RSA VIII

Number-field sieve

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

with some slides by

Daniel J. Bernstein

Generalizing beyond $\mathbf{Q}$

The $\mathbf{Q}$ sieve is a special case of the number-field sieve.

Recall how the $\mathbf{Q}$ sieve factors 611:

Form a square as product of $i(i + 611j)$ for several pairs (i, j):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd(611, 14 \cdot 64 \cdot 75 - 4410000)$
$= 47$.

The $\mathbf{Q}(\sqrt{14})$ sieve factors 611 as follows:

Form a square as product of $(i + 25j)(i + \sqrt{14}j)$ for several pairs (i, j):

$$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14})$$
$$\cdot (3 + 25)(3 + \sqrt{14})$$
$$= (112 - 16\sqrt{14})^2.$$

Compute

$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,

$t = 112 - 16 \cdot 25$,

$\gcd(611, s - t) = 13$.

Why does this work?

Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:

$$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25) \cdot (3 + 25)(3 + 25) = (112 - 16 \cdot 25)^2 \text{ in } \mathbf{Z}/611.$$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Diagram of ring morphisms:

$$
\begin{array}{ccc}
\mathbf{Q}[x] & \xrightarrow{x \mapsto \sqrt{14}} & \mathbf{Q}[\sqrt{14}] = \mathbf{Q}(\sqrt{14}) \\
\uparrow & & \uparrow \\
\mathbf{Z}[x] & \xrightarrow{x \mapsto \sqrt{14}} & \mathbf{Z}[\sqrt{14}] \\
 & & \downarrow {\scriptstyle \sqrt{14} \mapsto 25} \\
 & & \mathbf{Z}/611
\end{array}
$$

$\mathbf{Z}[x]$ uses poly arithmetic on $\{i_0 x^0 + i_1 x^1 + \cdots : \text{all } i_m \in \mathbf{Z}\}$;

$\mathbf{Z}[\sqrt{14}]$ uses $\mathbf{R}$ arithmetic on $\{i_0 + i_1\sqrt{14} : i_0, i_1 \in \mathbf{Z}\}$;

$\mathbf{Z}/611$ uses arithmetic mod 611 on $\{0, 1, \ldots, 610\}$.

Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity.

Pick $\alpha \in \mathbf{C}$, root of f.

$$\mathbf{Q}(\alpha) \leftarrow \mathcal{O} \leftarrow \mathbf{Z}[\alpha] \xrightarrow{\alpha \mapsto m} \mathbf{Z}/n$$

Here α matches $\sqrt{14}$
for $n = 611, d = 2$.

$$\mathbf{Q}(\alpha) = \left\{ \begin{array}{l} r_0 + r_1\alpha + r_2\alpha^2 + \\ \cdots + r_{d-1}\alpha^{d-1} : \\ r_0, \ldots, r_{d-1} \in \mathbf{Q} \end{array} \right\}$$

$$\uparrow$$

$$\mathcal{O} = \left\{ \begin{array}{c} \text{algebraic integers} \\ \text{in } \mathbf{Q}(\alpha) \end{array} \right\}$$

$$\uparrow$$

$$\mathbf{Z}[\alpha] = \left\{ \begin{array}{l} i_0 + i_1\alpha + \\ \cdots + i_{d-1}\alpha^{d-1} : \\ i_0, \ldots, i_{d-1} \in \mathbf{Z} \end{array} \right\}$$

$$\downarrow \alpha \mapsto m$$

$$\mathbf{Z}/n = \{0, 1, \ldots, n-1\}$$

Several more details, e.g., $\mathbf{Q} \neq \mathbf{Z}[\alpha]$,
so need to deal with denminators.

How to factor in $\mathcal{O}$?
Actually work with
norm$(i - j\alpha) =$
$i^d + \cdots + f_0 j^d = j^d f(i/j)$.

Asymptotic cost exponents

Number of bit operations
in number-field sieve,
is $L^{b+o(1)}$ where
$L = \exp((\ln n)^{1/3}(\ln \ln n)^{2/3})$.
and $b = (92 + 26\sqrt{13})^{1/3}/3$
$= 1.9018836118\ldots$.