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

Next, we choose a large prime p (or, if our elliptic curve is defined over an extension field K of $\mathbf{Q}$, then we choose a prime ideal of K) and consider the *reduction* of E and B modulo p. More precisely, for all p except for some small primes the coefficients in the equation for E have no p in their denominators, so we may consider the coefficients in this equation modulo p. If we make a change of variables taking the resulting equation over $\mathbf{F}_p$ to the form $y^2 = x^3 + ax + b$, the cubic on the right has no multiple roots (except in the case of a few small primes p), and so gives an elliptic curve (which we shall denote E *mod* p) over $\mathbf{F}_p$. The coordinates of B will also reduce modulo p to give a point (which we shall denote B *mod* p) on the elliptic curve E *mod* p.

When we use this second method, we fix E and B once and for all, and then get many different possibilities by varying the prime p.

Order of the point B. What are the chances that a "random" point B on a "random" elliptic curve is a generator? Or, in the case of our second method of selecting (E, B), what are the chances, as p varies, that the point B reduces modulo p to a generator of E *mod* p? This question is closely analogous to the following question concerning the multiplicative groups of finite fields: Given an integer b, what are the chances, as p varies, that b is a generator of $\mathbf{F}_p^*$? The question has been studied both in the finite–field and elliptic–curve situations. For further discussion, see the paper by Gupta and Murty cited in the references.

As mentioned before, for the security of the above cryptosystems it is not really necessary for B to be a generator. What is needed is for the cyclic subgroup generated by B to be a group in which the discrete log problem is intractible. This will be the case — i.e., all known methods for solving the discrete logarithm problem in an arbitrary abelian group will be very slow — provided that the order of B is divisible by a very large prime, say, having order of magnitude almost as large as N.

One way to guarantee that our choice of B is suitable — and, in fact, that B generates the elliptic curve — is to choose our elliptic curve and finite field so that the number N of points is itself a prime number. If we do that, then every point $B \neq O$ will be a generator. Thus, if we use the first method described above, then for a fixed $\mathbf{F}_q$ we might keep choosing pairs (E, B) until we find one for which the number of points on E is a prime number (as determined by one of the primality tests discussed in § V.1). If we use the second method, then for a fixed global elliptic curve E over $\mathbf{Q}$ we keep choosing primes p until we find a prime for which the number of points on E *mod* p is a prime number. How long are we likely to have to wait? This question is analogous to the following question about the groups $\mathbf{F}_p^*$: is $(p-1)/2$ prime, i.e., is any element $\neq \pm 1$ either a generator or the square of a generator (see Exercise 13 of § II.1)? Neither the elliptic curve nor the