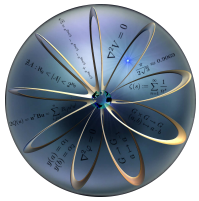

# planetmath.org

Math for the people, by the people.

## echelon factoring algorithm

| | |
|---|---|
| Canonical name | EchelonFactoringAlgorithm |
| Date of creation | 2013-03-22 19:36:43 |
| Last modified on | 2013-03-22 19:36:43 |
| Owner | leavemsg2 (21852) |
| Last modified by | leavemsg2 (21852) |
| Numerical id | 11 |
| Author | leavemsg2 (21852) |
| Entry type | Algorithm |
| Classification | msc 11Y05 |
| Synonym | step |
| Synonym | echelon |
| Defines | factoring algorithm |

Here's a specific example that's missing from everyone's repertoire, when it comes to having a general factoring method:

**Example one** Let $N = 7477 = 61 * 127$, and $\sqrt{N} \approx 88.01$, and compute the following:

$$M = 2^{(7477+1)} = 2^{7478}$$

now, $X =$ mod $(M, N-1)$, and $\gcd(X - [2^0], N)$, $\gcd(X - [2^1], N)$,..., $\gcd(X - [2^k]^2, N)$ such that $[2^k]^2 \leq \sqrt{N}$.

It'll find the factor, but we would have to use George Woltman's FFT's method to compute the $M$'s for larger numbers. In this example, $M$ mod $(N-1) = 246$, and $\gcd(246 - 2, N) = 61$.

Also, calculate $ln(7477) \approx 8.955$, so, you could continue to check

$$\gcd(X - [3^1], N), ..., \gcd(X - [3^k], N)$$

such that $[3^k]^2 \leq sqrt(N)$, and $\gcd(X - [5^2])$ such that $[5^k]^2 \leq \sqrt{N}$, if a factor hasn't shown itself. Unlike primality-proving, finding the factor would be the "proof-in-the-pudding"!

We'd have the answer; that's for sure! I call it a step or "echelon"-factoring algorithm.

**Example two**

$$1500450271 * 5915587277 = 8876044532898802067$$

You'd use this fact to get past the first modpow()

$N+1 = 8876044532898802067+1 = 2^2*3*(2^4+1)*(2*3^4*(2*(2^2*5*(2^2*5^3*(2*(2^2*7+1)+1)+1)+1)+$

$M = 2^(8876044532898802067 + 1)$

$k = log2[\sqrt{\sqrt{8876044532898802067}}] = 15$ so, 1 huge step and 31 base two subtractions, and some base 3, 5, ..., 43, etc! ... find mod $(2^{N+1}, N-1)$, and $\gcd(M - [2^0], N)$, $\gcd(M - [2^1], N)$..., $\gcd(M - [2^{30}], N)$, etc. and you'll have a factor.

It's the best, shortest method that you'll ever use to check for factors, and it's definitive, assuming we can conquer the enormous modular calculation!

In this last example, the number of steps is comparable to the 2 times 16th Root of $N$ for the base 2 calculations alone. I couldn't do the calculations by hand.