"Pollard's Algorithm"
John Smith

Pollard's $p-1$ algorithm

Pollard's $p-1$ *method* is an integer factorization algorithm devised by John Pollard in 1974 to take advantage of Fermat's little theorem. Theoretically, trial division always returns a result (though of course in practice the computing engine's resources could be exhausted or the user might not to be around to care for the result). Pollard's $p-1$ algorithm, on the other hand, was designed from the outset to cope with the possibility of failure to return a result.
Choose a test cap B and call Pollard's $p-1$ algorithm with a positive integer.

1. Use a simple method (such as the sieve of Eratosthenes) to find primes $p \quad B$, or even probable primes.
2. Choose an integer a coprime to n . If n is odd (which can be tested easily enough by looking at the least significant bit) then one possible choice is$a=2$. For even n , we could choose $\lfloor\sqrt{n}\rfloor+1$.
3. Find the exponent e such that $p^e \leq B$. Then for each $p<B$, compute $b=a^{p^e} \bmod n$ and see if $1<\gcd(b-1,n)<n$. If that's the case, return those results of the greatest common divisor function, exit.
4. If the GCD function consistently returned 1s, one could try a higher test cap and try again from step 1.
5. If the GCD function consistently returned n itself, this could indicate that a is in fact not coprime to n , in which case one could try going back to step 2 to pick a different a .
6. Throw a failure exception.

For example, $n=221$. Of course it's overkill to use the Pollard $p-1$ algorithm on such a small number, but it helps to keep the example simple. Since the running time of the algorithm is exponential, Crandall and Pomerance suggest picking small B . So for this example let's pick $B=10$, the primes are then 2, 3, 5, 7, and the exponents are 3, 2, 1, 1. Since 221 is odd, we try $a=2$. So we see that $2^8 \bmod 221=35$, and $\gcd(34,221)=17$. We also see$3^9 \bmod 221=14$ and $\gcd(13,221)=13$. Multiplication immediately verifies that $13 \times 17=221$.

Source URL: http://planetmath.org/encyclopedia/PollardsP1Algorithm.html
Saylor URL: http://www.saylor.org/courses/cs409

Attributed to [John Smith]
(cc) BY-SA

As of version 5.2, Pollard's $p-1$ algorithm is one of the methods used by Mathematica's `FactorInteger` function after ferreting out small factors by trial division.

Bibliography

1

R. Crandall & C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, NY, 2001: 5.4.1

Pollard's $p-1$ algorithm is owned by John Smith.

View style:

Source URL: http://planetmath.org/encyclopedia/PollardsP1Algorithm.html
Saylor URL: http://www.saylor.org/courses/cs409

Attributed to [John Smith]
(cc) BY-SA