finite field question has been definitively answered, but it is conjectured in both cases that the probability that a chosen p has the desired property is $O(1/log\, p)$.

Remark. In order for E *mod* p to have any chance of being of prime order N for large p, E must be chosen so as to have trivial torsion, i.e., to have no points except O of finite order. Otherwise, N will be divisible by the order of the torsion subgroup.

Exercises

1. Give a probabilistic algorithm for finding a nonsquare in $\mathbf{F}_q$.
2. Describe a polynomial time *deterministic* algorithm for imbedding plaintexts m as points on an elliptic curve in the following cases:
   (a) E has equation $y^2 = x^3 - x$ and $q \equiv 3$ *mod* 4.
   (b) E has equation $y^2 + y = x^3$ and $q \equiv 2$ *mod* 3.
3. Let E be the elliptic curve $y^2 + y = x^3 - x$ defined over the field of $p = 751$ elements. (A change of variables of the form $y' = y + 376$ will convert this equation to the form (1) of §1.) This curve contains $N = 727$ points. Suppose that the plaintext message units are the decimal digits 0—9 and the letters A—Z with numerical equivalents 10—35, respectively. Take $\kappa = 20$.
   (a) Use the method in the text to write the message "STOP007" as a sequence of seven points on the curve.
   (b) Translate the sequence of points (361, 383), (241, 605), (201, 380), (461, 467), (581, 395) into a reply message.
4. Let E be an elliptic curve defined over $\mathbf{Q}$, and let p be a large prime, in particular, large enough so that reducing the equation $y^2 = x^3 + ax + b$ modulo p gives an elliptic curve over $\mathbf{F}_p$. Show that (a) if the cubic $x^3 + ax + b$ splits into linear factors modulo p, then E *mod* p is not cyclic; (b) if this cubic has a root modulo p, then the number N of elements on E *mod* p is even.
5. Let E be the elliptic curve in Example 5 of §1. Let $q = 2^r$, and let N_r be the number of $\mathbf{F}_{2^r}$-points on E.
   (a) Show that N_r is never prime for $r > 1$.
   (b) When $4|r$, find conditions that are equivalent to N_r being divisible by an $(r/4)$-bit or $(r/4 + 1)$-bit prime.
6. Let E be an elliptic curve defined over $\mathbf{F}_p$, and let N_r denote the number of $\mathbf{F}_{p^r}$-points on E.
   (a) Prove that if $p > 3$, then N_r is never prime for $r > 1$.
   (b) Give a counterexample to part (a) when $p = 2$ and when $p = 3$.
7. (a) Find an elliptic curve E defined over $\mathbf{F}_4$ which has only one $\mathbf{F}_4$-point (the point at infinity O).
   (b) Show that the number of $\mathbf{F}_{4^r}$-points on the curve in part (a) is the square of the Mersenne number $2^r - 1$.