# Tiny MPQS

Paul Zimmermann

ANR Catrel, Palaiseau, 14 January 2015

# References


The Multiple Polynomial Quadratic Sieve, Robert D. Silverman, Math. of Comp., vol. 48, num. 177, 1987 (attributes the idea to Montgomery)

The Quadratic Sieve Factoring Algorithm, Eric Landquist, MATH 488: Cryptographic Algorithms, December 14, 2001

Implementing the Hypercube Quadratic Sieve with Two Large Primes, Brian Carrier and Samuel S. Wagstaff, Jr., 2003

Factoring Small to Medium Size Integers: An Experimental Comparison, Jérôme Milan, `hal.inria.fr/inria-00188645v3`, 2010

# Motivation

In CADO-NFS cofactorization, we currently use only $P-1$, $P+1$ and ECM

Goal: compare to MPQS (also used by Franke-Kleinjung GNFS)

Target size: up to 128 bits

# Quadratic Sieve

First explicit version by Carl Pomerance (1981)

0. Set up a factor base $F = \{-1\} \cup \{p \text{ prime}, p \leq P\}$
1. Let $b = \lfloor n^{1/2} \rceil$
2. Factor $S(x) := (x+b)^2 - n$ for $x$ in $[-M, M]$
3. If $m > \#F$ complete factorizations over $F$ are found, find a subset that gives a square product and write:

$$S(x_1)S(x_2)\cdots S(x_m) = (x_1 x_2 \cdots x_m)^2 \bmod n$$

4. If $X = \sqrt{S(x_1)S(x_2)\cdots S(x_m)}$ and $Y = x_1 x_2 \cdots x_m$, then $\gcd(X-Y, n)$ gives a non-trivial factor of $n$ with probability $\geq 1/2$

Example: $n = 2^{80-17} = 20885856281 \times 57882511655239$

$b = \lfloor n^{1/2} \rceil = 2^{40} = 1099511627776$

$P = 2^{16}$: $F$ contains (at most) 6542 primes

For $|x| \leq 108916$, we get 2508 relations over 2507 primes, for example:

$$(-108916 + b)^2 - n = -1 \cdot 7 \cdot 67 \cdot 149^2 \cdot 787 \cdot 3767 \cdot 7759$$

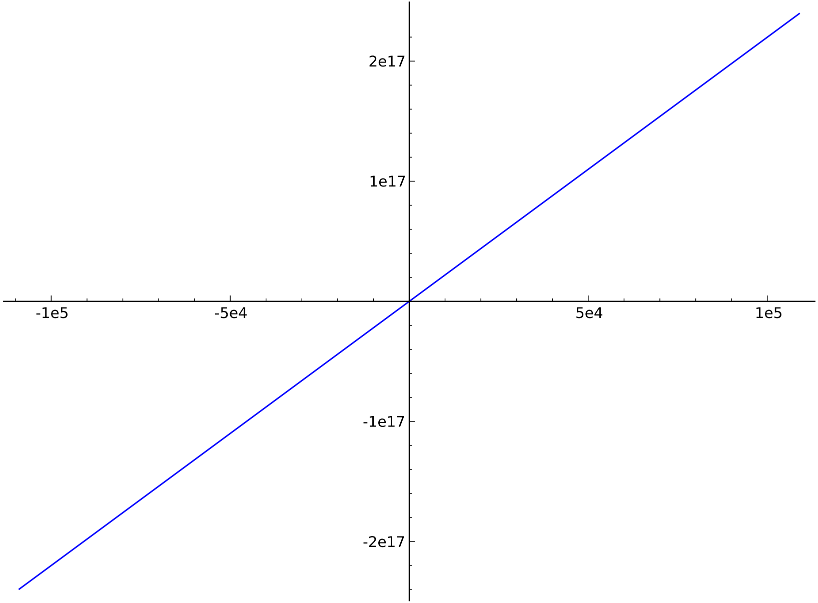
# Which primes can appear?

If $(x+b)^2 - n = \cdots \times p \times \cdots$, then $n$ is a square (quadratic residue) modulo $p$, thus

$$\left(\frac{n}{p}\right) = 1$$

For $n = 2^{80} - 17$, we have 3329 odd primes $p$ with $\left(\frac{n}{p}\right) = 1$ up to $2^{16}$, plus 2 plus $-1$, thus 3331 factor base elements

$(x+b)^2 - n$ for $-108916 \le x \le 108916$:



# MPQS: Multiple Polynomial Quadratic Sieve

Main idea: for $a$ positive integer, use

$$S(x) = (ax + b)^2 - n$$

The integer $b$ is chosen so that $0 \leq b < a$ and $b^2 - n$ is divisible by $a$, say $b^2 - n = ac$. Then:

$$S(x) = a^2x^2 + 2abx + ac = aQ(x) \quad \text{for} \quad Q(x) := ax^2 + 2bx + c$$

If in addition $a$ is a square, then it suffices to split $Q(x)$ over the factor base

# MPQS: how to choose $a$?

We choose $a$ to be a square to only consider $Q(x) = ax^2 + 2bx + c$

Basic MPQS: take $a = p^2$ where $p$ is a prime. Since $b^2 - n = ac$, $n$ is a square modulo $a$, thus we need $\left(\frac{n}{a}\right) = 1$.

Then take $b$ as one of the square roots of $n$ modulo $a$.

If we sieve $x \in [-M, M]$, then $[(ax + b)^2 - n]/a$ goes from about $-n/a$ for $x = 0$ to about $aM^2 - n/a$ for $x = \pm M$.

The optimal value is $a \approx \sqrt{2n}/M$, with values up to $M\sqrt{n/2}$. In contrast for QS with $(x + b)^2 - n$, we have values up to $2M\sqrt{n}$: $\sqrt{8}$ improvement.

# Sieve initialization

For each factor base prime $p$, precompute the (two) roots $r$ of $x^2 - n \bmod p$

Remember we want to sieve $Q(x) = (ax + b)^2 - n$ over $[-M, M]$

$(p, r)$ divides $(ax + b)^2 - n$ whenever $ax + b = r \bmod p$

We thus need to compute $x_p = (r - b)/a \bmod p$ for each new polynomial $ax^2 + 2bx + c$ and each factor base prime $p$!

The computation of $1/a \bmod p$ is expensive

SIQS (Self Initializing) or HMPQS (Hypercube): taking $\sqrt{a} = p_1 p_2 \cdots p_s$ gives $2^s$ square roots.

# Fast MPQS without SIQS/HMPQS (1/2)

Use Caramel technology!

We want to compute $1/a \bmod p_1, 1/a \bmod p_2, \ldots, 1/a \bmod p_s$

Using Montgomery's batch inversion, we know how to compute $1/p_1 \bmod a, 1/p_2 \bmod a, \ldots, 1/p_s \bmod a$

Kruppa's dual batch inversion: if $t_j = 1/p_j \bmod a$, then $t_j p_j + u_j a = 1$ for some $u_j$, thus $u_j = 1/a \bmod p_j$

# Fast MPQS without SIQS/HMPQS (2/2)

1. Compute $q_1 = p_1$, $q_2 = p_1 p_2 \bmod a$, ... $q_s = p_1 \cdots p_s \bmod a$ [$s-1$ modular products]

2. Compute $r_s = 1/q_s \bmod a$ [one modular inverse]

3. Get $t_j = r_j q_{j-1} \bmod a$ and $r_{j-1} = r_j q_j \bmod a$ for $j = s, s-1, \ldots 1$ [$2s-2$ modular products]

4. Get $u_j = (1 - t_j p_j)/a$ [$s$ exact divisions]

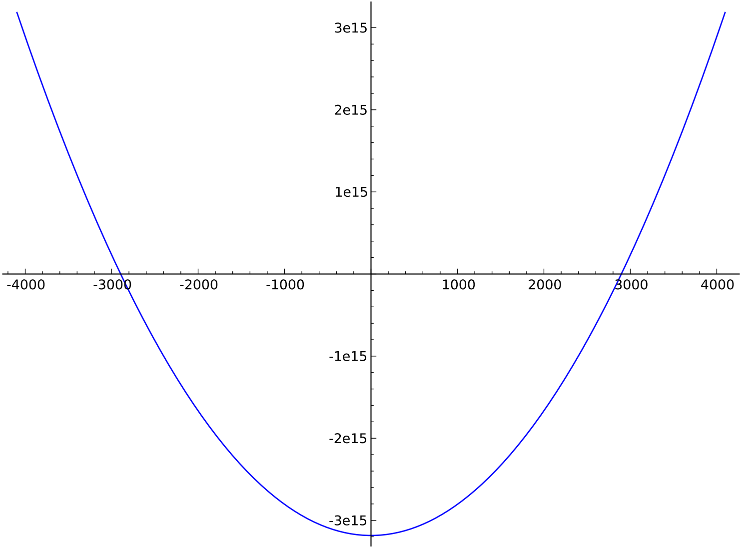
Total cost: 3 modular products and one exact division per factor base prime for the batch inversion, and 2 modular products to compute $(r-b)u_j$ and $(-r-b)u_j$.

Remark: if $a = z^2$, we can perform all computations modulo $z$, and if $u_j = 1/z \bmod p_j$, then $u_j^2 = 1/a \bmod p_j$

For $n = 2^{80} - 17$, about 4% of the total time is spent in the batch inversion, and about 9% in the computation of $(r_j - b)u_j^2 \bmod p_j$

# MPQS parameters for 80 bits

$M = 2^{12}$, $\#F = 150$, $a \approx \sqrt{2n}/M \approx 379625062$



# The multiplier

Let $n = 2^{80} - 17$.

$n = 3 \bmod 4$, thus is not a square modulo 2. $n$ is a square modulo 5, 7, 17, 19, ... In other words, $\alpha(x^2 - n, 2000) = 1.10$.

If we factor $kn$ instead of $n$, norms $Q(x)$ are multiplied by $\sqrt{k}$, but the $\alpha$ value might compensate.

$k = 11$, $\alpha = -0.55$, $\log \sqrt{k} = 1.20$, total 0.65

$k = 15$, $\alpha = -0.74$, $\log \sqrt{k} = 1.35$, total 0.61

# Timings

All timings on Catrel cluster (Intel Xeon E5-2650, 2.4GHz).

TIFA: version 0.1.0 (devel:20100610).

CADO-NFS: revision 73e583f, average of 100 RSA-like numbers.

ECM: default CADO-NFS strategy with enough curves (not optimal for RSA-like numbers)

| bits | tiny MPQS | ECM | TIFA SIQS |
|---|---|---|---|
| 64 | 1.3ms | **0.12ms** | 636ms |
| 80 | 3.0ms | **2.4ms** | 3.2ms |
| 96 | 7.5ms | 10.7ms | **4.7ms** |
| 112 | 22ms | 46ms | **15ms** |
| 128 | 73ms | 2350ms | **37ms** |

Still work in progress!

# Saving a factor 2 (not tested yet)

If $b^2 - n = ac$, then with $Q(x) = ax^2 + 2bx + c$:

$$(ax + b)^2 - n = a^2x^2 + 2abx + ac = aQ(x)$$

Classical case: $a = p^2$.

If $c$ is even, we can use $a = 2p^2$, then $Q(x)$ is always divisible by 2.

When $n = 1 \bmod 4$, $b^2 - n = 0 \bmod 4$, thus $c$ is even.

# Rational multiplier (not tested yet)

Choose a small odd integer $\ell > 1$

Factor base: roots of $\ell x^2 = n \bmod p$.

Choose $a$ such that $n/\ell$ is a square modulo $a$

Choose $b$ such that $\ell b^2 - n = ac$

Then $\ell(ax+b)^2 - n = aQ(x)$ with $Q(x) := \ell a x^2 + 2\ell b x + c$

The minimum value of $Q(x)$ is still $-n/a$ for $x \approx 0$, the maximum is now $\approx \ell a M^2 - n/a$ for $x = \pm M$

We want $\ell a M^2 \approx 2n/a$ thus $a \approx \sqrt{2n/\ell}/M$

The maximum is now $\sqrt{\ell n/2}M$, increased by $\sqrt{\ell}$ wrt $\ell = 1$

Multiplier $k/\ell$: roots of $\ell x^2 = kn \bmod p$, norms increased by $\sqrt{k\ell}$.