

## Re: Factoring problem solution

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2005-02/3902.html>

---

**From:** Décio Luiz Gazzoni Filho (*decio\_at\_decpp.removethis.net*)

**Date:** 02/11/05

Date: Fri, 11 Feb 2005 12:41:46 -0200

tomstdenis@gmail.com wrote:

> *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.*

>

> *Prolly confused relations with polynomials.*

>

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

>

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

> bound].

No, what you're describing is how the basic quadratic sieve (not the multiple-polynomial version) works. I'll try to explain in simplified terms how the NFS works.

NFS works (I'll simplify it a lot) this way: you have two polynomials, generally one (call it  $F(a,b)$ ) being a 4th/5th/6th degree polynomial while the other (call it  $G(a,b)$ ) is a linear polynomial. When factoring smaller integers, there's a construction by Montgomery where  $F(a,b)$  and  $G(a,b)$  are both quadratic, but this no longer makes sense for composites of interest.

The NFS seeks pairs  $(a,b)$  such that  $a$  and  $b$  are coprime, and both  $F(a,b)$  and  $G(a,b)$  are divisible by small primes only (those in the so-called factor base). In fact, they could be divisible by 1 or 2 larger primes (not in the factor base), but I won't take this into account because it just complicates matters.

Now pick the prime factorization of both  $F(a,b)$  and  $G(a,b)$  and reduce the exponents in these factorizations modulo 2. Make a matrix where each column has those exponents concatenated together, then each row corresponds to a different factorization (arising from a different pair  $(a,b)$ ). Now finding a linear dependence in this matrix means that the product of  $F(a,b)$  for the different pairs  $(a,b)$  has all even exponents in its prime factorization, and the same happens simultaneously for  $G(a,b)$ , using the same set of pairs  $(a,b)$ . Having all even exponents in a prime factorization means that both products are squares.

Thus we can try to use the fact that if  $x^2 \equiv y^2 \pmod N$  are congruent squares, but  $x \not\equiv y, -y$ , then  $\gcd(x-y, N)$  is a non-trivial factor of  $N$ .

I won't explain everything that is done, especially because I'm not an expert, but the point is that having  $F(a_1, b_1) \cdot F(a_2, b_2) \cdot \dots \cdot F(a_k, b_k)$  being a square means that a certain element in an algebraic number field is also a square (this is not strictly true, but using a trick due to Adleman this becomes true with sufficient probability in practice). Now one can use a certain homomorphism (essentially, a mapping) between the number field in question and the integers modulo  $N$  to obtain a square modulo  $N$ . One can show that this square is congruent to the square  $G(a_1, b_1) \cdot G(a_2, b_2) \cdot \dots \cdot G(a_k, b_k)$  modulo  $N$ . It's easy to compute the square root of the product of  $G(a,b)$ 's, by computing its prime factorization from the information already known, then dividing each exponent by half. The situation isn't so easy with the algebraic number that arises from the product of  $F(a,b)$ 's, but one can indeed compute a square root in that algebraic number field. Now map that square root back to  $N$ , and try to compute a gcd between the difference of those square roots (the one arising from  $F$  and the one from  $G$ ) and  $N$ ; with 50% probability a non-trivial factor of  $N$  is found. If that doesn't work out, use another linear dependency from the matrix, do the square-rooting stuff and try the gcd again, and so on until you find factors.

Hope that helps.

Décio