

## Re: Factoring problem solution

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2005-02/3838.html>

---

*tomstdenis\_at\_gmail.com*

**Date:** 02/11/05

Date: 11 Feb 2005 00:54:03 -0800

Paul Leyland wrote:

> "Larry Hammick" <larryhammick@OMIT-MEtelus.net> writes:  
>  
> > True, because you are just guessing at what quadratics to  
> > use and, if they don't work, guessing again. Real sieves use  
> > large tables of polynomials. RSA-576 was factored with  
> > the aid of over half a million quadratic polynomials.  
>  
> Eh?  
>  
> RSA-576 was factored by GNFS using a single quintic and a single  
> linear polynomial.

Proly confused relations with polynomials.

For the benefit of others the GNFS like QS finds relations of the sort

$x^2 - N == p_1^{e_1} * p_2^{e_2} \dots * p_n^{e_n}$  [for p's in some factor bound].

You can rewrite this [mod N] as

$x^2 - p_1^{e_1} * \dots == 0 \pmod{N}$

which if all the 'e's' are even gives you a difference of squares.

Then given all these relations you want a square so you take the exponents [e\_1, e\_2, ...] and reduce them modulo two and then reduce the entire system.

So you have a huge matrix like

[e\_1,1 e\_1,2 ... ]  
[e\_2,1 e\_2,2 ... ]

Adding rows is multiplying the corresponding " $x^2 - N$ " and subtracting is dividing [modulo N]. Once you get a row that is all zeroes it's either going to lead to a solution or N. Multiplying the " $x^2 - N$ "

sci.math: Re: Factoring problem solution

doesn't change the fact that they're still a square since modulo N it's equivalent to  $x^2 - 0$  and multiplying two squares results in a squares.

All basically taking advantage of the fact that if

$x^2 - y^2 \equiv 0 \pmod{N}$  and  $x \neq y$  then you have a good chance of factoring N.

Tom