# Real Cubic Hypersurfaces and Group Laws 

Johannes Huisman<br>Département de Mathématiques<br>UFR Sciences et Techniques<br>Université de Bretagne Occidentale<br>6, avenue Victor Le Gorgeu<br>B.P. 809<br>29285 Brest Cedex - France<br>johannes.huisman@univ-brest.fr

Recibido: 20 de Enero de 2003
Aceptado: 19 de Febrero de 2004


#### Abstract

Let $X$ be a real cubic hypersurface in $\mathbb{P}^{n}$. Let $C$ be the pseudo-hyperplane of $X$, i.e., $C$ is the irreducible global real analytic branch of the real analytic variety $X(\mathbb{R})$ such that the homology class $[C]$ is nonzero in $H_{n-1}\left(\mathbb{P}^{n}(\mathbb{R}), \mathbb{Z} / 2 \mathbb{Z}\right)$. Let $\mathcal{L}$ be the set of real linear subspaces $L$ of $\mathbb{P}^{n}$ of dimension $n-2$ contained in $X$ such that $L(\mathbb{R}) \subseteq C$. We show that, under certain conditions on $X$, there is a group law on the set $\mathcal{L}$. It is determined by $L+L^{\prime}+L^{\prime \prime}=0$ in $\mathcal{L}$ if and only if there is a real hyperplane $H$ in $\mathbb{P}^{n}$ such that $H \cdot X=L+L^{\prime}+L^{\prime \prime}$. We also study the case when these conditions on $X$ are not satisfied.


Key words: real cubic hypersurface, real cubic curve, real cubic surface, pseudohyperplane, pseudo-line, pseudo-plane, linear subspace, group.
2000 Mathematics Subject Classification: 14J70, 14P25.

## 1. Introduction

The group law on the set of rational points of a cubic curve does not admit a generalization to cubic hypersurfaces [4]. That is, the set of rational points of a cubic hypersurface does not have a group law for which colinear points have zero sum. The idea of the present paper is that the higher dimensional analogue of a rational point of a cubic curve should not be a rational point of a cubic hypersurface, but should be a rational linear subspace of $\mathbb{P}^{n}$ of dimension $n-2$ that is contained in a cubic hypersurface.

## 2. Pseudo-hyperplanes of real hypersurfaces

Let $n$ be a natural integer satisfying $n \geq 2$. Let $X \subseteq \mathbb{P}^{n}$ be a real hypersurface, i.e., $X$ is defined by a nonconstant homogeneous real polynomial. Note that we do not assume $X$ to be reduced, irreducible or smooth. The set of real points $X(\mathbb{R})$ of $X$ is a real analytic subvariety of $\mathbb{P}^{n}(\mathbb{R})$. Let $C$ be an irreducible global real analytic branch of $X(\mathbb{R})$. Then $C$ is a compact connected real analytic subvariety of $\mathbb{P}^{n}(\mathbb{R})$. Its dimension is at most $n-1$. By [1], $C$ realizes a $\mathbb{Z} / 2 \mathbb{Z}$-homology class $[C]$ in $H_{n-1}\left(\mathbb{P}^{n}(\mathbb{R}), \mathbb{Z} / 2 \mathbb{Z}\right)$. This homology class vanishes if $\operatorname{dim}(C)<n-1$. We say that $C$ is a pseudo-hyperplane of $X$ if $[C] \neq 0$. In particular, the dimension of a pseudo-hyperplane of $X$ is equal to $n-1$. If $n=2$, a pseudo-hyperplane is called a pseudo-line. If $n=3$, a pseudo-hyperplane is called a pseudo-plane.

Proposition 2.1. Let $n$ and $d$ be natural integers. Let $X$ be a real hypersurface of $\mathbb{P}^{n}$ of degree $d$. Then, the number of pseudo-hyperplanes of $X$, when counted with multiplicities, is congruent to $d(\bmod 2)$.
Proof. We may assume that $X$ is reduced. Denote by $[X(\mathbb{R})]$ the homology class of $X(\mathbb{R})$ in $H_{n-1}\left(\mathbb{P}^{n}(\mathbb{R}), \mathbb{Z} / 2 \mathbb{Z}\right)$. One has $[X(\mathbb{R})]=d\left[\mathbb{P}^{n-1}(\mathbb{R})\right]$. Let $L$ be a general real projective line in $\mathbb{P}^{n}$. Then,

$$
[X(\mathbb{R})] \cdot[L(\mathbb{R})]=d\left[\mathbb{P}^{n-1}(\mathbb{R})\right] \cdot[L(\mathbb{R})]=d
$$

in $\mathbb{Z} / 2 \mathbb{Z}$. But the intersection number $[X(\mathbb{R})] \cdot[L(\mathbb{R})]$ is equal to the number of pseudo-hyperplanes of $X$. Therefore, the statement follows.

Proposition 2.2. Let $n$ and $d$ be natural integers. Let $X$ be a real hypersurface of $\mathbb{P}^{n}$ of degree d. Then, $X$ has at most d pseudo-hyperplanes, when counted with multiplicities.
Proof. Let $L \subseteq \mathbb{P}^{n}$ be a general real projective line. Let $C$ be a pseudo-hyperplane of $X$. Since $[C] \neq 0$ and $[L(\mathbb{R})] \neq 0$, the homological intersection product $[C]$. $[L(\mathbb{R})]$ is nonzero. In particular, the subsets $C$ and $L(\mathbb{R})$ of $\mathbb{P}^{n}(\mathbb{R})$ intersect each other. Therefore, any pseudo-hyperplane of $X$ intersects $L(\mathbb{R})$. Hence, the number of pseudo-hyperplanes of $X$, counted with multiplicities, is not greater than the degree of the intersection product $X \cdot L$. Since the latter degree is equal to $d$, the statement follows.

Proposition 2.3. Let $n$ and $d$ be natural integers. Let $X$ be a real hypersurface of $\mathbb{P}^{n}$ of degree $d$. Then, $X$ has exactly d pseudo-hyperplanes if and only if $X$ is the scheme-theoretic union of d real hyperplanes.

Proof. Suppose that $X$ is the scheme-theoretic union of $d$ real hyperplanes. Then it is clear that $X$ has exactly $d$ pseudo-hyperplanes, when counted with multiplicities.

Conversely, suppose that $X$ has exactly $d$ pseudo-hyperplanes, when counted with multiplicities. We show that $X$ is a scheme-theoretic union of real hyperplanes.

Clearly, one may assume that $X$ is reduced. Let $C$ be a pseudo-hyperplane of $X$. Since $\operatorname{dim}(C)=n-1$, there is a smooth point $P$ of $X$ that belongs to $C$. We show that the projective tangent space $T_{P} X$ of $X$ at $P$ is contained in $X$. It will follow that $X$ is the scheme-theoretic union of real hyperplanes.

Let $L$ be a real projective line in $T_{P} X$ passing through $P$. We show that $L$ is contained in $X$. Suppose that $L \nsubseteq X$. Then the intersection product $L \cdot X$ contains $P$ with multiplicity $\geq 2$. Moreover, $L(\mathbb{R})$ intersects each of the $d-1$ pseudohyperplanes $C^{\prime}$ of $X$ that are distinct from $C$. It follows that $\operatorname{deg}(L \cdot X) \geq 2+(d-1)=$ $d+1$, contradiction.

From Propositions 2.1, 2.2 and 2.3 one deduces the following consequence.
Corollary 2.4. Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface. Then $X$ has exactly one pseudo-hyperplane.

## 3. Real cubic hypersurfaces

Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface. Then, by Corollary 2.4 above, $X$ has exactly one pseudo-hyperplane. Let $C$ be the pseudo-hyperplane of $X$. Let $\mathcal{L}$ be the set of real linear subspaces $L$ of $\mathbb{P}^{n}$ of dimension $n-2$ that are contained in $X$ and that satisfy $L(\mathbb{R}) \subseteq C$. Note that the last condition on $L$ is superfluous if $C$ is entirely contained in the smooth locus of $X$. To put it otherwise, if all points of $C$ are smooth points of $X$ then $\mathcal{L}$ is nothing but the set of real linear subspaces of $\mathbb{P}^{n}$ of dimension $n-2$ that are contained in $X$.

The set $\mathcal{L}$ is well understood. If $n=2$, the set $\mathcal{L}$ is equal to the pseudo-line of $X$. If $n=3$, the set $\mathcal{L}$ is finite if $X$ is smooth or if $X$ is singular with isolated rational singularities [3, p. 66]. More generally, for arbitrary $n \geq 2$, let $X \subseteq \mathbb{P}^{n}$ have rational singularities in codimension $\geq 2$, i.e., the singular locus of $X$ has codimension $\geq 2$ and any general section of $X$ by a real 3 -dimensional linear subspace of $\mathbb{P}^{n}$ has only rational singularities. Then $\mathcal{L}$ is finite. This follows easily from [3].

Let $Z$ be the subset of $\mathcal{L} \times \mathcal{L}$ consisting of all pairs $(L, L)$ such that there is either no real hyperplane $H$ with $H \cdot X \geq 2 L$, or there are several such hyperplanes. Equivalently, $Z$ is the subset of the diagonal $\Delta$ of $\mathcal{L} \times \mathcal{L}$ whose complement in $\Delta$ consists of all pairs $(L, L)$ such that there is exactly 1 real hyperplane $H$ in $\mathbb{P}^{n}$ with $H \cdot X \geq 2 L$.

Proposition 3.1. Suppose that $C$ is homeomorphic to $\mathbb{P}^{n-1}(\mathbb{R})$. There is a unique partial composition law

$$
\circ: \mathcal{L} \times \mathcal{L} \backslash Z \longrightarrow \mathcal{L}
$$

determined by $L^{\prime \prime}=L \circ L^{\prime}$ if and only if there is a real hyperplane $H$ in $\mathbb{P}^{n}$ such that $H \cdot X=L+L^{\prime}+L^{\prime \prime}$.

Proof. Let $L, L^{\prime} \in \mathcal{L}$ with $\left(L, L^{\prime}\right) \notin Z$. The homology classes $[L(\mathbb{R})]$ and $\left[L^{\prime}(\mathbb{R})\right]$ are nonzero in $H_{n-2}(C, \mathbb{Z} / 2 \mathbb{Z})$. Since $C$ is homeomorphic to $\mathbb{P}^{n-1}(\mathbb{R})$, the intersection product $[L(\mathbb{R})] \cdot\left[L^{\prime}(\mathbb{R})\right]$ is nonzero. It follows that the linear subspaces $L$ and $L^{\prime}$ intersect in a real linear subspace of $\mathbb{P}^{n}$ of dimension $\geq n-3$. If $L \neq L^{\prime}$, the dimension of the intersection is equal to $n-3$. Hence, if $L \neq L^{\prime}$, there is a unique real hyperplane $H$ in $\mathbb{P}^{n}$ such that $H \cdot X \geq L+L^{\prime}$. If $L=L^{\prime}$ then there is also a unique real hyperplane $H$ in $\mathbb{P}^{n}$ such that $H \cdot X \geq L+L^{\prime}$ since $\left(L, L^{\prime}\right) \notin Z$.

Now, $H \cdot X$ is a real cubic hypersurface in the real projective space $H$. It has at least 2 pseudo-hyperplanes, when counted with multiplicities. From Propositions 2.1 and 2.3 it follows that there is a unique real linear subspace $L^{\prime \prime}$ of $\mathbb{P}^{n}$ of dimension $n-2$ such that $H \cdot X=L+L^{\prime}+L^{\prime \prime}$. Since Since $[H(\mathbb{R})] \cdot[C] \neq 0$ and $[L(\mathbb{R})]+\left[L^{\prime}(\mathbb{R})\right]=0$ in $H_{n-2}(C(\mathbb{R}), \mathbb{Z} / 2 \mathbb{Z})$, one has $L^{\prime \prime}(\mathbb{R}) \subseteq C$, i.e., $L^{\prime \prime} \in \mathcal{L}$.

It will be convenient, as in the case of cubic curves, to have an element $O \in \mathcal{L}$ such that there exist a unique real hyperplane $H_{0}$ in $\mathbb{P}^{n}$ with $H_{0} \cdot X=3 O$. Therefore, we consider the following conditions on $X$ :
(i) $X$ is smooth in codimension 1 ,
(ii) $C$ is homeomorphic to $\mathbb{P}^{n-1}(\mathbb{R})$, and
(iii) there is a real hyperplane $H_{0}$ in $\mathbb{P}^{n}$ such that $H_{0} \cdot X=3 O$ in $\operatorname{Div}(X)$.

There are lots of real cubic hypersurfaces satisfying conditions (i), (ii) and (iii): smooth real cubic curves in $\mathbb{P}^{2}$ satisfy the conditions (i) and, whenever an irreducible real cubic hypersurface in $\mathbb{P}^{n}$ satisfies the conditions, then a projective cone over it in $\mathbb{P}^{n+1}$ also satisfies the conditions (i), (ii) and (iii). And these are not the only ones [3].

Note, however, that a real cubic hypersurface $X$ satisfying conditions (i), (ii) and (iii) is necessarily singular if $n \geq 3$. Indeed, after a change of coordinates, one may assume that $H_{0}$ is given by the equation $X_{0}=0$, and that $O$ is the linear subspace of $\mathbb{P}^{n}$ defined by the equations $X_{0}=0$ and $X_{1}=0$. Then, $X$ is defined by a homogeneous polynomial of the form $X_{1}^{3}+X_{0} F$, where $F$ is a real quadratic form in $X_{0}, \ldots, X_{n}$. The closed subscheme of $X$ defined by the equations $X_{0}=0$, $X_{1}=0$ and $F=0$ is contained in the singular locus of $X$. If $n \geq 3$ then this closed subscheme is nonempty. Therefore, $X$ is singular if $n \geq 3$.

Lemma 3.2. Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface satisfying conditions (i), (ii) and (iii) above. Then $O \in \mathcal{L}$ and $(O, O) \notin Z$.

Proof. Since $H_{0} \cdot X=3 O, O$ is a real linear subspace of $\mathbb{P}^{n}$ of dimension $n-2$. Since $n-2 \geq 0$, the set of real points $O(\mathbb{R})$ of $O$ is nonempty. Since $O(\mathbb{R}) \subseteq X(\mathbb{R})$ and $O(\mathbb{R})$ is irreducible, there is an irreducible global real analytic branch $C^{\prime}$ of $X(\mathbb{R})$ such that $O(\mathbb{R}) \subseteq C^{\prime}$. Since $X$ is smooth in codimension $1, O$ is not contained in the singular locus of $X$. It follows that $O(\mathbb{R})$ contains a smooth point of $X$. In
particular, $C^{\prime}$ is a real analytic variety of dimension $n-1$. Suppose that $\left[C^{\prime}\right]=0$ then also $\left[H_{0}(\mathbb{R})\right] \cdot\left[C^{\prime}\right]=[O(\mathbb{R})]=0$. But $[O(\mathbb{R})] \neq 0$, contradiction. Therefore, $\left[C^{\prime}\right] \neq 0$, i.e., $C^{\prime}$ is a pseudo-hyperplane of $X$. It follows from Corollary 2.4 that $C^{\prime}=C$ and $O \in \mathcal{L}$.

Since $X$ is smooth in codimension 1 , the hyperplane $H_{0}$ is the unique real hyperplane satisfying $H_{0} \cdot X \geq 2 O$. Hence, $(O, O) \notin Z$.

From now on, suppose that $X \subseteq \mathbb{P}^{n}$ is an irreducible real cubic hypersurface satisfying conditions (i), (ii) and (iii) above. Define a partial composition law $\oplus$ on $\mathcal{L}$,

$$
\oplus: \mathcal{L} \times \mathcal{L} \backslash Z \longrightarrow \mathcal{L}
$$

by $L \oplus L^{\prime}=O \circ\left(L \circ L^{\prime}\right)$ for all $\left(L, L^{\prime}\right) \in \mathcal{L}^{2} \backslash Z$. Note that this is well defined by Lemma 3.2. Define also a map

$$
\ominus: \mathcal{L} \longrightarrow \mathcal{L}
$$

by $\ominus L=O \circ L$ for all $L \in \mathcal{L}$. Note again that this well defined.
Let $\operatorname{Pic}(X)$ be the Picard group of $X$. Since $X$ is smooth in codimension 1, the group $\operatorname{Pic}(X)$ is the group of linear equivalence classes of divisors on $X$ [2]. Define a map

$$
\varphi: \mathcal{L} \longrightarrow \operatorname{Pic}(X)
$$

by $\varphi(L)=\operatorname{cl}(L-O)$, for all $L \in \mathcal{L}$, where cl denotes the linear equivalence class.
Theorem 3.3. Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface satisfying conditions (i), (ii) and (iii) above. Then the map $\varphi$ is injective. Moreover, for all $\left(L, L^{\prime}\right) \in \mathcal{L}^{2} \backslash Z$ one has

$$
\varphi\left(L \oplus L^{\prime}\right)=\varphi(L)+\varphi\left(L^{\prime}\right)
$$

And, for all $L \in \mathcal{L}$ one has

$$
\varphi(\ominus L)=-\varphi(L)
$$

Proof. Let $L, L^{\prime} \in \mathcal{L}$ such that $\varphi(L)=\varphi\left(L^{\prime}\right)$. Then the invertible sheaves $\mathcal{O}(L)$ and $\mathcal{O}\left(L^{\prime}\right)$ on $X$ are isomorphic. Let $P \subseteq \mathbb{P}^{n}$ be a general real linear subspace of dimension 2. Then, $E=P \cap X$ is a smooth real cubic curve, $P \cap L$ and $P \cap L^{\prime}$ are real points of $E$, and the invertible sheaves $\mathcal{O}(P \cap L)$ and $\mathcal{O}\left(P \cap L^{\prime}\right)$ on $E$ are isomorphic. It follows (cf. [5]) that $P \cap L=P \cap L^{\prime}$. Since $P$ is general, one has $L=L^{\prime}$. This proves that $\varphi$ is injective.

Let $L \in \mathcal{L}$. By Proposition 3.1, there is a real hyperplane $H$ of $\mathbb{P}^{n}$ such that

$$
H \cdot X=O+L+\ominus L
$$

Then

$$
\operatorname{div}\left(\frac{H}{H_{0}}\right)=(O+L+\ominus L)-3 O=(L-O)+(\ominus L-O)
$$

It follows that $\varphi(\ominus L)=-\varphi(L)$.
Similarly, if $\left(L, L^{\prime}\right) \in \mathcal{L}^{2} \backslash Z$, then $\varphi\left(L \oplus L^{\prime}\right)=\varphi(L)+\varphi\left(L^{\prime}\right)$.

Corollary 3.4. Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface satisfying conditions (i), (ii) and (iii) above. Suppose that for each $L \in \mathcal{L}$ there is a real hyperplane $H$ in $\mathbb{P}^{n}$ such that $H \cdot X \geq 2 L$. Then $(\mathcal{L}, \oplus, \ominus, O)$ is an abelian group and the map $\varphi$ is an isomorphism from $\mathcal{L}$ onto a subgroup of $\operatorname{Pic}(X)$.

If $n=2$, then $X$ is a smooth real cubic curve, $C$ is the pseudo-line of $X$, the set $\mathcal{L}$ is equal to $C$, and $Z=\emptyset$. Therefore, Corollary 3.4 reconstructs the classical group structure on $C$ [5]. This is not surprising since we used in the proof of Theorem 3.3 the classical fact that the map $\varphi$ is injective if $n=2$. More generally, if $X \subseteq \mathbb{P}^{n}$ is a real projective cone over a nonsingular real cubic curve $E$, then there is an obvious bijection between $\mathcal{L}$ and the real pseudoline of $E$, and, again, $Z=\emptyset$. Therefore, $\mathcal{L}$ is a group that is isomorphic to the group structure on the pseudo-line of $E$. More interesting cases are the cases where $X$ has rational singularities in codimension $\geq 2$.

Let $\mathbb{Z}[\mathcal{L}]$ be the free abelian group generated by the elements of $\mathcal{L}$. Let $H$ be the subgroup of $\mathbb{Z}[\mathcal{L}]$ generated by the elements

$$
L \oplus L^{\prime}-L-L^{\prime}
$$

for $\left(L, L^{\prime}\right) \in \mathcal{L}^{2} \backslash Z$, and the elements

$$
\ominus L+L
$$

for $L \in \mathcal{L}$, and the element $O$. Let $G$ be the quotient group $\mathbb{Z}[\mathcal{L}] / H$.
Proposition 3.5. Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface satisfying conditions (i), (ii) and (iii) above. Then

$$
G=\mathcal{L} \cup\{m L \mid(L, L) \in Z \text { and } m \geq 2\}
$$

Proof. Let $R$ be the right-hand side of the equation. Let $g$ be an element of $G$. We may assume that $g=\sum_{i=1}^{\ell} L_{i}$, where $L_{i} \in \mathcal{L}$ for $i=1, \ldots, \ell$. We show that one can reduce $\ell$ successively to get in the end $g \in R$.

If $\ell \leq 1$ then we are done. Suppose therefore that $\ell \geq 2$. If $\left(L_{\ell-1}, L_{\ell}\right) \notin Z$ then put $L_{\ell-1}^{\prime}=L_{\ell-1} \oplus L_{\ell}$. One has $g=\sum_{i=1}^{\ell-1} L_{i}^{\prime}$, where $L_{i}^{\prime}=L_{i}$ for $i=1, \ldots, \ell-2$. Continuing in this way, one has in the end either $g \in \mathcal{L}$ or $g=m L$ for some $L \in \mathcal{L}$ with $(L, L) \in Z$ and $m \geq 2$, i.e., $g \in R$.

Corollary 3.6. Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface satisfying conditions (i), (ii) and (iii) above. Suppose that $X$ has rational singularities in codimension $\geq 2$. Then $\operatorname{rank}(G) \leq 1$.

Proof. Since $X$ has rational singularities in codimension $\geq 2$, the set $\mathcal{L}$ is finite [3]. By Proposition 3.5, the $\mathbb{Q}$-vector space $\mathbb{Q} \otimes G$ is a union of finitely many 1-dimensional subspaces. Hence, $\operatorname{dim}(\mathbb{Q} \otimes G) \leq 1$. Since $G$ is a $\mathbb{Z}$-module of finite type, $\operatorname{rank}(G) \leq 1$.

Corollary 3.7. Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface satisfying conditions (i), (ii) and (iii) above. Suppose that $X$ has rational singularities in codimension $\geq 2$. Then the map $\varphi: \mathcal{L} \longrightarrow \operatorname{Pic}(X)$ induces a morphism

$$
\psi: G \longrightarrow \operatorname{Pic}(X)
$$

The image of $\psi$ is a subgroup of $\operatorname{Pic}(X)$ of rank $\leq 1$.
Let $X \subseteq \mathbb{P}^{n}$ be an irreducible real cubic hypersurface satisfying conditions (i), (ii) and (iii) above, and having rational singularities in codimension $\geq 2$. One of the following three conditions hold:
(i) $\psi(G)=\varphi(\mathcal{L})$,
(ii) $\psi(G) \neq \varphi(\mathcal{L})$ and $\psi(G)$ is finite, or
(iii) $\psi(G)$ is not finite.

The first case occurs when, for each $L \in \mathcal{L}$, there is a real hyperplane $H$ in $\mathbb{P}^{n}$ such that $H \cdot X \geq 2 L$ (see Proposition 3.5). Explicit examples of real cubic hypersurfaces $X$ having this property can be easily constructed using [3, p. 66]. It would be interesting to construct real cubic hypersurfaces $X$ for which one of the other conditions hold. It would also be interesting to determine the group $\psi(G)$ explicitly in each of the above three cases.

Acknowledgements. I am grateful to Louis Mahé for our discussions on cubic hypersurfaces and group laws.

## References

[1] A. Borel and A. Haefliger, La classe d'homologie fondamentale d'un espace analytique, Bull. Soc. Math. France 89 (1961), 461-513.
[2] R. Hartshorne, Algebraic geometry, Springer-Verlag, New York, 1977, ISBN 0-387-90244-9.
[3] H. Knörrer and T. Miller, Topologische Typen reeller kubischer Flächen, Math. Z. 195 (1987), 51-67.
[4] Y. I. Manin, Cubic forms, North-Holland Mathematical Library, vol. 4, North-Holland Publishing Co., Amsterdam, 1986, ISBN 0-444-87823-8.
[5] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986, ISBN 0-387-96203-4.

