## Coppersmith's Theorem XVII: Coppersmith UNLEASHED

Henry Cohn and Nadia Heninger

Which theorem gives us all these awesome things?

1. RSA key recovery

- 2. cryptanalysis of low-exponent stereotyped RSA
- 3. RSA-OAEP+

4. finding smooth integers in short intervals

#### Coppersmith/Howgrave-Graham

#### Let

- $f(x) = x^d + f_{d-1}x^{d-1} + \dots + f_0$ ,
- ► *N* of unknown factorization,
- 0 < β ≤ 1.</li>

## Theorem Can find all $x_0$ such that

$$\gcd(f(x_0), N) > N^eta$$
 $|x_0| < N^{eta^2/d}$ 

in time polynomial in log N and d.

1. Form lattice from coefficients of  $\{f(x)^i N^{k-i}\}_{i=0}^k$ .

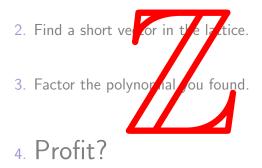
◆□▶ ◆□▶ ◆臣▶ ◆臣▶ □臣 = のへで

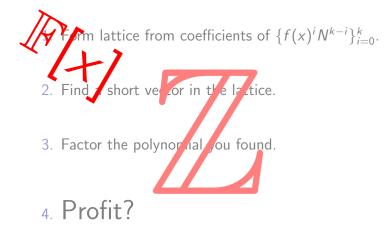
2. Find a short vector in the lattice.

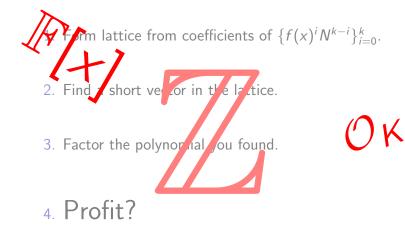
3. Factor the polynomial you found.

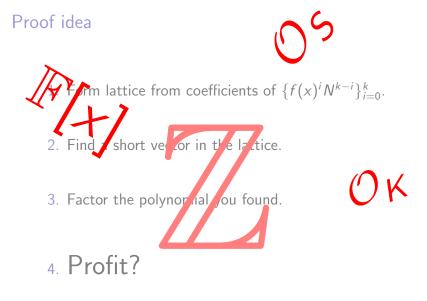
### 4. Profit?

1. Form lattice from coefficients of  $\{f(x)^i N^{k-i}\}_{i=0}^k$ .









#### Polynomials!

Let

- $f(x,y) = y^d + f_{d-1}(x)y^{d-1} + \cdots + f_0(x)$ ,
- N(x) of degree n,
- $0 < \beta \leq 1.$

Theorem Can find all g(x) such that

> $\deg_x \gcd(f(x, g(x)), N(x)) \ge neta$  $\deg_x g(x) \le neta^2/d$

in time polynomial in n and d.

#### Polynomials!

Let

- $f(x,y) = y^d + f_{d-1}(x)y^{d-1} + \dots + f_0(x)$ ,
- N(x) of degree n,

# Reed-Solomon list decoding!

## noisy polynomial interpolation!

 $\deg_x \gcd(f(x,g(x)),N(x)) \ge n\beta$ 

 $\deg_{x} g(x) \leq n\beta^{2}/d$ 

くロン 人間 とくほう 人間 くうへつ

in time polynomial in n and d.

#### Number fields!

Let K n.f. of degree n,  $\mathcal{O}_K$  ring of integers,

• 
$$f(x) = x^d + f_{d-1}x^{d-1} + \dots + f_0 \in \mathcal{O}_K[x]$$

• 
$$I \subseteq \mathcal{O}_K$$
 an ideal,

0 < β ≤ 1.</li>

#### Theorem Can find all $x_0$ with $|x_0|_i < \lambda_i$ such that

$$egin{aligned} &\mathcal{N}(\operatorname{gcd}(f(w)\mathcal{O}_{K},I))>\mathcal{N}(I)^{eta}\ &\prod_{i}\lambda_{i}<(2+o(1))^{-n^{2}/2}\mathcal{N}(I)^{eta^{2}/d} \end{aligned}$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

in time polynomial in n,  $\log N(I)$ , and d.

#### Number fields!

Let K n.f. of degree n,  $\mathcal{O}_{K}$  ring of integers, •  $f(x) = x^d + f_{d-1}x^{d-1} + \dots + f_0 \in \mathcal{O}_K[x]$ solving BDD in ideal lattices! finding smooth elements in number fields!  $N(I)^{\beta}$  $\prod \lambda_i < (2 + o(1))^{-n^2/2} N(I)^{\beta^2/d}$ 

in time polynomial in n,  $\log N(I)$ , and d.

#### Function fields!

Let K f.f., over curve  $\mathcal{X}$ , D divisor,  $S \subseteq \mathcal{X}(\mathbb{F}_q)$ ,

- $f(x) = x^d + f_{d-1}x^{d-1} + \cdots + f_0 \in \mathcal{O}_S$ ,
- $I \subset \mathcal{O}_S$  an ideal,
- 0 < β ≤ 1.</li>

## Theorem Can find all $x_0 \in (D)$ such that

$$egin{aligned} &\mathcal{N}( ext{gcd}(f(x_0)\mathcal{O}_{\mathcal{S}},I)) \geq \mathcal{N}(I)^eta \ & q^{ ext{deg}(D)} < \mathcal{N}(I)^{eta^2/d} \end{aligned}$$

in probabilistic polynomial time.

#### Function fields!

Let K f.f., over curve  $\mathcal{X}$ , D divisor,  $S \subseteq \mathcal{X}(\mathbb{F}_q)$ , •  $f(x) = x^d + f_{d-1}x^{d-1} + \dots + f_0 \in \mathcal{O}_S$ , •  $I \subset \mathcal{O}_S$  an ideal, •  $0 < \beta \leq 1$ . **list decoding of multi-point list decoding of multi-point b** 

 $N(\operatorname{gcd}(f(x_0)\mathcal{O}_S,I)) \geq N(I)^{\beta}$ 

 $q^{\deg(D)} < N(I)^{\beta^2/d}$ 

in probabilistic polynomial time.

## Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding

http://arxiv.org/abs/1008.1284