(c) Find a very simple formula for the double of an $\mathbf{F}_{4^r}$-point on this elliptic curve.

(d) Prove that, if $2^r - 1$ is a Mersenne prime, then every $\mathbf{F}_{4^r}$-point (except O) has exact order $2^r - 1$.

8. Let r be odd, and let K denote the field $\mathbf{F}_{2^r}$. For $z \in K$ let $g(z)$ denote $\sum_{j=0}^{(r-1)/2} z^{2^{2j}}$, and let $tr(z)$ (called the "trace") denote $\sum_{j=0}^{r-1} z^{2^j}$.
(a) Prove that $tr(z) \in \mathbf{F}_2$; $tr(z_1 + z_2) = tr(z_1) + tr(z_2)$; $tr(1) = 1$; and $g(z) + g(z)^2 = z + tr(z)$.
(b) Prove that $tr(z) = 0$ for exactly half of the elements of K and $tr(z) = 1$ for the other half.
(c) Describe a probabilistic algorithm for generating $\mathbf{F}_{2^r}$-points on the elliptic curve $y^2 + y = x^3 + ax + b$.
9. Let E be the elliptic curve $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}$. Let $P \in E$. Let $p > 3$ denote a prime that does not divide either $4a^3 + 27b^2$ or the denominator of the x- or y-coordinate of P. Show that the order of P *mod* p on the elliptic curve E *mod* p is the smallest positive integer k such that either (1) $kP = O$ on E; or (2) p divides the denominator of the coordinates of kP.
10. Let E be the elliptic curve $y^2 + y = x^3 - x$ defined over $\mathbf{Q}$, and let $P = (0,0)$. By computing $2^j P$ for $j = 1, 2, \ldots$, find an example of a prime p such that E *mod* p is *not* generated by P *mod* p. (Note: it can be shown that the point P *does* generate the group of rational points of E.)
11. Use the elliptic curve analog of ElGamal to send the message in Exercise 3(a) with E and p as in Exercise 3 and $B = (0,0)$. Suppose that your correspondent's public key is the point (201, 380) and your sequence of random k's (one used to send each message unit) is 386, 209, 118, 589, 312, 483, 335. What sequence of 7 pairs of points do you send?

    Note that in this exercise we used a rather small value of p; a more realistic example of the sort one would encounter in practice would require working with numbers of several dozen decimal digits.

References for § VI.2

1. G. Agnew, R. Mullin, and S. A. Vanstone, An implementation of elliptic curve cryptosystems over $\mathbf{F}_{2^{155}}$, *IEEE J. Selected Areas in Communications* **11** (1993), 804–813.
2. R. Gupta and M. R. Murty, "Primitive points on elliptic curves," *Compositio Math.* **58** (1986), 13–44.
3. N. Koblitz, "Elliptic curve cryptosystems," *Math. Comp.* **48** (1987).
4. N. Koblitz, "Primality of the number of points on an elliptic curve over a finite field," *Pacific J. Math.* **131** (1988), 157–165.