CSE291-14: The Number Field Sieve

https://cseweb.ucsd.edu/classes/wi22/cse291-14

Emmanuel Thomé

January 13, 2022

Part 3a

NFS: using higher degree

Factoring with cubic integers

A rosy example

Can we go further?

MPQS is great. Can we do better?

Yes: NFS.

NFS is a compicated algorithm, and we will approach it from several angles.

- Earliest example: cubic integers.
- A simple example where everything goes well.
- We need some mathematical background.
- (next week) sometimes, things are more complicated.

Plan

Factoring with cubic integers

A rosy example

Factoring with cubic integers

John Pollard (who had invented the ρ and $p - 1$ methods decades earlier) came up in 1988 with a nice idea to factor integers of a special form using cubic integers.

The Number Field Sieve (NFS) was born. Note that NFS is not an extension of QS. It is more related on an algorithm by Coppersmith, Odlyzko and Schroeppel (1986) called the linear sieve, to compute discrete logarithms. (not discussed here).

As it turns out, it took a few exciting years to go from Pollard's nifty idea to a full-fledged factoring algorithm.

Factoring with cubic integers

Pollard's method is well suited to numbers of a special form.

Target: $N = 2F_7 = 2(2^{128} + 1) = m^3 + 2$ for $m = 2^{43}$.

A mathematical object that is poised to take a key role is the number field $\mathbb{Q}(\sqrt[3]{-2})$.

A number field

A number field is field that contains $\mathbb{Q}$, and is defined by a defining polynomial with integer coefficients.

Analogy:

$\mathbb{Z}/p\mathbb{Z}$	$K = \mathbb{Q}[x]/f(x)$
quotient of $\mathbb{Z}$ by modulus p.	quotient of $\mathbb{Q}[x]$ by f.
• Work with integers.	• polynomials in $\mathbb{Q}[x]$.
• $\bmod p$ when needed.	• $\bmod f$ when needed.
• field $\Leftrightarrow$ p prime.	• field $\Leftrightarrow$ f irreducible.

Number fields are the main topic of algebraic number theory.

Basic operations work without surprises: $+$, $\times$, inversion with extended Euclidean algorithm (on polynomials).

Notation

In $K = \mathbb{Q}[x]/f(x)$, it is common to use a greek letter, say α, to denote $x \mod f(x)$.

- x is the indeterminate in the polynomial ring $\mathbb{Q}[x]$.
- α is an element of K.

By construction:

- α is a root of $f(x)$ in K.
- α is a generator of K: we have $K = \mathbb{Q}(\alpha)$.

At times, we may also write $\mathbb{Q}(\sqrt[3]{-2})$.

Number fields in software

Nowadays, readily available software can deal with number fields: SageMath, Magma, . . .

```
~ $ sage
+--------------------------------------------------------------------+
| SageMath version 9.4, Release Date: 2021-08-22                     |
| Using Python 3.9.5. Type "help()" for help.                        |
+--------------------------------------------------------------------+
sage: ZP.<x> = ZZ['x']
sage: K.<alpha> = NumberField(x^3+2)
sage: foo = 1 + alpha
sage: foo^2
alpha^2 + 2*alpha + 1
sage: foo^3
3*alpha^2 + 3*alpha - 1
sage: foo^17
-3160*alpha^2 - 44999*alpha - 51679
```

Common traits with $\mathbb{Q}$

$K = \mathbb{Q}[x]/f(x)$ shares many properties with $\mathbb{Q}$.

- ring of integers: the most $\mathbb{Z}$-like ring in K.
  - Usually noted $\mathcal{O}_K$ (my preferred one) or $\mathbb{Z}_K$.
  - The ring of integers of $\mathbb{Q}(\sqrt[3]{-2})$ is $\mathbb{Z}[\sqrt[3]{-2}]$.
  - Unfortunately it's not that easy in general.
- There is a notion that relates to prime numbers and unique factorization.

This is pretty handwavy, but it's enough for us at this point.

Note: a number field can be embedded into a subfield of $\mathbb{C}$.

Two paths to $\mathbb{Z}/N\mathbb{Z}$

We work in $K = \mathbb{Q}[x]/f(x)$, and assume that $f(m) \equiv 0 \mod N$.
Take $\phi(x) \in \mathbb{Z}[x]$. We map it to $\mathbb{Z}/N\mathbb{Z}$ in two ways.

- $\phi(m) \in \mathbb{Z}$, once reduced $\bmod N$, is in $\mathbb{Z}/N\mathbb{Z}$.
- $\phi(\alpha) \in K = \mathbb{Q}(\alpha)$.
  There is a ring morphism:

$$\begin{cases} \mathbb{Z}[\alpha] & \to \mathbb{Z}/N\mathbb{Z} \\ \alpha & \mapsto m. \end{cases}$$

Proof: if two polynomials in $\mathbb{Z}[x]$ differ by a multiple of f, their evaluations at m differ by a multiple of $f(m) \equiv 0 \mod N$.

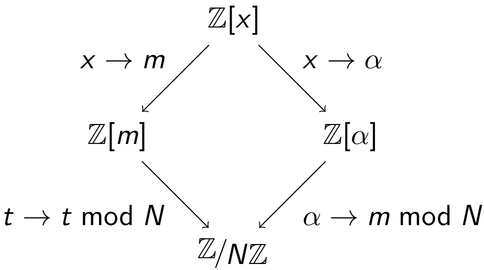
These are two ways to reach $\phi(m) \bmod N \in \mathbb{Z}/N\mathbb{Z}$.

Example

$N = 2F_7 = 2(2^{128}+1)$, $m = 2^{43}$, $f(x) = x^3 + 2$,
$K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f(x)$.

```
sage: N=2^129+2; m=2^43
sage: a=56; b=89
sage: a-b*m
-782852278976456
sage: a-b*alpha
-89*alpha + 56
sage: Integers(N)(a-b*m)
680564733841876926926748432011257446458
sage: Integers(N)((a-b*alpha).polynomial()(m))
680564733841876926926748432011257446458
```

The diagram



This diagram commutes.

We will come back to it later on.

Units

In $\mathbb{Z}$ some elements are invertible: ± 1.

In the ring of integers of a number field, some elements are invertible. These are called units.
There are many units in $\mathbb{Z}[\sqrt[3]{-2}]$.

```
sage: foo = 1 + alpha
sage: foo^-1
-alpha^2 + alpha - 1
sage: foo^17
-3160*alpha^2 - 44999*alpha - 51679
sage: foo^-17
-1861604361*alpha^2 + 2345474521*alpha - 2955112721
```

Find many ϕ

Let B be a smoothness bound.

Consider many polynomials $a - bx$ such that:

- The integer $a - bm$ is B-smooth.
- The element $a - b\alpha$ is smooth in $\mathbb{Q}(\alpha = \sqrt[3]{-2})$: it "factors" into "things" ("primes").

Then maybe we can do something with that.

```
sage: (a-b*m).factor()
-1 * 2^3 * 13 * 23 * 41 * 109 * 211 * 449 * 773
sage: (a-b*alpha).factor()
alpha * (-alpha + 1) * (alpha^2 - 6*alpha + 1) * (7*alpha + 3)
```

Combine many of these so as to get squares on both sides?

Factoring with number fields

TL;DR: It works.

However, in order to make it work, one needs to:

- Describe precisely the “primes” in $\mathbb{Z}[\alpha]$.
  And are we sure that it makes sense at all?
- Describe precisely the units in this ring.

This is entirely doable and we will do it, but we are first going to work with a simpler (made up) example.

Plan

Factoring with cubic integers

A rosy example

Create something absurdly easy

Our goal is to create an example that is even simpler than Pollard's example.

- We're not going to factor anything of computational interest.
- One of my goals is to have all relevant data fit on my slides.

Some number fields are simpler than others, so let's pick a very simple one:

- The degree of a number field is the degree of its definition polynomial. The field in Pollard's example has degree 3. Let's pick one of degree 2: a quadratic field.
- We want to keep control on units.

Units in quadratic fields

When it comes to units, quadratic fields are particularly easy.

In a quadratic field defined by a degree 2 polynomial $f(x) \in \mathbb{Z}[x]$ of discriminant Δ:

- if $\Delta > 1$ units are ± 1, and one unit of infinite order.
- if $\Delta < 0$, all units are of finite order.
  - in most cases, it's only ± 1.
  - special case $\Delta = -\mu^2$ has 4-th roots of unity.
  - special case $\Delta = -3\mu^2$ has 6-th roots of unity.

Quadratic fields are often classified as real quadratic fields and imaginary quadratic fields (they embed in $\mathbb{R}$ or $\mathbb{C}$).

A simple imaginary quadratic field

Let us pick $f(x) = x^2 - x + 3$.

Nice facts about $f(x)$

The number field K defined by f is an imaginary quadratic field.

- K is generated by $\alpha = \frac{1}{2}(1 + \sqrt{-11})$), which is a root of f.
- The of integers $\mathcal{O}_K$ of K is $\mathbb{Z}[\alpha]$.
- There are no units in $\mathcal{O}_K$ beyond ± 1.
- $\mathcal{O}_K$ happens to be a unique factorization domain.
- Primes in $\mathcal{O}_K$:
  - Integer primes p are still prime in $\mathcal{O}_K$ if $\left(\frac{-11}{p}\right) = -1$.
  - Otherwise, p splits into two prime factors.

Primes in $\mathcal{O}_K$

The computer will tell us the following.

$$\begin{array}{c|c} 2, & 17, \\ 3 = \alpha \times (1-\alpha), & 19, \\ 5 = (1+\alpha) \times (2-\alpha), & 23 = (4+\alpha) \times (5-\alpha), \\ 7, & 29, \\ 11 = -(1-2\alpha)^2, & 31 = (4-3\alpha) \times (1+3\alpha), \\ 13, & 37 = (2+3\alpha) \times (5-3\alpha), \quad \ldots \end{array}$$

It is possible to obtain this by hand, but somewhat tedious.

Can we factor a number?

Let us fix $N = 16259 = 16384 - 128 + 3$, and $m = 128$.

Given that $f(x) = x^2 - x + 3$, we have $f(m) \equiv 0 \mod N$.

We will do exactly as hinted at in the description of Pollard's algorithm.

- Enumerate many polynomials $\phi(x) = a - bx$.
- Look for those such that:
  - The integer $\phi(m)$ is smooth.
  - The element $\phi(\alpha)$ in K is smooth as well.

We fix a smoothness bound $B = 40$ (for factors of $f(m)$).

We will soon get to what this may mean on the number field side.

Relations

Try to factor values $f(m)$.

$1 - 1m = -127 = -127,$
$1 - 2m = -255 = -3 \times 5 \times 17,$
$1 - 3m = -383 = -383,$
$1 - 4m = -511 = -7 \times 73,$
$1 - 5m = -639 = -3^2 \times 71,$
$2 - 1m = -126 = -2 \times 3^2 \times 7,$
$2 - 3m = -382 = -2 \times 191,$
$2 - 5m = -638 = -2 \times 11 \times 29,$
$3 - 1m = -125 = -5^3,$
$3 - 2m = -253 = -11 \times 23,$
$3 - 4m = -509 = -509,$
$3 - 5m = -637 = -7^2 \times 13,$
$4 - 1m = -124 = -2^2 \times 31,$
$4 - 3m = -380 = -2^2 \times 5 \times 19,$
$4 - 5m = -636 = -2^2 \times 3 \times 53,$
$5 - 1m = -123 = -3 \times 41,$
$5 - 2m = -251 = -251,$
$5 - 3m = -379 = -379,$
$5 - 4m = -507 = -3 \times 13^2,$
$6 - 1m = -122 = -2 \times 61,$
$6 - 5m = -634 = -2 \times 317,$
$7 - 1m = -121 = -11^2,$
$7 - 2m = -249 = -3 \times 83,$
$7 - 3m = -377 = -13 \times 29,$
$7 - 4m = -505 = -5 \times 101,$
$7 - 5m = -633 = -3 \times 211,$
$8 - 1m = -120 = -2^3 \times 3 \times 5,$
$8 - 3m = -376 = -2^3 \times 47,$

Keep only the smooth ones!

Here are all the first few smooth $a - bm$ values for small a, b.

$1 - 2m = -255 = -3 \times 5 \times 17,$
$2 - 1m = -126 = -2 \times 3^2 \times 7,$
$2 - 5m = -638 = -2 \times 11 \times 29,$
$3 - 1m = -125 = -5^3,$
$3 - 2m = -253 = -11 \times 23,$
$3 - 5m = -637 = -7^2 \times 13,$
$4 - 1m = -124 = -2^2 \times 31,$
$4 - 3m = -380 = -2^2 \times 5 \times 19,$
$5 - 4m = -507 = -3 \times 13^2,$
$7 - 1m = -121 = -11^2,$
$7 - 3m = -377 = -13 \times 29,$
$8 - 1m = -120 = -2^3 \times 3 \times 5,$
$9 - 1m = -119 = -7 \times 17,$
$9 - 2m = -247 = -13 \times 19,$
$10 - 3m = -374 = -2 \times 11 \times 17,$
$11 - 1m = -117 = -3^2 \times 13,$
$11 - 2m = -245 = -5 \times 7^2,$
$11 - 5m = -629 = -17 \times 37,$
$12 - 1m = -116 = -2^2 \times 29,$
$13 - 1m = -115 = -5 \times 23,$
$13 - 2m = -243 = -3^5,$
$13 - 5m = -627 = -3 \times 11 \times 19,$
$14 - 1m = -114 = -2 \times 3 \times 19,$
$14 - 3m = -370 = -2 \times 5 \times 37,$
$16 - 1m = -112 = -2^4 \times 7,$
$16 - 3m = -368 = -2^4 \times 23,$
$16 - 5m = -624 = -2^4 \times 3 \times 13,$
$17 - 1m = -111 = -3 \times 37,$

Number field side

Same deal.
I haven't said how we can factor in K yet.

$$\begin{aligned}
1-\alpha &= (1-\alpha), \\
1-2\alpha &= (1-2\alpha), \\
1-3\alpha &= (2-\alpha)^2, \\
1-4\alpha &= (1-\alpha)^2 \times (1+\alpha), \\
1-5\alpha &= (1-5\alpha), \\
2-\alpha &= (2-\alpha), \\
2-3\alpha &= -(1+\alpha)^2, \\
2-5\alpha &= (1-\alpha) \times (5-\alpha), \\
3-\alpha &= -(\alpha)^2,
\end{aligned}
\qquad
\begin{aligned}
3-2\alpha &= -(\alpha) \times (1+\alpha), \\
3-4\alpha &= -(\alpha)^2 \times (2-\alpha), \\
3-5\alpha &= -(\alpha) \times (4+\alpha), \\
4-\alpha &= (1-\alpha) \times (1+\alpha), \\
4-3\alpha &= (4-3\alpha), \\
4-5\alpha &= (4-5\alpha), \\
5-\alpha &= (5-\alpha), \\
5-2\alpha &= -(1-\alpha)^3, \\
5-3\alpha &= (5-3\alpha),
\end{aligned}$$

Side note: there are no "integer primes" in these factorizations.
There is a reason for that.

When are both sides smooth?

$$
\begin{aligned}
1+3m &= 5\times 7\times 11 & 1+3\alpha &= (3\alpha+1),\\
1-2m &= -3\times 5\times 17 & 1-2\alpha &= -(2\alpha-1),\\
2+1m &= 2\times 5\times 13 & 2+1\alpha &= -(-\alpha+1)^2,\\
2-1m &= -2\times 3^2\times 7 & 2-1\alpha &= (-\alpha+2),\\
2-5m &= -2\times 11\times 29 & 2-5\alpha &= (-\alpha+1)\times(-\alpha+5),\\
3+2m &= 7\times 37 & 3+2\alpha &= -(\alpha)^3,\\
3-1m &= -5^3 & 3-1\alpha &= -(\alpha)^2,\\
3-2m &= -11\times 23 & 3-2\alpha &= -(\alpha)\times(\alpha+1),\\
3-5m &= -7^2\times 13 & 3-5\alpha &= -(\alpha)\times(\alpha+4),\\
4+5m &= 2^2\times 7\times 23 & 4+5\alpha &= -(-\alpha+1)\times(-3\alpha+5),\\
4+1m &= 2^2\times 3\times 11 & 4+1\alpha &= (\alpha+4),\\
4-1m &= -2^2\times 31 & 4-1\alpha &= (-\alpha+1)\times(\alpha+1),\\
4-3m &= -2^2\times 5\times 19 & 4-3\alpha &= (-3\alpha+4),\\
5+1m &= 7\times 19 & 5+1\alpha &= (-\alpha+1)\times(2\alpha-1),\\
7-1m &= -11^2 & 7-1\alpha &= -(-\alpha+1)^2\times(-\alpha+2),
\end{aligned}
$$

$$\ldots$$

Put these in a matrix

	-1	2	3	5	7	11	13	17	19	23	29	31	37	-1	$1-\alpha$	α	$2-\alpha$	$1+\alpha$	$2\alpha-1$	$\alpha-5$	$\alpha+4$	$-3\alpha+4$	$3\alpha+1$	$-3\alpha-2$	$3\alpha-5$
$(1,-3)$				1	1	1																	1		
$(1,2)$	1		1	1				1						1					1						
$(2,-1)$		1		1			1							1	2										
$(2,1)$	1	1	2		1												1								
$(2,5)$	1	1				1					1				1					1					
$(3,-2)$					1								1	1		3									
$(3,1)$	1			3										1		2									
$(3,2)$	1					1				1				1		1		1							
$(3,5)$	1				2		1							1		1					1				
$(4,-5)$		2			1					1				1	1										1
$(4,-1)$		2	1			1															1				
$(4,1)$	1	2										1			1			1							
$(4,3)$	1	2		1					1													1			
$(5,-1)$					1				1						1				1						
$(7,1)$	1					2								1	2		1								

(a few more rows below!)

Put these in a matrix

	-1	2	3	5	7	11	13	17	19	23	29	31	37	-1	$1-\alpha$	α	$2-\alpha$	$1+\alpha$	$2\alpha-1$	$\alpha-5$	$\alpha+4$	$-3\alpha+4$	$3\alpha+1$	$-3\alpha-2$	$3\alpha-5$
$(1,-3)$				1	1	1																	1		
$(1,2)$	1		1	1				1						1					1						
$(2,-1)$		1		1			1							1											
$(2,1)$	1	1			1												1								
$(2,5)$	1	1				1					1				1					1					
$(3,-2)$					1								1	1		1									
$(3,1)$	1			1										1											
$(3,2)$	1					1				1				1		1		1							
$(3,5)$	1						1							1		1					1				
$(4,-5)$					1					1				1	1										1
$(4,-1)$			1			1															1				
$(4,1)$	1											1			1			1							
$(4,3)$	1			1					1													1			
$(5,-1)$					1				1						1				1						
$(7,1)$	1													1			1								

(a few more rows below!)

Linear algebra

We must find a nullspace element.

This will guarantee an even valuation for all primes that appear, and also an even number of -1's (on both sides).

Here is what the knowledge of a nullspace element tells us:

$$\begin{aligned} R(x) = {} & (2x+3) \times (-3x+7) \times (x+8) \times (-2x+9) \\ & \times (-x+14) \times (-x+16) \times (-x+17) \times (-4x+19). \end{aligned}$$

This gives:

$$\begin{aligned} R(m) &= 2^8 \times 3^2 \times 7^2 \times 13^2 \times 17^2 \times 19^2 \times 29^2 \times 37^2, \\ R(\alpha) &= (\alpha)^4 \times (-\alpha+1)^8 \times (\alpha+1)^2 \times (-\alpha+2)^6 \\ &\quad \times (2\alpha-1)^2 \times (-3\alpha+5)^2. \end{aligned}$$

Done!

At this point we are pretty much done.

$$\begin{aligned}
\sqrt{R(128)} &= 2^4 \times 3 \times 7 \times 13 \times 17 \times 19 \times 29 \times 37 \\
&= 1513857072 \equiv 14100 \mod N. \\
\sqrt{R(\alpha)} &= (\alpha)^2 \times (-\alpha + 1)^4 \times (\alpha + 1) \times (-\alpha + 2)^3 \\
&\quad \times (2\alpha - 1) \times (-3\alpha + 5), \\
\sqrt{R(\alpha)} &= -3735\alpha + 13995. \\
\sqrt{R(\alpha)} &\mapsto -464085 \equiv 7426 \mod N.
\end{aligned}$$

And

$$\gcd(14100 - 7426, 16259) = 71.$$

Yes, this is all cheating

Some hurdles were deliberately sidestepped in the previous example.

- No real use case for number fields of degree 2.
- The ring of integers (which we haven't properly defined) is rarely as simple as $\mathbb{Z}[\alpha]$.
- Units are never as simple as $\{\pm 1\}$.
- We don't even have unique factorization in general! However, we do have something interesting with ideals in the ring of integers $\mathcal{O}_K$.

Next: algebraic number theory background.