$383 \cdot 1283$. We have $383 - 1 = 2 \cdot 191$ and $1283 - 1 = 2 \cdot 641$ (both 191 and 641 are primes). Except for $a \equiv 0, \pm 1$ *mod* 383, all other a's have order modulo 383 either 191 or 382; and except for $a \equiv 0, \pm 1$ *mod* 1283, all other a's have order modulo 1283 either 641 or 1282. So unless k is divisible by 191 (or 641), we are likely to find again and again that $g.c.d.(a^k - 1, n) = 1$ in step 4.

The basic dilemma with Pollard's $p - 1$ method is that we are pinning our hopes on the group $(\mathbf{Z}/p\mathbf{Z})^*$ (more precisely, the various such groups as p runs through the prime divisors of n). For a fixed n, these groups are fixed. If all of them happen to have order divisible by a large prime, we are stuck.

The key difference in Lenstra's method, as we shall see, is that, by working with elliptic curves over $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, we suddenly have a whole gaggle of groups to use, and we can realistically hope always to find one whose order is not divisible by a large prime or prime power.

We start our description of Lenstra's algorithm with some comments about reducing points on elliptic curves modulo n, where n is a composite integer (unlike in §2, where we worked modulo prime numbers and in finite fields).

Elliptic curves — reduction modulo n. For the remainder of the section we let n denote an odd composite integer and p an (as yet unknown) prime factor of n. We shall suppose that $p > 3$. For any integer m and any two rational numbers x_1, x_2 with denominators prime to m, we shall write $x_1 \equiv x_2$ *mod* m if $x_1 - x_2$, written in lowest terms, is a fraction with numerator divisible by m. For any rational number x_1 with denominator prime to m there is a unique integer x_2 (called the "least nonnegative residue") between 0 and $m - 1$ such that $x_1 \equiv x_2$ *mod* m. Sometimes we shall write "x_1 *mod* m" to denote this least nonnegative residue.

Suppose that we have an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}$ and a point $P = (x, y)$ which satisfies it. In practice, the curve E together with the point P will be generated in some "random" way, for example, by choosing three random integers a, x, y in some range and then setting $b = y^2 - x^3 - ax$. We shall assume that the cubic has distinct roots, i.e., $4a^3 + 27b^2 \neq 0$; this is almost certain if the coefficients were chosen in the random way described. For simplicity, in what follows we shall also suppose that $4a^3 + 27b^2$ has no common factor with n; in other words, $x^3 + ax + b$ has no multiple roots modulo p for any prime divisor p of n. In practice, once we have made a choice of a and b, we can check this by computing $g.c.d.(4a^3 + 27b^2, n)$. If this is > 1, then either $n | 4a^3 + 27b^2$ (in which case we must make another choice of a and b) or else we have obtained a nontrivial divisor of n (in which case we're done). So we shall suppose that $g.c.d.(4a^3 + 27b^2, n) = 1$.

Now suppose that we want to find the multiple kP, using the repeated doubling method described in § VI.2. This can be done in $O(log\ k)$ steps, each involving a doubling or an addition of two distinct points. There are