



Universiteit  
Leiden  
The Netherlands

## Split Jacobians and Lower Bounds on Heights

Djukanovic, M.

### Citation

Djukanovic, M. (2017, November 1). *Split Jacobians and Lower Bounds on Heights*. Retrieved from <https://hdl.handle.net/1887/54944>

Version: Not Applicable (or Unknown)

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/54944>

**Note:** To cite this publication please use the final published version (if applicable).

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/54944> holds various files of this Leiden University dissertation.

**Author:** Djukanovic, M.

**Title:** Split Jacobians and Lower Bounds on Heights

**Issue Date:** 2017-11-01

# Summary

This thesis deals with properties of Jacobians of genus two curves that cover elliptic curves.

Let  $E$  be a curve in the plane, given by an equation  $y^2 = F(x)$ , where

$$F(x) = x^3 + a_2x^2 + a_1x + a_0$$

is a polynomial with rational coefficients and with three distinct roots. For historical reasons, such a curve is known as an *elliptic curve*. It is known that every elliptic curve  $E$  can be equipped with a structure of a commutative group – its points can be added and subtracted. A point  $O$  “at infinity”, which is contained in all vertical lines (lines of form  $x = c$ ), is the neutral element. This group structure is described by the condition that three points  $P, Q, R \in E$  satisfy  $P + Q + R = O$  if and only if they are collinear. Surfaces with a commutative group structure are called *abelian*. For example, a product  $E_1 \times E_2$  of two elliptic curves is an abelian surface in the obvious way.

Next we consider a planar curve  $C$  given by an equation  $y^2 = G(x)$ , where

$$G(x) = x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

is a polynomial with rational coefficients and six distinct roots. The curve  $C$  is called *hyperelliptic* and it does not have a group structure. However, we can associate to it, in a natural way, an abelian surface  $\text{Jac}(C)$ , called the *Jacobian* of  $C$ . Moreover, we can embed  $C$  into it.

Some hyperelliptic curves, of the form  $y^2 = G(x)$  as above, are special because they cover elliptic curves. For example, consider a curve  $C$  given by  $y^2 = x^6 + ax^4 + bx^2 + c$ , so that only even powers of  $x$  appear. If  $(x, y)$

is a point on this curve then so is  $(-x, y)$  and we can define an algebraic map  $f: (x, y) \mapsto (x^2, y)$ , that is of degree 2, i.e. 2-to-1. Now  $(X, Y) = (x^2, y)$  is a point on the elliptic curve  $E$  given by  $Y^2 = X^3 + aX^2 + bX + c$  and we say that  $C$  is a double cover of  $E$ .

If  $E$  is an elliptic curve, if  $C$  is a hyperelliptic curve, and if  $C \rightarrow E$  is an  $n$ -to-1 covering that is not a composition of coverings, then we can embed  $E$  into the surface  $\text{Jac}(C)$  as a subgroup. Moreover, there exists another elliptic curve  $\tilde{E}$  and an  $n$ -to-1 covering  $C \rightarrow \tilde{E}$ , such that the surface  $\text{Jac}(C)$  has a special property – it can be obtained as the quotient of the surface  $E \times \tilde{E}$  by a finite subgroup.

The first chapter of the thesis deals with the geometric aspects of this setup. We investigate which curves can form this special relationship and we focus mostly on the cases  $n = 2$  and  $n = 3$ , which have already been analysed in literature. We also gain some insight into the general case, but a full description proves to be very difficult computationally.

The second chapter deals with the arithmetic aspects of the setup, via the theory of *height functions*, which are a very useful tool in answering questions about rational points on curves and surfaces. To every rational number  $x = a/b$ , where  $a$  and  $b$  are coprime integers, one can associate its height  $h(x)$ , in a very precise way, as a measurement of its arithmetic complexity – the height roughly tells us how many digits are needed to write down the integers  $a$  and  $b$ . Likewise, the height of a rational point on a curve or surface tells us about the number of digits of the coordinates. For example,  $(3, 5)$  and  $(1749/1331, -1861/1331)$  are two rational points of rather different complexity on the curve  $y^2 = x^3 - x + 1$ , while  $(2, \sqrt{7})$  is not a rational point. It is also possible to associate a height to an elliptic curve or an abelian surface and measure its arithmetic complexity as a whole. A specific relation between these two heights is conjectured and we investigate it in the context of the setup above. We show that this relation holds for  $E \times \tilde{E}$  if and only if it holds for  $\text{Jac}(C)$ .