

Let  $E$  be an elliptic curve defined over the finite field  $F_q$  with  $q = p^k$  elements. Since any element of our field will also be in  $F_{q^r}$ , for integers  $r \geq 1$ , every point on  $E$  will also be a point on the curve with the same equation defined over  $F_{q^r}$ .

We let  $N_r$  be the number of points on the curve with the same equation as  $E$  which is defined over the field  $F_{q^r}$ . We then define a generating function  $Z(E; T)$  as:

$$Z(E; T) = \exp\left(\sum_{r=1}^{\infty} (N_r) \frac{T^r}{r}\right)$$

The idea is that this function will “keep track” of our values  $N_r$ . The log of this function is a polynomial of infinite degree, and can therefore be thought of as an infinite length vector whose  $r$ th component corresponds to the coefficient of  $T^r$  and has the value  $\frac{N_r}{r}$ . If we differentiate this polynomial  $r$  times, we’ll end up with a polynomial whose constant term is equal to  $(r-1)!N_r$ . Evaluating this polynomial at  $T = 0$  and dividing by  $(r-1)!$  will therefore recover  $N_r$ . Thus:

$$N_r = \frac{1}{(r-1)!} \frac{d^r}{dT^r} \log Z(E; T) \Big|_{T=0}$$

The so-called Weil Conjecture states that:

$$Z(E; T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}$$

where  $a = q + 1 - N_1$ . Applying Hasse’s Theorem to the numerator, we see that its discriminant is negative and therefore we get:

$$Z(E; T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}$$

where  $\alpha, \beta$  are the complex conjugate roots of the numerator. Combining this with our expression for  $N_r$  we find that  $N_r = 1 - \alpha^r - \beta^r + q^n$ .