Tôhoku Math. J.
49 (1997), 149–163

HASSE-WITT MATRICES FOR THE FERMAT CURVES OF PRIME DEGREE

JOSEP GONZÁLEZ

(Received October 31, 1995, revised July 22, 1996)

Abstract. We study a class of curves which includes the hyperelliptic curves and the Fermat curves of prime degree. We compute their Hasse-Witt matrix when the curves are defined over an algebraically closed field of positive characteristic. In particular, we get a formula for the Hasse-Witt invariant of the Fermat curves at each prime not equal to the degree. These invariants depend only on residue degrees.

We show that there are infinitely many Fermat curves for which there exists a set of primes p with positive density such that the geometric fibre at p of the Fermat Jacobian is not isogenous to a power of a supersingular elliptic curve, but the Hasse-Witt invariant at p is equal to zero.

1. Introduction. Let C be a non-singular projective curve of genus $g>0$, defined over an algebraically closed field k of characteristic $p>0$. Hasse and Witt [Ha34], [Ha-Wi36] determined the maximum number, $r(C)$, of cyclic unramified independent extensions of degree p of the function field $k(C)$. This number is called the Hasse-Witt invariant of the curve.

Serre [Se58] characterized the Hasse-Witt invariant by means of the action of the absolute Frobenius F^* on the first cohomology group of the curve:

$$r(C)=\dim_{\mathbf{F}_p} H^1(C, \mathcal{O})^{F^*}=\dim_k \operatorname{Im}(F^*)^g .$$

The curve C is said to be *ordinary* if $r(C)=g$. When $g=1$, it is said to be *supersingular* if $r(C)=0$.

The computation of this invariant for elliptic curves is well known. Manin [Ma62] computed the Hasse-Witt invariant for hyperelliptic curves by means of the matrix of the Cartier operator acting on an explicit basis of regular differentials. The structure of the p-divisible groups arising from Fermat curves over finite fields of characteristic p was studied by Yui in [Yu80]; arithmetical invariants for Fermat curves and Fermat varieties were also consider in [Yu86] and Toki [To88]. In this paper we compute the Hasse-Witt invariant for curves of a special family, which includes, as particular cases, the hyperelliptic curves and the Fermat curves. We use for it the absolute Frobenius operator acting on an explicit basis of repartitions. The advantage of using the absolute Frobenius instead of the Cartier operator will be apparent when we compute the matrix

1991 *Mathematics Subject Classification.* Primary 14H45; Secondary 14H40.
This research was partially supported by DGICYT, PB-93-0034.

of the iterated operators.

I would like to end this introduction by expressing my gratitude to Professor Pilar Bayer for her constant help and encouragement.

2. General facts. Let A be an abelian variety over k of dimension g. We write

$$r(A) := \dim_{\mathbf{F}_p} H^1(A, \mathcal{O})^{F^*} = \dim_k \operatorname{Im}(F^*)^g .$$

We have that $r(A) = \dim_{\mathbf{F}_p} \operatorname{Pic}^0(A)[p]$ is the p-rank of A (cf. [Mu70]). If A is the jacobian of the curve C, then $r(C) = r(A)$. Given abelian varieties A, B defined over k, we have $r(A \times B) = r(A) + r(B)$. If A is isogenous to a product of abelian varieties $\prod_{i=1}^m A_i$, we have $r(A) = \sum_{i=1}^m r(A_i)$ due to the fact that $r(A)$ is invariant under isogenies.

We recall that a *repartition* of the curve C is a family $r = \{r_x\}_{x \in C}$ such that $r_x \in k(C)$ and for almost all $x \in C$ we have $r_x \in \mathcal{O}_x$. We identify the elements of $H^1(C, \mathcal{O})$ with classes of repartitions as in [Se58], where $r \equiv 0$ in $H^1(C, \mathcal{O})$ if and only if there exists a function h on C such that $h - r_x \in \mathcal{O}_x$ for all $x \in C$.

Given a repartition $r = \{r_x\}_{x \in C}$ and a regular differential $\omega \in H^0(C, \Omega^1)$, we consider Serre's pairing defined by $\langle r, \omega \rangle = \sum_{x \in C} \operatorname{res} r_x \omega$. For each morphism of curves $\pi : C_2 \to C_1$, we denote by $\pi^* : H^1(C_1, \mathcal{O}) \to H^1(C_2, \mathcal{O})$ the homomorphism given by $\pi^*(r)_y = r_{\pi(y)} \circ \pi$ for all $y \in C_2$. It commutes with the absolute Frobenius $F^*_{C_1}$, $F^*_{C_2}$ and satisfies $\langle \pi^*(r), \pi^*(\omega) \rangle = \deg \pi \langle r, \omega \rangle$, where $\deg \pi$ denotes the degree of π.

3. A family of curves. Let l be a prime and k an algebraically closed field of characteristic not equal to l. Let C' be the projective curve in $\mathbf{P}^2$ associated to the affine curve defined by the equation

$$Y^l = F(X) ,$$

where $F(X) \in k[X]$ is a separable polynomial of degree n. Let us note that for $l = 2$ and $n > 2$ we obtain all the hyperelliptic curves defined over k. If $F(X) = X^l + 1$, we obtain the Fermat curves over k with prime degree l.

Let us suppose that $F(X) = a_n \prod_{i=1}^n (X - x_i)$, with $x_i \neq x_j$ if $i \neq j$. If $|n - l| \leq 1$, the curve C' is non-singular. Fermat curves are examples. Otherwise, C' has a singularity at infinity, given by (0, 1, 0) or (1, 0, 0), depending on whether $l + 1 < n$ or $l > n + 1$.

Let $\pi : C \to C'$ be the normalization of the curve C' and $\psi : C' \to \mathbf{P}^1$ the morphism defined by

$$\psi(x, y, z) := \begin{cases} x/z & \text{if } z \neq 0 \\ \infty & \text{otherwise} . \end{cases}$$

The composite $\phi = \psi \circ \pi : C \to \mathbf{P}^1$ is a cyclic covering of degree l, unramified outside $\{x_1, \ldots, x_n, \infty\}$. Let $P_i = \phi^{-1}(x_i)$, $1 \leq i \leq n$ and $\mathcal{P} = \phi^{-1}(\{\infty\})$. The set $\mathcal{P}$ is $\{P_\infty\}$ or $\{P^1_\infty, \ldots, P'_\infty\}$, depending on whether or not ϕ is ramified at ∞. We note that if $n \equiv 0 \pmod{l}$, then C is isomorphic to the non-singular projective curve determined by the

equation $Y^l = X^n F(1/X + x_n)$ where $X^n F(1/X+x_n)$ is a separable polynomial of degree $n-1$. It is easily seen that ϕ is unramified at infinity if and only if $n \equiv 0 \pmod{l}$. In this case the genus of C is equal to $(n-2)(l-1)/2$; otherwise, $g=(n-1)(l-1)/2$.

We still denote by X, Y the functions $\pi^*(X)$, $\pi^*(Y)$, respectively. We define the set

$$\mathscr{S} := \{(i,j) \in \mathbf{N} \times \mathbf{N} \mid 1 \leq i \leq l-1,\ 1 \leq j \leq [(ni-1)/l]\},$$

where [ ] denotes the integer part. We note that $\sharp \mathscr{S} = g$ and consider the differentials

$$\omega_{i,j} := X^{j-1} dX / Y^i, \qquad (i,j) \in \mathscr{S}.$$

3.1. PROPOSITION. *The set of differentials $\{\omega_{i,j}\}_{(i,j)\in\mathscr{S}}$ form a basis of $H^0(C, \Omega^1)$.*

For each $(i,j) \in \mathscr{S}$, let us consider the repartition defined by

$$(r_{i,j})_x := \begin{cases} Y^i/X^j & \text{if } x \in \mathscr{P} \\ 0 & \text{otherwise.} \end{cases}$$

Let us denote by $\mathscr{Q}$ the set of points of C such that $X=0$. Thus,

$$\mathscr{Q} = \begin{cases} \{Q_1, \ldots, Q_l\} & \text{if } F(0) \neq 0 \\ \{P\}, \text{ where } P \in \{P_1, \ldots, P_n\} & \text{otherwise,} \end{cases}$$

for some points Q_i. Notice that, given a regular differential ω and a function h regular outside $\mathscr{P} \cup \mathscr{Q}$ (for instance $h = Y^i/X^j$), we have $\sum_{P\in\mathscr{P}} \operatorname{res}_P h\omega = -\sum_{Q\in\mathscr{Q}} \operatorname{res}_Q h\omega$.

3.2. PROPOSITION. *We have that*

$$\langle r_{i,j}, \omega_{i',j'} \rangle = \begin{cases} -l & \text{if } (i,j) = (i',j') \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $\{r_{i,j}\}_{(i,j)\in\mathscr{S}}$ is a basis of $H^1(C, \mathscr{O})$.

PROOF. Without loss of generality, we may assume that $F(0) \neq 0$, since otherwise C is isomorphic to the curve determined by the equation $Y^l = F(X+a)$, where $F(a) \neq 0$. We have to consider the following cases separately:

(i) $(i,j) = (i',j')$: $\langle r_{i,j}, \omega_{i,j} \rangle = \sum_{P\in\mathscr{P}} \operatorname{res} dX/X = -l$, since if $n \not\equiv 0 \pmod{l}$ then $\operatorname{ord}_{P_\infty} X = -l$, while $\operatorname{ord}_{P_\infty^s} X = -1$ if $n \equiv 0 \pmod{l}$.

(ii) $i = i'$, $j \neq j'$: The proof is obvious in this case.

(iii) $j < j'$: $\langle r_{i,j}, \omega_{i',j'} \rangle = -\sum_{Q\in\mathscr{Q}} \operatorname{res}_Q Y^{i-i'} dX/X^{j-j'+1} = 0$, since for all $Q \in \mathscr{Q}$ we have that $\operatorname{ord}_Q Y^{i-i'} dX/X^{j-j'+1} \geq 0$.

(iv) $j \geq j'$, $i < i'$: $\langle r_{i,j}, \omega_{i',j'} \rangle = 0$, since $\operatorname{ord}_P Y^{i-i'} dX/X^{j-j'+1} \geq 0$ for all $P \in \mathscr{P}$.

(v) $j \geq j'$, $i > i'$: Given two natural numbers s, m we have

$$d^m Y^s / dX^m = R_{m,s}(X) Y^s / F(X)^m,$$

where $R_{m,s}(x) \in k[x]$. Since X is a uniformizer at all $Q \in \mathscr{Q}$, we have

$$\langle r_{i,j}, \omega_{i',j'}\rangle = -\frac{R_{j-j',i-i'}(0)}{(j-j')!F(0)^{j-j'}} \sum_{Q\in\mathscr{Q}} Y(Q)^{i-i'} = 0\,,$$

due to the fact that the sum of all l-th roots of an element in k is zero. □

4. The Hasse-Witt matrix. From now on, k denotes a field of characteristic $p>0$. For each i such that $1\le i\le l-1$, let us write $j_i := [(ni-1)/l]$. We will say that a value i is *effective* if $j_i>0$; this is equivalent to saying that a repartition $r_{i,j}$ with the first index equal to i does exist. Let us note that if $n\not\equiv 0 \pmod l$, then $j_i=[ni/l]$, while if $n\equiv 0 \pmod l$ then $j_i=ni/l-1$. Let $W=(w_{i,j}^{i',j'})$ be the matrix of the absolute Frobenius F^* acting on $H^1(C,\mathscr{O})$, relative to the basis $\{r_{i,j}\}_{(i,j)\in\mathscr{S}}$. That is,

$$r_{i,j}^p \equiv \sum_{(i',j')\in\mathscr{S}} w_{i,j}^{i',j'} r_{i',j'}\,.$$

W is called the Hasse-Witt matrix for C. These equations are equivalent to the existence, for each $(i,j)\in\mathscr{S}$, of a function $h_{i,j}$, determined up to an additive constant and regular outside $\mathscr{P}$ such that at each point of $\mathscr{P}$ it has a pole with the same polar part as

$$(Y^i/X^j)^p - \sum_{(i',j')\in\mathscr{S}} w_{i,j}^{i',j'} Y^{i'}/X^{j'}\,.$$

Given $i, s\in\mathbf{Z}$, with $1\le i\le l-1$, the divisor of the function Y^i/X^s is

$$i\sum_{m=1}^{n} P_m - s\frac{l}{\#\mathscr{Q}}\sum_{Q\in\mathscr{Q}} Q - \frac{ni-ls}{\#\mathscr{P}}\sum_{P\in\mathscr{P}} P\,.$$

Thus, for $s\le 0$, the function Y^i/X^s has poles only in $\mathscr{P}$, while for $s>0$, Y^i/X^s has poles only in $\mathscr{Q}$ if $s>j_i$, and in $\mathscr{P}$ and $\mathscr{Q}$ if $s\le j_i$.

Given a rational l-integer a, we denote by $\langle a\rangle$ the least natural number such that $a\equiv\langle a\rangle \pmod l$. If $a\in\mathbf{N}$, $\langle a\rangle = a-l[a/l]$.

4.1. PROPOSITION. *Given a natural number i such that $1\le i\le l-1$, we denote by $F_i(X)$ the polynomial $F(X)^{[pi/l]}=\sum_{m=0}^{n[pi/l]} b_{i,m}X^m$. The Hasse-Witt matrix $W=(w_{i,j}^{i',j'})$ for C is given by*

$$w_{i,j}^{i',j'} = \begin{cases} b_{i,jp-j'} & \text{if } i'=\langle pi\rangle\,,\ jp-j'\ge 0\,,\\ 0 & \text{otherwise}\,. \end{cases}$$

PROOF. Let us write

$$h(X,Y) := (Y^i/X^j)^p - \sum_{(i',j')\in\mathscr{S}} w_{i,j}^{i',j'} Y^{i'}/X^{j'}\,,$$

where the $w_{i,j}^{i',j'}$ are as above. Since $Y^{ip}=Y^{l[pi/l]}Y^{\langle pi\rangle}$, we have

$$h(X, Y)=F_i(X)Y^{\langle pi\rangle}/X^{jp}-\sum_{(i',j')\in\mathscr{S}} w_{i,j}^{i',j'}Y^{i'}/X^{j'}\ .$$

The terms $Y^{\langle pi\rangle}/X^s$, for $1\leq s\leq j_{\langle pi\rangle}=[(n\langle pi\rangle-1)/l]$, cancel themselves out, and the function $h(X, Y)$ can be expressed as the sum of two functions $h_{i,j}$, $g_{i,j}$, where the first one (which contains the monomials $Y^{\langle pi\rangle}/X^s$, for $s\leq 0$) is regular outside $\mathscr{P}$, and the second one (which contains the monomials $Y^{\langle pi\rangle}/X^s$, for $s>j_{\langle pi\rangle}$) is regular outside $\mathscr{Q}$. Hence, $h_{i,j}$ has at each point of $\mathscr{P}$ the same polar part as $h(X, Y)$ and is regular outside $\mathscr{P}$; thus,

$$r_{i,j}^p-\sum_{(i',j')\in\mathscr{S}} w_{i,j}^{i',j'}Y^{i'}/X^{j'}\equiv 0\ .$$

□

Let $I=\{i\in N\mid 1\leq i\leq l-1, j_i>0\}$ be the set of effective indices. For each pair $(i, i')\in I\times I$, we denote by $W_i^{i'}$ the matrix $(w_{i,j}^{i',j'})$, where $1\leq j\leq j_i$, $1\leq j'\leq j_{i'}$.

4.2. PROPOSITION. *The relation* $\operatorname{rank} W=\sum_{(i,\langle pi\rangle)\in I\times I}\operatorname{rank} W_i^{\langle pi\rangle}$ *holds.*

PROOF. Let $I=\{i_1<\cdots<i_m\}$ and let us put the elements of $\mathscr{S}$ in the lexicographic order. Then,

$$W=\begin{pmatrix} W_{i_1}^{i_1} & \cdots & W_{i_m}^{i_1} \\ \vdots & \vdots & \vdots \\ W_{i_1}^{i_m} & \cdots & W_{i_m}^{i_m} \end{pmatrix}.$$

Taking into account the previous proposition, the submatrices $W_{i_j}^{i_k}$ such that $i_k\neq\langle pi_j\rangle$ are zero. Since $\langle pi_j\rangle=\langle pi_k\rangle$ implies $i_j=i_k$, the proposition follows. □

Given an integer $m>0$, let

$W(m):=(w(m)_{i,j}^{i',j'})$, the matrix of $(F^*)^m$ acting on $H^1(C, \mathcal{O})$, relative to the basis $\{r_{i,j}\}$,

$q_i(m):=[p^m i/l]$,

$F_{i,m}(X):=F(X)^{q_i(m)}=:\sum b(m)_{i,k}X^k$,

$W_i^{i'}(m):=(w(m)_{i,j}^{i',j'})$, for $(i, i')\in I\times I$, with $1\leq j\leq j_i$, $1\leq j'\leq j_{i'}$.

The following proposition can be proved along the same lines as the previous ones.

4.3. PROPOSITION. *The entries of the matrix* $W(m)$ *are*

$$w(m)_{i,j}^{i',j'}=\begin{cases} b(m)_{i,jp^m-j'} & \text{if } i'=\langle p^m i\rangle\ ,\quad jp^m-j'\geq 0\ , \\ 0 & \text{otherwise}\ . \end{cases}$$

The relation $\operatorname{rank} W(m)=\sum_{(i,\langle p^m i\rangle)\in I\times I}\operatorname{rank} W_i^{\langle p^m i\rangle}(m)$ *holds.*

Let us note that, if $F(X)$ is a polynomial defined over $\boldsymbol{F}_{p^s}$, then the matrices $W(m)$

have their entries in $\boldsymbol{F}_{p^s}$ and $W(sm)=W(s)^m$. In this case, the Hasse-Witt invariant coincides with the sum of the multiplicities of the non-zero roots of the characteristic polynomial of the matrix $W(s)$.

4.4. PROPOSITION. *If $p\not\equiv 1 \pmod{l}$, then C is non-ordinary.*

PROOF. Without loss of generality, we may suppose that $n\not\equiv 0 \pmod{l}$. The submatrix $W_i^{\langle pi\rangle}$, with $(i,\langle pi\rangle)\in I\times I$, has exactly j_i columns and $j_{\langle pi\rangle}$ rows. We have that

$$\operatorname{rank} W=\sum_{(i,\langle pi\rangle)\in I\times I}\operatorname{rank} W_i^{\langle pi\rangle}\leq\sum_{i=1}^{l-1}\operatorname{Min}\{j_i,j_{\langle pi\rangle}\}\,.$$

It remains only to show that there exists an index i_0 such that $j_{i_0}<j_{\langle pi_0\rangle}$ since, in this case, we have

$$\operatorname{rank} W<\sum_{i=1}^{l-1}j_{\langle pi\rangle}=g\,.$$

Let $r=\langle p\rangle$ and $i_0:=[l/r]$. It is obvious that $2\leq r\leq l-1$, $1\leq i_0\leq l-1$. We will show that i_0 satisfies the above mentioned condition. Indeed, we have that

$$j_i=[ni/l]\,,\quad j_{\langle pi\rangle}=[(npi-n[pi/l]l)l]=[npi/l]-n[pi/l]\,.$$

It is easily seen that $j_{\langle pi\rangle}=[nir/l]-n[ri/l]$. Thus, we get

$$j_{i_0}=[ni_0/l]\,,\quad j_{\langle pi_0\rangle}=[ni_0r/l]-n[ri_0/l]=[ni_0r/l]\,.$$

If $n\geq r+1$, then $ni_0r-ni_0=ni_0(r-1)\geq(r+1)i_0(r-1)\geq ri_0+(r-1)\geq l$; and hence $j_{i_0}<j_{\langle pi_0\rangle}$. If $2\leq n\leq r$, then

$$j_{i_0}=0\,,\quad j_{\langle pi_0\rangle}=[ni_0r/l]\geq[2i_0r/l]\geq[(i_0r+r)/l]\geq 1\,.$$

□

In the case of an elliptic curve defined over $\boldsymbol{Q}$, the density of the set of primes of good ordinary reduction is 1/2 or 1, depending on whether or not the curve has complex multiplication. We note that if the polynomial $F(X)$ belongs to $\boldsymbol{Q}[X]$, then the set of primes of good ordinary reduction has a natural density less than or equal to $1/(l-1)$. Thus, for any $\varepsilon>0$, we note the existence of non-singular projective curves defined over $\boldsymbol{Q}$ such that the set of primes of good ordinary reduction has density less than ε.

5. Hasse-Witt matrices for the Fermat curves. Let us denote by C_l the Fermat curve over $\boldsymbol{Q}$, defined as the projective closure of the affine curve $Y^l=X^l+1$, where l is an odd prime. Let $\boldsymbol{Q}(\mu_l)$ be the field of the l-th roots of unity. Let us choose a prime $p\neq l$ and let f be its residue degree in $\boldsymbol{Q}(\mu_l)$. Let $G:=(\boldsymbol{Z}/l\boldsymbol{Z})^*$ and let H be the subgroup of G of order f. The curve C_l has good reduction at p and we denote $r_p(C_l)$ its Hasse-Witt invariant. The Hasse-Witt matrix W of the reduced curve C_l over $\bar{\boldsymbol{F}}_p$ has its entries in $\boldsymbol{F}_p$. Hence, $W(m)=W^m$ for $m\geq 1$.

Let us recall that the genus of C_l is $g=(l-2)(l-1)/2$. According to the previous section, we take $\mathscr{S}=\{(i,j)\,|\,2\le i\le l-1,\ 1\le j\le j_i=i-1\}$. Given an integer $m>0$, let

$$q_i(m):=[p^m i/l]\,,\quad F_{i,m}(X):=(X^l+1)^{q_i(m)}\,,\quad q(f):=(p^f-1)/l\,.$$

Then, $q_i(f)=q(f)i$, for $2\le i\le l-1$.

5.1. PROPOSITION. (i) *The matrix* $W(m)=(w_{i,j}^{i',j'}(m))$ *is given by*

$$w_{i,j}^{i',j'}(m)=\begin{cases}\begin{pmatrix} q_i(m) \\ (jp^m-j')/l\end{pmatrix}, & \text{if } i'=\langle p^m i\rangle\,,\ jp^m-j'\ge 0\,,\ jp^m-j'\equiv 0\,(\mathrm{mod}\,l)\,,\\ 0 & \text{otherwise}\,.\end{cases}$$

(ii) *The matrix* $W(f)$ *is diagonal and its eigenvalues are*

$$w_{i,j}^{i,j}(f)=\begin{pmatrix} q(f)i \\ q(f)j\end{pmatrix}.$$

(iii) C_l *is ordinary at* p *if and only if* $f=1$.

(iv) *If* f *is even, then* $r_p(C_l)=0$.

PROOF. Consider $F_{i,m}(X)=\sum_{s=0}^{q_i(m)}\binom{q_i(m)}{s}X^{l(q_i(m)-s)}$. If $l(q_i(m)-s)=jp^m-j'$, then $jp^m\equiv j'\,(\mathrm{mod}\,l)$; hence for each j corresponding to an index i we have a single j'. If, moreover, we have $i'=\langle p^m i\rangle$, $j'<i'$ and $jp^m-j'\ge 0$, then the coefficient of the monomial with exponent jp^m-j' is

$$\begin{pmatrix} q_i(m) \\ s\end{pmatrix}=\begin{pmatrix} q_i(m) \\ q_i(m)-s\end{pmatrix}=\begin{pmatrix} q_i(m) \\ (jp^m-j')/l\end{pmatrix}.$$

If $p^f\equiv 1\,(\mathrm{mod}\,l)$, then $i'=\langle p^f i\rangle=i$ and, for each j corresponding to a given i, we have that $j'=j$. Thus, the matrix of $(F^*)^f$ is diagonal and has eigenvalues

$$\begin{pmatrix} q_i(f) \\ j(p^f-1)/l\end{pmatrix}=\begin{pmatrix} q(f)i \\ q(f)j\end{pmatrix}.$$

If $p\not\equiv 1\,(\mathrm{mod}\,l)$, we have already proved that C_l is non-ordinary at p. If $p\equiv 1\,(\mathrm{mod}\,l)$, then W is diagonal and all its eigenvalues are different from zero mod p, since i runs from 2 to $l-1$. Thus, C_l is ordinary at p.

If f is even, let $m=f/2$. We have $p^m\equiv -1\,(\mathrm{mod}\,l)$, $i'=\langle p^m i\rangle=l-i$. For each j corresponding to a given i, the associated j' is $j'=l-j$, since $j\equiv -j'\,(\mathrm{mod}\,l)$. If $j<i$ then $j'>i'$, therefore we have that $W(m)$ is the zero matrix and $r_p(C_l)=0$. □

5.2. EXAMPLE: THE HASSE-WITT INVARIANT $r_{11}(C_7)$. We will compute $r_{11}(C_7)$ in two different ways. In the first, we will calculate the matrix W; this will allow us to obtain the invariant by means of the characteristic polynomial of W. In the second way, using the fact that $11^3\equiv 1\,(\mathrm{mod}\,7)$, we will compute the number of non-zero eigenvalues of $W(3)$. As we will see, this second method is much shorter; we will develop

TABLE 1.

i	q_i	i'	j	j'	$(jp-j')/l$	$w_{i,j}^{i',j'}$
2	3	1	1	4	—	0
3	4	5	1	4	1	$\binom{4}{1}=4$
			2	1	3	$\binom{4}{3}=4$
4	6	2	1	4	—	0
			2	1	3	$\binom{6}{3}=9$
			3	5	—	0
5	7	6	1	4	1	$\binom{7}{1}=7$
			2	1	3	$\binom{7}{3}=2$
			3	5	4	$\binom{7}{4}=2$
			4	2	6	$\binom{7}{6}=7$
6	9	3	1	4	—	0
			2	1	3	$\binom{9}{3}=7$
			3	5	—	0
			4	2	6	$\binom{9}{6}=7$
			5	6	—	0

it in the remaining proposition of this section.

(a) The indices (i, j) of $\mathscr{S}$ in the lexicographic order are: (2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3), (5, 1), (5, 2), (5, 3), (5, 4), (6, 1), (6, 2), (6, 3), (6,4), (6, 5). Since $7(q_i-s)=j11-j'$, we have $j'\equiv 4j \pmod 7$. Hence, the possibly non-zero entries of W are computed in Table 1.

Thus, $\det(W-T\,\mathrm{Id})=-T^9(T^3+2)^2$ and the Hasse-Witt invariant is 6.

(b) The matrix $W(3)$ is diagonal; its eigenvalues are

$$\lambda_{i,j}=\begin{pmatrix}190i\\190j\end{pmatrix}, \qquad (i,j)\in\mathscr{S}.$$

Thus, $\lambda_{i,j}\not\equiv 0 \pmod{11}$ if and only if $v_{11}((190i)!)=v_{11}((190j)!)+v_{11}((190(i-j))!)$. Since the valuation of $n!$ at a prime p is $v_p(n!)=\sum_{m>0}[n/p^m]$, we get that $v_{11}((190r)!)$ equals

18, 37, 55, 75, 93, 102 for $r=1, 2, 3, 4, 5, 6$, respectively. It is easy to check that the number of non-zero eigenvalues is 6, corresponding to the indices: (3, 1), (3, 2), (5, 1), (5, 4), (6, 2), (6, 4).

Let us denote $\mathscr{S}'=\{(j',j)\in \boldsymbol{N}^*\times \boldsymbol{N}^* \mid j+j'<l\}$. The mapping $(i,j)\mapsto(i-j,j)$ is a bijection of $\mathscr{S}$ onto $\mathscr{S}'$.

5.3. PROPOSITION. (i)

$$r_p(C_l)=\#\left\{(i,j)\in\mathscr{S}\,\middle|\,\left[\frac{p^s i}{l}\right]=\left[\frac{p^s j}{l}\right]+\left[\frac{p^s(i-j)}{l}\right],\ 1\le s\le f-1\right\}.$$

(ii) *$r_p(C_l)$ agrees with the cardinality of the set*

$$\mathscr{M}=\{(j',j)\in\mathscr{S}'\mid(\langle j'h\rangle,\langle jh\rangle)\in\mathscr{S}',\ \textit{for all}\ h\in H\}\,.$$

(iii) *If two primes $p, p'\neq l$ have the same residue degree f in $\boldsymbol{Q}(\mu_l)$, then $r_p(C_l)=r_{p'}(C_l)$.*

(iv) $r_p(C_l)\equiv 0 \pmod f$.

PROOF. From the computation of the eigenvalues of the matrix $W(f)$, we deduce that

$$r_p(C_l)=\#\left\{(i,j)\in\mathscr{S}\,\middle|\,\sum_{k>0}\left[\frac{q(f)i}{p^k}\right]=\sum_{k>0}\left[\frac{q(f)j}{p^k}\right]+\sum_{k>0}\left[\frac{q(f)(i-j)}{p^k}\right]\right\}.$$

We have $[(p^f-1)i/(p^k l)]=0$ if $k>f-1$ and, given two positive real numbers a, b, then $[a+b]\ge[a]+[b]$. Thus,

$$r_p(C_l)=\#\left\{(i,j)\in\mathscr{S}\,\middle|\,\left[\frac{q(f)i}{p^k}\right]=\left[\frac{q(f)j}{p^k}\right]+\left[\frac{q(f)(i-j)}{p^k}\right],\ 1\le k\le f-1\right\}.$$

For $1\le i\le l-1$ and $1\le k\le f-1$, the condition

$$\left[\frac{(p^f-1)i}{lp^k}\right]=\left[\frac{ip^{f-k}}{l}\right],$$

holds. Indeed, we have that

$$\left[\frac{(p^f-1)i}{lp^k}\right]=\left[\left[\frac{ip^{f-k}}{l}\right]+\frac{\langle ip^{f-k}\rangle}{l}-\frac{i}{ip^k}\right]=\left[\left[\frac{ip^{f-k}}{l}\right]+\frac{(\langle ip^{f-k}\rangle p^k-i)}{lp^k}\right].$$

Since $\langle ip^{f-k}\rangle p^k-i\equiv 0 \pmod l$ and $1\le i\le l-1$, one has $\langle ip^{f-k}\rangle p^k-i\ge 0$. Hence,

$$\left[\frac{(p^f-1)i}{lp^k}\right]=\left[\frac{ip^{f-k}}{l}\right]+\left[\frac{(\langle ip^{f-k}\rangle p^k-i)}{lp^k}\right]=\left[\frac{ip^{f-k}}{l}\right]$$

and the first part of the statement is proved.

Let us prove (ii). For each $(i,j)\in\mathscr{S}$ we have that

$$p^s i=\left[\frac{p^s i}{l}\right] l+\langle ip^s\rangle\,,\quad p^s j=\left[\frac{p^s j}{l}\right] l+\langle jp^s\rangle\,,\quad p^s(i-j)=\left[\frac{p^s(i-j)}{l}\right] l+\langle (i-j)p^s\rangle\,.$$

The condition $[p^s j/l]+[p^s(i-j)/l]=[p^s i/l]$ for $1\le s\le f-1$ is equivalent to

$$\langle jp^s\rangle+\langle (i-j)p^s\rangle=\langle ip^s\rangle<l\,,\qquad 1\le s\le f-1\,.$$

Notice that this condition holds for $s=f$, since $p^f\equiv 1 \pmod l$. Due to the fact that the class of p in G is a generator of order f of H, the statement (ii) of the proposition is proved. Since H is the only subgroup of G of order f, (iii) follows immediately. If $(j',j)\in\mathscr{M}$, then $(\langle j'h\rangle,\langle jh\rangle)\in\mathscr{M}$ for each $h\in H$. This shows that $r_p(C_l)$ is multiple of f. □

6. Questions of densities. The natural density of the set of primes p such that C_l has good ordinary reduction at p in the set of all prime integers is $1/(l-1)$. It is known that $J(C_l/\bar{\boldsymbol{F}}_p)$ is isogenous to a power of a supersingular elliptic curve if and only if f is even (cf. [Sh-Ka79 Prop. 3.10]). Thus, if $l-1=2^k m$, with m odd, the natural density of the set of primes p such that $J(C_l/\bar{\boldsymbol{F}}_p)$ is isogenous to a power of a supersingular elliptic curve is

$$\sum_{d|m}\frac{\varphi(2d)}{l-1}+\cdots+\sum_{d|m}\frac{\varphi(2^k d)}{l-1}=\left(\sum_{d|m}\frac{\varphi(d)}{l-1}\right)\left(\sum_{i=1}^{k}\varphi(2^i)\right)=\frac{m}{l-1}(2^k-1)=1-\frac{1}{2^k}\ge\frac{1}{2}\,,$$

where φ denotes the Euler function. Table 2 in the appendix displays a large quantity of primes l for which the set of primes p with good reduction, such that $r_p(C_l)=0$ and $J(C_l/\bar{\boldsymbol{F}}_p)$ is not isogenous to a power of a supersingular elliptic curve, has positive density. At the end of this section we will prove the existence of infinitely many primes l which satisfy this condition.

From now on, K denotes the field $\boldsymbol{Q}$ or $\boldsymbol{F}_p$, $\bar{K}$ is a fixed algebraic closure of K and $\zeta\in\bar{K}$ is a primitive l-th root of unity. For $2\le k\le l-1$, let $C_{l,k}$ be the normalization over $\bar{K}$ of the projective plane curve

$$V^l=U(W+U)^{l-k}W^{k-1}\,.$$

Let $\phi_k: C_l\to C_{l,k}$ be the morphism given by $u=x^l$, $v=xy^{l-k}z^{k-1}$, $w=z^l$. We denote by $\sigma_k: C_l\to C_l$ the automorphism defined by $(x,y,z)\mapsto(x\zeta^k, y\zeta, z)$, which has no fixed points and is of order l. We have that $\phi_k=\phi_k\circ\sigma_k$ and the curve $C_{l,k}$ is isomorphic to the quotient curve of C_l with respect to the action of the group of order l generated by σ_k. Let $\pi_k: C_l\to C_{l,k}$ be the corresponding projection which is not ramified. Note that π_k is defined on any extension of K which contains the l-th roots of unity.

For each of these values of k, we denote by $r_p(C_{l,k})$ the Hasse-Witt invariant of $C_{l,k}$ when $K=\boldsymbol{F}_p$. The Jacobian $J(C_l)$ is $\bar{K}$-isogenous to $\prod_{k=2}^{l-1}J(C_{l,k})$ (cf. [Sc84]). Thus, we obtain that

(i) $r_p(C_l)=\sum_{k=2}^{l-1} r_p(C_{l,k})$.
(ii) $H^1(C_l, \mathcal{O})\simeq \bigoplus_{k=2}^{l-1} H^1(C_{l,k}, \mathcal{O})$.

In particular, we have that $r_p(C_l)=0$ if and only if $r_p(C_{l,k})=0$ for $2\leq k\leq l-1$. We shall prove in the proposition below that, moreover, $H^1(C_l, \mathcal{O})=\bigoplus_{k=2}^{l-1} \pi_k^*(H^1(C_{l,k}, \mathcal{O}))$. We shall make use of this last result to computer $r_p(C_{l,k})$.

Let us consider the set

$$\mathcal{S}_k:=\{(i,j)\in\mathcal{S}\mid \langle i/j\rangle=k\}=\{(\langle mk\rangle, \langle m\rangle)\in\mathcal{S}\mid m\in G\}\ .$$

The condition $\langle mk\rangle>\langle m\rangle$ is equivalent to $\langle m(k-1)\rangle+\langle m\rangle=\langle mk\rangle$. Thus, if we denote by $\mathcal{S}_k'$ the image of $\mathcal{S}_k$ in $\mathcal{S}'$ by the mapping $(i,j)\mapsto(i-j,j)$, we have

$$\mathcal{S}_k'=\left\{(j',j)\in\mathcal{S}'\,\middle|\,\left\langle\frac{j'}{j}\right\rangle=k-1\right\}=\{(\langle m(k-1)\rangle, \langle m\rangle)\in\mathcal{S}'\mid m\in G\}\ .$$

The group G acts on $[1, l-1]\times[1, l-1]$ by $m(i,j):=(\langle mi\rangle, \langle mj\rangle)$. Thus, $\mathcal{S}_k=\{m(k, 1)\in\mathcal{S}\mid m\in G\}$, $\mathcal{S}_k'=\{m(k-1, 1)\in\mathcal{S}'\mid m\in G\}$. Notice that $\mathcal{S}$ (resp. $\mathcal{S}'$) is the disjoint union of the sets $\mathcal{S}_k$ (resp. $\mathcal{S}_k'$), since these sets are the equivalence classes defined by the relation $(i,j)\sim(i,j')$ if and only if there exists an $m\in G$ such that $(i,j)=m(i',j')$.

6.1. PROPOSITION. (i) *The set* $\{r_{i,j}\}_{(i,j)\in\mathcal{S}_k}$ *is a basis of the* $\bar{K}$*-vector space* $\pi_k^*(H^1(C_{l,k}, \mathcal{O}))$. *In particular,* $H^1(C_l, \mathcal{O})=\bigoplus_{k=2}^{l-1}\pi_k^*(H^1(C_{l,k}, \mathcal{O}))$.
(ii) $r_p(C_{l,k})=\#\{(j',j)\in\mathcal{S}_k'\mid h(j',j)\in\mathcal{S}_k', \text{ for all } h\in H\}$.
(iii) *If two prime* $p, p'\neq l$ *have the same residue degree* f *in* $\boldsymbol{Q}(\mu_l)$, *then* $r_p(C_{l,k})=r_{p'}(C_{l,k})$.
(iv) $r_p(C_{l,k})\equiv 0 \pmod f$.

PROOF. Let us consider (i). The set $\mathcal{S}_k$ has $(l-1)/2$ elements, since $(\langle mk\rangle, \langle m\rangle)\in\mathcal{S}_k$ if and only if $(\langle -mk\rangle, \langle -m\rangle)\notin\mathcal{S}_k$. By the Hurwitz formula, we get that the genus of $C_{l,k}$ is $(l-1)/2$. The functions $Y^{\langle mk\rangle}/X^{\langle m\rangle}$ are invariant under σ_k. Thus, they are functions on $C_{l,k}$. We have that $\pi_k(P_\infty^1)=\cdots=\pi_k(P_\infty^l)$. Thus, the repartitions $\{r_{\langle mk\rangle,\langle m\rangle}\}$, for $(\langle mk\rangle, \langle m\rangle)\in\mathcal{S}_k$, belong to $\pi_k^*(H^1(C_{l,k}, \mathcal{O}))$. Since they are linearly independent and $\dim \pi_k^*(H^1(C_{l,k}, \mathcal{O}))\leq(l-1)/2$, the statement is proved.

If $K=\boldsymbol{F}_p$, the subspace $\pi_k^*(H^1(C_{l,k}, \mathcal{O}))$ of $H^1(C_l, \mathcal{O})$ is invariant under the absolute Frobenius $F_{C_l}^*$, because $\pi_k^*\circ F_{C_{l,k}}^*=F_{C_l}^*\circ\pi_k^*$, and the rest of proposition can be proved along the same line of reasoning as that used in Proposition 5.3. □

The proposition above makes it clear that the properties (iii) and (iv) stated in Proposition 5.3 are consequences of their being satisfied on each of the subvarieties $J(C_{l,k})$ over $\bar{\boldsymbol{F}}_p$.

Next we will show the existence of isomorphy relations among some of these jacobian subvarieties. Let $T, S: \mathcal{S}\to\mathcal{S}$ be the maps defined by

$$T(i,j)=(l-j, l-i)\ ,\quad S(i,j)=(i, i-j)\ .$$

S and T are bijective maps. Given $m \in G$ and $(i,j) \in \mathscr{S}$ we have that $m(i,j) \in \mathscr{S}$ if and only if $mT(i,j) \in \mathscr{S}$, and if and only if $mS(i,j) \in \mathscr{S}$. Hence, S and T map equivalence classes into equivalence classes. Thus $T(\mathscr{S}_k) = \mathscr{S}_{\langle 1/k \rangle}$ and $S(\mathscr{S}_k) = \mathscr{S}_{\langle k/(k-1) \rangle}$, since $T(k,1) = (l-1, l-k)$ and $S(k,1) = (k, k-1)$. If we put $T(k) = \langle 1/k \rangle$ and $S(k) = \langle k/(k-1) \rangle$, the two mappings are involutions on the indices of the curves, and $(S \circ T)^3(k) = k$. Namely, S and T acting on the set of indices k generate the dihedral group D_3 and $(S \circ T \circ S)(k) = \langle 1-k \rangle$.

6.2. PROPOSITION. *Given $M \in D_3$, the curves $C_{l,k}$ and $C_{l,M(k)}$ are $\bar{\mathbf{Q}}$-isomorphic, hence they have the same Hasse-Witt invariant at any prime $p \neq l$.*

PROOF. Let us introduce the involutions $\lambda, \mu : C_l \to C_l$ defined by

$$\lambda(x, y, z) := (y, x, -z), \quad \mu(x, y, z) := (z, y, x).$$

We have that $\sigma_{\langle 1/k \rangle}^k \circ \lambda = \lambda \circ \sigma_k$, $\sigma_{\langle k/(k-1) \rangle}^{1-k} \circ \mu = \mu \circ \sigma_k$. It follows that λ (resp. μ) induces an isomorphism between $C_{l,\langle 1/k \rangle}$ and $C_{l,k}$ (resp. $C_{l,\langle k/(k-1) \rangle}$ and $C_{l,k}$). □

In general, each set of subindices S_k has an orbit, under the action of the group D_3, formed by six sets:

$$\mathscr{S}_k, \ \mathscr{S}_{\langle -1/(k-1) \rangle}, \ \mathscr{S}_{\langle (k-1)/k \rangle}, \ \mathscr{S}_{\langle k/(k-1) \rangle}, \ \mathscr{S}_{\langle 1-k \rangle}, \ \mathscr{S}_{\langle 1/k \rangle}.$$

These sets are different, except in the following cases:

(a) For $l = 3$, k can only take the value 2, and the six sets are the same.

(b) The orbit of $\mathscr{S}_k$ has three elements if and only if $k \in \{2, (l+1)/2, l-1\}$ and $l \neq 3$.

(c) The orbit of $\mathscr{S}_k$ has two elements if and only if $l \equiv 1 \pmod 3$ and k is a solution of $T^2 - T + 1 \equiv 0 \pmod l$.

Notice that if p is a prime of residue degree $f = 3$, then $r_p(C_l) \geq 6$, since the subgroup $\{p, p^2, 1\}$ of $(\mathbf{Z}/l\mathbf{Z})^*$ always satisfies $\langle p \rangle + \langle p^2 \rangle + 1 = l$ and the six pairs $(\langle p^{j'} \rangle, \langle p^j \rangle)$ for $j', j = 1, 2, 3$ and $j \neq j'$, belong to $\mathscr{S}'$.

6.3. PROPOSITION. *Let $l \neq 3, 7$. If $p \neq l$ is a prime of residue degree $f = (l-1)/2$, then $r_p(C_l) = 0$.*

PROOF. The elements of the subgroup H of $(\mathbf{Z}/l\mathbf{Z})^*$ generated by a prime p of residue degree $f = (l-1)/2$ are the quadratic residues mod l. Since $r_p(C_{l,k}) \equiv 0 \pmod f$ and $C_{l,k}$ has genus f, we have that $C_{l,k}$ is ordinary at p or $r_p(C_{l,k}) = 0$. Thus, we only need to prove that $C_{l,k}$ is non-ordinary at p for all k, $2 \leq k \leq l-1$.

We consider the following cases:

(a) $l \neq 3$ and -2 is a quadratic residue (mod l). Let k be the index corresponding to an ordinary curve. Since $l-2$ is a quadratic residue, the inequality

$$\langle (l-2)(k-1) \rangle + l - 2 < l$$

holds. This condition forces $-2(k-1) \equiv 1 \pmod l$; hence $k = (l+1)/2$. This is a con-

tradiction because this curve is isomorphic to the curves corresponding to $k=2$, $l-1$.

(b) $l\neq 7$ and -3 is a quadratic residue (mod l). Let k be the index corresponding to an ordinary curve. Since $l-3$ is a quadratic residue, we have $\langle (l-3)(k-1)\rangle + l - 3 < l$. Thus $k \equiv 1/3 \pmod{l}$ or $k \equiv 2/3 \pmod{l}$. The curve $C_{l,k}$ has the same invariant as the curve corresponding to $k/(k-1)$, and we have $k \equiv -1/2 \pmod{l}$ or $k \equiv -2 \pmod{l}$; these values are different from the previous ones if $l \neq 5, 7$. The case $l=5$ does not have to be considered, since -3 is not a quadratic residue (mod 5).

(c) -1 is a quadratic residue (mod l). The result is obvious, since f is even.

(d) -2, -3 and -1 are not quadratic residues (mod l). These conditions imply that 2 and 3 are quadratic residues. Let $t=k-1$ be a value such that the curve corresponding to $k=t+1$ is ordinary. We show that t is a quadratic residue. Let m be the minimum non-quadratic positive residue; then $l-m$ is a quadratic residue and $\langle -mt\rangle + \langle -m\rangle < l$. Thus $\langle -mt\rangle < m$ and consequently $-mt$ and t are quadratic residues.

Since 1/2 is a quadratic residue, for $k=2$ the curve is non-ordinary, because $((l+1)/2)(1, 1)$ does not belong to $\mathscr{S}'$. Due to the fact that -3 and -1 are not quadratic residues, we have that $l \not\equiv 1 \pmod{3}$. Thus, each subindex k of an ordinary curve yields six different subindices of ordinary curves, since we have excluded the cases $l=3$, $k \in \{2, (l+1)/2, l-1\}$ and $l \equiv 1 \pmod{3}$. For each value of t, the values obtained are the following t, $\langle -(t+1)/t\rangle$, $\langle -1/(1+t)\rangle$, $\langle 1/t\rangle$, $\langle -(t+1)\rangle$, $\langle -t/(t+1)\rangle$. Let α be the minimum value of t such that the curve is ordinary. Since $-(\alpha+1)/\alpha$ is a quadratic residue, we have

$$\left\langle -\frac{\alpha+1}{\alpha}\alpha\right\rangle + \left\langle -\frac{\alpha+1}{\alpha}\right\rangle < l\,.$$

Thus, $l-(\alpha+1)+\langle -(\alpha+1)/\alpha\rangle < l$, that is, $\langle -(\alpha+1)/\alpha\rangle < \alpha+1$. This result contradicts either the fact that α is the minimum ordinary value or that $\langle -(\alpha+1)/\alpha\rangle \neq \alpha$. □

6.4. COROLLARY. *If $l \geq 11$ and $l \equiv 3 \pmod{4}$ then the density of the set of primes p such that $r_p(C_l)=0$ and $J(C_l/\bar{F}_p)$ is not isogenous to a power of a supersingular elliptic curve is greater than or equal to* $(l-1)^{-1}\varphi((l-1)/2)$.

7. Appendix.

7.1. NOTATION.

l, $2<l<500$, prime,

δ, density of the set of primes p such that $r_p(C_l)=0$ and $J(C_l/\bar{F}_p)$ is not isogenous to a power of a supersingular elliptic curve.

TABLE 2.

l	δ	l	δ	l	δ	l	δ	l	δ
3	0	73	0	173	21/86	277	11/46	397	5/22
5	0	79	6/13	179	44/89	281	3/35	401	1/20
7	0	83	20/41	181	8/45	283	23/47	409	2/17
11	2/5	89	0	191	9/19	293	18/73	419	104/209
13	0	97	0	193	0	307	8/17	421	23/105
17	0	101	6/25	197	3/14	311	15/31	431	21/43
19	1/3	103	8/17	199	5/11	313	3/26	433	1/24
23	5/11	107	26/53	211	2/5	317	39/158	439	36/73
29	3/14	109	1/6	223	18/37	331	79/165	443	110/221
31	4/15	113	3/56	227	56/113	337	0	449	0
37	1/6	127	8/21	229	9/38	347	86/173	457	9/76
41	1/10	131	6/13	233	7/58	349	7/29	461	11/46
43	3/7	137	2/17	239	8/17	353	5/176	463	106/231
47	11/23	139	11/23	241	1/30	359	89/179	467	116/233
53	3/13	149	9/37	251	12/25	367	30/61	479	119/239
59	14/29	151	2/5	257	0	373	15/62	487	13/27
61	1/5	157	3/13	263	65/131	379	29/63	491	117/245
67	5/11	163	4/9	269	33/134	383	95/191	499	41/83
71	12/35	167	41/83	271	61/135	389	24/97		

BIBLIOGRAPHY

[Ba58] I. BARSOTTI, Repartitions on abelian varieties, Illinois J. Math. 2 (1958), 43–70.

[Ha34] H. HASSE, Existenz separabler zyklischer unverzweigter Erweiterungskörpern vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p, J. Reine Angew Math. 172 (1934), 77–85.

[Ha-Wi36] H. HASSE AND E. WITT, Zyklische unverzweigte Erweiterungskörpern vom Primzahlgrade p über einem algebraischen Funktionenkörpern der Charakteristik p, Monats. Math. Phys. 43 (1936), 477–492.

[Ko75] N. KOBLITZ, p-adic variation of the zeta function over families of varieties defined over finite fields, Compositio Math. 31 (1975), 119–218.

[Ma62] YU. I. MANIN, On the theory of abelian varieties over fields of finite characteristic, Izv. Akad. Nauk. SSSR Ser. Mat. 26 (1962), 281–292.

[Ma63] YU. I. MANIN, The theory of commutative formal groups over fields of finite characteristic, Russian Math. Surveys 18 (1963), 3–90.

[Mu70] D. MUMFORD, Abelian Varieties, Oxford Univ. Press, 1970.

[Se58] J-P. SERRE, Sur la topologie des variétés algébriques en caractéristique p, Symp. Int. Top. Alg., México (1958), 24–53. In J. P. Serre, ŒUVRES, vol. I, Springer, 1986.

[Sc84] C.-G. SCHMIDT, Arithmetik Abelscher Varietäten mit komplexer Multiplikation, Lecture Notes in Math. 1082, Springer, 1984.

[Sh-Ka79] T. SHIODA AND T. KATSURA, On Fermat Varieties, Tôhoku Math. J. 31 (1979), 97–115.

[To88] K. TOKI, On Hasse-Witt matrices of Fermat varieties, Hiroshima Math. J. 18 (1988), 95–111.

[Yu80] N. YUI, On the Jacobian variety of the Fermat curve, J. Algebra 65 (1980), 1–45.

[Yu86] N. YUI, On certain arithmetical invariants of Fermat varieties, J. Algebra 101 (1986), 127–135.

ESCOLA UNIVERSITÀRIA POLITÈCNICA DE VILANOVA I LA GELTRÚ
AV. VICTOR BALAGUER S/N
E-08800 VILANOVA I LA GELTRÚ
SPAIN

E-mail address: josepg@mat.upc.es