obtain a new factorization method that in many respects is better than the earlier known ones. The improvement in efficiency is not significant enough in practice to pose a threat to the security of cryptosystems based on the assumed intractability of factoring (its time estimate has the same form that we encountered in § V.3); nevertheless, the discovery of an improvement using an unexpected new device serves as a warning that one should never be too complacent about the supposed imperviousness of the factoring problem to dramatic breakthroughs. The purpose of this final section is to describe Lenstra's method.

Before proceeding to Lenstra's elliptic curve factorization algorithm, we give a classical factoring technique which is analogous to Lenstra's method.

Pollard's $p-1$ method. Suppose that we want to factor the composite number n, and p is some (as yet unknown) prime factor of n. If p happens to have the property that $p-1$ has no large prime divisor, then the following method is virtually certain to find p.

The algorithm proceeds as follows:

1. Choose an integer k that is a multiple of all or most integers less than some bound B. For example, k might be $B!$, or it might be the least common multiple of all integers $\leq B$.
2. Choose an integer a between 2 and $n-2$. For example, a could equal 2, or 3, or a randomly chosen integer.
3. Compute $a^k \ mod \ n$ by the repeated squaring method.
4. Compute $d = g.c.d.(a^k - 1, n)$ using the Euclidean algorithm and the residue of a^k modulo n from step 3.
5. If d is not a nontrivial divisor of n, start over with a new choice of a and/or a new choice of k.

To explain when this algorithm will work, suppose that k is divisible by all positive integers $\leq B$, and further suppose that p is a prime divisor of n such that $p-1$ is a product of small prime powers, all less than B. Then it follows that k is a multiple of $p-1$ (because it is a multiple of all of the prime powers in the factorization of $p-1$), and so, by Fermat's Little Theorem, we have $a^k \equiv 1 \ mod \ p$. Then $p | g.c.d.(a^k - 1, n)$, and so the only way we could fail to get a nontrivial factor of n in step 4 is if it so happens that $a^k \equiv 1 \ mod \ n$.

Example 1. We factor $n = 540143$ by this method, choosing $B = 8$ (and hence $k = 840$, which is the least common multiple of $1, 2, \ldots, 8$) and $a = 2$. We find that $2^{840} \ mod \ n$ is 53047, and $g.c.d.(53046, n) = 421$. This leads to the factorization $540143 = 421 \cdot 1283$.

The main weakness of the Pollard method is clear if we attempt to use it when all of the prime divisors p of n have $p-1$ divisible by a relatively large prime (or prime power).

Example 2. Let $n = 491389$. We would be unlikely to find a nontrivial divisor until we chose $B \geq 191$. This is because it turns out that $n =$