10. The denominator of the zeta function is always $(1-T)(1-pT)$; the following table shows the numerator for $p = 5, 7, 11, 13$:

$y^2 = x^3 - x$	$1+2T+5T^2$	$1+7T^2$	$1+11T^2$	$1-6T+13T^2$
$y^2 = x^3 - 1$	$1+5T^2$	$1-4T+7T^2$	$1+11T^2$	$1-2T+13T^2$

11. In both cases there is no solution (x, y) to the equation over $\mathbf{F}_p$, so the only point is the point at infinity. The numerator of the zeta function is $1-2T+2T^2$ and $1-3T+3T^2$, respectively. Then $N_r = \mathbf{N}((1+i)^r - 1)$ and $\mathbf{N}((1+\omega)^r - 1)$, respectively, where $\omega = (-1+i\sqrt{3})/2$.

§ VI.2.

1. Pick elements of $\mathbf{F}_q$ at random, and stop when you find g such that $g^{(q-1)/2} = -1$ (rather than $+1$).
2. Let $x \in \mathbf{F}_q$ correspond to m. (a) Let $f(x) = x^3 - x$. Note that precisely one of $f(x)$, $f(-x) = -f(x)$ is a square. Let $y = f(x)^{(q+1)/4}$. Then show that either (x, y) or $(-x, y)$ is a point on the curve. (b) Choose any y, set $x = (y^2+y)^{(2-q)/3}$ (unless $y = 0$ or -1, in which case set $x = 0$), and show that (x, y) is on the curve.
3. (a) The sequence of points (x, y) is:

   $(562, 576)$, $(581, 395)$, $(484, 214)$, $(501, 220)$, $(1, 0)$, $(1, 0)$, $(144, 565)$.

   (b) ICANT (I can't).
4. (a) $E \bmod p$ has a noncyclic subgroup, namely, the group of points of order 2; (b) $E \bmod p$ has a subgroup of order 2 or 4, namely, the points of order 2.
5. Use the formulas in Example 5 of §1. (a) Use congruence modulo 3 to show that in both cases (r odd and r even) one has $3|N_r$. (b) When $4|r$ we have: $N_r = (2^{r/2} - 1)^2 = (2^{r/4} + 1)^2(2^{r/4} - 1)^2$, which is divisible by an $(r/4)$-bit prime if and only if $r/4$ is a prime for which $2^{r/4} - 1$ is a Mersenne prime; it is divisible by an $(r/4+1)$-bit prime if and only if $r/4 = 2^k$ with $2^{2^k} + 1$ a Fermat prime.
6. (a) The $\mathbf{F}_p$-points then form a proper subgroup of the $\mathbf{F}_{p^r}$-points (by Hasse's theorem), and that subgroup has more than 1 element (also by Hasse's theorem). Thus, N_r has a proper divisor. (b) In both cases let E have equation $y^2 + y = x^3 - x + 1$; one easily checks that over $\mathbf{F}_2$ or $\mathbf{F}_3$ the curve has no points except for the point at infinity O. Thus, the argument in part (a) does not apply, and one finds that when $p = 2$ we have $N_2 = 5$, $N_3 = 13$, $N_5 = 41$, $N_7 = 113$, $N_{11} = 2113$ (note that the zeta–function is $(1 - 2T + 2T^2)/(1-T)(1-2T)$; for r prime N_r is prime if and only if the so-called "complex Mersenne number" $(1+i)^r - 1$ is a prime in the Gaussian integers, or equivalently, if and only if $2^r + 1 - (\frac{2}{r})2^{(r+1)/2}$ is a prime, where $(\frac{2}{r})$ is the Legendre symbol); when $p = 3$ we have $N_2 = 7$, $N_5 = 271$, $N_7 = 2269$ (here the zeta-function is $(1 - 3T + 3T^2)/(1-T)(1-3T)$).
7. (a) $y^2 + y = x^3 + \alpha$, where α is either of the elements of $\mathbf{F}_4$ not in $\mathbf{F}_2$. (b) The zeta-function is $(1 - 4T + 4T^2)/(1-T)(1-4T)$, and the two