Pollard p – 1 Method.

$$p = \gcd(2^{B!} - 1, n)$$

John pollard developed a method that finds a prime factor ‘p’ of a number based on the condition that p-1 has no factor larger than a predefined value ‘B’, called the bound.

Algorithm 9.5 *Pseudocode for Pollard p −1 factorization*

```
Pollard_ (p − 1) _Factorization (n, B)              // n is the number to be factored
{
    a ← 2
    e ← 2
    while (e ≤ B)
    {
        a ← a^e mod n
        e ← e + 1
    }
    p ← gcd (a −1, n)
    if 1 < p < n    return p
    return failure
}
```

Pollard p – 1 Method Continued

Example

Use the Pollard $p - 1$ method to find a factor of 57247159 with the bound B = 8.

Pollard p – 1 Method Continued

Example

Use the Pollard $p - 1$ method to find a factor of 57247159 with the bound B = 8.

Solution

Factors for $57247159 = 421 \times 135979$

Note that 421 is a prime and $p - 1$ has no factor greater than 8

$$421 - 1 = 2^2 \times 3 \times 5 \times 7$$

Pollard p – 1 Method Example-1

Use Pollard's p-1 method to factor N=13927189. Starting with gcd($2^{9!}$-1, N) and take successively large factorials in the exponent.

Pollard p – 1 Method Example-1

Example 3.29. We use Pollard's $p-1$ method to factor $N = 13927189$. Starting with $\gcd(2^{9!}-1, N)$ and taking successively larger factorials in the exponent, we find that

$$\begin{aligned}
2^{9!}-1 &\equiv 13867883 \pmod{13927189}, & \gcd(2^{9!}-1, 13927189) &= 1,\\
2^{10!}-1 &\equiv 5129508 \pmod{13927189}, & \gcd(2^{10!}-1, 13927189) &= 1,\\
2^{11!}-1 &\equiv 4405233 \pmod{13927189}, & \gcd(2^{11!}-1, 13927189) &= 1,\\
2^{12!}-1 &\equiv 6680550 \pmod{13927189}, & \gcd(2^{12!}-1, 13927189) &= 1,\\
2^{13!}-1 &\equiv 6161077 \pmod{13927189}, & \gcd(2^{13!}-1, 13927189) &= 1,\\
2^{14!}-1 &\equiv 879290 \pmod{13927189}, & \gcd(2^{14!}-1, 13927189) &= 3823.
\end{aligned}$$

The final line gives us a nontrivial factor $p = 3823$ of N. This factor is prime, and the other factor $q = N/p = 13927189/3823 = 3643$ is also prime. The reason that an exponent of 14! worked in this instance is that $p-1$ factors into a product of small primes,

$$p - 1 = 3822 = 2 \cdot 3 \cdot 7^2 \cdot 13.$$

The other factor satisfies $q - 1 = 3642 = 2 \cdot 3 \cdot 607$, which is not a product of small primes.

Pollard p – 1 Method Example 2

Factor the large number N=168441398857 using Pollard "p-1" method

$$2^{50!} - 1 \equiv 114787431143 \pmod{N}, \qquad \gcd(2^{50!} - 1, N) = 1,$$
$$2^{51!} - 1 \equiv 36475745067 \pmod{N}, \qquad \gcd(2^{51!} - 1, N) = 1,$$
$$2^{52!} - 1 \equiv 67210629098 \pmod{N}, \qquad \gcd(2^{52!} - 1, N) = 1,$$
$$2^{53!} - 1 \equiv 8182353513 \pmod{N}, \qquad \gcd(2^{53!} - 1, N) = 350437.$$

So using $2^{53!} - 1$ yields the prime factor $p = 350437$ of N, and the other (prime) factor is 480661. We were lucky, of course, that $p - 1$ is a product of small factors,

$$p - 1 = 350436 = 2^2 \cdot 3 \cdot 19 \cdot 29 \cdot 53.$$