UNRAMIFIED COVERS OF GALOIS COVERS OF LOW GENUS CURVES

BJORN POONEN

ABSTRACT. Let $X \to Y$ be a Galois covering of curves, where the genus of X is ≥ 2 and the genus of Y is ≤ 2. We prove that under certain hypotheses, X has an unramified cover that dominates a hyperelliptic curve; our results apply, for instance, to all tamely superelliptic curves. Combining this with a theorem of Bogomolov and Tschinkel shows that X has an unramified cover that dominates $y^2 = x^6 - 1$, if $\operatorname{char} k$ is not 2 or 3.

1. INTRODUCTION

1.1. **Definitions.** Let k be an algebraically closed field. Let p be the characteristic of k (we allow the case $p = 0$). In this paper, a *curve* is a smooth, projective, integral, 1-dimensional variety over k. If we write an affine equation for a curve, its smooth projective model is implied. We write $g(X)$ for the genus of a curve X. By an *unramified cover* of a curve X, we mean a curve Z with a finite étale morphism $Z \to X$. As usual, one says that X *dominates* Y if there is a rational map $X \dashrightarrow Y$ whose image is Zariski dense in Y; for curves (satisfying our hypotheses), this is equivalent to the existence of a surjective morphism.

Definition 1.1. Let X and Y be curves. Following [BT04], we write $X \Rightarrow Y$ if there exists an unramified cover Z of X such that Z dominates Y. Write $X \Leftrightarrow Y$ if $X \Rightarrow Y$ and $Y \Rightarrow X$.

The relation $\Rightarrow$ is reflexive and transitive. For any X, we have $X \Rightarrow \mathbb{P}^1$. On the other hand, $\mathbb{P}^1$ has no nontrivial unramified covers; thus $\mathbb{P}^1 \Rightarrow X$ only if $X \simeq \mathbb{P}^1$. Hence the relation $\Rightarrow$ is not symmetric.

Remark 1.2. One motivation for introducing the relation $\Rightarrow$ arises from arithmetic geometry. Suppose that X, Y are curves over a number field F and that Y has genus at least 2. If $X \Rightarrow Y$, then by [CW30], the problem of determining the F-points on X can be reduced to finding the F'-points on Y for some effectively computable finite extension F' of F.

1.2. **Previous results.** Belyĭ [Bel79] proved that every curve over $\overline{\mathbb{Q}}$ admits a morphism to $\mathbb{P}^1$ ramified only above $\{0, 1, \infty\}$. Almost immediately thereafter, Manin proved that Belyĭ's Theorem implies the following theorem:

Theorem 1.3 ([BH00, Proposition 7.1])**.** *For any curve X over $\overline{\mathbb{Q}}$, there exists $N \geq 1$ such that the modular curve $X(N)$ satisfies $X(N) \Rightarrow X$.*

Date: December 30, 2004 (minor correction July 31, 2007).

2000 *Mathematics Subject Classification.* Primary 14H30; Secondary 14H45.

Key words and phrases. Galois cover, unramified cover, Abhyankar's lemma, superelliptic curve.

This research was supported by NSF grant DMS-0301280 and a Packard Fellowship. This article has appeared in *Math. Res. Letters* **12** (2005), no. 4, 475–481.

Call a curve X *hyperelliptic* if there exists a degree-2 map $X \to \mathbb{P}^1$ and $g(X) \geq 2$.

Theorem 1.4 ([BT02, Theorem 1.7])**.** *If X is a hyperelliptic curve over $\overline{\mathbb{F}}_p$, and Y is any curve over $\overline{\mathbb{F}}_p$, then $X \Rightarrow Y$.*

Let C_n be (the smooth projective model of) the curve $y^2 = x^n - 1$.

Theorem 1.5 ([BT02, Proposition 1.8])**.** *Suppose $p \neq 2, 3$. If X is a hyperelliptic curve over k, then $X \Rightarrow C_6$.*

Theorem 1.6 ([BT04])**.** *Suppose $k = \overline{\mathbb{Q}}$. For any $m \geq 5$ and $n \in \{2, 3, 5\}$, we have $C_m \Leftrightarrow C_{mn}$.*

Proof. The direction $C_{mn} \Rightarrow C_m$ is trivial. For $C_m \Rightarrow C_{mn}$, the case $m \geq 6$ is [BT04, Theorem 1.2], and the case $m = 5$ is a consequence of [BT04, Corollary 2.8]. □

1.3. **New results.** If $X \to Y$ is a dominant morphism of curves, call X a *Galois cover* of Y if the corresponding function field extension $k(X)$ over $k(Y)$ is Galois (thus we do not require that X be unramified over Y). If moreover $\mathrm{Gal}(k(X)/k(Y))$ is cyclic, then call X a *cyclic cover* of Y. If G is a subgroup of $\mathrm{Aut}\, X$, then X/G denotes the curve whose function field is the fixed field $k(X)^G$.

Theorem 1.7. *Let X be a curve. Let G be a subgroup of $\mathrm{Aut}(X)$ of order not divisible by the characteristic of k. Let $Y = X/G$. Suppose $g(X) \geq 2 \geq g(Y)$. Suppose in addition that at least one of the following holds:*

1. *$g(Y) \in \{1, 2\}$.*
2. *G is solvable.*
3. *There are two distinct points of Y above which the ramification indices have a non-trivial common factor.*
4. *There are three points of Y above which the ramification indices are divisible by 2, 3, ℓ, respectively, where ℓ is a prime with either $\ell \leq 89$ or*

$$\ell \in \{101, 103, 107, 131, 167, 191\}.$$

Then $X \Rightarrow H$ for some hyperelliptic curve H.

Corollary 1.8. *If in addition to the hypotheses of Theorem 1.7 we have $p \neq 2, 3$, then $X \Rightarrow C_6$.*

Proof. Combine Theorem 1.7 with Theorem 1.5, and use transitivity of $\Rightarrow$. □

Call a curve X *tamely superelliptic* if X is a cyclic cover of $\mathbb{P}^1$ of degree not divisible by p, and $g(X) \geq 2$. These are the curves of genus ≥ 2 with equations of the form $y^n = f(x)$ with $p \nmid n$.

Corollary 1.9. *If X is tamely superelliptic, then $X \Rightarrow H$ for some hyperelliptic curve H.*

Proof. Theorem 1.7 applies because the Galois group is solvable. □

2. Lemmas

In this section we gather various results needed for the proof of Theorem 1.7 and for the remarks at the end of this paper.

2.1. **Abhyankar's lemma.** We will construct unramified covers using Abhyankar's lemma, a version of which we now state. If $\pi\colon X \to Y$ and $\phi\colon Y' \to Y$ are surjective morphisms of curves, then by a *compositum* of X and Y' over Y, we mean a curve whose function field is a compositum of $k(X)$ and $k(Y')$ over $k(Y)$.

Lemma 2.1 (Abyhankar's lemma)**.** *Let $\pi\colon X \to Y$ and $\phi\colon Y' \to Y$ be surjective morphisms of curves. Assume that for all closed points $x \in X$ and $y' \in Y'$ with $\pi(x) = \phi(y')$, the ramification index of ϕ at y' divides the ramification index of π at x and is not divisible by p. Let X' be a compositum of X and Y' over Y. Then X' is an unramified cover of X.*

Proof. This follows from a local version of Abhyankar's lemma, such as [SGA 1, XIII.5.2]. □

Remark 2.2. Even if $k(X)$ and $k(Y')$ are linearly disjoint over $k(Y)$, the fiber product $X \times_Y Y'$ need not be a compositum in our sense, since it could be singular.

2.2. **Modular curves $X_0^*(\ell)$ of small genus.**

Lemma 2.3. *Let ℓ be a prime. Let $X_0^*(\ell)$ be the quotient of the modular curve $X_0(\ell)$ over $\overline{\mathbb{Q}}$ (or over any field of characteristic not divisible by ℓ) by its Atkin-Lehner involution. Let g be the genus of $X_0^*(\ell)$. Then*

$$\begin{aligned} g = 0 &\iff \ell \in \{2, 3, 5, 7, 13, 23, 29, 31, 37, 41, 47, 59, 71\} \\ g = 1 &\iff \ell \in \{11, 17, 19, 37, 43, 53, 61, 79, 83, 89, 101, 131\} \\ g = 2 &\iff \ell \in \{67, 73, 103, 107, 167, 191\}. \end{aligned}$$

If $g > 2$, then $\operatorname{Aut} X_0^*(\ell)_{\overline{\mathbb{Q}}}$ is trivial.

Proof. The values of ℓ for which $g \leq 2$ can be deduced by combining the list of $X_0(\ell)$ for which $g(X_0(\ell)) \leq 1$ (by the general formula, these are the primes $\ell \leq 19$), the list of hyperelliptic $X_0(\ell)$ [Ogg74], the list of bielliptic $X_0(\ell)$ [Bar99], and the list of hyperelliptic $X_0^*(\ell)$ [HH96]. The final statement is proved in [BH03]. □

Remark 2.4. In fact, the papers cited above together with [Has97] contain the information needed to list all (not necessarily prime) $\ell \in \mathbb{Z}_{>0}$ with $g(X_0^*(\ell)) = 0, 1, 2$.

2.3. **Existence of covers of $\mathbb{P}^1$ unramified outside 3 points.** The following lemma is well known. It was used, for instance, in [DG95] to prove that $x^p + y^q = z^r$ has at most finitely many pairwise relatively prime integer solutions for any fixed $p, q, r \in \mathbb{Z}_{>1}$ with $1/p + 1/q + 1/r < 1$.

Lemma 2.5. *Let k be an algebraically closed field of characteristic 0. Let $n_0, n_1, n_\infty \in \mathbb{Z}_{>1}$. Then there exists a Galois cover $X \to \mathbb{P}^1_k$ unramified outside $0, 1, \infty$ and with ramification indices exactly n_0, n_1, n_∞ above $0, 1, \infty$ respectively.*

Proof. We elaborate on the suggestion in the paragraph before Proposition 3a in [DG95] to use results stated in [Ser92]. By [Ser92, Theorem 6.3.3], it suffices to construct the cover for $k = \mathbb{C}$. Let π_1 be the topological fundamental group of $\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$, and let s_0, s_1, s_∞ be the monodromy generators at the three points. Let N be the smallest normal subgroup of π_1 containing $s_0^{n_0}, s_1^{n_1}, s_\infty^{n_\infty}$. By [Ser92, Theorem 6.4.2] (with $s = 3$, $t = 0$), the images of s_0, s_1, s_∞ in π_1/N have orders exactly n_0, n_1, n_∞. By the last paragraph of [Ser92, Section 6.3], the map from π_1 to its profinite completion is injective, so π_1 contains a normal

subgroup N' of finite index such that the images of s_0, s_1, s_∞ in π_1/N' have orders exactly n_0, n_1, n_∞. By [Ser92, Theorem 6.1.4], the analytic covering of $\mathbb{P}^1_C - \{0, 1, \infty\}$ corresponding to N' is an *algebraic* curve X_0. The corresponding smooth projective curve X is the desired Galois covering of $\mathbb{P}^1$. □

3. Proof of the main theorem

3.1. **Case 1: $g(Y) \in \{1, 2\}$.** If $g(Y) = 2$, then Y is hyperelliptic and $X \Rightarrow Y$, so there is nothing to show. So assume that Y is an elliptic curve E. Since $g(X) \geq 2$, X is ramified above some point of E, which we may assume is the identity of E. Let e be a prime dividing the ramification index there. Replace $X \to E$ by its (unramified) base extension by the multiplication-by-ℓ map $E \to E$ for some prime $\ell \geq 5$ not equal to p (and choose an irreducible component if necessary, so that the new X is again a curve). Thus we reduce to the case where $X \to E$ has ramification index divisible by e above each ℓ-torsion point of E. Fix a Weierstrass model of E. The $\ell^2 - 1$ nonzero ℓ-torsion points come in pairs sharing the same x-coordinate: let $a_1, \ldots, a_{(\ell^2-1)/2}$ be all these x-coordinates.

By Lemma 2.1, a compositum of X and

$$H \colon z^e = \frac{(x - a_1)(x - a_2)}{(x - a_3)(x - a_4)}.$$

over $\mathbb{P}^1$ (with coordinate x) gives an unramified cover of X that dominates H. The function z on H is of degree 2, and applying the Hurwitz formula to $x \colon H \to \mathbb{P}^1$ shows that $g(H) = e-1$. Thus if $e \geq 3$, then H is hyperelliptic. If $e = 2$, instead use

$$H \colon z^2 = \frac{(x - a_1)(x - a_2)(x - a_3)}{(x - a_4)(x - a_5)(x - a_6)}.$$

which is hyperelliptic of genus 2.

We assume $Y \simeq \mathbb{P}^1$ from now on. By the Hurwitz formula, there are ≥ 3 branch points.

3.2. **Case 2: G is solvable.** We use induction on $\#G$. If $H \subsetneq G$ is a nontrivial normal subgroup, then depending on whether $g(X/H) \geq 2$, $g(X/H) = 1$, or $g(X/H) = 0$, we apply the inductive hypothesis to $X/H \to Y$, Case 2 to $X \to X/H$, or the inductive hypothesis to $X \to X/H$, respectively. Thus we may assume that G is simple. But G is solvable, so $G \simeq \mathbb{Z}/\ell\mathbb{Z}$ for some prime $\ell \neq p$. Thus X is a $\mathbb{Z}/\ell\mathbb{Z}$-cover of $\mathbb{P}^1$. If $\ell = 2$ then X itself is hyperelliptic, so assume $\ell \geq 3$.

If we take a compositum with a $\mathbb{Z}/\ell\mathbb{Z}$-cover $\mathbb{P}^1 \to \mathbb{P}^1$ ramified above exactly two branch points of $X \to \mathbb{P}^1$, we find a new $\mathbb{Z}/\ell\mathbb{Z}$-cover $X' \to \mathbb{P}^1$. By Lemma 2.1, X' is unramified over X. Since $g(X') > g(X)$, the $\mathbb{Z}/\ell\mathbb{Z}$-cover $X' \to \mathbb{P}^1$ is ramified above ≥ 4 points of $\mathbb{P}^1$. Let x be a parameter on $\mathbb{P}^1$ whose values $a_1, \ldots, a_4$ at these points are not ∞. Applying Lemma 2.1 to a compositum with the $\mathbb{Z}/\ell\mathbb{Z}$-cover $H \to \mathbb{P}^1$ given by

$$H \colon y^\ell = \frac{(x - a_1)(x - a_2)}{(x - a_3)(x - a_4)}$$

shows that $X' \Rightarrow H$. And H is hyperelliptic.

3.3. **Case 3: There are two branch points whose associated ramification indices have a nontrivial common factor.** Let e be a prime dividing the ramification indices above two branch points, and let e' be a prime dividing the ramification index above some other branch point y'. A compositum of $X \to \mathbb{P}^1$ with a $\mathbb{Z}/e\mathbb{Z}$-cover $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ branched above exactly the first two branch points is a Galois cover X' of (a new) $\mathbb{P}^1$, and X' is unramified over X. The new cover $X' \to \mathbb{P}^1$ has ramification index e' above each of the e points in $\phi^{-1}(y')$. In particular, e' divides the ramification indices above two branch points of the new cover, so we can repeat the process to obtain an infinite commutative (though not necessarily cartesian) diagram

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & X^{(n)} & \longrightarrow & \cdots & \longrightarrow & X'' & \longrightarrow & X' & \longrightarrow & X \\
 & & \downarrow{\scriptstyle \pi^{(n)}} & & & & \downarrow{\scriptstyle \pi''} & & \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\
\cdots & \xrightarrow{e^{(n)}} & \mathbb{P}^1 & \xrightarrow{e^{(n-1)}} & \cdots & \xrightarrow{e''} & \mathbb{P}^1 & \xrightarrow{e'} & \mathbb{P}^1 & \xrightarrow{e} & \mathbb{P}^1,
\end{array}$$

in which the integers $e^{(n)}$ indicate the degrees of cyclic covers. By commutativity, the degree of $X^{(n)} \to X$ is at least $e^{(n-1)} \cdots e'e/(\deg \pi)$, which tends to ∞, so $X^{(n+1)} \to X^{(n)}$ must be of degree > 1 for infinitely many n. Since $g(X) \geq 2$ and all morphisms are separable, it follows that $g(X^{(n)}) \to \infty$ as $n \to \infty$. On the other hand, $\deg \pi^{(n)} \leq \deg \pi$, so by the Hurwitz formula, the number of branch points of $\pi^{(n)}$ tends to ∞. The ramification indices are bounded by that of π, so for some n, there is an integer $\ell \geq 2$ that is the ramification index above more than 6 branch points. Let S be a $\mathbb{Z}/\ell\mathbb{Z}$-cover of $\mathbb{P}^1$ branched above 6 points, with ramification index ℓ above each. Applying Lemma 2.1 to a compositum of $X^{(n)}$ and S over $\mathbb{P}^1$ shows that $X^{(n)} \Rightarrow S$. Hence $X \Rightarrow S$. The Hurwitz formula shows that $g(S) \geq 2$. Also, by construction, $p \nmid \ell$, so S is tamely superelliptic. By Case 3, $S \Rightarrow H$ for some hyperelliptic curve H. By transitivity, $X \Rightarrow H$.

3.4. **Case 4: Ramification divisible by $2, 3, \ell$.** By Case 3, we may assume $\ell \geq 5$. The modular curve $X(\ell)$ is a Galois cover of $\mathbb{P}^1$ ramified above three points, with ramification indices $2, 3, \ell$. We may assume those three points are the same of the branch points for $X \to \mathbb{P}^1$. Let Z be a compositum of X and $X(\ell)$ over $\mathbb{P}^1$. By Lemma 2.1, Z is unramified over X. Also Z is Galois over $X(\ell)$.

Suppose $\ell = 5$. By the Hurwitz formula, the original cover $X \to \mathbb{P}^1$ must have had either a fourth branch point P, or else extra ramification (more than $2, 3, 5$, respectively) above one of the three branch points P. In either case, the preimages of P under $X(5) \to \mathbb{P}^1$ are branch points of $Z \to X(5)$ having the same ramification index > 1, so Case 3 shows that $Z \Rightarrow H$ for some hyperelliptic curve H. Then $X \Rightarrow Z \Rightarrow H$.

Thus we may assume $\ell \geq 7$. We have $X \Rightarrow X(\ell)$ (through Z). Since $X(\ell)$ is a solvable cover of the modular curve $X_0(\ell)$, we are done by Case 2 if $g(X_0(\ell)) \leq 2$. Otherwise, let $X_0^*(\ell)$ be the quotient of $X_0(\ell)$ by its Atkin-Lehner involution. If $g(X_0^*(\ell)) \leq 2$, we apply Case 2 to $X_0(\ell) \to X_0^*(\ell)$.

Summing up, we are done whenever $g(X_0^*(\ell)) \leq 2$. These primes ℓ are given by Lemma 2.3. This completes the proof of Theorem 1.7.

4. Final remarks

Remark 4.1. Here we show that in order to prove Theorem 1.7 in characteristic 0 without making any of the additional assumptions (1) through (4), it would suffice to do the case of Galois covers of $\mathbb{P}^1$ with non-abelian simple Galois group, ramified above exactly 3 points, above which the ramification indices are distinct primes p_1, p_2, p_3.

First exclude cases already covered by Theorem 1.7. Choose three branch points (we may assume they are $0, 1, \infty$ on $\mathbb{P}^1$) and primes p_1, p_2, p_3 dividing the associated ramification indices. The p_i will be distinct, since otherwise apply Case 3. If $\{p_1, p_2, p_3\} = \{2, 3, 5\}$, apply Case 4. Lemma 2.5 gives a Galois cover $Z \to \mathbb{P}^1$ ramified above exactly these three branch points, and with ramification indices p_1, p_2, p_3. Since $1/p_1 + 1/p_2 + 1/p_3 < 1$, the Hurwitz formula gives $g(Z) > 1$. Applying Lemma 2.1 to a compositum of X and Z shows that $X \Rightarrow Z$, so we have reduced to proving the result for $Z \to \mathbb{P}^1$. Finally, apply induction as in Case 2 to reduce to the case of a simple Galois group (no new primes are introduced into ramification indices during the induction).

Remark 4.2. In the previous remark, if Z_1 and Z_2 are two Galois covers of $\mathbb{P}^1$ each ramified above exactly 3 points with ramification indices p_1, p_2, p_3, then Lemma 2.1 applied to a compositum of Z_1 and Z_2 over $\mathbb{P}^1$ shows that $Z_1 \Leftrightarrow Z_2$.

Acknowledgements

I thank Matt Baker for suggesting the references for the proof of Lemma 2.3.

References

[BH03] Matthew Baker and Yuji Hasegawa, *Automorphisms of $X_0^*(p)$*, J. Number Theory **100** (2003), no. 1, 72–87.MR1971247 (2004c:11100) ↑2.2

[Bar99] Francesc Bars, *Bielliptic modular curves*, J. Number Theory **76** (1999), no. 1, 154–165.MR1688168 (2000d:11078) ↑2.2

[Bel79] G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479 (Russian).MR534593 (80f:12008) ↑1.2

[BH00] Fedor Bogomolov and Dale Husemöller, *Geometric properties of curves defined over number fields*, 2000. Preprint MPIM2000-1 at `http://www.mpim-bonn.mpg.de/html/preprints/preprints.html`. ↑1.3

[BT02] Fedor Bogomolov and Yuri Tschinkel, *Unramified correspondences*, Algebraic number theory and algebraic geometry, 2002, pp. 17–25.MR1936365 (2003k:14032) ↑1.4, 1.5

[BT04] ———, *Couniformization of curves over number fields*, Geometric methods in algebra and number theory (Miami, Florida, December 2003), Progress in Mathematics, vol. 235, Birkhäuser, 2004, pp. 43–57. ↑1.1, 1.6, 1.2

[CW30] C. Chevalley and A. Weil, *Un théorème d'arithmétique sur les courbes algébriques*, Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **195** (1930), 570–572. ↑1.2

[DG95] Henri Darmon and Andrew Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*, Bull. London Math. Soc. **27** (1995), no. 6, 513–543.MR1348707 (96e:11042) ↑2.3, 2.3

[Has97] Yuji Hasegawa, *Hyperelliptic modular curves $X_0^*(N)$*, Acta Arith. **81** (1997), no. 4, 369–385.MR1472817 (99a:11075) ↑2.4

[HH96] Yuji Hasegawa and Ki-ichiro Hashimoto, *Hyperelliptic modular curves $X_0^*(N)$ with square-free levels*, Acta Arith. **77** (1996), no. 2, 179–193.MR1411031 (97m:11082) ↑2.2

[Ogg74] Andrew P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.MR0364259 (51 #514) ↑2.2

[Ser92] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon]; With a foreword by Darmon and the author.MR1162313 (94d:12006) ↑2.3

[SGA 1] *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3, Société Mathématique de France, Paris, 2003 (French). Séminaire de géométrie algébrique du Bois Marie 1960–61. [Geometric Algebra Seminar of Bois Marie 1960-61]; Directed by A. Grothendieck. With two papers by M. Raynaud. Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin].MR2017446 (2004g:14017) ↑2.1

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