$\chi((-x)^3-(-x)) = \chi(-1)\chi(x^3-x)$, and $\chi(-1) = -1$ because $71 \equiv 3 \mod 4$. Thus, $N = q+1 = 72$. Notice that there are exactly four points of order 2 (including the identity O), because they correspond to the roots of $x^3 - x = x(x-1)(x+1)$ (see Exercise 4(a) below). This means that the 2-primary part of the group has type $(4, 2)$, and so the type of the group is either $(4, 2, 3, 3)$ or else $(4, 2, 9)$, depending on whether there are 9 or 3 points of order 3, respectively. So it remains to determine whether or not there can be 9 points of order 3. Note that for any $P \neq O$ the equation $3P = O$ is equivalent to $2P = \pm P$, i.e., to the condition that the x-coordinates of P and $2P$ be the same. By (5), this means that $((3x^2-1)/2y)^2 - 2x = x$, i.e., $(3x^2-1)^2 = 12xy^2 = 12x^4 - 12x^2$. Simplifying, we obtain $3x^4 - 6x^2 - 1 = 0$. There are at most 4 roots to this equation in $\mathbf{F}_{71}$. If there are four roots, then each root can give at most 2 points (by taking $y = \pm\sqrt{x^3-x}$ if $x^3 - x$ has a square root modulo 71), and so we may in this way obtain 9 points of order 3 (including the identity O at infinity). Otherwise, there must be fewer than 9 points of order 3 (and hence exactly 3 points of order 3). But if the root x of the quartic polynomial has $x^3 - x$ a square modulo 71, then the root $-x$ of the quartic has $(-x)^3 - (-x) = -(x^3 - x)$ a nonsquare modulo 71. Thus, we cannot get 9 points of order 3, and so the type of the group is $(4, 2, 9)$.

Extensions of finite fields, and the Weil conjectures. If an elliptic curve E is defined over $\mathbf{F}_q$, then it is also defined over $\mathbf{F}_{q^r}$ for $r = 1, 2, \ldots$, and so it is meaningful to consider the $\mathbf{F}_{q^r}$-points, i.e., to look at solutions of (1) over extension fields. If we start out with $\mathbf{F}_q$ as the field over which E is defined, we let N_r denote the number of $\mathbf{F}_{q^r}$-points on E. (Thus, $N_1 = N$ is the number of points with coordinates in our "ground field" $\mathbf{F}_q$.)

From the numbers N_r one forms the "generating series" $Z(T; E/\mathbf{F}_q)$, which is the formal power series in $\mathbf{Q}[[T]]$ defined by setting

$$Z(T; E/\mathbf{F}_q) = e^{\sum N_r T^r/r}, \tag{7}$$

in which T is an indeterminate, the notation $E/\mathbf{F}_q$ designates the elliptic curve and the field we're taking as our ground field, and the sum on the right is over all $r = 1, 2, \ldots$. It can be shown that the series on the right (obtained by taking the infinite product of the exponential power series $e^{N_r T^r/r}$) actually has positive integer coefficients. This power series is called the *zeta-function* of the elliptic curve (over $\mathbf{F}_q$), and is a very important object associated with E.

The "Weil conjectures" (now a theorem of P. Deligne) say in a much more general context (algebraic varieties of any dimension) that the zeta-function has a very special form. In the case of an elliptic curve $E/\mathbf{F}_q$ Weil proved the following.

Weil conjectures [theorem] for an elliptic curve. *The zeta-function is a rational function of T having the form*