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, $E(\mathbb{Z}_q)_j$ be the elliptic curve defined by

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

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

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

where β is a quadratic non-residue in $\mathbb{Z}_q$.
Then

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

for some $T_f(j)$, which is the trace of $E(\mathbb{Z}_q)_j$.
We observe that the mapping between the j-invariant and c, as defined in XXXX, is an isomorphism.

3 Numerical methods

3.1 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.

3.2 Range

We calculate $T_f(j)$for each $E(\mathbb{Z}_q)_j$for $0 < j < 2^2 0, j! = 1728$.

4 Results

q	N_π	$N_{\pi'}$	$N\pi'/N\pi$
P_{224}			
P_{256}			
P_{384}			