Distribution of $\#E^t$ for prime-order elliptic curves: Numerical results

David Leon Gil

June 3, 2015

1 Introduction

This is a preliminary note of some numerical experiments; the results may be rather wrong.

2 Prime-order curves

Let $\mathbb{Z}_q$ be a finite field in characteristic greater than 3, and $\mathbb{E}_j(\mathbb{Z}_q)$ be the elliptic curve defined by

$$\mathbb{E}_j(\mathbb{Z}_q) \equiv x^3 = y^2 + \frac{36x}{j-1728} - \frac{1}{j-1728} \tag{1}$$

and $\mathbb{E}^t_j(\mathbb{Z}_q))$ be some curve automorphic to its quadratic twist

$$\mathbb{E}^t_j(\mathbb{Z}_q)) \equiv x^3 = y^2 + \beta^2\frac{36x}{j-1728} - \beta^3\frac{1}{j-1728} \tag{2}$$

where β is a quadratic non-residue in $\mathbb{Z}_q$.
Then the trace, $T_f(j)$, of $\mathbb{E}_j(\mathbb{Z}_q)$, is defined by:

$$\begin{aligned} \#\mathbb{E}_j(\mathbb{Z}_q) &= q - T_f(j) + 1 \\ \#\mathbb{E}^t_j(\mathbb{Z}_q)) &= q + T_f(j) + 1 \end{aligned} \tag{3}$$

3 Primes

We consider the SECP primes, first suggested by (**Solinas**), which are, where $N \coloneqq 2^{32}$:

$$\begin{aligned} \mathrm{P}_{224} &= N^7 - N^3 + N^0 \\ \mathrm{P}_{256} &= N^8 - N^7 + N^6 + N^3 - N^0 \\ \mathrm{P}_{384} &= N^{12} - N^4 - N^3 + N^1 - N^0 \end{aligned} \tag{4}$$

as well as the two curves proposed for IETF use, the nearly-Mersenne $\mathrm{M}_{255} = 2^{255} - 19$ and the Goldilocks prime $\mathrm{H}_{448} = 2^{448} - 2^{224} - 1$.

4 Numerical methods

4.1 Finding prime-order curves

A slightly modified version of PARI/GP was used to calculate the traces of prime-order curves. Point-counting was aborted early if $\#K$ was found to have a small prime factor.

4.2 Range

We calculate $T_f(j)$ for each $\mathbb{E}_j(\mathbb{Z}_q)$ for $0 < j < 2^{20}, j \neq 1728$, then test $\#\mathbb{E}_j(\mathbb{Z}_q)$ and $\#\mathbb{E}_j^t(\mathbb{Z}_q))$ for (pseudo-)primality.

4.3 Results

	N_π	$N_{\pi'}$	$N_{\pi'}/N_\pi$
P_{224}	2790	31	1.11e-2
P_{256}	1956	15	0.77e-2
P_{384}	1131	20	1.77e-2

5 Stopping times for prime and doubly-prime curves

Because the above method results in fairly low precision in estimating $N_{\pi'}/N_\pi$ because of the small number of doubly-prime curves, we use a slightly different method, essentially similar to that of (Shparlinski and Sutantyo, 2014).

We generate a random j-invariant, $j_{0,0}$, and increment it by 1 until we find a doubly prime curve (using the early-stop technique both for the curve and its twist).

We can then roughly approximate the probability of finding a doubly-prime curve over each field as …

6 Distribution of factors for the twists of prime curves

We consider the following question:

7 Acknowledgments

The patch to PARI/GP used is derived from a patch by Michael Hamburg.

Appendix. Cofactors for SafeCurves

Define $h(\mathbb{E}_j(\mathbb{Z}_q))$ as $\{p^n : p^n \mid \#\mathbb{E}_j(\mathbb{Z}_q)\} \setminus \{p^n : p^n \mid \#\mathbb{E}_j^t(\mathbb{Z}_q)), \nexists p' < p\}$.
This table is adapted (read stolen directly) from Bernstein, 2013.

Curve	$h(\mathbb{E}_j(\mathbb{Z}_q))$	$h(\mathbb{E}_j^t(\mathbb{Z}_q)))$
M221	2^3	2^2
E222	2^2	$\mathbf{2^2}$
secp224r1	1	$3^2 \cdot 11 \cdot 47 \cdot 3015283 \cdot 40375823 \cdot 267983539294927$
Curve1174	2^2	$\mathbf{2^2}$
Curve25519	2^3	2^2
BN(2,254)	1	$3^3 \cdot 3583 \cdot 298908837206431 \cdot 1171118464301578290369761 6449$
brainpoolP256	1	$5^2 \cdot 175939 \cdot 492167257 \cdot 8062915307 \cdot 2590895598527 \cdot 4233394996199$
FRP256v1	1	$7 \cdot 439 \cdot 11760675247 \cdot 3617872258517821$
secp256r1	1	$3 \cdot 5 \cdot 13 \cdot 179$
secp256k1	1	$3^2 \cdot 13^2 \cdot 3319 \cdot 22639$
E382	2^2	$\mathbf{2^2}$
M383	2^3	2^2
Curve383187	2^3	2^2
brainpoolP384	1	$7 \cdot 11^2 \cdot 241 \cdot 5557 \cdot 125972502705620325124785968921221517$
secp384r1	1	$\mathbf{1}$
Curve41417	2^3	$\mathbf{2^3}$
Ed448	2^2	$\mathbf{2^2}$
M511	2^3	2^2
E521	2^2	$\mathbf{2^2}$

References

Bernstein, Daniel J. (2013). *SafeCurves: choosing safe curves for elliptic-curve cryptography: Twist security*. URL: http://safecurves.cr.yp.to/twist.html.

Shparlinski, Igor E and Daniel Sutantyo (2014). "Distribution of elliptic twin primes in isogeny and isomorphism classes". In: *Journal of Number Theory* 137, pp. 1–15.