shall assume that the characteristic is > 3, so that elliptic curves are given by equation (1) in §1; one makes the obvious modifications if $q = 2^r$ or 3^r.) First let x, y, a be three random elements of $\mathbf{F}_q$. Then set $b = y^2 - (x^3 + ax)$. Check that the cubic $x^3 + ax + b$ does not have multiple roots, which is equivalent to: $4a^3 + 27b^2 \neq 0$. (If this condition is not met, make another random choice of x, y, a.) Set $B = (x, y)$. Then B is a point on the elliptic curve $y^2 = x^3 + ax + b$.

If you need to know the number N of points, there are several techniques now available for computing N. The first polynomial time algorithm to compute $\#E$ was discovered by René Schoof. Schoof's algorithm is even deterministic. It is based on the idea of finding the value of $\#E$ modulo l for all primes l less than a certain bound. This is done by examining the action of the "Frobenius" (the p-th power map) on points of order l.

In Schoof's original paper the bound for running time was essentially $O(\log^8 q)$, which is polynomial but quite unpleasant. At first it looked like the algorithm was not practical. However, since then many people have worked on speeding up Schoof's algorithm (V. Miller, N. Elkies, J. Buchmann, V. Müller, A. Menezes, L. Charlap, R. Coley, and D. Robbins). In addition, A. O. L. Atkins has developed a somewhat different method that, while not guaranteed to work in polynomial time, functions extremely well in practice. As a result of all of these efforts it has become feasible to compute the order of an arbitrary elliptic curve over $\mathbf{F}_q$ if q is, say, a 50-digit or even a 100-digit prime power. Some of the methods for computing the number of points on an elliptic curve are discussed in the references listed at the end of the section.

It should also be remarked that, even though one does not have to know N in order to implement the Diffie–Helman or the ElGamal system, in practice one wants to be confident in its security, which depends upon N having a large prime factor. If N is a product of small primes, then the method of Pohlig–Silver–Hellman (see §IV.3) can be used to solve the discrete log problem. Note that the Pohlig–Silver–Hellman method carries over to the discrete log problem in any finite abelian group (unlike the index–calculus algorithm also discussed in §IV.3, which depends upon the specific nature of $\mathbf{F}_q^*$). Thus, one has to know that N is not a product of small primes, and it is not likely that you will know this unless you have the actual value of N.

Reducing a global (E, B) modulo p. We now mention a second way to determine a pair consisting of an elliptic curve and a point on it. We first choose once and for all a "global" elliptic curve and a point of infinite order on it. Thus, let E be an elliptic curve defined over the field of rational numbers (or, more generally, we could use an elliptic curve defined over a number field), and let B be a point of infinite order on E.

Example 2. It turns out that the point $B = (0,0)$ is a point of infinite order on the elliptic curve $E: y^2 + y = x^3 - x$, and in fact generates the entire group of rational points on E.