$$\begin{aligned} y_2^2 &= (x_1 + p^r x)^3 + a(x_1 + p^r x) + b \\ &\equiv x_1^3 + ax_1 + b + p^r x(3x_1^2 + a) = y_1^2 + p^r x(3x_1^2 + a) \; mod \; p^{r+1}. \end{aligned} \tag{1}$$

But since $x_2 \equiv x_1 \; mod \; p$ and $y_2 \equiv y_1 \; mod \; p$, it follows that $P_1 \; mod \; p = P_2 \; mod \; p$, and so $P_1 \; mod \; p + P_2 \; mod \; p = 2P_1 \; mod \; p$, which is $O \; mod \; p$ if and only if $y_1 \equiv y_2 \equiv 0 \; mod \; p$. If the latter congruence held, then $y_2^2 - y_1^2 = (y_2 - y_1)(y_2 + y_1)$ would be divisible by p^{r+1} (i.e., its numerator would be), and so the congruence (1) would imply that $3x_1^2 + a \equiv 0 \; mod \; p$. This is impossible, because the polynomial $x^3 + ax + b$ modulo p has no multiple roots, and so x_1 cannot be a root both of this polynomial and its derivative modulo p. We conclude that $P_1 \; mod \; p + P_2 \; mod \; p \neq O \; mod \; p$, as claimed.

Conversely, suppose that for all prime divisors p of n we have $P_1 \; mod \; p + P_2 \; mod \; p \neq O \; mod \; p$. We must show that the coordinates of $P_1 + P_2$ have denominators prime to n, i.e., that the denominators are not divisible by p for any $p|n$. Fix some $p|n$. If $x_2 \not\equiv x_1 \; mod \; p$, then the formula (4) of §1 shows that there are no denominators divisible by p. So suppose that $x_2 \equiv x_1 \; mod \; p$. Then $y_2 \equiv \pm y_1 \; mod \; p$; but since $P_1 \; mod \; p + P_2 \; mod \; p \neq O \; mod \; p$, we must have $y_2 \equiv y_1 \not\equiv 0 \; mod \; p$. First, if $P_2 = P_1$, then the formula (5) of §1 together with the fact that $y_1 \not\equiv 0 \; mod \; p$ shows that the coordinates of $P_1 + P_2 = 2P_1$ have denominators prime to p. Finally, if $P_2 \neq P_1$, we again write $x_2 = x_1 + p^r x$ with x not divisible by p, and we use the congruence (1) above to write $(y_2^2 - y_1^2)/(x_2 - x_1) \equiv 3x_1^2 + a \; mod \; p$. Since p does not divide $y_2 + y_1 \equiv 2y_1 \; mod \; p$, it follows that there is no p in the denominator of $\frac{y_2^2 - y_1^2}{(y_2+y_1)(x_2-x_1)} = \frac{y_2 - y_1}{x_2 - x_1}$, and hence, by formula (4) of §1, there is no p in the denominator of the coordinates of $P_1 + P_2$. This completes the proof.

Lenstra's method. We are given a composite odd integer n and want to find a nontrivial factor $d|n$, $1 < d < n$. We start by taking some elliptic curve $E : y^2 = x^3 + ax + b$ with integer coefficients along with a point $P = (x, y)$ on it. The pair (E, P) is probably generated in some random way, although we could choose to use some deterministic method which is capable of generating many such pairs (as in Example 4 below). We attempt to use E and P to factor n, as will be presently explained; if our attempt fails, we take another pair (E, P), and continue in this way until we find a factor $d|n$. If the probability of failure is $\rho < 1$, then the probability that h successive choices of (E, P) all fail is ρ^h, which is very small for h large. Thus, with a very high probability we will factor n in a reasonable number of tries.

Once we have a pair (E, P), we choose an integer k which is divisible by powers of small primes ($\leq B$) which are less than some bound C. That is, we set

$$k = \prod_{\ell \leq B} \ell^{\alpha_\ell}, \tag{2}$$

where $\alpha_\ell = \left[log\, C / log\, \ell \right]$ is the largest exponent such that $\ell^{\alpha_\ell} \leq C$. We then attempt to compute kP, working all the time modulo n. This compu-