$p-1$ Factorization Method

Justin Wyss-Gallifent

February 27, 2022

0.1 What it Does

Finds a factor of a number n.

0.2 How it Works

Suppose we wish to factor n. We follow these steps:

1. Choose a base a and a large B. Generally a is fairly small.
2. Compute $b \equiv a^{B!} \mod n$ progressively. Note that $a^{B!}$ itself can be very large so it's best not to calculate it directly. Instead we note that:

$$a^{B!} = \left(\left(\left(a^1\right)^2\right)^3 ...\right)^B$$

   So we progressively raise to powers and mod as we go.

3. Let $d = \gcd(b-1, n)$ and hope we get a factor.

0.3 Why it Works

If n has a prime factor p such that $p-1$ has only "small" prime factors then chances are that $(p-1) \mid B!$ because $B! = (B)(B-1)...(3)(2)(1)$ and so chances are that all the factors of $p-1$ appear within factors of $B!$.

If this is the case then $B! = k(p-1)$ for $k \in \mathbb{Z}$ and then:

$$b \equiv a^{B!} \equiv \left(a^{p-1}\right)^k \equiv 1^k \equiv 1 \mod p$$

Note that since a is fairly small we probably have $a < p-1$ and hence $p \nmid a$ and Fermat's Little Theorem applies.

From here we get $p \mid (b-1)$ and since $p \mid n$ we have $\gcd(b-1, p) \neq 1$.

0.4 Notes

Choosing a larger B will result in a higher probability of picking up all factors of $p-1$ but it will be more computationally intensive.

0.5 Examples

Using the following un-optimized Python code:

Here is my code:

```
import sys
import math
n = int(sys.argv[1])
a = int(sys.argv[2])
B = int(sys.argv[3])
# Calculate b = a^(B!) mod n
b = a
p = 1
while p <= B:
    b = pow(b,p,n)
    p = p + 1
g = math.gcd(b-1,n)
print(b)
print(g)
```

These results were produced almost instantly:

$n = 569482811$ with $a = 2$ and $B = 1000$ ends with $b = 288830325$ and $\gcd(288830325 - 1, 569482811) = 1439$.

$n = 22122361361$ with $a = 2$ and $B = 10000$ ends with $b = 7654936140$ and $\gcd(7654936140 - 1, 22122361361) = 111317$. Here $n = 22122361361$ is the product of two six-digit primes.

$n = 16461679220973794359$ with $a = 2$ and $B = 1000000$ ends with $b = 175964042692823278$ and $\gcd(175964042692823278 - 116461679220973794359) = 2860486313$. Here $n = 16461679220973794359$ is the product of two ten-digit primes.