Cryptanalytic world records, summer 2014

World record! The factorization of RSA-768

Dr. Daniel Loebenberger

We are heading towards the fastest known algorithm for factoring integers N, the *general number field sieve*. As the name suggests, it employs the algebraic concept of a *number field* (or a *number ring*).
For Dixon's random squares, we constructed (using linear algebra) a square on the right-hand side of a congruence $u^2 = v^2$. The left-hand side was by construction a square already. In the number field sieve, we use the linear algebra on *both* sides of the desired congruence!

Assume we have an element θ of a number ring and a homomorphism ϕ mapping elements from that ring to $\mathbb{Z}_N$. Furthermore, suppose we have a set of pairs θ_i, $\phi(\theta_i)$ for $1 \leq i \leq k$, such the the product of the θ_i is a square γ^2 in the number ring and also the product of the $\phi(\theta_i)$ is congruent to an integer square modulo N. Then if $\phi(\gamma) = u \in \mathbb{Z}_N$, we have

$$u^2 = \phi(\gamma)^2 = \phi(\gamma^2) = \phi(\theta_1 \cdots \theta_k) = \phi(\theta_1) \cdots \phi(\theta_k) = v^2 \text{ in } \mathbb{Z}_N$$

This is (hopefully) a non-trivial congruence of squares!

To construct the number ring, consider an irreducible polynomial

$$f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0 \in \mathbb{Z}[x]$$

with some (complex) root α and consider the ring $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(f(x))$. Additionally, we require the there is some integer m, such that $f(m) = 0$ in $\mathbb{Z}_N$
The homomorphism $\phi\colon \mathbb{Z}[\alpha] \to \mathbb{Z}_N$ is defined by $\phi(\alpha) = m$.

We are heading to find $\gamma \in \mathbb{Z}[\alpha]$ and $v \in \mathbb{Z}$, which will (hopefully) give us a non-trivial factorization of our integer N.
For the following we assume that the elements θ in the ring $\mathbb{Z}[\alpha]$ are all of the very special form $a - b\alpha$, with coprime $a, b \in \mathbb{Z}$.
Thus, we try to find a set S of such integer pairs (a, b), such that

$$\prod_{(a,b)\in S} (a - b\alpha) = \gamma^2 \text{ for some } \gamma \in \mathbb{Z}[\alpha]$$

$$\prod_{(a,b)\in S} (a - bm) = v^2 \text{ for some } v \in \mathbb{Z}$$

How to find such a set S? Sieve the polynomial $G(a, b) = a - bm$ for smooth values and build from that using linear algebra a square on the rational side. The problem is, that we have to simultaneously ensure that the corresponding product of the $a - b\alpha$ has to be a square in $\mathbb{Z}[a]$ as well.

Definition (Norm of an algebraic element)

Let $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ be the roots of the degree d polynomial f with $\alpha = \alpha_1$. The *norm* $N(\beta) \in \mathbb{Q}$ of an element

$$\beta = s_0 + s_1\alpha + \cdots + s_{d-1}\alpha^{d-1}$$

in the algebraic number field $\mathbb{Q}[\alpha]$ is the product of all conjugates of β, i.e. the product of all $s_0 + s_1\alpha_j + \cdots + s_{d-1}\alpha_j^{d-1} \in \mathbb{Q}[\alpha]$.

If $\beta = \gamma^2$ for some $\gamma \in \mathbb{Z}[\alpha]$, then $N(\beta) = N(\gamma)^2 \in \mathbb{Z}$. So, a *necessary* condition for the product of the $a - b\alpha$ to be a square is that the product of the integers $N(a - b\alpha)$ is a square.
If $F(x, y) = x^d + c_{d-1}x^{d-1}y + \cdots c_0 y^d$ is the homogeneous form of f, then $N(a - b\alpha) = F(a, b)$. Thus, we need to sieve for smooth values of $F(a, b)$ and $G(a, b)$ simultaneously and perform then linear algebra to find our congruence of squares!

The problem is that this does not work, the above stated condition is far from *sufficient*.

Example

Consider $f(x) = x^2 + 1$ with $f(i) = 0$. Then $N(a + bi) = a^2 + b^2$. If $a^2 + b^2$ is a square then $a + bi$ needs not to be a square in $\mathbb{Z}[i]$. If a is a non-square integer, so it is in $\mathbb{Z}[i]$, but $N(a) = a^2$ is a square. Also, one can show that $5i = (2 + i)(1 + 2i)$ is not a square in $\mathbb{Z}[i]$, but $N(5i) = 25$ is a square in $\mathbb{Z}$.

For each prime p, write

$$R(p) = \{r \in \{0, \ldots, p-1\} \mid f(r) = 0 \text{ in } \mathbb{Z}_p\}.$$

If a and b are coprime then

$$F(a,b) = 0 \in \mathbb{Z}_p \iff a = br \text{ in } \mathbb{Z}_p \text{ for some } r \in R(p)$$

Thus, we store for each entry of our exponent vector corresponding to the factorization of $F(a,b)$ also the value $r \in R(p)$.

Example

Consider the polynomial $f(x) = x^2 + 1$ and take $B = 5$. Then the exponent vectors for B-smooth elements of $\mathbb{Z}[i]$ consist of three entries, corresponding to the pairs $(2, 1)$, $(5, 2)$ and $(5, 3)$. We get

$$\begin{aligned} F(3,1) &= 10 \text{ with exponent vector } (1,0,1) \\ F(2,1) &= 5 \text{ with exponent vector } (0,1,0) \\ F(1,1) &= 2 \text{ with exponent vector } (1,0,0) \\ F(2,-1) &= 5 \text{ with exponent vector } (0,0,1) \end{aligned}$$

Then $F(3,1)F(2,1)F(1,1) = 100$, but the corresponding exponent vector $(0,1,1)$ shows, that $(3+i)(2+i)(1+i)$ is *not* a square in $\mathbb{Z}[i]$. On the other hand $F(3,1)F(1,1)F(2,-1) = 100$ has exponent vector $(0,0,0)$ and $(3+i)(1+i)(2-i) = 8+6i = ((1+i)(2-i))^2$ is a square in $\mathbb{Z}[i]$.

The problem is that this still does not work, since some non-squares on the algebraic side will correspond to zero-vectors.

We introduce yet another algebraic concept: Denote by I the ring of algebraic integers in the algebraic number field $\mathbb{Q}[\alpha]$, i.e. the set of elements that are the root of some monic polynomial in $\mathbb{Z}[x]$. This is a ring, the *ring of algebraic integers* in the number field.

Lemma

If S is a set of coprime integer pairs (a, b) such that $a - b\alpha$ is B-smooth, and if $\prod_{(a,b)\in S}(a - b\alpha)$ is a square of an algebraic integer of the number field $\mathbb{Q}[\alpha]$. Then

$$\sum_{(a,b)\in S} v(a - b\alpha) = 0 \text{ over } \mathbb{F}_2.$$

Here,

$$v(a - b\alpha)_{p,r} = \begin{cases} 0 & \text{, if } a \neq br \text{ in } \mathbb{Z}_p, \\ e(p) & \text{, if } a = br \text{ in } \mathbb{Z}_p \text{ and } p^{e(p)} \parallel N(a - b\alpha). \end{cases}$$

Given the last lemma, we still have to overcome various obstructions. However, most of the principles needed here are beyond the scope of this course.

The runtime estimate crucially depends on the following:

Theorem (Pomerance 1996)

If $m_1, m_2, \ldots$ is a sequence of independent, uniformly selected integers in $\{1, \ldots, X\}$. Let N be the smallest integer, such that there is a nonempty subsequence of $m_1, \ldots, m_N$ has product being a square. Then the expected value for N is

$$\exp((\sqrt{2} + o(1))(\ln X)^{1/2}(\ln \ln X)^{1/2}),$$

even if we insist that each m_j is B-smooth, where

$$B = \exp(2^{-1/2}(\ln X)^{1/2}(\ln \ln X)^{1/2}).$$

Theorem

The general number field sieve on an integer N of bit-size n has an heuristic asymptotic complexity of $L_{1/3}(n)$. More precisely, its complexity can be estimated as

$$\exp(((64/9)^{1/3} + o(1))n^{1/3}(\log n)^{2/3}).$$

We are pleased to announce the factorization of RSA768, the following 768-bit, 232-digit number from RSA's challenge list:

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3.

The factorization, found using the Number Field Sieve (NFS), is:

334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994893674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

[...]

On December 12, 2009, we found the factors at the first solution. A few minutes later four of the other seven jobs produced the factorization as well.

Thorsten Kleinjung (1),
Kazumaro Aoki (2), Jens Franke (3), Arjen K. Lenstra (1), Emmanuel Thome (4), Joppe W. Bos (1), Pierrick Gaudry (4), Alexander Kruppa (4), Peter L. Montgomery (5,6), Dag Arne Osvik (1), Herman te Riele (6), Andrey Timofeev (6), and Paul Zimmermann (4)
1: EPFL; 2: NTT; 3: Bonn University; 4: INRIA; 5: MS Research; 6: CWI