Pollard’s $p - 1$ Method

**Given:** An integer $n$ (known to be composite).

**Task:** Find a proper divisor $d | n$.

**Procedure:**

0) Fix an integer $B$.

1) Choose an integer $k$ which is a multiple of most (or of all) of the numbers $b \leq B$; e.g. $k = B!$.

2) Choose a (random) number $a$ with $2 \leq a \leq n - 2$.

3) Compute $r = \text{rem}(a^k, n)$ by the power-mod method.

4) Compute $d = (r - 1, n)$ by the Euclidean algorithm.

5) If $d = 1$ or $d = n$, start over (new $a$ or new $k$). Otherwise: $d | n$ is a proper divisor of $n$.

**Example 1:** $n = 540, 143$.

Take $B = 8$ and $k = \text{lcm}(2, 3, \ldots, 8) = 840$. Choose $a = 2$. Then $r = \text{rem}(2^{840}, n) = 53,047$ and $d = (r - 1, n) = 421$. Thus: $n = 421 \cdot 1283$.

**Example 2:** $n = 491, 389 = 383 \cdot 1283$.

Since $383 - 1 = 2 \cdot 191$, we must take $B \geq 191$ for the method to be successful. Thus $k$ has to be huge and so the method is not practical in this case.