Number Field Sieve

Ruben Spaans

NTNU

2013-06-06
Overview

- The Number Field Sieve is the fastest known general algorithm for factoring integers of more than 120 digits
  - The largest factored integer (of general form) is RSA-768 having 232 digits.

- Mathematical requirements for the algorithm
  - Number theory
  - Algebra (fields and ideals)
  - Algebraic number theory
  - Linear algebra
    - Specialized methods for solving sparse systems of equations in $GF(2)$
  - Assorted stuff, like factoring polynomials over $\mathbb{Z}$ and $\mathbb{Z}_p$. 

Ruben Spaans
Number Field Sieve
What I was supposed to do in my thesis:

- Study the required mathematics
- Study the NFS algorithm
- Implement the NFS algorithm in some programming language
- Do some experiments with the implementation
We want to factor a composite integer \( n \). \( n \) is odd and not a power.

\[
n = p \cdot q \\
= (u - v)(u + v) \quad \text{where } u = \frac{p + q}{2}, \quad v = \frac{p - q}{2} \\
= u^2 - v^2
\]

\[\Rightarrow u^2 \equiv v^2 \pmod{n}\]
We want to somehow find \( u \neq v \) satisfying

\[ u^2 \equiv v^2 \pmod{n}. \]

Then \( \gcd(n, u - v) \) will give us a non-trivial factor. This is also what other factorization algorithms such as Pollard rho and Quadratic Sieve does.
What we want to do

- How to find such \( u, v \)?
- We do it by instead finding squares

\[
x \equiv u^2 \pmod{n}
\]

and

\[
y \equiv v^2 \pmod{n}.
\]

and by taking the square root of \( x \) and \( y \).
What we will do

- We will use a fancy scheme that lets us find these $x$ and $y$ simultaneously.
- Search for “smooth numbers” (numbers with “small” prime factors) on both sides of the congruence.
- Pick a subset of these smooth numbers such that their product is a square on both sides of the congruence.
- Take the square roots $u = \sqrt{x}$ and $v = \sqrt{y}$ and get a non-trivial factor $\gcd(n, u - v)$. 
The fancy scheme to let us find the squares $x$ and $y$ is called sieving.
Here follows an overly simplified sieving example that only demonstrates how to find smooth integers

- The actual procedure that also finds $x, y$ simultaneously is slightly more complex.

- Say we want to find all integers between 10 and 20 with no prime factors larger than 5.

- First, initialize an array with the actual values:

  $(10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19 \ 20)$
Then, get rid of all occurrences of the prime factor 2 by dividing them out.

\[(10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19 \ 20)\]

\[\downarrow\]

\[(5 \ 11 \ 3 \ 13 \ 7 \ 15 \ 1 \ 17 \ 9 \ 19 \ 5)\]
Proceed with prime factor 3.

\[
(5 \ 11 \ 3 \ 13 \ 7 \ 15 \ 1 \ 17 \ 9 \ 19 \ 5) \\
\downarrow \\
(5 \ 11 \ 1 \ 13 \ 7 \ 5 \ 1 \ 17 \ 1 \ 19 \ 5)
\]
Process the last prime, 5:

\[(5 \ 11 \ 1 \ 13 \ 7 \ 5 \ 1 \ 17 \ 1 \ 19 \ 5)\]

\[\Downarrow\]

\[(1 \ 11 \ 1 \ 13 \ 7 \ 1 \ 1 \ 17 \ 1 \ 19 \ 1)\]
Sieve example

- The array elements containing 1 correspond to the smooth integers we are seeking.
- \((1 \ 11 \ 1 \ 13 \ 7 \ 1 \ 17 \ 1 \ 19 \ 1)\)

\[
\begin{align*}
10 &= 2 \cdot 5 \\
12 &= 2^2 \cdot 3 \\
15 &= 3 \cdot 5 \\
16 &= 2^4 \\
18 &= 2 \cdot 3^2 \\
20 &= 2^2 \cdot 5
\end{align*}
\]
While we’re at it, we might as well try to find a subset whose product is square:

\[
\begin{align*}
10 &= 2 \cdot 5 \\
12 &= 2^2 \cdot 3 \\
15 &= 3 \cdot 5 \\
16 &= 2^4 \\
18 &= 2 \cdot 3^2 \\
20 &= 2^2 \cdot 5
\end{align*}
\]

\[12 \cdot 15 \cdot 20 = 2^4 \cdot 3^2 \cdot 5^2\]
There’s more to it

- The procedure we just showed only finds one square, not two.
- The NFS uses a rather complicated setup where we sieve over “generators” that give us integers from both sides of the congruence.
- The new idea that NFS introduces is to work in $\mathbb{Z}_n$ on one side of the congruence, and in a different ring $R$ on the other side!
- A “generator” pair of integers $a, b$ give rise to an integer $x$ and an element $r \in R$, with the unique homomorphism $\sigma : R \mapsto \mathbb{Z}_n$ with $\sigma(r) = x$ and $\sigma(\alpha) = m$ where the important constants $\alpha$ and $m$ are defined later.
- The goal is pretty much the same as earlier. We want to find a subset of these $a, b$ pairs so that the product of all the resulting $x$ and $r$ are squares (simultaneously).
Let $f(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial of degree $d$, and let $\alpha \in \mathbb{C}$ be a root.

Then $\mathbb{Q}(\alpha)$ is a field. Also, it is a field extension of $\mathbb{Q}$ of degree $d$.

An element in $\mathbb{Q}(\alpha)$ is of the form $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$ with $a_i \in \mathbb{Q}$.

The actual ring we will be working in is the subring $\mathbb{Z}[\alpha] \subseteq \mathbb{Q}(\alpha)$ having elements as above, but with $a_i \in \mathbb{Z}$. 
In accordance with our grand goal we want to find smooth elements in this ring.

But how do we define smoothness here?

Problem: $\mathbb{Z}[\alpha]$ is not even guaranteed to be a unique factorization domain (UFD).
Problem: \( \mathbb{Z}[\alpha] \) is not even guaranteed to be a unique factorization domain (UFD). This makes it quite impossible to guarantee that an element has no prime factors larger than a given bound.

Solution: Work temporarily in a slightly bigger ring \( \mathcal{O} \) where \( \mathbb{Z}[\alpha] \subseteq \mathcal{O} \subseteq \mathbb{Q}(\alpha) \).

\( \mathcal{O} \) is the ring of algebraic integers in \( \mathbb{Q}(\alpha) \). An element \( \theta \in \mathbb{Q}(\alpha) \) is an *algebraic integer* if there exists a monic polynomial with integer coefficients having \( \theta \) as a root.

\( \mathcal{O} \) is not UFD either. But there is a way out:

Fundamental theorem: Every non-zero ideal of \( \mathcal{O} \) has unique factorization into prime ideals.
We can now define a smooth number in our ring. An element $\theta$ is smooth if the ideal $\langle \theta \rangle$ has no prime ideals larger than a given bound.

In order to determine whether a prime ideal is “larger” than a given bound, define the norm of a non-zero ideal $\mathcal{N}(\langle \theta \rangle)$ to be the size of the quotient ring $|\mathcal{O}/\langle \theta \rangle|$.

Now we can in principle sieve an algebraic element $\theta$ by considering the factors of the ideal $\langle \theta \rangle$!

There are still a lot of gory details to be worked out, see my thesis.
As mentioned earlier, we sieve over “generator” values that produce integers on both sides of our congruence, from which we try to obtain smooth values.

A generator is a pair of integers $a, b$. This gives rise to an integer $a - bm \in \mathbb{Z}$ and an algebraic integer $a - b\alpha \in \mathbb{Z}[\alpha]$.

In the above, $\alpha$ is the root of $f(x)$ that defines our ring, and $m$ is an integer satisfying $f(m) = n$.

Sieving is usually done in a rectangle $|a| \leq M, 0 < b \leq N$ for some bounds $M, N$. We want to find pairs $a, b$ such that $a - bm$ and $a - b\alpha$ are both smooth. In addition, we require $\gcd(a, b) = 1$ to avoid pairs that are “redundant”.
After the sieving is done, we hopefully have a lot of $a, b$ pairs. We want to find a subset of these pairs so that the product of all $a - bm$ and $a - b\alpha$ are squares.

Find a subset using linear algebra!

Construct a matrix $A$ where $a_{ij}$ contains the prime power of the prime $p_j$ for the $i$-th pair $a, b$, and reduce everything modulo 2.

Then find a vector $v$ such that $Av \equiv 0 \pmod{2}$ and use $v$ to get the actual subset of pairs. The product of the numbers resulting from these pairs have even prime powers and are therefore squares.
Another example

Here is our old example, along with the matrix that would be formed.

\[
\begin{align*}
10 &= 2 \cdot 5 \\
12 &= 2^2 \cdot 3 \\
15 &= 3 \cdot 5 \\
16 &= 2^4 \\
18 &= 2 \cdot 3^2 \\
20 &= 2^2 \cdot 5
\end{align*}
\]

\[
A = \begin{bmatrix}
1 & 0 & 1 \\
0 & 1 & 0 \\
0 & 1 & 1 \\
0 & 0 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{bmatrix}
\]
Square roots

- Let $\mathcal{S}$ be the subset of pairs we found on the last page.
- Now we have the squares

$$x = \prod_{(a,b) \in \mathcal{S}} (a - bm)$$

and

$$\gamma = \prod_{(a,b) \in \mathcal{S}} (a - b\alpha).$$

- We can find the square root $u$ of $x$ by having all exponents from the known factorization of $x$. 
Square roots

- Taking the square root of $\gamma$ by halving the exponents of the prime ideals will not work, as we cannot just move from ideals in $O$ to elements in $\mathbb{Z}[\alpha]$ (long story with many complications).

- We use a specialized algorithm that calculates $\beta = \sqrt{\gamma}$ with a mixture of Chinese Remainder Theorem, norm calculations and square roots in finite fields (also a long story, see thesis).
Finding a factor

- Our congruence $u^2 \equiv v^2 \pmod{n}$ requires two integers in $\mathbb{Z}_n$, and we got $u$ two pages ago. Let’s use our homomorphism $\sigma$ on our algebraic square root $\beta$ to get

$$v = \sigma(\beta)$$

- (We recall that $\sigma : \mathbb{Z}[\alpha] \mapsto \mathbb{Z}_n$ with $\sigma(\alpha) = m$.)

- If we are unlucky, we get $u = v$. In this case, find another solution to the matrix equation (this might require more sieving).

- Otherwise, get a factor by calculating $\gcd(n, u - v)$ and rejoice!
Implementation

- The NFS algorithm was implemented in 1770 lines of C code. (Can be found at http://github.com/stubbscroll/nfs)
- We didn’t implement the best algorithm for each step in the NFS. Therefore our implementation will struggle with integers having more than 50 digits.
The end

- The end!
- Any questions?