Numerical Introductory Seminar - Prime Factorization
Anna Friesen

Motivation:	The cryptosystem RSA multiplies two large primes to create one part of the keys
Example:	Trial Division (inefficient for large prime factors)
Modification:	Test in Trial Division only primes
Sieve of Eratosthenes:	Creates list of primes (and zeros)

Code in Mathematica (Sieve of Eratosthenes)

```
SoE[n]:=Module[{v = Table[t, {t, 1, n}], y = 2, k},
v = ReplacePart[v, 0, 1];
While[y * y ≤ n, k = y + y;
    While[k ≤ n,
        v = ReplacePart[v, 0, k];
        k = k + y];
    y = y + 1];
    Return[v]]
```

Pollard (p-1) factorization method

Theoretical base:	Fermat´s little theorem
Previous algorithm:	Pollard rho method

Algorithm (Pollard (p-1) factorization method)

1. Input: $n \geq 2$
2. choose a with $1 \leq a \leq n-1$ and arbitrary $B \in \mathbb{N}$
3. $\forall q \in \mathbb{P}, q \leq B$:
   - $a := a^q \pmod{n}$
   - $p := gcd(a-1, n)$
   - if $p \mid n$ break
   - else select new a and go to step 3
4. return p