ON A THEOREM OF MESTRE AND SCHOOF

JOHN E. CREMONA AND ANDREW V. SUTHERLAND

Abstract. A well known theorem of Mestre and Schoof implies that the order of an elliptic curve E over a prime field $\mathbb{F}_q$ can be uniquely determined by computing the orders of points on E and its quadratic twist, provided that $q > 229$. We extend this result to all finite fields with $q > 49$, and all prime fields with $q > 29$.

Let E be an elliptic curve over the finite field $\mathbb{F}_q$ with q elements. The number of points on $E/\mathbb{F}_q$, which we simply denote $\#E$, is known to lie in the Hasse interval:

$$\mathcal{H}_q = [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]. \tag{1}$$

Equivalently, the trace of Frobenius $t = q + 1 - \#E$ satisfies $|t| \le 2\sqrt{q}$. A common strategy to compute $\#E$ (when q is not too large[1]) relies on the fact that the points on $E/\mathbb{F}_q$ form an abelian group $E(\mathbb{F}_q)$ of order $\#E$. For any $P \in E(\mathbb{F}_q)$, the integer $\#E$ is a multiple of the order of P, and the multiples of $|P|$ lying in $\mathcal{H}_q$ can be efficiently determined using a baby-steps giant-steps search. If there is only one multiple in the interval, it must be $\#E$; if not, we may try other $P \in E(\mathbb{F}_q)$ in the hope of uniquely determining $\#E$. This strategy will eventually succeed if and only if the group exponent

$$\lambda(E) = \operatorname{lcm}\{|P| : P \in E(\mathbb{F}_q)\}$$

has a unique multiple in $\mathcal{H}_q$. When this condition holds we expect to determine $\#E$ quite quickly: with just two random points in $E(\mathbb{F}_q)$ we already succeed with probability greater than $6/\pi^2$ [2, Theorem 8.1].

Unfortunately, $\lambda(E)$ need not have a unique multiple in $\mathcal{H}_q$. However, for prime q we have the following theorem of Mestre, as extended by Schoof [1, Theorem 3.2].[2]

Theorem 1 (Mestre-Schoof)**.** *Let $q > 229$ be prime and E an elliptic curve over $\mathbb{F}_q$ with quadratic twist E'. Either $\lambda(E)$ or $\lambda(E')$ has a unique multiple in $\mathcal{H}_q$.*

The quadratic twist E' is an elliptic curve defined over $\mathbb{F}_q$ that is isomorphic to E over the quadratic extension $\mathbb{F}_{q^2}$, and is easily derived from E. The orders of the groups $E(\mathbb{F}_q)$ and $E'(\mathbb{F}_q)$ satisfy $\#E + \#E' = 2(q + 1)$. For prime fields with $q > 229$, Theorem 1 implies that we may determine one of $\#E$ and $\#E'$ by alternately computing the orders of points on E and E', and once we know either $\#E$ or $\#E'$, we know both.

Note that Theorem 1 does not hold for $q = 229$, or for non-prime finite fields, since there are counterexamples whenever q is a square. The argument in the proof of [1, Theorem 3.2] does not use the primality of q, but only that q is not a square, so that the Hasse bound on t cannot be attained. If $q = r^2$ is an even power of a

[1] When q is large (e.g., of cryptographic size) one uses the asymptotically faster method of Schoof.

[2] Theorem 3.2 in [1] refers to the order of a particular point P, but Theorem 1 above is equivalent.

prime, then there are supersingular elliptic curves E over $\mathbb{F}_q$ such that

$$E(\mathbb{F}_q) \cong (\mathbb{Z}/(r-1)\mathbb{Z})^2 \qquad \text{and} \qquad E'(\mathbb{F}_q) \cong (\mathbb{Z}/(r+1)\mathbb{Z})^2\,.$$

One may easily check that there are at least 5 multiples of $r-1$, and at least 3 multiples of $r+1$, in $\mathcal{H}_q$; however for $r > 7$ ($q > 49$), the only pair that sum to $2(q+1)$ are $(r-1)^2$ and $(r+1)^2$. This resolves the ambiguity in these cases.[3]

The preceding observation led to this note, whose purpose is to extend Theorem 1 to treat all finite fields (not just prime fields) $\mathbb{F}_q$ with $q > 49$, and all prime fields with $q > 29$. Specifically, we prove the following:

Theorem 2. *Let $E/\mathbb{F}_q$ be an elliptic curve with $q \notin \{3,4,5,7,9,11,16,17,23,25,29,49\}$. There is a unique integer t with $|t| \le 2\sqrt{q}$ such that $\lambda(E) | (q+1-t)$ and $\lambda(E') | (q+1+t)$.*

Our proof is entirely elementary, relying on just two properties of elliptic curves over finite fields:

(a) $\#E = q+1-t$ and $\#E' = q+1+t$ for some integer t with $|t| \le 2\sqrt{q}$;

(b) $E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with n_1 dividing both n_2 and $q-1$.

Proofs of (a) and (b) may be found in most standard references, including [3]. When $E(\mathbb{F}_q)$ is cyclic we have $n_1 = 1$, and we always have $n_2 = \lambda(E)$.

Proof of Theorem 2. Let E be an elliptic curve over $\mathbb{F}_q$, and put $\#E = mM$ with $M = \lambda(E)$, and $\#E' = nN$ with $N = \lambda(E')$. Without loss of generality, we assume $a = q+1-\#E \ge 0$. Taking $t = a$ shows existence (by (a) and (b) above), so we need only prove that $t = a$ is the unique t satisfying the conditions stated in the theorem. For any such t we have $t \equiv q+1 \bmod M$ and $t \equiv -(q+1) \bmod N$; hence t lies in an arithmetic sequence with difference $\operatorname{lcm}(M,N)$. We also have $|t| \le 2\sqrt{q}$; thus if $\operatorname{lcm}(M,N) > 4\sqrt{q}$, then $t = a$ is certainly unique.

We now show that $\operatorname{lcm}(M,N) \le 4\sqrt{q}$ can occur only for $q \le 1024$. We start from

$$mMnN = (q+1-a)(q+1+a) = (q+1)^2 - a^2 \ge (q+1)^2 - 4q = (q-1)^2, \tag{2}$$

which implies that

$$mn \ge \frac{(q-1)^2}{MN} = \frac{(q-1)^2}{\gcd(M,N)\operatorname{lcm}(M,N)}. \tag{3}$$

Let $d = \gcd(m,n)$. Then d^2 divides $mM + nN = 2(q+1)$, so $d|(q+1)$, but also $d|(q-1)$, hence $d \le 2$. This implies $2\operatorname{lcm}(M,N) \ge 2\operatorname{lcm}(m,n) \ge mn$. We also have $\gcd(M,N) \le \gcd(m,n)\gcd(M/m,N/n) \le 2\gcd(M/m,N/n)$. From (3) we obtain

$$\operatorname{lcm}(M,N)^2 \ge \frac{(q-1)^2}{4\gcd(M/m,N/n)}. \tag{4}$$

We now suppose $\operatorname{lcm}(M,N) \le 4\sqrt{q}$, for otherwise the theorem holds. We have $nN = q+1+a > q$, since we assumed $a \ge 0$, and $N \le 4\sqrt{q}$ implies that $n > \sqrt{q}/4$, so $N/n < 16$. Applying $\gcd(M/m,N/n) \le N/n < 16$ to (4) yields

$$4\sqrt{q} \ge \operatorname{lcm}(M,N) > (q-1)/8, \tag{5}$$

which implies that the prime power q is at most 1024.

The cases for $q \le 1024$ are addressed by a simple program listed in the appendix that outputs the values of q, $M = \lambda(E)$, and $N = \lambda(E')$ for which exceptions can arise. This yields the set of excluded q and completes the proof. ∎

[3] But when $q = 49$ we have $100 = 36 + 64$ and also $100 = 60 + 40$.

Application. The proof of Theorem 2 suggests an algorithm to compute $\#E$, provided that q is small enough for the orders of randomly chosen points in $E(\mathbb{F}_q)$ to be easily computed. It suffices to determine integers a and m for which the set $S = \{x : x \equiv a \bmod m\}$ contains $t = q + 1 - \#E$ but no $t' \neq t$ with $|t'| \leq 2q$. Beginning with $m = 1$ and $a = 0$, we compute $|P|$ for random P in $E(\mathbb{F}_q)$ or $E'(\mathbb{F}_q)$ and update a and m to reflect the fact that $t \equiv q+1 \bmod |P|$ (when $P \in E(\mathbb{F}_q)$), or $t \equiv -(q+1) \bmod |P|$ (when $P \in E'(\mathbb{F}_q)$). The new values of a and m may be determined via the extended Euclidean algorithm. When the set S contains a unique t with $|t| \leq 2\sqrt{q}$, we can conclude that $\#E = q + 1 - t$ (and also that $\#E' = q + 1 + t$).

The probabilistic algorithm we have described is a *Las Vegas* algorithm, that is, its output is always correct and its expected running time is finite. The correctness of the algorithm follows from property (a), Theorem 2 ensures that the algorithm can terminate (provided that q is not in the excluded set), and [2, Theorem 8.2] bounds its expected running time.

An examination of Table 1 reveals that in many cases an ambiguous t' could be ruled out if $\lambda(E)$ or $\lambda(E')$ were known. For example, when $q = 49$, the trace $t' = -10$ yields $\#E = 60$ and $\#E' = 40$, so both $\lambda(E)$ and $\lambda(E')$ are divisible by 5 (and are not 6 or 8). If the trace of E is -10 the algorithm above will likely discover this and terminate within a few iterations. But when the trace of E is 14 (and $\lambda(E) = 6$ and $\lambda(E') = 8$), we can never be completely certain that we have ruled out -10 as a possibility. Thus when an unconditional result is required, we must avoid $q \in \{3, 4, 5, 7, 9, 11, 16, 17, 23, 25, 29, 49\}$.

However, when $\lambda(E)$ and $\lambda(E')$ are known we have the following corollary, which extends Proposition 4.19 of [3].

Corollary 1. *Let E be an elliptic curve over $\mathbb{F}_q$. The integers $\lambda(E)$ and $\lambda(E')$ uniquely determine the isomorphism types of $E(\mathbb{F}_q)$ and $E'(\mathbb{F}_q)$ for all $q \notin \{5, 7, 9, 11, 17, 23, 29\}$, and they uniquely determine the set $\{E(\mathbb{F}_q), E'(\mathbb{F}_q)\}$ for all q.*

Note that $\lambda(E)$ and $\#E$ together determine $E(\mathbb{F}_q)$, by property (b). To prove the corollary, apply Theorem 1 with a modified version of the algorithm in the appendix that also requires $(q+1-t')/M$ to divide M and $(q+1+t')/N$ to divide N.

As a final remark, we note that all the exceptional cases listed in Table 1 can be eliminated if the orders of the 2-torsion and 3-torsion subgroups of $E(\mathbb{F}_q)$ are known (these orders may be computed using the division polynomials). Alternatively, one can simply enumerate the points on $E/\mathbb{F}_q$ to determine $\#E$ when $q \leq 49$.

1. Appendix

For a prime power q, we wish to enumerate all M, N, and t such that:

(i) M divides $q + 1 - t$ and N divides $q + 1 + t$, with $0 \leq t \leq 2\sqrt{q}$.
(ii) $(q + 1 - t)/M$ divides M and $q - 1$, and $(q + 1 + t)/N$ divides N and $q - 1$.
(iii) M divides $q + 1 - t'$ and N divides $q + 1 + t'$ for some $t' \neq t$ with $|t'| \leq 2\sqrt{q}$.

Any exception to Theorem 2 must arise from an elliptic curve $E/\mathbb{F}_q$ with $\lambda(E) = M$, $\lambda(E') = N$, and $\#E = q + 1 - t$ (or from its twist, but the cases are symmetric, so we restrict to $t \geq 0$). Properties (i) and (ii) follow from (a) and (b) above, and (iii) implies that t does not uniquely satisfy the requirements of the theorem.

Algorithm 1 below finds all M, N, and t satisfying (i), (ii), and (iii). For $q \leq 1024$, exceptional cases are found only for $q \in \{3, 4, 5, 7, 9, 11, 16, 17, 23, 25, 29, 49\}$. Not every case output by Algorithm 1 is actually realized by an elliptic curve[4], but for each combination of q and t at least one is. An example of each such case is listed in Table 1, where we only list cases with $t \geq 0$: for the symmetric cases with $t < 0$, change the sign of t and swap M and N.

Algorithm 1. *Given a prime power q, output all quadruples of integers (M, N, t, t') satisfying (i), (ii), and (iii) above:*

```
for all pairs of integers (M, N) with √q − 1 ≤ M, N ≤ 4√q do
  for all integers t ∈ [0, 2√q] with M|(q + 1 − t) and N|(q + 1 + t) do
    Let m = (q + 1 − t)/M and n = (q + 1 + t)/N.
    if m|M and m|(q − 1) and n|N and n|(q − 1) then
      for all integers t′ ∈ [−2√q, 2√q] do
        if M|(q + 1 − t′) and N|(q + 1 + t′) then
          print M, N, t, t′.
        end if
      end for
    end if
  end for
end for
```

q	M	N	t	E	t'
3	2	2	0	$y^2 = x^3 - x$	-2,2
4	1	3	4	$y^2 + y = x^3 + \alpha^2$	-2,1
5	2	4	2	$y^2 = x^3 + x$	-2
7	2	6	4	$y^2 = x^3 - 1$	-2
7	4	4	0	$y^2 = x^3 + 3x$	-4,4
9	2	4	6	$y^2 = x^3 + \alpha^2 x$	-6,-2,2
11	4	8	4	$y^2 = x^3 + x + 9$	-4
11	6	6	0	$y^2 = x^3 + 2x$	-6,6
16	3	5	8	$y^2 + y = x^3$	-7
17	6	12	6	$y^2 = x^3 + x + 7$	-6
23	8	16	8	$y^2 = x^3 + 5x + 15$	-8
25	4	6	10	$y^2 + y = x^3 + \alpha^7$	-2
29	10	20	10	$y^2 = x^3 + x$	-10
49	6	8	14	$y^2 = x^3 + \alpha^2 x$	-10

TABLE 1. Exceptional Cases with $t \geq 0$.

The coefficient α denotes a primitive element of $\mathbb{F}_q$.

References

1. René Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux **7** (1995), 219–254.
2. Andrew V. Sutherland, *Order computations in generic groups*, PhD thesis, M.I.T., 2007, available at `http://groups.csail.mit.edu/cis/theses/sutherland-phd.pdf`.
3. Lawrence C. Washington, *Elliptic curves: Number theory and cryptography*, 2nd ed., CRC Press, 2008.

[4]All but one of the exceptions fail the condition that $(q+1-t)/M \equiv (q+1+t)/N \pmod 2$.