tation is uneventful and useless, unless we run into the following difficulty: when attempting to find the inverse of $x_2 - x_1$ in the formula (4) of §1 or the inverse of $2y_1$ in (5), we encounter a number that is *not* prime to n. According to Proposition VI.3.1, this will happen when we have some multiple k_1P (a partial sum encountered along the way in our computation of kP) which for some $p|n$ has the property $k_1(P \; mod \; p) = O \; mod \; p$, i.e., the point $P \; mod \; p$ in the group $E \; mod \; p$ has order dividing k_1. In the process of using the Euclidean algorithm to try to find the inverse modulo n of a denominator which is divisible by p, we instead find the *g.c.d.* of n with that denominator. That *g.c.d.* will be a proper divisor of n, unless it is n itself, i.e., unless the denominator is divisible by n. That would mean, by Proposition VI.3.1, that $k_1P \; mod \; p = O \; mod \; p$ for *all* prime divisors p of n — something which is highly unlikely if n has two or more very large prime divisors. Thus, it is virtually certain that as soon as we try to compute k_1P modulo n for a k_1 which is a multiple of the order of $P \; mod \; p$ for some $p|n$, we will obtain a proper divisor of n.

Notice the similarity with Pollard's $p-1$ method. Instead of the group $(\mathbf{Z}/p\mathbf{Z})^*$, we are using the group $E \; mod \; p$. However, this time, if our E proves to be a bad choice — i.e., for each $p|n$ the group $E \; mod \; p$ has order divisible by a large prime (and so $kP \; mod \; p$ is not likely to equal $O \; mod \; p$ for k given by (2)) — all we have to do is throw it away and pick out another elliptic curve E together with a point $P \in E$. We did not have such an option in the Pollard method.

The algorithm. Let n be a positive odd composite integer. We now describe Lenstra's probabilistic method for factoring n.

We suppose we have a method for generating pairs (E, P) consisting of an elliptic curve $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}$ and a point $P = (x, y) \in E$. Given such a pair, we go through the procedure about to be described. If that procedure fails to yield a nontrivial factor of n, then we generate a new pair (E, P) and repeat the process.

Before working with our E modulo n, we must verify that it is in fact an elliptic curve modulo any $p|n$, i.e., that the cubic on the right has distinct roots modulo p. This holds if and only if the discriminant $4a^3 + 27b^2$ is prime to n. Thus, if $g.c.d.(4a^3 + 27b^2, n) = 1$, we may proceed. Of course, if this *g.c.d.* is strictly between 1 and n, we have a divisor of n, and we're done. If this *g.c.d.* equals n, then we must choose a different elliptic curve.

Next, we suppose that we have chosen two positive integer bounds B, C. Here B is a bound for the prime divisors of the integer k by which we multiply the point P. If B is large, then there is a greater probability that our pair (E, P) has the property that $kP \; mod \; p = O \; mod \; p$ for some $p|n$; on the other hand, the larger B the longer it will take to compute $kP \; mod \; p$. So B must be chosen in some way which we estimate minimizes the running time. C, roughly speaking, is a bound for the prime divisors $p|n$ for which we are at all likely to obtain a relation $kP \; mod \; p = O \; mod \; p$. We then choose k to be given by (2), i.e., k is the product of all prime powers $\leq C$