# Models of curves : the birch and Swinnerton-Dyer conjecture & ordinary reduction

Bommel, R. van

# Chapter 4

# Primes of ordinary reduction for hyperelliptic curves

**Abstract.** In this chapter we show for all positive integers $M$ and $g$, and all number fields $K$ except for $\mathbb{Q}$, 100% of hyperelliptic curves of genus $g$ over $K$ have at least $M$ primes of ordinary good reduction.

## 4.1 Introduction

In arithmetic statistics, the occurrence of different types of reduction is often studied. For example Wong proved that 17.9% of elliptic curves over $\mathbb{Q}$ are everywhere semi-stable ([Wong01]), and Elkies showed that every elliptic curve over $\mathbb{Q}$ has infinitely many primes of good supersingular reduction ([Elk87]).

Ogus proved that elliptic curves and abelian surfaces over number fields have infinitely many primes of ordinary good reduction ([Ogus82, Cor. 2.9, p. 372]). In this chapter, we study the occurrence of ordinary good primes for Jacobians of hyperelliptic curves of genus greater than 2 over number fields.

The organisation of this chapter is as follows. First, we generalise Yui's criterion to determine whether a hyperelliptic curve over a finite field is ordinary to hyperelliptic curves given by an even degree model. Then we define several notions of density on $\operatorname{Specmax} \mathcal{O}_K$ and on $\mathcal{O}_K^N$, where $\mathcal{O}_K$ the ring of integers of a number field. Then we combine several results to prove, for all positive integers $M$ and $g$, all number fields $K$ except for $\mathbb{Q}$, that 100% of hyperelliptic curves of genus $g$ over $K$ have at least $M$ primes of ordinary good reduction.

## 4.2 Generalisation of Yui's criterion

The following criterion by Yui gives a practical way to determine whether a hyperelliptic curve has ordinary reduction.

**Theorem 4.2.1** ([Yui78, Cor. 2.3, p. 387])**.** *Let $g$ be a positive integer. Let $k$ be a perfect field of characteristic $p > 2$ and let $C$ be a proper smooth curve over $k$ defined by $y^2 = f(x)$ for some separable polynomial $f \in k[x]$ of degree $2g+1$. Write $f(x)^{(p-1)/2} = \sum_j c_j x^j$. Then $C$ is ordinary, i.e. the $p$-rank of $J(C)$ is $g$, if and only if* $\det(A) \neq 0$*, where*

$$A = \left(c_{ip-j}\right)_{i,j=1}^{g}$$

*is the Cartier-Manin matrix.*

**Example 4.2.2.** Consider the hyperelliptic curve

$$H\colon y^2 = f(x) = x^5 + x^4 + x^3 + 3x^2 + x + 2$$

of genus 2 over $\mathbb{F}_5$. Then $f(x)^2 = x^{10} + 2x^9 + 3x^8 + 3x^7 + 4x^6 + 2x^5 + 3x^2 + 4x + 4$, and the Cartier-Manin matrix is

$$\begin{pmatrix} 0 & 2 \\ 0 & 3 \end{pmatrix},$$

and its determinant is 0, which means that $\mathrm{Jac}(H)$ is not ordinary.

The criterion is only formulated for hyperelliptic curves defined by an odd degree model. We prove that the criterion also holds for an even degree model.

**Theorem 4.2.3.** *Let $g$ be a positive integer. Let $k$ be a perfect field of characteristic $p > 2$ and let $C$ be a proper smooth curve over $k$ defined by $y^2 = f(x)$ for some separable polynomial $f \in k[x]$ of degree $2g+2$. Suppose that $g \leq p$. Write $f(x)^{(p-1)/2} = \sum_j c_j x^j$. Then $C$ is ordinary, i.e. the $p$-rank of $J(C)$ is $g$, if and only if* $\det(A) \neq 0$*, where*

$$A = \left(c_{ip-j}\right)_{i,j=1}^{g}$$

*is the Cartier-Manin matrix.*

*Proof.* To prove the statement, we may extend the field $k$ if necessary. Hence, we may and will assume that $f \in k[x]$ has a zero $\alpha \in k^*$. Now $C$ has another model $y^2 = h(x)$ where $h(x) = f(x+\alpha)$. We will prove that the condition $\det A \neq 0$ does not depend on the model chosen.

Write $h(x) = \sum_j d_j x^j$. Then $d_j = \sum_{\ell \geq j} c_\ell \cdot \binom{\ell}{j} \cdot \alpha^{\ell - j}$. Then we find that

$$d_{ip-j} = \sum_{g \geq I \geq i} \sum_{1 \leq J \leq j} \binom{I-1}{i-1} \cdot \binom{p-J}{p-j} \cdot c_{Ip-J} \cdot \alpha^{Ip-J-ip+j}, \tag{4.1}$$

as $\binom{pI-J}{pi-j} \equiv \binom{I-1}{i-1} \cdot \binom{p-J}{p-j} \mod p$ by Lucas's theorem (note that $i, j \leq g \leq p$) and using the fact that

$$\binom{\ell}{pi-j} \equiv 0 \mod p$$

if $\ell \not\equiv -1, -2, \ldots, -j \mod p$. Note that the coefficient in front of $c_{ip-j}$ in the right hand side of Eq. 4.1 is 1 and hence this shows that the matrix $(d_{ip-j})_{i,j=1}^{g}$ can be obtained from the matrix $(c_{ip-j})_{i,j=1}^{g}$ by means of elementary row and column operations: for $I > i$ you add $\binom{I-1}{i-1} \cdot \alpha^{Ip-ip}$ times the $I$-th row to the $i$-th row, starting from $i = 1$, working up to $i = g-1$, and for $J < j$ you add $\binom{p-J}{p-j} \cdot \alpha^{j-J}$ times the $J$-th column to the $j$-th column, starting from $j = g$. In other words, we have

$$\left(d_{pi-j}\right)_{i,j=1}^{g} = \left(\binom{I-1}{i-1} \cdot \alpha^{Ip-ip}\right)_{i,I=1}^{g} \cdot \left(c_{pi-j}\right)_{i,j=1}^{g} \cdot \left(\binom{p-J}{p-j} \cdot \alpha^{j-J}\right)_{J,j=1}^{g},,$$

and the second and fourth matrix occuring in the formula are triangular with 1's on the diagonal. Here, it should also be understood that $\binom{n}{k} = 0$ in case $k > n$.

Hence, the matrices $(c_{ip-j})_{i,j=1}^{g}$ and $(d_{ip-j})_{i,j=1}^{g}$ have the same determinant, which proves the claim. Now we may and will reduce without loss of generality to the case in which $x \mid f$. The curve given by

$$y^2 = f(x) = \sum_{i=1}^{2g+2} f_i x^i$$

has another model, namely $Y^2 = F(X)$, where we write $X = \frac{1}{x}$ and $Y = \frac{y}{x^{g+1}}$, and where

$$F(X) := \sum_{i=0}^{2g+1} f_{2g+2-i} X^i$$

is the polynomial $f$ but with its coefficients in reversed order. Note that $f_1 \neq 0$ as $f$ is separable and hence $F$ has degree $2g+1$. Now we apply Theorem 4.2.1 to the model $Y^2 = F(X)$. Write

$$F(X)^{(p-1)/2} = \sum_j C_j X^j.$$

It is the polynomial $f^{(p-1)/2}$ (as polynomial of degree $(g+1)(p-1)$) with its coefficients in reversed order, i.e. $C_j = c_{(g+1)(p-1)-j}$. Then

$$\left(C_{ip-j}\right)_{i,j=1}^{g} = \left(c_{(g+1-i)p-(g+1-j)}\right)_{i,j=1}^{g} = \left(c_{ip-j}\right)_{i,j=g,g-1,\ldots,2,1}.$$

Hence, the statement we want to prove follows from Theorem 4.2.1. □

## 4.3 Counting ordinary polynomials over $\mathbb{F}_q$

**Definition 4.3.1.** Let $g$ be a positive integer. A monic polynomial $f$ of degree $2g+2$ in $\mathbb{F}_q[x]$ is said to be *ordinary* if it has non-zero discriminant and the hyperelliptic curve $C$ of genus $g$ defined by $y^2 = f$ is ordinary.

**Corollary 4.3.2.** *Let $g > 0$ be an integer and let $q = p^a$ be an odd prime power. Suppose that $g \leq p$. Then there are at least $q^{2g+2} - (4g+3+\frac{p-1}{2} \cdot g) \cdot q^{2g+1}$ ordinary polynomials of degree $2g+2$ in $\mathbb{F}_q[x]$.*

*Proof.* Let $f = x^{2g+2} + c_{2g+1}x^{2g+1} + \ldots + c_0$ be a generic monic polynomial of degree $2g+2$. Its discriminant $\Delta(f)$ is a polynomial of total degree at most $2(2g+2)-1 = 4g+3$ in $\mathbb{F}_q[c_0, \ldots, c_{2g+1}]$. On the other hand, $\det(A)$ from Theorem 4.2.3 is a polynomial of total degree at most $g \cdot \frac{p-1}{2}$. Hence, the curve $y^2 = f$ is an ordinary hyperelliptic curve if and only if $h := \Delta(f) \cdot \det(A) \in \mathbb{F}_q[c_0, \ldots, c_{2g+1}]$, which is of total degree at most $4g + 3 + \frac{p-1}{2} \cdot g$, is not vanishing in the coefficients of $f$.

First of all note that $h \neq 0$, because there do exist ordinary hyperelliptic curves of genus $g$ over $\mathbb{F}_q$, see [GlPr05, Thm. 2.3], or Chapter 3 of this thesis. Hence, we have $0 \leqslant \deg h \leqslant 4g + 3 + \frac{p-1}{2} \cdot g$. By standard counting arguments, there can be at most $\deg h \cdot q^{2g+1}$ rational zeros of $h$. This proves the statement. □

## 4.4 Density in $\operatorname{Specmax} \mathcal{O}_K$

Let $K = \mathbb{Q}(\alpha)$ be a number field of degree $n > 1$. Let $\mathcal{O} = \mathcal{O}_K$ be its ring of integers. We will put the following density on the set of primes $\operatorname{Specmax} \mathcal{O}$ of $\mathcal{O}$.

**Definition 4.4.1.** For a subset $I \subset \operatorname{Specmax} \mathcal{O}$ we define its *natural density*, if it exists, as

$$\lim_{N \to \infty} \frac{\sum_{p \in \operatorname{Specmax} \mathbb{Z} : p \leqslant N} \sum_{\mathfrak{p} \in I : p\mathcal{O} \subset \mathfrak{p}} \kappa(\mathfrak{p})}{n \cdot |\{p \in \operatorname{Specmax} \mathbb{Z} : p \leqslant N\}|},$$

where $\kappa(\mathfrak{p})$ is the absolute residue field degree of $\mathfrak{p}$.

**Remark 4.4.2.** This density is non-standard. Often primes are weighted by $\frac{1}{|\mathbb{F}|}$, where $\mathbb{F}$ is the residue field. In other cases, the primes are ordered by the size of $|\mathbb{F}|$, rather than the size of the underlying prime number $p$. Here we chose to weigh the primes by the degree of their residue fields. The reason is that we want the set of primes having residue field degree 1 not to have density 1 (which it would have using the other notion of density).

Let $\mathcal{P}$ be the set of odd prime numbers that ramify nowhere in $\mathcal{O}$ and at which $\mathbb{Z}[\alpha]$ is regular. This set contains almost all prime numbers. By Kummer-Dedekind the splitting pattern of $p \in \mathcal{P}$ in the ring $\mathcal{O}$ is the factorisation pattern of $g := f_{\mathbb{Q}}^{\alpha}$ in $\mathbb{F}_p[X]$. By using the Frobenius density theorem ([LS96, p. 32]) in combination with Burnside's orbit-counting theorem, we can determine the proportion of linear primes in $\mathcal{O}$, i.e. primes of $\mathcal{O}$ having residue field degree 1.

**Lemma 4.4.3.** *Let $\Omega$ be the set of primes in $\operatorname{Specmax} \mathcal{O}$ with residue field degree 1. Then $\Omega$ has natural density $\frac{1}{n}$.*

*Proof.* As all but finitely many prime numbers are in $\mathcal{P}$, it suffices to only consider primes lying above elements of $\mathcal{P}$. Let $G$ be the Galois group of a Galois closure of $K$, considered as a subgroup of $S_n$, permuting the roots of $g$.

By the Frobenius density theorem the usual natural density of the set of prime numbers (in $\mathbb{Z}$) for which $g$ has decomposition type $(n_1, \ldots, n_t)$, where $n_1 \leq \ldots \leq n_t$ are positive

integers such that $n_1 + \ldots + n_t = n$, equals the proportion of elements in $G$ having cycle type $(n_1, \ldots, n_t)$.

Hence, the density of the set of primes in $\Omega$ is

$$\sum_{(n_1,\ldots,n_t)} \frac{|\{g \in G : g \text{ has cycle type } (n_1,\ldots,n_t)\}|}{|G|} \cdot \frac{|\{i : n_i = 1\}|}{n},$$

i.e., $\frac{1}{n}$ times the average, over the elements of $G$, of the number of fixed points. By Burnside's orbit-counting theorem, this average equals the number of orbits under $G$, which is 1 as $g$ is irreducible. Hence, the density of $\Omega$ is $\frac{1}{n}$. □

**Corollary 4.4.4.** *Both $\Omega$ and $\operatorname{Specmax}\mathcal{O} \setminus \Omega$ are infinite.*

## 4.5 Density in $\mathcal{O}^N$

Let $K$ and $\mathcal{O}$ be as before. Let $N$ be a positive integer. First, let us define a density on the set $\mathcal{O}^N$ (which we will then later identify with the set of monic polynomials of degree $N$ with coefficients inside $\mathcal{O}$).

**Definition 4.5.1.** Let $x = (x_1, \ldots, x_N) \in \mathcal{O}^N$, then we define its height as

$$h(x) := \sqrt{\sum_{i=1,\ldots,N} \sum_{\iota\colon K \hookrightarrow \mathbb{C}} |\iota(x_i)|^2}.$$

**Proposition 4.5.2.** *For every $M \in \mathbb{R}_{>0}$ there are only finitely many elements $x \in \mathcal{O}^N$ with $h(x) \leqslant M$.*

*Proof.* For every $i \in \{1, \ldots, N\}$ and every $\iota\colon K \hookrightarrow \mathbb{C}$ we have $|\iota(x_i)| \leqslant M$. Order the set $\{\iota\colon K \hookrightarrow \mathbb{C}\}$ and consider the map $\mathcal{O} \to \mathbb{C}^n\colon x \mapsto (\iota(x))_{\iota\colon K \hookrightarrow \mathbb{C}}$, which embeds $\mathcal{O}$ inside $\mathbb{C}^n$ as a discrete subgroup. The cube $\{(y_1, \ldots, y_n) \in \mathbb{C}^n : \forall j : |y_j| \leqslant M\}$ is compact. Hence, its intersection with the image of $\mathcal{O}$ is finite. In particular, there are only finitely many possibilities for the $x_i$ inside $\mathcal{O}$. □

The previous proposition proves that the following definition makes sense.

**Definition 4.5.3.** Let $S$ be a subset of $\mathcal{O}^N$, then the *natural density* of $S$, if it exists, is:

$$\lim_{M\to\infty} \frac{|\{x \in S : h(x) \leqslant M\}|}{|\{x \in \mathcal{O}^N : h(x) \leqslant M\}|}.$$

**Proposition 4.5.4.** *For each $M \in \mathbb{R}_{>0}$, let $E(M)$ be the number of elements in $\mathcal{O}$ of height at most $M$. Then there exists a constant $c \in \mathbb{R}_{>0}$ such that*

$$E(M) = c \cdot M^n + \varepsilon(M),$$

*where $\varepsilon$ is such that $\lim_{M\to\infty} \varepsilon(M)/M^n = 0$.*

*Proof.* Proof omitted. In fact, much stronger results are true, see [Div76]. □

The following lemma tells us that the natural density of a coset of a non-zero ideal is what one would expect.

**Lemma 4.5.5.** *Let $I \subset \mathcal{O}$ be a non-zero ideal and let $I'$ be a coset of $I$. Then the natural density of $I'$ is $[\mathcal{O} : I]^{-1}$.*

*Proof.* As abelian group, $I'$ is a union of cosets of $[\mathcal{O} : I]\mathcal{O}$, hence we may and will assume that $I$ is generated by an element in $\mathbb{Z}$, say $I = L\mathcal{O}$ for $L \in \mathbb{Z}$. Now choose some $x \in I'$ and let $s := h(x)$ be its height.

Let $M \in \mathbb{R}_{>s}$ and consider the elements in $\mathcal{O}$ of height at most $M$. There are $c \cdot M^n + \varepsilon(M)$ of them, where $c$ and $\varepsilon$ are as in Proposition 4.5.4. On the other hand, there are $c \cdot \left(\frac{M-s}{L}\right)^n + \varepsilon\left(\frac{M-s}{L}\right)$ elements $y \in \mathcal{O}$ of height at most $\frac{M-s}{L}$. For each such $y$, the point $L \cdot y + x$ has height at most $M$ and is in $I'$. Hence,

$$\liminf_{M\to\infty} \frac{|\{x \in I' : h(x) \leqslant M\}|}{|\{x \in \mathcal{O} : h(x) \leqslant M\}|} \geqslant \lim_{M\to\infty} \frac{c \cdot \left(\frac{M-s}{L}\right)^n + \varepsilon\left(\frac{M-s}{L}\right)}{c \cdot M^n + \varepsilon(M)} = \frac{1}{L^n}.$$

As this is true for every of the $L^n$ cosets of $I$, it follows that $I'$ has natural density $\frac{1}{L^n}$ as desired. □

## 4.6 Density of hyperelliptic curves with ordinary primes

Again, let $K$ be a number field of degree $n > 1$ over $\mathbb{Q}$, and let $\mathcal{O}$ be its ring of integers. Let $g$ be a positive integer and take $N = 2g + 2$. Now we will consider the hyperelliptic curves defined by monic polynomials of degree $N$ with coefficients in $\mathcal{O}$ with non-zero discriminant. We identify this set of polynomials with $\mathcal{O}^N$ to define a density on it.

**Theorem 4.6.1.** *Let $M$ be a positive integer. Let $S_M$ be the subset of $\mathcal{O}^N$ consisting of polynomials $f$ for which there exist at least $M$ distinct prime ideals $\mathfrak{p}$ such that $\overline{f} \in k_\mathfrak{p}[x]$ is ordinary. Then $S_M$ has (natural) density 1.*

*Proof.* Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ be those elements of $\operatorname{Specmax} \mathcal{O} \setminus \Omega$, the set of primes with residue field degree greater than 1, such that the prime numbers $p_i$ lying above the $\mathfrak{p}_i$ are all greater than $g$. For every $i = 0, 1, \ldots$, let $I_i := \prod_{j=i+1}^{i+M} \mathfrak{p}_i$. Then by Corollary 4.3.2 for at least

$$\prod_{j=i+1}^{i+M} \left(1 - \left(4g + 3 + \frac{p_i - 1}{2} \cdot g\right) \cdot q_i^{-1}\right) \geqslant 1 - \sum_{j=i+1}^{i+M} \left(4g + 3 + \frac{p_i - 1}{2} \cdot g\right) \cdot q_i^{-1}$$

of the residue classes modulo $I_i$, hyperelliptic curves reducing to this residue class are ordinary at $\mathfrak{p}_{i+1}, \ldots, \mathfrak{p}_{i+M}$. Here, $q_i$ is the order of $k(\mathfrak{p}_i)$. As the primes have residue

field degree at least 2, we have $q_i \geqslant p_i^2$ and hence

$$\sum_{j=i+1}^{i+M} \left(4g+3+\frac{p_i-1}{2}\cdot g\right)\cdot q_i^{-1} \leqslant (5g+3)\cdot \sum_{j=i+1}^{i+M} p_i^{-1}.$$

This converges to 0 as $i \to \infty$. By applying Lemma 4.5.5 we find that the density of $S_M$ equals 1. □

**Remark 4.6.2.** The methods used in this chapter seem to be unable to yield any result stronger than Theorem 4.6.1. In fact, even if one can prove, for example, that a proportion of at most $\frac{\log\log q}{q}$ of hyperelliptic curves over $\mathbb{F}_q$ are not ordinary, then it still seems to be possible that these hyperelliptic curves are exactly the ones with the smallest coefficients, in which case you cannot even prove the existence of a single hyperelliptic curve with infinitely many primes of ordinary good reduction.