Factoring pq^2 with hints

Antoine Joux

September 2009

Main motivation: NICE cryptosystem

- Many cryptosystems make use of pq^2
  - Esign
  - Okamoto/Uchiyama encryption
  - Fast RSA variants

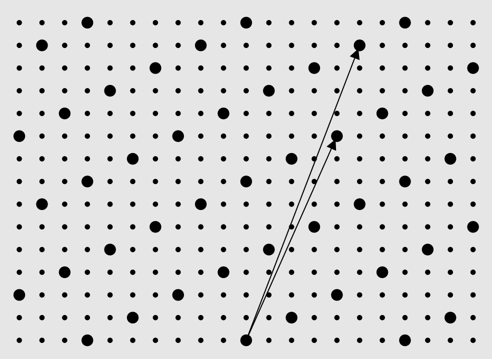
- A large family uses pq^2 with quadratic fields
  - Buchmann and Williams key exchange
  - NICE cryptosystems

A little detour

Lattices

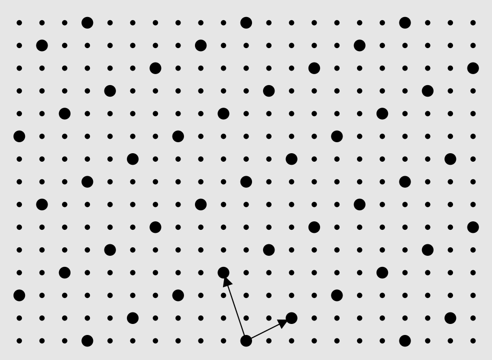
- A lattice is a discrete subgroup of $\mathbb{R}^n$
- Equivalently, set of integral linear combinations:

$$\alpha_1 \vec{b_1} + \cdots + \alpha_n \vec{b}_m \quad \text{with } m \leq n$$



Lattice reduction

- Lattice reduction looks for a "good" basis
- Easy to view in dimension 2



Gauss's reduction algorithm

Require: Initial lattice basis $(\vec{u}, \vec{v})$

if $\|\vec{u}\| < \|\vec{v}\|$ **then**

Exchange $\vec{u}$ and $\vec{v}$

end if

repeat

Minimize $\|\vec{u} - \lambda\vec{v}\|$, i.e., $\lambda \longleftarrow \left\lfloor (\vec{u}|\vec{v})/\|\vec{v}\|^2 \right\rceil$

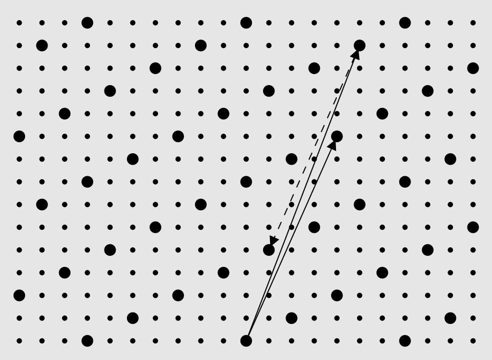
Let $\vec{u} \longleftarrow \vec{u} - \lambda\vec{v}$

Swap $\vec{u}$ and $\vec{v}$

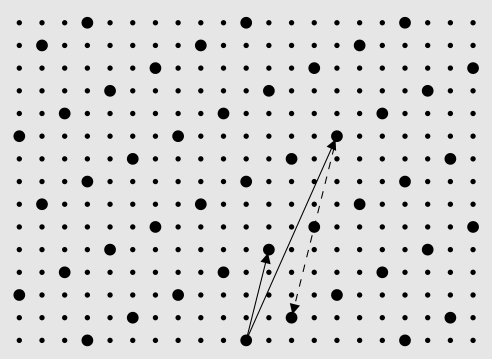
until $\|u\| \leq \|v\|$

Output $(\vec{u}, \vec{v})$ as reduced basis

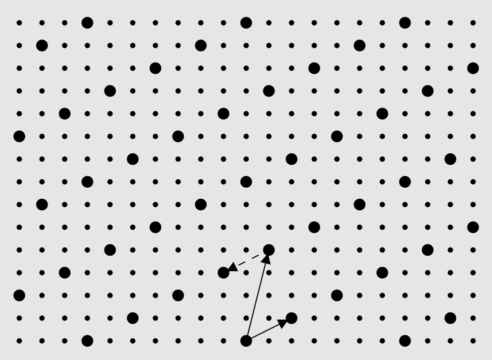
Gauss's reduction algorithm



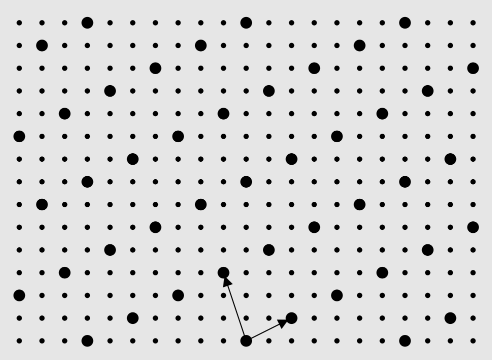
Gauss's reduction algorithm



Gauss's reduction algorithm



Gauss's reduction algorithm



Lenstra-Lenstra-Lovász (1982)

- Polynomial time algorithm for arbitrary dimension
- Combines Gauss's algorithm and Gram-Schmidt orthogonalization
- Enforces the following properties on the output basis:

$$\forall\, i < j \quad : \quad \left|(\vec{b}_j|\vec{b}_i^*)\right| \leq \frac{\|\vec{b}_i^*\|^2}{2}$$

$$\forall\, i \quad : \quad \delta\|\vec{b}_i^*\|^2 \leq \left(\|\vec{b}_{i+1}^*\|^2 + \frac{(\vec{b}_{i+1}|\vec{b}_i^*)^2}{\|b_i^*\|^2}\right)$$

- Implies (note: $1/4 < \delta \leq 1$):

$$(\delta - 1/4)\,\|\vec{b}_i^*\|^2 \leq \|\vec{b}_{i+1}^*\|^2$$

A key property of LLL-reduced bases

- First vector is "quite short"

$$\lambda_1 \geq \left(\delta - \frac{1}{4}\right)^{(n-1)/2} \|\vec{b}_1\|$$

$$\det(L) \geq \left(\delta - \frac{1}{4}\right)^{n(n-1)/4} \|\vec{b}_1\|^n$$

- Often used with $\delta = 3/4$:

$$\|\vec{b}_1\| \leq 2^{(n-1)/2}\lambda_1$$

$$\|\vec{b}_1\| \leq 2^{(n-1)/4}\det(L)^{1/n}$$

Back to NICE

Quadratic Fields

- Fields obtained by adjoining $\sqrt{d}$ (d squarefree) to $\mathbb{Q}$
- The conjugate of $x = a + b \cdot \sqrt{d}$ is $\bar{x} = a - b \cdot \sqrt{d}$
- The norm N_x of x is $x\,\bar{x} = a^2 - d \cdot b^2$
- The trace T_x of x is $x + \bar{x} = 2 \cdot a$
- The values x and $\bar{x}$ are the solutions of

$$X^2 - T_x \cdot X + N_x = 0.$$

- When N_x and T_x are integers: x is an algebraic integer
  - Either a and b are integers
  - Or $a = A/2$, $b = B/2$ (A, B odd integers)
    And $d \equiv 1 \pmod 4$

Quadratic Fields

- Define $\Delta = 4d$ or d (when $d \equiv 1 \pmod 4$)
- Let:

$$\omega = \frac{1}{2}(\Delta + \sqrt{\Delta})$$

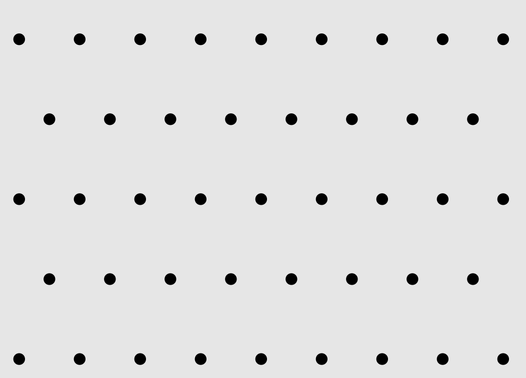
- Algebraic integers are numbers of the form:

$$a + b\omega$$

for all integers a, b

Imaginary Quadratic Fields ($d < 0$)

- If $x \neq 0$ and $x \neq \pm 1$ then $N_x > 1$ (except $d = -1$ and -3)
- Algebraic integers ($\mathcal{O}_{\Delta_K}$)form a lattice (here $\sqrt{-7}$):



Ideals and fractional ideals

- An ideal of $\mathcal{O}_{\Delta_K}$ is simply a sublattice
- Fractional ideal:
  - Becomes an ideal after multiplication by some integer
- Invertible fractional ideals form a group
- For x is in $\mathbb{Q}[\sqrt{d}]$, $x \cdot \mathcal{O}_{\Delta_K}$ is a fractional ideal
  - Subgroup of principal ideals
- Quotient group is the **Ideal class group**
- Cardinality is called **Class number** or $h(\mathcal{O}_{\Delta_K})$
- Notion of **reduced ideal** makes this effective

Representing ideals

- Any ideal can be written as:

$$m\left(a\mathbb{Z} + \frac{-b+\sqrt{\Delta}}{2}\mathbb{Z}\right),$$

  with $a > 0$ and $b^2 \equiv \Delta \pmod{4a}$.
- When $m = 1$, **primitive** ideal
- Representation is normal when $-a < b \leq a$
- Reduction Step (on normal rep.)
  - Multiply ideal by $\frac{-b-\sqrt{\Delta}}{2}$
  - Obtain:

$$a\left(\left(\frac{b^2-\Delta}{4a}\right)\mathbb{Z} + \frac{-b-\sqrt{\Delta}}{2}\mathbb{Z}\right) \Rightarrow \left(c\,\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right)$$

- Yields unique reduced form (with $a \leq c$)

Real Quadratic Fields ($d > 0$)

- Algebraic integers form a dense subset of $\mathbb{R}$
- There is a class group

- When $N_x = \pm 1$ and $x \neq \pm 1$, we say that x is a unit
  - Example: $(1+\sqrt{5})/2$ is a unit in $\mathbb{Q}[\sqrt{5}]$:

$$\frac{(1+\sqrt{5})\cdot(1-\sqrt{5})}{4} = (1-5)/4 = -1$$

- There exists $\epsilon > 0$ such that all units are of the form:

$$\pm\epsilon^i$$

- The **Regulator** is $R_d = \log\epsilon$

$$\log\left(\frac{1}{2}(\sqrt{\Delta-4}+\sqrt{\Delta})\right) \leq R_d < \sqrt{\frac{1}{2}\Delta}\left(\frac{1}{2}\log\Delta + 1\right).$$

- Cycle of reduced forms (short for small regulator)

Reduced forms for real fields

- Form considered normal when:

$$-|a| < b \leq |a| \text{ for } |a| \geq \sqrt{\Delta}$$

$$\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta} \text{ for } |a| < \sqrt{\Delta}$$

- Reduced when:

$$\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta}$$

- Example of reduced form, the principal form:

$$(a, b, c) = \left(1, \lfloor\lfloor\sqrt{\Delta}\rfloor\rfloor, \frac{\left(\lfloor\lfloor\sqrt{\Delta}\rfloor\rfloor^2 - \Delta\right)}{4}\right)$$

Cycle of reduced forms

- Take $\Delta = 101$, the principal form is: $(1, 9, -5)$
- Reduction takes it to $(-5, 1, 5)$
- Then $(5, 9, -1)$, $(-1, 9, 5)$, $(5, 1, -5)$,$(-5, 9, 1)$
- And back to $(1, 9, -5)$

- A reduction step sends (a, b, c) to

$$\left(c, r(-b, c), \frac{r(-b, c)^2 - \Delta}{4c}\right)$$

The NICE cryptosystem

- Makes use of “hidden” quadratic field:

$$\mathbb{Q}[\sqrt{N}],$$

  with $N = \pm pq^2$
- This is essentially $\mathbb{Q}[\sqrt{\pm p}]$
- Usual NICE (imaginary case):
  - Gives as public information an ideal in $\mathbb{Q}[\sqrt{-pq^2}]$ which vanishes in $\mathbb{Q}[\sqrt{-p}]$
- Real NICE
  - p chosen with small regulator

$$\Rightarrow \text{Hints on the factorization of } pq^2$$

How to express the hints

- In both cases, can be rewritten as a polynomial:

$$f(X_0, X_1) = aX_0^2 + bX_0X_1 + cX_1^2$$

  with a small root (x_0, x_1) modulo q^2
- Finding (x_0, x_1) yields the factorization

- Imaginary: further reduction of kernel element in $\mathbb{Q}[\sqrt{-p}]$
- Real: On cycle, we have (a, b, c) close to $(q^2, kq, (k^2 - p)/4)$
  - Need several trials (small number for short cycles)

Coppersmith's small root algorithms

- Modular version, solve polynomial equation:

$$f(x) = 0 \pmod N.$$

  Easy when factorization of N is known. Hard in general.

- Bivariate version, find integral roots of:

$$f(x, y) = 0.$$

  Diophantine equations. Hard in general.

- Modular bivariate: heuristic method.

Homogeneous Variant

- Search rational solutions
- Equivalently, consider homogeneous polynomials
- Modular version, solve polynomial equation:

$$f(x_0, x_1) = 0 \pmod{N}.$$

- Bivariate version, find integral roots of:

$$f(x_0, x_1, y_0, y_1) = 0.$$

  Homogeneous separately in x and y.

A simple case (Howgrave-Graham's variation)

- Search small solutions of:

$$f(x_0, x_1) = a\,x_0^2 + b\,x_0\,x_1 + c\,x_1^2 = 0 \pmod{N}.$$

  W.l.o.g, we may assume $c = 1$.
- Fix two parameters, D and t
- Consider homogeneous polynomials of degree D with root (x_0, x_1) modulo N^t
- Obtained by linearly combining:

$$x_0^{D-2i}\, f(x_0, x_1)^i\, N^{\max(0,t-i)} \qquad \text{and}$$
$$x_0^{D-2i-1}\, x_1\, f(x_0, x_1)^i\, N^{\max(0,t-i)}$$

A simple case

- Use monomial ordering with $x_1 > x_0$
- Head monomial in

$$x_0^{D-2i-\theta} \, x_1^{\theta} \, f(x_0, x_1)^i \, N^{\max(0,t-i)}$$

is $x_1^{2i+\theta} \, x_0^{D-2i-\theta}$ and has coefficient $N^{\max(0,t-i)}$

Interpret polynomials as lattice points

$$([x_0^D], [x_0^{D-1} x_1], \cdots, [x_0 x_1^{D-1}], [x_1^D])$$

A simple case

- Dimension of the lattice $D+1$
- Determinant of the lattice is $N^{t(t+1)}$
- LLL produces a short vector of norm:

$$\leq \; 2^{D/4}\, N^{t(t+1)/(D+1)}$$

- If $|x_0| \leq B$ and $|x_1| \leq B$ the corresponding polynomial at (x_0, x_1) has value less than:

$$\sqrt{D+1}\, 2^{D/4}\, N^{t(t+1)/(D+1)}\, B^D$$

- With $D = 2t$ and letting $t \to \infty$, assuming $B < N^{1/4-\epsilon}$:

$$\sqrt{D+1}\, 2^{D/4}\, N^{t(t+1)/(D+1)}\, B^D < N^t$$

End of the simple case

- As a consequence, get polynomial F with $F(x_0, x_1) = 0$ over $\mathbb{Z}$
- Dehomogenizing, we find $F_a(x_0/x_1) = 0$
- Solve over $\mathbb{R}$
- Recover x_0 and x_1 from root r using continued fractions

f of degree d $\Rightarrow$ Works up to $N^{1/2d}$ bound on x_0 and x_1

Almost what we need

- Here:

$$f(x_0, x_1) = a\,x_0^2 + b\,x_0\,x_1 + c\,x_1^2 = 0 \pmod{q^2}.$$

- But q^2 unknown, instead we know $N = pq^2$
- We need relative sizes and write:

$$q^2 \approx N^{\alpha}$$

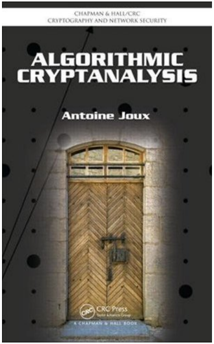
  for $0 < \alpha < 1$.
- The bound on (x_0, x_1) now depends on α, we need:

$$\sqrt{D+1}\,2^{D/4}\,N^{t(t+1)/(D+1)}\,B^D < N^{\alpha t}$$

- Let $D = 2t\alpha$ and get asymptotic bound $B < N^{\alpha^2/4-\epsilon}$.

Homogeneous Coppersmith

- Also used in Bernstein08:
  List decoding for binary Goppa code
- Case $\alpha = 1$ presented in:



Conclusion

Questions ?