$$Z(T; E/\mathbf{F}_q) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}, \tag{8}$$

where only the integer a depends on the particular elliptic curve E. The value a is related to $N = N_1$ as follows: $N = q + 1 - a$. In addition, the discriminant of the quadratic polynomial in the numerator is negative (i.e., $a^2 < 4q$, which is Hasse's Theorem) and so the quadratic has two complex conjugate roots α, β both of absolute value $\sqrt{q}$. (More precisely, $1/\alpha$ and $1/\beta$ are the roots, and α, β are the "reciprocal roots.")

For a proof, see § V.2 of Silverman's book.

Remark. If we write the numerator of (8) in the form $(1-\alpha T)(1-\beta T)$ and then take the derivative of the logarithm of both sides (replacing the left side by its definition (7)), we soon see that the formula (8) is equivalent to writing the sequence of relations

$$N_r = q^r + 1 - \alpha^r - \beta^r, \qquad r = 1, 2, \ldots.$$

Since α and β, along with a, are determined once you know $N = N_1$, this means that the number of points over $\mathbf{F}_q$ uniquely determines the number of points over any extension field. Thus, among other things, Weil's conjectures for elliptic curves are useful for determining the number of points over extension fields of large degree.

Example 5. The zeta-function of the elliptic curve $y^2 + y = x^3$ over $\mathbf{F}_2$ is easily computed from the fact that there are three $\mathbf{F}_2$-points. It is $(1 + 2T^2)/(1 - T)(1 - 2T)$, i.e., the reciprocal roots of the numerator are $\pm i\sqrt{2}$. This leads to the formula

$$N_r = \begin{cases} 2^r + 1, & \text{if } r \text{ is odd;} \\ 2^r + 1 - 2(-2)^{r/2}, & \text{if } r \text{ is even.} \end{cases} \tag{9}$$

To conclude this section, we remark that there are many analogies between the group of $\mathbf{F}_q$-points on an elliptic curve and the multiplicative group $(\mathbf{F}_q)^*$. For example, they have approximately the same number of elements, by Hasse's Theorem. But the former construction of an abelian group has a major advantage that explains its usefulness in cryptography: for a single (large) q there are many different elliptic curves and many different N that one can choose from. Elliptic curves offer a rich source of "naturally occurring" finite abelian groups. We shall take advantage of this in the next three sections.

Exercises

1. If E is an elliptic curve defined over $\mathbf{C}$ whose equation (1) actually has coefficients $a, b \in \mathbf{R}$, then the points of E with real coordinates form a subgroup. What are the possible subgroups of the complex curve E (which as a group is isomorphic to the product of the circle group with