Almost Primality of Group Orders of Elliptic Curves Defined over Small Finite Fields

Neal Koblitz

CONTENTS

Let E be an elliptic curve defined over a small finite field $\mathbb{F}_q$, and let p be a prime number. We give a conjectural formula for the probability that the order of the quotient group $E(\mathbb{F}_{q^p})/E(\mathbb{F}_q)$ is prime, and compare it with experimental data. The motivation for this study comes from public key cryptography.

1. INTRODUCTION

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ of q elements. We say that E has *almost prime order* over the degree-p extension if

$$M_p = M_p(E/\mathbb{F}_q) = \frac{\#E(\mathbb{F}_{q^p})}{\#E(\mathbb{F}_q)}$$

is prime. Note that $E(\mathbb{F}_{q^r})$ is a subgroup of $E(\mathbb{F}_{q^s})$ whenever $r \mid s$; this means that $\#E(\mathbb{F}_{q^p})$ is divisible by $\#E(\mathbb{F}_q)$, and that the ratio of these two numbers can be prime only if p is prime. (There are two trivial exceptions: $q = 2$, $p = 4$, $\#E(\mathbb{F}_2) = 5$; and $q = 3$, $p = 4$, $\#E(\mathbb{F}_3) = 7$.)

In this paper we are interested in almost primality of $E(\mathbb{F}_{q^p})$ for fixed small q and variable p. The motivation for this study comes from public key cryptography, where elliptic curve groups should be of almost prime order in order to avoid the Silver–Pohlig–Hellman attack on the elliptic curve discrete logarithm problem; see, for example, [Koblitz 1998, p. 133]. Curves defined over small fields often have special efficiency advantages. The case that has been studied most extensively is the nonsupersingular curves defined over $\mathbb{F}_2$; the most detailed study of such curves is [Solinas 2000]. These are also the only curves defined over small fields that are currently used in industrial applications; see [FIPS 2000].

According to Hasse's Theorem, if we set

$$a = a(E/\mathbb{F}_q) = q + 1 - \#E(\mathbb{F}_q)$$

© A K Peters, Ltd.
1058-6458/2001 $0.50 per page

and

$$T^2 - aT + q = (T - \alpha)(T - \overline{\alpha}),$$

where $\alpha \in \mathbb{Q}\big(\sqrt{a^2 - 4q}\big)$, then $a^2 - 4q \le 0$ and

$$M_p = \left|\frac{\alpha^p - 1}{\alpha - 1}\right|^2.$$

Thus, M_p is a generalization of the Mersenne numbers, as we see by replacing α by 2. The conjecture that follows is based on an analogous conjecture for Mersenne numbers (see [Wagstaff 1983]).

Conjecture A. *For fixed E over $\mathbb{F}_q$, the number $M(x)$ of $M_p < x$ that are prime is asymptotic to*

$$\frac{e^\gamma}{\log q}\log\log x,$$

where γ is Euler's constant and log *denotes the natural logarithm.*

Our purpose in this paper is to discuss the heuristics of this conjecture and give some numerical evidence.

2. PROBABILITY OF PRIMALITY

Recall that the Prime Number Theorem, stating that the number of primes $< x$ is asymptotic to $x/\log x$, can be interpreted informally as saying that the probability that an integer n is prime is $1/\log n$. This is because

$$\frac{n+1}{\log(n+1)} - \frac{n}{\log n} \sim \frac{n+1}{\log n} - \frac{n}{\log n} = \frac{1}{\log n}.$$

In the same way, Conjecture A can be interpreted as saying that the probability that M_p is prime is about

$$\frac{e^\gamma}{\log q}\,\frac{\log p}{p}.$$

Indeed, if the conjecture holds, then the probability that M_p is prime is roughly $M(q^p) - M(q^{p-\log p})$. But

$$\log\log(q^p) - \log\log(q^{p-\log p}) = -\log\frac{p-\log p}{p}$$
$$\sim \frac{\log p}{p}.$$

3. HEURISTICS

Proposition. *$p \mid M_p$ if and only if $p \mid q+1-a$. If $l \ne p$ is a prime divisor of M_p, then $l \equiv \pm 1$ (mod p), and $l \equiv 1$ (mod p) if l splits or ramifies in $\mathbb{Q}(\alpha)$.*

Corollary. *The smallest prime that divides M_p is at least $p-1$, and if $p > \max(3,\, q+1-a)$, then it is at least $2p-1$.*

Proof of Proposition. First suppose that l is a prime divisor of M_p not dividing $q + 1 - a = |\alpha - 1|^2$. Let I be a prime ideal of $\mathbb{Q}(\alpha)$ lying over l, and let F be the corresponding residue field. Since $l \nmid |\alpha-1|^2$ and l divides $|\alpha^p - 1|^2$, it follows that either α mod I or $\overline{\alpha}$ mod I has exact order p in F. Thus, $p \mid l - 1$ if l splits or ramifies in $\mathbb{Q}(\alpha)$, and $p \mid l^2 - 1$ if l remains prime.

Now suppose that l is a prime dividing $q + 1 - a$. Writing

$$\frac{\alpha^p - 1}{\alpha - 1} = \frac{(1 + (\alpha - 1))^p - 1}{\alpha - 1}$$
$$= p + \binom{p}{2}(\alpha - 1) + \binom{p}{3}(\alpha - 1)^2 + \cdots + (\alpha - 1)^{p-1},$$

we see that if $l = p$, then

$$p \;\Big|\; \frac{\alpha^p - 1}{\alpha - 1}\,\frac{\overline{\alpha}^p - 1}{\overline{\alpha} - 1} = M_p.$$

If $l \ne p$ and I and F as before denote a prime ideal over l and its residue field, then without loss of generality we may assume that $\alpha - 1 \in I$. If $l \mid \alpha - 1$, then the above equality shows that $M_p \equiv p^2 \not\equiv 0$ (mod l). If $l \nmid \alpha - 1$, then the same equality still gives $(\alpha^p-1)/(\alpha-1) \notin I$. If l remains prime or ramifies in $\mathbb{Q}(\alpha)$, this means that $l \nmid M_p$. If l splits, then $l \mid M_p$ only if $\overline{\alpha}^p - 1 \in I$; since $\overline{\alpha} - 1 \notin I$, this means that $\overline{\alpha}$ mod I has exact order p in F, and so $l \equiv 1$ (mod p). □

Recall two classical asymptotic results from analytic number theory [Hardy and Wright 1979, pp. 348 and 351, Theorems 425 and 429]:

$$\sum_{\text{primes } l<x} \frac{\log l}{l} \sim \log x \tag{3–1}$$

$$\prod_{\text{primes } l<x} \left(1 - \frac{1}{l}\right)^{-1} \sim e^\gamma \log x \tag{3–2}$$

(The second is Mertens' Theorem.)

Now, the probabilistic interpretation of the Prime Number Theorem says that the probability that a random integer n is prime is $1/\log n$. The conditional probability that n is prime given that it is not divisible by any prime $< x$ is

$$\frac{1}{\log n}\prod_{\text{primes } l<x}\left(1-\frac{1}{l}\right)^{-1}\sim e^{\gamma}\frac{\log x}{\log n}$$

by Mertens' Theorem. We now take $n = M_p \sim q^{p-1}$. By the above Corollary we can take $x = p-1$. This gives us the following heuristic formula for the probability that M_p is prime:

$$e^{\gamma}\frac{\log(p-1)}{(p-1)\log q}\sim\frac{e^{\gamma}}{\log q}\,\frac{\log p}{p}.$$

Then the number $M(x)$ of $M_p < x$ that are prime is approximately

$$\frac{e^{\gamma}}{\log q}\sum_{M_p<x}\frac{\log p}{p}\sim\frac{e^{\gamma}}{\log q}\sum_{p<\frac{\log x}{\log q}}\frac{\log p}{p}$$
$$\sim\frac{e^{\gamma}}{\log q}\log\log x$$

by asymptotic formula (3–1). This is Conjecture A.

4. REMARKS ON ATTEMPTS TO REFINE THE CONJECTURE

1. In the conjectural expression

$$\frac{e^{\gamma}}{\log q}\,\frac{\log p}{p}$$

for the probability that M_p is prime, we see from the Proposition and Corollary in Section 3 that $\log p$ can be replaced by $\log(2p-1)$ if $p > \max(3, q+1-a)$. Actually, $\log p$ can be replaced by $\log p'$, where p' is the smallest prime such that either (i) $p' \equiv 1 \pmod p$, or (ii) $\left(\frac{p'}{D}\right) = -1$ and $p' \equiv -1 \pmod p$ (here $D = a^2 - 4q$ is the discriminant). However, in view of other considerations that are ignored by the heuristics in Section 3 (see Remarks 2–4 below), we would be on weak ground if we claimed that

$$\frac{e^{\gamma}}{\log q}\,\frac{\log p'}{p}$$

is a better formula than

$$\frac{e^{\gamma}}{\log q}\,\frac{\log p}{p}.$$

2. The likelihood that a prime l divides M_p is much greater if l splits in the quadratic imaginary field $\mathbb{Q}(\alpha)$ than if it remains prime. Roughly speaking, in the former case α^p has about a $2/l$ chance of equaling 1 in either of the two residue fields at l, whereas in the latter case it has about a $1/l^2$ chance of equaling 1 in the unique residue field at l. Compared to the probability that l divides a random integer, the probability $2/l$ is twice as great and the probability $1/l^2$ is negligible. Because half of all primes l split and half remain prime, these two effects cancel each other out asymptotically. However, in Remark 1 above we might want to redefine p' as the smallest prime such that $p' \equiv 1 \pmod p$ and $\left(\frac{p'}{D}\right) = 1$.

3. In Remark 2, in the case when l splits it is not quite correct to say that the probability that $l \mid M_p$ is approximately $2/l$. Rather, by the Proposition in Section 2, this probability is zero if $l \not\equiv 1 \pmod p$; and if $l \equiv 1 \pmod p$, then it is approximately $2p/l$. The reason for the latter expression is that α^p is in the subgroup of (l/p)-th roots of unity in each of the residue fields at l. Since the probability that l satisfies $l \equiv 1 \pmod p$ is roughly $1/p$, the asymptotics should not be affected by treating M_p as a random integer with a $1/l$ chance of being divisible by any prime l.

4. Discussions of divisors of Mersenne numbers (see [Wagstaff 1983]) often start out by noting that 2 must be a quadratic residue modulo $l = 2l'p + 1$ — i.e., l' must be $\equiv 0$ or $-p \pmod 4$) — in order for l to divide $2^p - 1$. Similarly, in our case α must be a square in a residue field at l in order for l to divide $|\alpha^p - 1|^2$. However, in our case this condition cannot be expressed simply as a congruence condition on l. The reason is that the condition that α is a square in the residue field can be rephrased as a condition on the factorization of the polynomial

$$T^4 - aT^2 + q = (T^2 - \alpha)(T^2 - \overline{\alpha})$$

modulo l (i.e., a condition on how the prime l decomposes in the splitting field of this polynomial). Since the splitting field of this quartic is generally nonabelian, we cannot express the condition as a congruence. (However, by the Chebotarev Density Theorem [Marcus 1977, Chapter 8], we do know that, of the primes l that split in $\mathbb{Q}(\alpha)$, asymptotically 25% satisfy the further condition that α is a square in both residue fields, 50% have α a square in exactly one of the residue fields, and 25% have α a nonsquare in both residue fields.)

q	a	D	E	p for which M_p is prime and less than 2^{1000}
2	0	−8	$Y^2+Y = X^3$	2,3,5,7,11,13,17,19,23,31,43,61,79,101,127,167,191,199,313,347,701
2	1	−7	$Y^2+XY = X^3+X^2+1$	3,5,7,11,17,19,23,101,107,109,113,163,283,311,331,347,359,701
2	−1	−7	$Y^2+XY = X^3+1$	2,5,7,13,19,23,41,83,97,103,107,131,233,239,277,283,349,409,571
2	2	−4	$Y^2+Y = X^3+X+1$	2,3,5,7,11,19,29,47,73,79,113,151,157,163,167,239,241,283,353,367, 379,457,997
2	−2	−4	$Y^2+Y = X^3+X$	5,7,11,13,17,29,43,53,89,283,557,563,613,691
3	0	−3	$Y^2 = X^3+X$	3,5,7,13,23,43,281,359,487,577
3	1	−11	$Y^2 = X^3+X^2-1$	2,5,7,37,67,271,281,409,449,599
3	−1	−11	$Y^2 = X^3-X^2+1$	2,7,23,59,179,269,383
3	2	−8	$Y^2 = X^3-X^2-1$	3,7,11,13,19,23,31,37,43,47,83,193,557
3	−2	−8	$Y^2 = X^3+X^2+1$	2,3,5,7,13,19,71,199,257,479,503
3	3	−3	$Y^2 = X^3-X-1$	2,5,7,11,17,19,79,163,193,239,317,353
3	−3	−3	$Y^2 = X^3-X+1$	5,11,31,37,47,53,97,163,167,509
4	1	−15	$Y^2+XY = X^3+\beta$	3,5,7,17,37,43,67,79,163
4	−1	−15	$Y^2+XY = X^3+\beta X^2+\beta$	5,7,31,59,167,227,379
4	2	−3	$Y^2+\beta Y = X^3$	2,5,7,13,29,61,383,401
4	−2	−3	$Y^2+\beta Y = X^3+\beta$	2,3,5,11,23,31,43,149,157,193
4	3	−7	$Y^2+XY = X^3+\beta X^2+1$	3,5,11,31,53,61,383
5	0	−20	$Y^2 = X^3+1$	5,67,101,103,229,347
5	1	−19	$Y^2 = X^3-2X+1$	2,7,73,79,113
5	−1	−19	$Y^2 = X^3+2x+1$	2,5,17,31,37,47,97,179,269
5	2	−4	$Y^2 = X^3+X$	3,5,17,47,53,181,227,353,401
5	−2	−4	$Y^2 = X^3-X$	3,5,13,19,29,37,43
5	3	−11	$Y^2 = X^3-X+2$	5,7,19,43,167,227,311
5	−3	−11	$Y^2 = X^3+X+1$	2,7,13,17,29,31,37,43,211
5	4	−4	$Y^2 = X^3+2X$	3,5,7,53,97,107,239
5	−4	−4	$Y^2 = X^3-2X$	2,3,7,17,43,61,137,151,167,191,317,397
7	0	−7	$Y^2 = X^3+X$	3,17,23,29,47,61
7	1	−3	$Y^2 = X^3-2$	5,13,19,23,103,107,181
7	−1	−3	$Y^2 = X^3+2$	2,7,11,29,43,53
7	2	−24	$Y^2 = X^3+X+3$	7,19,29,59
7	−2	−24	$Y^2 = X^3+X-3$	3,7,11,23
7	3	−19	$Y^2 = X^3+X+1$	2
7	−3	−19	$Y^2 = X^3+X-1$	2,5,7,31,89
7	4	−3	$Y^2 = X^3-1$	5,7,17,43,47,127,223
7	−4	−3	$Y^2 = X^3+1$	5,11,53,59,109
7	5	−3	$Y^2 = X^3-3$	2,19,61,71,167
7	−5	−3	$Y^2 = X^3+3$	2,5,11,17,103,191
8	1	−31	$Y^2+XY = X^3+\beta X$	3,19,23,139,167
8	−1	−31	$Y^2+XY = X^3+X^2+\beta X$	7,11,19,47,59
8	3	−7	$Y^2+XY = X^3+X^2+\beta X+1$	5,19,37,41,47,59
8	−3	−7	$Y^2+XY = X^3+\beta X+1$	5,7,11,19,31,73,139,233
9	0	−4	$Y^2 = X^3+(1+\beta)X$	3,59,223
9	1	−35	$Y^2 = X^3+X^2+\beta$	2,5,11
9	−1	−35	$Y^2 = X^3+(1+\beta)X^2+(1+\beta)$	23
9	2	−8	$Y^2 = X^3+(1+\beta)X^2+(1-\beta)$	3,5,13,79,83,97,157,233
9	−3	−3	$Y^2 = X^3+\beta X+1$	2,5,7,11
9	4	−20	$Y^2 = X^3+\beta X^2+(1+\beta)$	11,13,37,167,223
9	−4	−20	$Y^2 = X^3+(-1+\beta)X^2-1$	5,13,19,41,103,313
9	5	−11	$Y^2 = X^3+(1+\beta)X^2+(-1+\beta)$	7,29,37

TABLE 1. For each a and q we list the discriminant D of the quadratic imaginary extension generated by α, the equation of one of the elliptic curves with the given value of a, and the primes p such that M_p is a prime of at most 1000 bits. By definition, $\beta^2+\beta+1=0$ when $q=4$, $\beta^3+\beta+1=0$ when $q=8$, and $\beta^2+1=0$ when $q=9$.

None of the possible adjustments that one would make as a result of the above considerations would cause a change asymptotically in the conjectural formula for $M(x)$. Moreover, experience with Mersenne numbers suggests that a "refined" conjecture is not likely to be significantly better than the crude one, at least not in the range of values where computations are feasible.

5. In the case of Mersenne numbers, the attempt to refine the conjectural formula for the probability of primality by replacing $\log(2p)$ by $\log(2bp)$ for suitable $b = b(p)$ has not been very successful. Ehrman [1967] and Wagstaff [1983] have argued for replacing $\log(2p)$ by $\log(2bp)$, where $b = 1$ if $p \equiv 3 \pmod 4$ and $b = 3$ if $p \equiv 1 \pmod 4$, and they discuss evidence that there are fewer Mersenne primes with p satisfying the former congruence. This b equals the least value of l' such that $2l'p + 1$ could possibly be a prime divisor of the p-th Mersenne number. But Ehrman and Wagstaff did not take into account the fact that if $p \equiv 7 \pmod{12}$, then neither $2p + 1$ nor $8p + 1$ can be prime (since they are divisible by 3), and so the smallest value of l' would be 5; thus, one should take $b = 5$ rather than $b = 1$ when $p \equiv 7 \pmod{12}$. And indeed, looking at all Mersenne primes with $p > 3$ and $p < 10^6$, we see that for 7 of them $p \equiv 1 \pmod{12}$, for 11 of them $p \equiv 5 \pmod{12}$, for 10 of them $p \equiv 7 \pmod{12}$, and for only 3 of them $p \equiv 11 \pmod{12}$. In other words, it is a little misleading to say that the congruence $p \equiv 3 \pmod 4$ works against primality of $2^p - 1$; in fact, both the heuristic argument and the numerical evidence support such a conclusion only when the congruence $p \equiv 2 \pmod 3$ also holds.

In any case, it seems that the divisibility properties of $2^p - 1$ behave in too irregular a manner for congruence conditions modulo 4, 12, or other numbers to correlate well with primality. For example, the same argument that was used above to predict that there would be more Mersenne primes with $p \equiv 7 \pmod{12}$ would also tell us that more Mersenne primes would have p congruent to $2 \pmod 5$ than would have p congruent to either 1, 3, or 4 (mod 5). But although the congruence $p \equiv 2 \pmod 5$ is satisfied by 6 out of the 14 Mersenne primes $< 2^{1000}$, it is satisfied by only 3 out of the 19 Mersenne primes between 2^{1000} and $2^{1000000}$.

5. TABLES

For each $q < 10$ and $a = q + 1 - \#E(\mathbb{F}_q)$, Table 1 gives the discriminant D of the quadratic imaginary extension generated by α, the equation of one of the elliptic curves with the given value of a, and a list of all primes p such that M_p is a prime of at most 1000 bits.

In the table β is a root of $X^2 + X + 1 = 0$ when $q = 4$, a root of $X^3 + X + 1 = 0$ when $q = 8$, and a root of $X^2 + 1 = 0$ when $q = 9$. The values $a = \pm 4$ when $q = 4$ and $a = \pm 6$ when $q = 9$ are not included, because it is easy to see that in those cases M_p is a perfect square. The values $a = 0, -3$ when $q = 4$, $a = 0, \pm 4, \pm 5$ when $q = 8$, and $a = -2, 3, -5$ when $q = 9$ are also disregarded, since those values come from elliptic curves defined over proper subfields of $\mathbb{F}_q$ and hence lead to composite M_p. Finally, the values $a = \pm 2$ cannot occur when $q = 8$ [Schoof 1987].

Below we compare the results in Table 1 with Conjecture A. The conjecture predicts that

$$M(2^{1000}) \approx \frac{e^\gamma}{\log q} \log\log(2^{1000}) \approx \frac{11.65}{\log q}.$$

The last column gives the average of $M(2^{1000})$ over all values of a for the given q.

q	$\frac{11.65}{\log q}$	average of $M(2^{1000})$
2	16.81	19.00
3	10.60	10.43
4	8.40	8.20
5	7.24	7.89
7	5.99	5.09
8	5.60	6.00
9	5.30	4.13

Taking into account the limitations on available data for a function that grows as slowly as $\log\log x$ and also the lack of evidence for a more refined conjecture, as discussed in Section 4, we conclude that the preceding table is in reasonable agreement with Conjecture A.

ACKNOWLEDGMENTS

I thank the anonymous referee for very helpful suggestions and simplifications.

NOTE ADDED IN PROOF

I recently learned that some of this work, including the formulation of Conjecture A, has also been done independently by Peter Beelen in his 2001 Ph.D. Thesis at Eindhoven Universitiy of Technology.

REFERENCES

[Ehrman 1967] J. R. Ehrman, "The number of prime divisors of certain Mersenne numbers", *Math. Comp.* **21** (1967), 700–704.

[FIPS 2000] FIPS, "Digital Signature Standard", FIPS Publication 186-2, February 2000.

[Hardy and Wright 1979] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Fifth ed., Clarendon, Oxford, 1979.

[Koblitz 1987] N. Koblitz, "Elliptic curve cryptosystems", *Math. Comp.* **48**:177 (1987), 203–209.

[Koblitz 1998] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Comp. in Math. **3**, Springer, Berlin, 1998.

[Marcus 1977] D. A. Marcus, *Number fields*, Universitext, Springer, New York, 1977.

[Schoof 1987] R. Schoof, "Nonsingular plane cubic curves over finite fields", *J. Combin. Theory Ser. A* **46**:2 (1987), 183–211.

[Solinas 2000] J. A. Solinas, "Efficient arithmetic on Koblitz curves", *Des. Codes Cryptogr.* **19**:2-3 (2000), 195–249.

[Wagstaff 1983] S. S. Wagstaff, Jr., "Divisors of Mersenne numbers", *Math. Comp.* **40**:161 (1983), 385–397.

Neal Koblitz, Department of Mathematics, University of Washington, Seattle, WA 98195, United States (koblitz@math.washington.edu)

Received September 29, 2000; accepted in revised form March 29, 2001