant DMS-0301280 and the Miller Institute for Basic Research in Science.

References

[Abr96] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011.MR1422373 (98b:11063)

[AC87] Enrico Arbarello and Maurizio Cornalba, *The Picard groups of the moduli spaces of curves*, Topology **26** (1987), no. 2, 153–171. MR **895568 (88e:**14032)

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985.MR770932 (86h:14019)

[Bak99] Matthew H. Baker, *Torsion points on modular curves*, 1999. Ph.D. thesis, University of California at Berkeley.

[BGJGP05] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen, *Finiteness results for modular curves of genus at least* 2, Amer. J. Math. **127** (2005), 1325–1387. `arXiv:math.NT/0211394`.

[CH05] Alina Carmen Cojocaru and Chris Hall, *Uniform results for Serre's theorem for elliptic curves*, Int. Math. Res. Not. (2005), no. 50, 3065–3080. MR 2189500

[Far66] Hershel M. Farkas, *Special divisors and analytic subloci of Teichmueller space*, Amer. J. Math. **88** (1966), 881–901.MR0213546 (35 #4406)

[Har83] John Harer, *The second homology group of the mapping class group of an orientable surface*, Invent. Math. **72** (1983), no. 2, 221–239.MR700769 (84g:57006)

[HS91] Joe Harris and Joe Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. **112** (1991), no. 2, 347–356.MR1055774 (91i:11067)

[HS99] Yuji Hasegawa and Mahoro Shimura, *Trigonal modular curves*, Acta Arith. **88** (1999), no. 2, 129–140.MR1700245 (2000d:11080)

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.MR772569 (86i:11024)

[KL72] Steven L. Kleiman and Dan Laksov, *On the existence of special divisors*, Amer. J. Math. **94** (1972), 431–436.MR0323792 (48 #2148)

[KL74] ———, *Another proof of the existence of special divisors*, Acta Math. **132** (1974), 163–176.MR0357398 (50 #9866)

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.MR1878556 (2003e:00003)

[Mar67] Henrik H. Martens, *On the varieties of special divisors on a curve*, J. Reine Angew. Math. **227** (1967), 111–120.MR0215847 (35 #6682)

[Mar68] ———, *Varieties of special divisors on a curve. II*, J. Reine Angew. Math. **233** (1968), 89–100.MR0241420 (39 #2760)

[Mer96] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449 (French).MR1369424 (96i:11057)

[Mes87] Nicole Mestrano, *Conjecture de Franchetta forte*, Invent. Math. **87** (1987), no. 2, 365–376 (French).MR870734 (88c:14039)

[Nee84] A. Neeman, *Weierstrass points in characteristic p*, Invent. Math. **75** (1984), no. 2, 359–376. MR **732551 (85h:**14009)

[New72] Morris Newman, *Conjugacy, genus, and class numbers*, Math. Ann. **196** (1972), 198–217.MR0311573 (47 #135)

[NS96] Khac Viet Nguyen and Masa-Hiko Saito, *d-gonality of modular curves and bounding torsions* (March 29, 1996). Preprint, `arXiv:alg-geom/9603024`.

[Ogg74] Andrew P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.MR0364259 (51 #514)

[Oss05] Brian Osserman, *Deformations of covers, Brill-Noether theory, and wild ramification*, Math. Res. Lett. **12** (2005), no. 4, 483–491.MR2155226

[Pac96] Amílcar Pacheco, *Rational points on Igusa curves and L-functions of symmetric representations*, J. Number Theory **58** (1996), no. 2, 343–360.MR1393620 (97e:11078)

[Sch04] Andreas Schweizer, *Torsion of Drinfeld modules and gonality*, Forum Math. **16** (2004), no. 6, 925–941.MR2096477 (2005f:11116)

[Sch05] ———, *On the p^e-torsion of elliptic curves and elliptic surfaces in characteristic p*, Trans. Amer. Math. Soc. **357** (2005), no. 3, 1047–1059 (electronic).MR2110432 (2005k:11111)

[Ser02] Jean-Pierre Serre, *Galois cohomology*, Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author.MR1867431 (2002i:12004)

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original; Kanô Memorial Lectures, 1.MR1291394 (95e:11048)

[Sti93] Henning Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.MR1251961 (94k:14016)

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: `poonen@math.berkeley.edu`
URL: `http://math.berkeley.edu/~poonen`