MATHEMATICS OF COMPUTATION
Volume 79, Number 271, July 2010, Pages 1833–1838
S 0025-5718(10)02305-7
Article electronically published on January 14, 2010

p^k-TORSION OF GENUS TWO CURVES OVER $\mathbb{F}_{p^m}$

MICHAEL E. ZIEVE

Abstract. We determine the isogeny classes of abelian surfaces over $\mathbb{F}_q$ whose group of $\mathbb{F}_q$-rational points has order divisible by q^2. We also solve the same problem for Jacobians of genus-2 curves.

In a recent paper [4], Ravnshøj proved: if C is a genus-2 curve over a prime field $\mathbb{F}_p$, and if one assumes that the endomorphism ring of the Jacobian J of C is the ring of integers in a primitive quartic CM-field, and that the Frobenius endomorphism of J has a certain special form, then $p^2 \nmid \#J(\mathbb{F}_p)$. Our purpose here is to deduce this conclusion under less restrictive hypotheses. We write $q = p^m$, where p is prime, and for any abelian variety J over $\mathbb{F}_q$ we let P_J denote the *Weil polynomial* of J, namely the characteristic polynomial of the Frobenius endomorphism π_J of J. As shown by Tate [6, Thm. 1], two abelian varieties over $\mathbb{F}_q$ are isogenous if and only if their Weil polynomials are identical. Thus, the following result describes the isogeny classes of abelian surfaces J over $\mathbb{F}_q$ for which $q^2 \mid \#J(\mathbb{F}_q)$.

Theorem 1. *The Weil polynomials of abelian surfaces J over $\mathbb{F}_q$ satisfying $q^2 \mid \#J(\mathbb{F}_q)$ are as follows*:

(1.1) $X^4 + X^3 - (q+2)X^2 + qX + q^2$ *(if q is odd and $q > 8$);*
(1.2) $X^4 - X^2 + q^2$*;*
(1.3) $X^4 - X^3 + qX^2 - qX + q^2$ *(if m is odd or $p \not\equiv 1 \bmod 4$);*
(1.4) $X^4 - 2X^3 + (2q+1)X^2 - 2qX + q^2$*;*
(1.5) $X^4 + aX^3 + bX^2 + aqX + q^2$, *where (a, b) occurs in the same row as q in the following table:*

q	(a,b)
13	$(9,42)$
9	$(6,20)$
7	$(4,16)$
5	$(3,6)$ or $(8,26)$
4	$(2,5)$, $(4,11)$, or $(6,17)$
3	$(1,4)$, $(3,5)$, or $(4,10)$
2	$(0,3)$, $(1,0)$, $(1,4)$, $(2,5)$, or $(3,6)$

The special form required of the Frobenius endomorphism in [4] has an immediate consequence for the shape of its characteristic polynomial, and by inspection the above polynomials do not have the required shape. Thus the main result of [4] follows from the above result.

Received by the editor May 29, 2007 and, in revised form, August 30, 2008.
2010 *Mathematics Subject Classification.* Primary 14H40.

Our proof of Theorem 1 relies on the classical results of Tate ([6, Thm. 1] and [8, Thm. 8]) and Honda [2] describing the Weil polynomials of abelian varieties over finite fields. An explicit version of their results in the case of simple abelian surfaces was given by Rück [5, Thm. 1.1]; together with the analogous results of Waterhouse [7, Thm. 4.1] for elliptic curves, this yields the following:

Lemma 2. *The Weil polynomials of abelian surfaces over* $\mathbb{F}_q$ *are precisely the polynomials* $X^4 + aX^3 + bX^2 + aqX + q^2$*, where* $a, b \in \mathbb{Z}$ *satisfy* $|a| \le 4\sqrt{q}$ *and* $2|a|\sqrt{q} - 2q \le b \le \frac{a^2}{4} + 2q$*, and where* a*,* b*, and the values* $\Delta := a^2 - 4(b - 2q)$ *and* $\delta := (b + 2q)^2 - 4qa^2$ *satisfy one of the conditions* (2.1)–(2.4) *below:*

(2.1) $v_p(b) = 0$*;*

(2.2) $v_p(b) \ge m/2$ *and* $v_p(a) = 0$*, and either* $\delta = 0$ *or* δ *is a non-square in the ring* $\mathbb{Z}_p$ *of* p*-adic integers;*

(2.3) $v_p(b) \ge m$ *and* $v_p(a) \ge m/2$ *and* Δ *is a square in* $\mathbb{Z}$*, and if* q *is a square and we write* $a = \sqrt{q}a'$ *and* $b = qb'$ *then*

$$p \not\equiv 1 \bmod 4 \quad \text{if } b' = 2,$$
$$p \not\equiv 1 \bmod 3 \quad \text{if } a' \not\equiv b' \bmod 2;$$

(2.4) *the conditions in one of the rows of the following table are satisfied:*

(a, b)	Conditions on p and q
$(0, 0)$	q is a square and $p \not\equiv 1 \bmod 8$, or q is a non-square and $p \ne 2$
$(0, -q)$	q is a square and $p \not\equiv 1 \bmod 12$, or q is a non-square and $p \ne 3$
$(0, q)$	q is a non-square
$(0, -2q)$	q is a non-square
$(0, 2q)$	q is a square and $p \equiv 1 \bmod 4$
$(\pm\sqrt{q}, q)$	q is a square and $p \not\equiv 1 \bmod 5$
$(\pm\sqrt{2q}, q)$	q is a non-square and $p = 2$
$(\pm 2\sqrt{q}, 3q)$	q is a square and $p \equiv 1 \bmod 3$
$(\pm\sqrt{5q}, 3q)$	q is a non-square and $p = 5$

Moreover, the surface J *is simple if and only if either*

- Δ *is a non-square in* $\mathbb{Z}$*; or*
- $(a, b) = (0, 2q)$ *and* q *is a square and* $p \equiv 1 \bmod 4$*; or*
- $(a, b) = (\pm 2\sqrt{q}, 3q)$ *and* q *is a square and* $p \equiv 1 \bmod 3$.

The p*-rank of* J *(namely, the rank of the* p*-torsion subgroup of* $J(\overline{\mathbb{F}}_q)$*) is* 2 *in* (2.1)*,* 1 *in* (2.2)*, and* 0 *in* (2.3) *and* (2.4).

Proof of Theorem 1. As shown by Weil [9], for any abelian surface J over $\mathbb{F}_q$, the Weil polynomial P_J is a monic quartic in $\mathbb{Z}[X]$ whose complex roots have absolute value $\sqrt{q}$. In particular, $\#J(\mathbb{F}_q) = \deg(\pi_J - 1) = P_J(1) \le (\sqrt{q}+1)^4$, so if $\#J(\mathbb{F}_q) = cq^2$ with $c \in \mathbb{Z}$ then $c \le (1 + q^{-1/2})^4$. It follows that $c = 1$ unless $q \le 27$. In light of the above lemma, there are just finitely many cases to consider with $c > 1$; we treated these cases using the computer program presented at the end of this paper, which gave rise to precisely the solutions in (1.5). Henceforth assume $c = 1$.

The Weil polynomials of abelian surfaces over $\mathbb{F}_q$ are the polynomials $P(X) := X^4 + aX^3 + bX^2 + aqX + q^2$ occurring in the above lemma. We must determine which of these polynomials satisfy $P(1) = q^2$, or equivalently, $b = -1 - a(q+1)$. The inequality $-1 - a(q+1) = b \le a^2/4 + 2q$ says that $q^2 \le (a/2 + q + 1)^2$, and since $a/2 + q + 1 \ge -2\sqrt{q} + q + 1 > 0$, this is equivalent to $q \le a/2 + q + 1$, or in other words $-2 \le a$. The inequality $2|a|\sqrt{q} - 2q \le b = -1 - a(q+1)$ always holds if $a \in \{0, -1, -2\}$, and if $a \ge 1$ it is equivalent to $a(\sqrt{q}+1)^2 \le 2q - 1$; since $2q - 1 < 2q < 2(\sqrt{q}+1)^2$, this implies $a = 1$, in which case $(\sqrt{q}+1)^2 \le 2q - 1$ is equivalent to $q \ge 8$.

Condition (2.1) holds if and only if $a \not\equiv -1 \bmod p$, or equivalently either $a \in \{0, -2\}$ or both $a = 1$ and $p \ne 2$. This accounts for (1.1), (1.2), and (1.4).

Condition (2.3) cannot hold, since $p \mid a$ implies $b \equiv -1 \bmod p$.

The condition $v_p(b) \ge m/2$ says that $a \equiv -1 \bmod p^{\lceil m/2 \rceil}$, or equivalently $a = -1$. In this case, $b = q$ and $\delta = 9q^2 - 4q$, so $\delta \ne 0$. If q is odd, then δ is a square in $\mathbb{Z}_p$ if and only if δ is a square modulo pq, or equivalently, m is even and -4 is a square modulo p, which means that $p \equiv 1 \bmod 4$. If q is even, then δ is not a square in $\mathbb{Z}_2$, since for $q \le 8$ we have $\delta \in \{28, 128, 544\}$, and for $q > 8$ we have $\delta \equiv -4q \bmod 16q$. Thus (2.2) gives rise to (1.3).

Finally, if $a = -2$ then $b = 2q + 1$, and if $a = 0$ then $b = -1$, so in either case $q \nmid b$. Thus (2.4) cannot hold, and the proof is complete. $\square$

Next we determine which of the Weil polynomials in (1.1)–(1.5) occur for Jacobians. We use the classification of Weil polynomials of Jacobians of genus-2 curves. This classification was achieved by the combined efforts of many mathematicians, culminating in the following result [3, Thm. 1.2]:

Lemma 3. *Let $P_J = X^4 + aX^3 + bX^2 + aqX + q^2$ be the Weil polynomial of an abelian surface J over $\mathbb{F}_q$.*

(1) *If J is simple, then J is not isogenous to a Jacobian if and only if the conditions in one of the rows of the following table are met:*

Condition on p and q	Conditions on a and b
—	$a^2 - b = q$ and $b < 0$ and all prime divisors of b are 1 mod 3
—	$a = 0$ and $b = 1 - 2q$
$p > 2$	$a = 0$ and $b = 2 - 2q$
$p \equiv 11 \bmod 12$ and q square	$a = 0$ and $b = -q$
$p = 3$ and q square	$a = 0$ and $b = -q$
$p = 2$ and q non-square	$a = 0$ and $b = -q$
$q = 2$ or $q = 3$	$a = 0$ and $b = -2q$

(2) *If J is not simple, then there are integers s, t such that $P_J = (X^2 - sX + q)(X^2 - tX + q)$, and s and t are unique if we require that $|s| \ge |t|$ and that if $s = -t$ then $s \ge 0$. For such s and t, J is not isogenous to a Jacobian if and only if the conditions in one of the rows of the following table are met:*

p-rank of J	Condition on p and q	Conditions on s and t
—	—	$\lvert s-t\rvert = 1$
2	—	$s = t$ and $t^2 - 4q \in \{-3, -4, -7\}$
	$q = 2$	$s = 1$ and $t = -1$
1	q square	$s^2 = 4q$ and $s - t$ squarefree
0	$p > 3$	$s^2 \neq t^2$
	$p = 3$ and q non-square	$s^2 = t^2 = 3q$
	$p = 3$ and q square	$s - t$ is not divisible by $3\sqrt{q}$
	$p = 2$	$s^2 - t^2$ is not divisible by $2q$
	$q = 2$ or $q = 3$	$s = t$
	$q = 4$ or $q = 9$	$s^2 = t^2 = 4q$

Theorem 4. *The polynomials in* (1.1)–(1.5) *which are not Weil polynomials of Jacobians are precisely the polynomials* $X^4 + aX^3 + bX^2 + aqX + q^2$*, where* q *and* (a, b) *satisfy the conditions in one of the rows of the following table:*

q	(a, b)
5	$(8, 26)$
4	$(6, 17)$
2	$(-2, 5)$, $(0, 3)$, $(1, 4)$, $(2, 5)$, or $(3, 6)$

Proof. Let J be an abelian surface over $\mathbb{F}_q$ whose Weil polynomial $P_J = X^4 + aX^3 + bX^2 + aqX + q^2$ satisfies one of (1.1)–(1.5). In each case, $a^2 - b \neq q$, and if $a = 0$ then $b \in \{-1, 3\}$, so if J is simple then Lemma 3 implies J is isogenous to a Jacobian.

Henceforth assume J is not simple, so $P_J = (X^2 - sX + q)(X^2 - tX + q)$ where $s, t \in \mathbb{Z}$; we may assume that $|s| \geq |t|$, and that $s \geq 0$ if $s = -t$. Note that $a = -s - t$ and $b = 2q + st$, so $(X - s)(X - t) = X^2 + aX + b - 2q$. In particular, $\Delta := a^2 - 4(b - 2q)$ is a square, say $\Delta = z^2$ with $z \geq 0$.

Suppose P_J satisfies (1.1), so $\Delta = 12q + 9$. Then $(z - 3)(z + 3) = 12q$ is even, so $z - 3$ and $z + 3$ are even and incongruent mod 4, whence their product is divisible by 8, so q is even, a contradiction.

Now suppose P_J satisfies (1.2), so $\Delta = 8q + 4$. Then $(z - 2)(z + 2) = 8q$, so at least one of $z - 2$ and $z + 2$ is divisible by 4; but these numbers differ by 4, so they are both divisible by 4, whence their product is divisible by 16, so q is even. Thus $8q$ is a power of 2 which is the product of two positive integers that differ by 4, so $q = 4$. In this case, $(q, a, b, s, t) = (4, 0, -1, 3, -3)$, which indeed satisfies (1.2). Moreover, (2.1) holds, so Lemma 2 implies J has p-rank 2. Since $|s-t| = 6 \notin \{0, 1\}$ and $q \neq 2$, Lemma 3 implies J is isogenous to a Jacobian.

Now suppose P_J satisfies (1.3), so $\Delta = 4q+1$. Then $(z-1)(z+1) = 4q$, so $z-1$ and $z + 1$ are even and incongruent mod 4, whence their product is divisible by 8, so q is even. Thus $4q$ is a power of 2 which is the product of two positive integers that differ by 2, so $q = 2$. In this case, $(q, a, b, s, t) = (2, -1, 2, 2, -1)$, which indeed satisfies (1.3). Moreover, (2.2) holds, so Lemma 2 implies J has p-rank 1. Since $|s-t| = 3 \neq 1$ and q is a non-square, Lemma 3 implies J is isogenous to a Jacobian.

Now suppose P_J satisfies (1.4), so $\Delta = 0$ and $a \notin \{0, \pm 2\sqrt{q}\}$, and thus Lemma 3 implies J is non-simple. Here $(a, b, s, t) = (-2, 2q + 1, 1, 1)$, so Lemma 2 implies J has p-rank 2. Since $s = t = 1$, Lemma 3 implies J is isogenous to a Jacobian if and only if $1-4q \notin \{-3,-4,-7\}$, or equivalently $q \neq 2$. This gives rise to the first entry in the last line of the table.

Finally, if P_J satisfies (1.5), then the result follows from Lemma 3 and Lemma 2 via a straightforward computation. $\square$

Remark 5. The result announced in the abstract of [4] is false, since its hypotheses are satisfied by every two-dimensional Jacobian over $\mathbb{F}_p$. This is because the abstract of [4] does not mention the various hypotheses assumed in the theorems of that paper.

We used the following Magma [1] program in the proof of Theorem 1.

```
for q in [2..27] do if IsPrimePower(q) then
Q:=Floor(4*Sqrt(q)); M:=Floor((Sqrt(q)+1)^4/q^2);
for c in [2..M] do
for a in [-Q..Q] do b:=-1-a*(q+1)+(c-1)*q^2;
if b le (a^2/4)+2*q and 2*Abs(a)*Sqrt(q)-2*q le b then
p:=Factorization(q)[1,1]; m:=Factorization(q)[1,2];
Delta:=a^2-4*(b-2*q); delta:=(b+2*q)^2-4*q*a^2;
  if GCD(b,p) eq 1 then <q,a,b,c>;
  elif GCD(b,q) ge Sqrt(q) and GCD(a,p) eq 1 and
    (delta eq 0 or not IsSquare(pAdicRing(p)!delta)) then
    <q,a,b,c>;
  elif IsDivisibleBy(b,q) and GCD(a,q) ge Sqrt(q) and
    IsSquare(Delta) then
    if not IsSquare(q) then <q,a,b,c>;
    else sq:=p^((m div 2)); ap:=a div sq; bp:=b div q;
      if not ((bp eq 2 and IsDivisibleBy(p-1,4)) or
        (IsDivisibleBy(ap-bp,2) and IsDivisibleBy(p-1,3)))
        then <q,a,b,c>;
      end if;
    end if;
  elif (a eq 0 and b eq 0) then
    if ((IsSquare(q) and not IsDivisibleBy(p-1,8)) or
      (not IsSquare(q) and p ne 2)) then <q,a,b,c>;
    end if;
  elif (a eq 0 and b eq -q) then
    if ((IsSquare(q) and not IsDivisibleBy(p-1,12)) or
      (not IsSquare(q) and p ne 3)) then <q,a,b,c>;
    end if;
  elif a eq 0 and b in {q,-2*q} and not IsSquare(q) then
    <q,a,b,c>;
  elif a eq 0 and b eq 2*q and IsSquare(q) and
    IsDivisibleBy(p-1,4) then <q,a,b,c>;
  elif Abs(a) eq p^(m div 2) and b eq q and IsSquare(q) and
    not IsDivisibleBy(p-1,5) then <q,a,b,c>;
  elif Abs(a) eq p^((m+1) div 2) and b eq q and
    not IsSquare(q) and p eq 2 then <q,a,b,c>;
  elif Abs(a) eq 2*p^(m div 2) and b eq 3*q and IsSquare(q)
    and IsDivisibleBy(p-1,3) then <q,a,b,c>;
```

```
  elif Abs(a) eq p^((m+1) div 2) and b eq 3*q and
    not IsSquare(q) and p eq 5 then <q,a,b,c>;
  end if;
end if;
end for;
end for;
end if;
end for;
```

References

1. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265. MR1484478
2. T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95. MR0229642 (37:5216)
3. E. W. Howe, E. Nart and C. Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Ann. Inst. Fourier (Grenoble), **59** (2009), 239–289, arXiv:math/0607515v3 [math.NT]. MR2514865 (2010b:11064)
4. C. R. Ravnshøj, *p-torsion of genus two curves over prime fields of characteristic p*, arXiv:0705.3537v1 [math.AG], 24 May 2007.
5. H.-G. Rück, *Abelian surfaces and Jacobian varieties over finite fields*, Compositio Math. **76** (1990), 351–366. MR1080007 (92e:14016)
6. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR0206004 (34:5829)
7. W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR0265369 (42:279)
8. W. C. Waterhouse and J. S. Milne, *Abelian varieties over finite fields*, pp. 53–64 in: 1969 Number Theory Institute AMS, Providence, 1971. MR0314847 (47:3397)
9. A. Weil, Variétés Abéliennes et Courbes Algébriques, Hermann, Paris, 1948. MR0029522 (10:621d)

Department of Mathematics, Hill Center–Busch Campus, Rutgers, The State University of New Jersey, 110 Frelinghuysen Road, Piscataway, New Jersey 08854–8019

Current address: Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109-1043

E-mail address: zieve@umich.edu

URL: www.math.lsa.umich.edu/~zieve/