reciprocal roots of the numerator are both 2; then use the remark at the end of §1. (c) The double of (x, y) is (x^4, y^4) (note that the 4th-power map is the "Frobenius" map, i.e., the generator of the Galois group of $\mathbf{F}_{4^r}$ over $\mathbf{F}_4$). (d) Doubling any point r times gives $(x^{4^r}, y^{4^r}) = (x, y)$, i.e., any $P \in E$ satisfies $2^r P = P$.

8. (a) Use the fact that something is in $\mathbf{F}_2$ if and only if it satisfies $x^2 = x$; and also the fact that $(a+b)^2 = a^2 + b^2$ in a field of characteristic 2. (b) The map $z \mapsto z+1$ gives a 1-to-1 correspondence between the z's with trace 0 and the z's with trace 1. (c) Choose random $x \in \mathbf{F}_{2^r}$, substitute the cubic $x^3 + ax + b$ for z in $g(z)$, and if $z = x^3 + ax + b$ lands in the 50% of elements with trace 0, then the point $(x, g(z))$ is on the curve.
9. When working with E modulo p, one uses the same formulas (4)–(5) of §1, and one gets the point at infinity when one adds two smaller multiples $kP = k_1P + k_2P$ which, when reduced modulo p, have the same x-coordinate and the negative of each other's y-coordinate. That is equivalent to conditions (1)–(2) in the exercise.
10. The denominator of $8P$ is divisible by $p = 23$, and so P *mod* 23 has order 8 on E *mod* 23, by Exercise 9. However, Hasse's theorem shows that E *mod* 23 has more than 8 points.
11. (676, 182), (385, 703); (595, 454), (212, 625); (261, 87), (77, 369); (126, 100), (66, 589); (551, 606), (501, 530); (97, 91), (733, 110); (63, 313), (380, 530).

§ VI.3.

1. (a) $1 - 1/q$; (b) $1 - 1/q$.
3. (a) If $n = 2^{2^k} + 1$ is prime, then any a with $\left(\frac{a}{n}\right) = -1$ has this property. See Exercise 15 of § II.2 concerning $a = 3, 5, 7$. On the other hand, if p is a proper prime divisor of n, and if $a^{2^{2^{k-1}}} \equiv -1$, then 2^{2^k} but not $2^{2^{k-1}}$ is a multiple of the order of a modulo p, i.e., this order is $2^{2^k} = n - 1 > p - 1$, which is impossible. (b) First suppose that $n = 2^p - 1$ is prime. To show that E *mod* n has 2^p points, see Exercise 7(a) of § VI.1. To show that the group is cyclic, prove that there are only two points of order 2, because the cubic $x^3 + x$ has only one root modulo n. Then any of the 50% of the points which generate E *mod* n (i.e., which are not the double of any point in E *mod* n) have the properties (1)–(2). Conversely, suppose that n has a proper prime divisor ℓ. If P satisfied properties (1)–(2), then on E *mod* ℓ the order of P would divide 2^p but not 2^{p-1}, i.e., it would be 2^p. But then $2^p = n+1$ would divide the number of points on E *mod* ℓ, and this contradicts Hasse's theorem, which tells us that this number is $< \ell + 2\sqrt{\ell} + 1$. To generate random points on E *mod* n, choose $x \in \mathbf{Z}/n\mathbf{Z}$ randomly. If $b = x^3 + x$ happens to be a square modulo n, then setting $y = b^{(n+1)/4}$ will give $y^2 \equiv b \cdot b^{(n-1)/2} \equiv x^3 + x$. (See Remark 1 at the end of § II.2.)