Polynomial factorization over $\mathbb{Q}$

MPRI – Efficient algorithms in computer algebra

Pierre Lairez

Factorization reveals interesting phenomena

1. pick a random $f \in \mathbb{Q}[t, x, y]$
2. compute $\Delta = \mathrm{disc}_x(\mathrm{disc}_y(f))$
3. compute the irreducible factors of Δ

Factorization reveals interesting phenomena

1. pick a random $f \in \mathbb{Q}[t, x, y]$
2. compute $\Delta = \operatorname{disc}_x(\operatorname{disc}_y(f))$
3. compute the irreducible factors of Δ

How to compute the irreducible factors of Δ?

1st step: factorization over $\mathbb{F}_q$, q odd

2nd step: factorization over $\mathbb{Q}$ $\leftarrow$ today

L. Busé, B. Mourrain (2009). "Explicit Factors of Some Iterated Resultants and Discriminants". In: *Math. Comp.* 78.265, pp. 345–386. DOI: 10/ccjgkw

Definitions

A polynomial $f \in \mathbb{Q}[x]$ is *irreducible* if it is not the product of two nonconstant polynomials.

Theorem

Let $f \in \mathbb{Q}[x]$ be a monic polynomial. There are monic irreducible polynomials $g_1, \ldots, g_r \in \mathbb{Q}[x]$, unique up to permutation, such that $f = g_1 \cdots g_r$.

Given f, we want the g_i.

General factorization is undecidable

Theorem (Van der Waerden 1930)

There exists an effective field K such that irreducibility in $K[x]$ is undecidable.

General factorization is undecidable

Theorem (Van der Waerden 1930)

There exists an effective field K such that irreducibility in $K[x]$ is undecidable.

⚠ No factorization algorithm for abstract fields.
We have to deal with specific properties of the base field.

General factorization is undecidable

Theorem (Van der Waerden 1930)

There exists an effective field K such that irreducibility in $K[x]$ is undecidable.

⚠ No factorization algorithm for abstract fields.
We have to deal with specific properties of the base field.

What are the properties of $\mathbb{Q}$?

B. L. van der Waerden (1930). "Eine Bemerkung über die Unzerlegbarkeit von Polynomen". In: *Math. Ann.* 102.1, pp. 738–739. DOI: 10/dmdkm6

1. Introduction

2. Integer and rational root finding
   2.1 Naive algorithms
   2.2 Better algorithms

3. Factorization
   3.1 Reduction to the integer case
   3.2 Modular algorithms
   3.3 Faster recombination

The problem

input $f \in \mathbb{Q}[x]$ nonzero

output $\{a \in \mathbb{Q} \mid f(a) = 0\}$

Reduction to finding integer roots of integer poly.

Lemma

Let $f \in \mathbb{Q}[x]$ be a monic polynomial and let m be a common denominator of the coefficients. Then $m^{\deg f} f(x/m)$ is monic and has integer coefficients.

NB: α is a zero of $f(x)$ if and only if $m\alpha$ is a zero of $m^{\deg f} f(x/m)$.

Reduction to finding integer roots of integer poly.

Lemma

Let $f \in \mathbb{Q}[x]$ be a monic polynomial and let m be a common denominator of the coefficients. Then $m^{\deg f} f(x/m)$ is monic and has integer coefficients.

NB: α is a zero of $f(x)$ if and only if $m\alpha$ is a zero of $m^{\deg f} f(x/m)$.

Lemma

Let $f \in \mathbb{Z}[x]$ and $\alpha \in \mathbb{Q}$. If f is monic and $f(\alpha) = 0$, then $\alpha \in \mathbb{Z}$.

Proof. Let $\alpha = a/b$, with a and b coprime and $f = x^d + \sum_{i=1}^{d} c_i x^{d-i}$.
Then $f(\alpha) = b^{-d}(a^d + b\sum_{i=1}^{d} c_i a^{d-i} b^{i-1})$. If $f(\alpha) = 0$ then b divides a^d. Since a and b are coprime, this implies that $b = \pm 1$.

Integer root finding: a well-known method

Lemma

Let $f \in \mathbb{Z}[x]$. Let $a \in \mathbb{Z}$. If $f(a) = 0$ then a divides $f(0)$.

Proof. If $f(x) = \sum_{k=0}^{d} c_k x^k$ then $f(0) = f(a) - a \sum_{k=1}^{d} c_k a^{k-1}$.

input $f \in \mathbb{Z}[x]$

output $\{a \in \mathbb{Z} \mid f(a) = 0\}$

Integer root finding: a well-known method

Lemma

Let $f \in \mathbb{Z}[x]$. Let $a \in \mathbb{Z}$. If $f(a) = 0$ then a divides $f(0)$.

Proof. If $f(x) = \sum_{k=0}^{d} c_k x^k$ then $f(0) = f(a) - a \sum_{k=1}^{d} c_k a^{k-1}$.

input $f \in \mathbb{Z}[x]$

output $\{a \in \mathbb{Z} \mid f(a) = 0\}$

def *IntegerRoots*(f)**:**
    $\pm p_1 \cdots p_r \leftarrow$ prime decomposition of $f(0)$
    $S \leftarrow \varnothing$
    for $I \subseteq \{1, \ldots, r\}$**:**
        $a \leftarrow \prod_{i \in I} p_i$
        if $f(a) = 0$ **then** $S \leftarrow S \cup \{a\}$
        If $f(-a) = 0$ **then** $S \leftarrow S \cup \{-a\}$
    return S

Is it good?

Not really...

A size bound

Lemma

Let $f \in \mathbb{Z}[x]$ *such that* $f(0) \neq 0$ *Let* $a \in \mathbb{Z}$*. If* $f(a) = 0$ *then* $|a| \leq |f(0)|$*.*

A size bound

Lemma

Let $f \in \mathbb{Z}[x]$ such that $f(0) \neq 0$ Let $a \in \mathbb{Z}$. If $f(a) = 0$ then $|a| \leq |f(0)|$.

input $f \in \mathbb{Z}[x]$

output $\{a \in \mathbb{Z} \mid f(a) = 0\}$

```
def IntegerRoots(f):
    if f(0) = 0:
        return IntegerRoots(f(x)/x) ∪ {0}
    else:
        S ← ∅
        for a ∈ {−|f(0)|, ..., |f(0)|}:
            if f(a) = 0 then S ← S ∪ {a}
        return S
```

Modular reduction

- To compute an integer a knowing an a priori bound $|a| \leq B$, it is enough to compute $a \pmod{N}$ for some $N > 2B$.

Modular reduction

- To compute an integer a knowing an a priori bound $|a| \leq B$, it is enough to compute $a \pmod N$ for some $N > 2B$.

Lemma

Let $f \in \mathbb{Z}[x]$, $f(0) \neq 0$. *Let* $N > 2|f(0)|$.
Let $A = \{a \in \mathbb{Z} \mid f(a) = 0\}$ *and* $B = \{b \in \mathbb{Z}/N\mathbb{Z} \mid f(b) = 0 \pmod N\}$
Then the reduction modulo N *induces an injection* $A \longrightarrow B$.

Modular reduction

- To compute an integer a knowing an a priori bound $|a| \leq B$, it is enough to compute $a \pmod N$ for some $N > 2B$.

Lemma

Let $f \in \mathbb{Z}[x]$, $f(0) \neq 0$. *Let* $N > 2|f(0)|$.
Let $A = \{a \in \mathbb{Z} \mid f(a) = 0\}$ *and* $B = \{b \in \mathbb{Z}/N\mathbb{Z} \mid f(b) = 0 \pmod N\}$
Then the reduction modulo N *induces an injection* $A \longrightarrow B$.

Proof. The reduction modulo N defines a map $A \longrightarrow B$. If $a, a' \in A$ and $a = a' \pmod N$, then $a = a'$ or $|a - a'| \geq N$, so at least one of a or a' has absolute value $\leq N/2$. The latter possibility contradicts the bound on the elements of A.

Reduction modulo p

input $f \in \mathbb{Z}[x]$ such that $f(0) \neq 0$

output $\{a \in \mathbb{Z} \mid f(a) = 0\}$

```
def IntegerRoots(f):
    p ← a prime number such that p > 2|f(0)|    [how?]
    S ← ∅
    U ← {u ∈ F_p | f(u) = 0}    [how?]
    for u ∈ U:
        compute a ∈ Z such that a ≡ u (mod p) and |a| ≤ p/2
        if f(a) = 0:
            S ← S ∪ {a}
    return S
```

Hensel lifting I

There is a great way to compute the roots of f modulo p^{2^l}.

input $f \in \mathbb{Z}[x], a, y, N \in \mathbb{Z}$

precondition $f(a) = 0 \pmod{N}$ and $yf'(a) = 1 \pmod{N}$

output $\tilde{a} \in \mathbb{Z}$

postcondition $\tilde{a} = a \pmod{N}$ and $f(\tilde{a}) = 0 \pmod{N^2}$

```
def HenselStep(f, a, y, N):
    e ← f(a)
    ã ← a − ey
    return ã
```

Proof. By hypothesis, $e = 0 \pmod{N}$, so $e^2 = 0 \pmod{N^2}$. Taylor's expansion yields

$$\begin{aligned} f(a - ey) &= f(a) - eyf'(a) + e^2(\cdots) \\ &= f(a) - e = 0 \mod N^2 \end{aligned}$$

Hensel lifting II

There is a great way to compute the roots of f modulo p^{2^l}.

input $f \in \mathbb{Z}[x], a, y, N \in \mathbb{Z}$

precondition $f(a) = 0 \pmod{N}$ and $yf'(a) = 1 \pmod{N}$

output $\tilde{a} \in \mathbb{Z}, \tilde{y} \in \mathbb{Z}$

postcondition $\tilde{a} = a \pmod{N}, \tilde{y} = y \pmod{N}, f(\tilde{a}) = 0 \pmod{N^2}$
and $\tilde{y}f'(\tilde{a}) = 1 \pmod{N^2}$

Hensel lifting II

There is a great way to compute the roots of f modulo p^{2^l}.

input $f \in \mathbb{Z}[x], a, y, N \in \mathbb{Z}$

precondition $f(a) = 0 \pmod N$ and $yf'(a) = 1 \pmod N$

output $\tilde{a} \in \mathbb{Z}, \tilde{y} \in \mathbb{Z}$

postcondition $\tilde{a} = a \pmod N, \tilde{y} = y \pmod N, f(\tilde{a}) = 0 \pmod{N^2}$ and $\tilde{y}f'(\tilde{a}) = 1 \pmod{N^2}$

def *HenselStep*(f, a, y, N)**:**

$\quad e \leftarrow f(a)$

$\quad \tilde{a} \leftarrow a - ey$

$\quad e \leftarrow yf'(\tilde{a}) - 1$

$\quad \tilde{y} \leftarrow y(1 - e)$

$\quad$ **return** $\tilde{a}, \tilde{y}$

Proof. $\tilde{y}f'(\tilde{a}) - 1 = (yf'(\tilde{a}) - 1) - eyf'(\tilde{a}) = e - e = 0 \mod N^2$.

Hensel lifting III

input $f \in \mathbb{Z}[x], a, N \in \mathbb{Z}, B > 0$

precondition $f(a) = 0 \pmod N$ and $f'(a)$ invertible modulo N

output $\tilde{a} \in \mathbb{Z}, M \in \mathbb{Z}$

postcondition $f(\tilde{a}) = 0 \pmod M$ and $M > B$

```
def HenselLift(f, a, N, B):
    y ← f'(a)^{-1} (mod N)    [How?]
    while N < B:
        a, y ← HenselStep(f, a, y, N)
        N ← N^2
    return a, N
```

Hensel lifting: full algorithm

input $f \in \mathbb{Z}[x]$ with $f(0) \neq 0$

output $\{a \in \mathbb{Z} \mid f(a) = 0\}$

def *IntegerRoots*(f)**:**

    $B \leftarrow |f(0)|$

    $f \leftarrow f/\gcd(f, f')$

    $p \leftarrow 2$

    while $\operatorname{disc}(f) = 0 \pmod{p}$**:**

        $p \leftarrow$ *nextprime*(p)

    $S \leftarrow \varnothing$

    $U \leftarrow \left\{u \in \mathbb{F}_p \,\middle|\, f(u) = 0\right\}$

    for $u \in U$**:**

        $a, N \leftarrow$ *HenselLift*$(f, a, p, 2B)$

        if $2a > N$ **then** $a \leftarrow a - N$

        if $f(a) = 0$ **then** $S \leftarrow S \cup \{a\}$ [do we need this?]

    return S

Outline

1. Introduction

2. Integer and rational root finding
   2.1 Naive algorithms
   2.2 Better algorithms

3. Factorization
   3.1 Reduction to the integer case
   3.2 Modular algorithms
   3.3 Faster recombination

Reduction to the integer case

Lemma

If $g \in \mathbb{Q}[x]$ is irreducible, then $m^{\deg g} g(x/m)$ is irreducible, for any nonzero $m \in \mathbb{Q}$.

Reduction to the integer case

Lemma

If $g \in \mathbb{Q}[x]$ *is irreducible, then* $m^{\deg g} g(x/m)$ *is irreducible, for any nonzero* $m \in \mathbb{Q}$.

Lemma

If $f = g_1 \cdots g_r$ *is the irreducible factorization of* f,
then $m^{\deg f} f(x/m) = \prod_i m^{\deg g_i} g_i(x/m)$ *is the irreducible factorization of* $m^{\deg f} f(x/m)$.

Reduction to the integer case

Lemma

If $g \in \mathbb{Q}[x]$ is irreducible, then $m^{\deg g} g(x/m)$ is irreducible, for any nonzero $m \in \mathbb{Q}$.

Lemma

*If $f = g_1 \cdots g_r$ is the irreducible factorization of f,
then $m^{\deg f} f(x/m) = \prod_i m^{\deg g_i} g_i(x/m)$ is the irreducible factorization of $m^{\deg f} f(x/m)$.*

Lemma

Let $f \in \mathbb{Q}[x]$ be a monic polynomial and let m be a common denominator of the coefficients. Then $m^{\deg f} f(x/m)$ is monic and has integer coefficients.

Reduction to the integer case

Lemma

If $g \in \mathbb{Q}[x]$ is irreducible, then $m^{\deg g} g(x/m)$ is irreducible, for any nonzero $m \in \mathbb{Q}$.

Lemma

If $f = g_1 \cdots g_r$ is the irreducible factorization of f, then $m^{\deg f} f(x/m) = \prod_i m^{\deg g_i} g_i(x/m)$ is the irreducible factorization of $m^{\deg f} f(x/m)$.

Lemma

Let $f \in \mathbb{Q}[x]$ be a monic polynomial and let m be a common denominator of the coefficients. Then $m^{\deg f} f(x/m)$ is monic and has integer coefficients.

Gauss Lemma

Let $f \in \mathbb{Z}[x]$. If f is monic, then every monic polynomial $g \in \mathbb{Q}[x]$ which divides f has integer coefficients.

Kronecker's algorithm

Let $f \in \mathbb{Z}[x]$ monic.
Observation: if $g \in \mathbb{Z}[x]$ divides f, then $g(n)$ divides $f(n)$ for all $n \in \mathbb{Z}$.

input $f \in \mathbb{Z}[x]$ monic

output the irreducible factorization of f

```
def Factor(f):
    pick I ⊂ ℤ such that #I = deg f and f(i) ≠ 0 for i ∈ I
    for every sequence (σ_i)_{i∈I} ∈ ℤ^I such that σ_i divides f(i):
        compute g ∈ ℚ[x] such that g is monic and g(i) = σ_i for i ∈ I
        if g divides f:
            return Factor(g) · Factor(f/g)
    return f
```

Kronecker's algorithm

Let $f \in \mathbb{Z}[x]$ monic.
Observation: if $g \in \mathbb{Z}[x]$ divides f, then $g(n)$ divides $f(n)$ for all $n \in \mathbb{Z}$.

input $f \in \mathbb{Z}[x]$ monic
output the irreducible factorization of f

def *Factor*(f)**:**
    pick $I \subset \mathbb{Z}$ such that $\#I = \deg f$ and $f(i) \neq 0$ for $i \in I$
    for every sequence $(\sigma_i)_{i \in I} \in \mathbb{Z}^I$ such that σ_i divides $f(i)$**:**
        compute $g \in \mathbb{Q}[x]$ such that g is monic and $g(i) = \sigma_i$ for $i \in I$
        if g divides f**:**
            return *Factor*$(g) \cdot$ *Factor*(f/g)
    return f

We can do much better!

A size bound

For $f = \sum_{i=0}^{d} c_i x^i$, let $\|f\|_2 = \left(c_0^2 + \cdots + c_d^2\right)^{\frac{1}{2}}$ and $\|f\|_\infty = \max\{|c_0|, \ldots, |c_d|\}$.

Lemma (Landau-Mignotte)

Let $f, g \in \mathbb{Z}[x]$ monic such that g divides f. Then $\|g\|_\infty \leq \|g\|_2 \leq 2^{\deg g}\|f\|_2$.

A size bound

For $f = \sum_{i=0}^{d} c_i x^i$, let $\|f\|_2 = \left(c_0^2 + \cdots + c_d^2\right)^{\frac{1}{2}}$ and $\|f\|_\infty = \max\{|c_0|, \ldots, |c_d|\}$.

Lemma (Landau-Mignotte)

Let $f, g \in \mathbb{Z}[x]$ monic such that g divides f. Then $\|g\|_\infty \leq \|g\|_2 \leq 2^{\deg g}\|f\|_2$.

Lead to a naive factorization algorithm, but not worth stating it.

Modular reduction

Lemma

Let $f \in \mathbb{Z}[x]$ *monic and* $p > 2^{\deg f + 1}\|f\|_2$ *be a prime number.*
Let $A = \{g \in \mathbb{Z}[x] \mid g$ *monic and divides* $f\}$
and $B = \left\{\bar{g} \in \mathbb{F}_p[x] \,\middle|\, \bar{g}\right.$ *monic and divides* $\left.\bar{f} \pmod p\right\}$
Then the reduction modulo p *induces an injection* $A \longrightarrow B$*.*

Modular reduction

Lemma

Let $f \in \mathbb{Z}[x]$ monic and $p > 2^{\deg f + 1} \|f\|_2$ be a prime number.
Let $A = \{g \in \mathbb{Z}[x] \mid g \text{ monic and divides } f\}$
and $B = \left\{\bar{g} \in \mathbb{F}_p[x] \,\middle|\, \bar{g} \text{ monic and divides } \bar{f} \pmod p\right\}$
Then the reduction modulo p induces an injection $A \longrightarrow B$.

⚠ Irreducible divisors of f may not be mapped to irreducible factors of $\bar{f}$

If $\bar{f}$ is squarefree and if $\bar{f} = g_1 \dots g_r$ is the irreducible decomposition of $\bar{f}$, then the map

$$S \subseteq \{1, \dots, r\} \quad \mapsto \quad \prod_{i \in S} g_i \in B$$

is a bijection.

A factorization algorithm (Musser 1971)

input $f \in \mathbb{Z}[x]$ squarefree and monic

output an irreducible factor of f

def *Factor*(f)**:**
  pick a prime $p > 2^{\deg f+1}\|f\|_2$ such that $\operatorname{disc}(f) \neq 0 \pmod{p}$
  $g_1, \ldots, g_r \leftarrow$ irreducible factors of $f \pmod{p}$
  for k from 1 to $\lfloor r/2 \rfloor$**:**
    for $S \subseteq \{1, \ldots, r\}$ **with** $\#S = k$**:**
      $\bar{h} \leftarrow \prod_{i \in S} g_i$
      compute $h \in \mathbb{Z}[x]$ with $\|h\|_\infty < \frac{p}{2}$ and $h = \bar{h} \pmod{p}$
      if h divides f in $\mathbb{Z}[x]$**:**
        return h
  return f

Combinatorial blowup

Lemma (Swinnerton-Dyer polynomials)

Let p_n be the nth prime number and let $f_n = \prod(x \pm \sqrt{2} \pm \sqrt{3} \pm \cdots \pm \sqrt{p_n}) \in \mathbb{Z}[x]$. The polynomial f_n has degree 2^n, is irreducible and is a product of polynomials of degree at most 2 modulo any prime p.

Combinatorial blowup

Lemma (Swinnerton-Dyer polynomials)

Let p_n be the nth prime number and let $f_n = \prod(x \pm \sqrt{2} \pm \sqrt{3} \pm \cdots \pm \sqrt{p_n}) \in \mathbb{Z}[x]$. The polynomial f_n has degree 2^n, is irreducible and is a product of polynomials of degree at most 2 modulo any prime p.

How do we compute these polynomials?

Combinatorial blowup

Lemma (Swinnerton-Dyer polynomials)

Let p_n be the nth prime number and let $f_n = \prod(x \pm \sqrt{2} \pm \sqrt{3} \pm \cdots \pm \sqrt{p_n}) \in \mathbb{Z}[x]$. The polynomial f_n has degree 2^n, is irreducible and is a product of polynomials of degree at most 2 modulo any prime p.

How do we compute these polynomials?

Why do they split into factors of degree at most two over $\mathbb{F}_p$ (for any prime p)?

Combinatorial blowup

Lemma (Swinnerton-Dyer polynomials)

Let p_n be the nth prime number and let $f_n = \prod(x \pm \sqrt{2} \pm \sqrt{3} \pm \cdots \pm \sqrt{p_n}) \in \mathbb{Z}[x]$. The polynomial f_n has degree 2^n, is irreducible and is a product of polynomials of degree at most 2 modulo any prime p.

How do we compute these polynomials?

Why do they split into factors of degree at most two over $\mathbb{F}_p$ (for any prime p)?

The problem of recombination seems clause to combinatorial NP-complete problems, like SUBSET-SUM.

Is *reducibility* in NP? in P?

Recall that a decision problem is in NP (resp. coNP) if additional data and a polynomial-time computation can convince you that an instance satisfies (resp. does not satisfy) the problem.

Is *reducibility* in NP? in P?

Recall that a decision problem is in NP (resp. coNP) if additional data and a polynomial-time computation can convince you that an instance satisfies (resp. does not satisfy) the problem.

REDUCIBLE

input $f \in \mathbb{Z}[x]$

output YES if f is not irreducible, NO otherwise

Is *reducibility* in NP? in P?

Recall that a decision problem is in NP (resp. coNP) if additional data and a polynomial-time computation can convince you that an instance satisfies (resp. does not satisfy) the problem.

REDUCIBLE

input $f \in \mathbb{Z}[x]$

output YES if f is not irreducible, NO otherwise

REDUCIBLE is in NP. Why?

Is *reducibility* in NP? in P?

Recall that a decision problem is in NP (resp. coNP) if additional data and a polynomial-time computation can convince you that an instance satisfies (resp. does not satisfy) the problem.

REDUCIBLE

input $f \in \mathbb{Z}[x]$

output YES if f is not irreducible, NO otherwise

REDUCIBLE is in NP. Why?

Do you think reducible is NP-complete?

Is *reducibility* in NP? in P?

Recall that a decision problem is in NP (resp. coNP) if additional data and a polynomial-time computation can convince you that an instance satisfies (resp. does not satisfy) the problem.

REDUCIBLE

input $f \in \mathbb{Z}[x]$

output YES if f is not irreducible, NO otherwise

REDUCIBLE is in NP. Why?

Do you think reducible is NP-complete?

REDUCIBLE is in coNP (Cantor 1981).

Is *reducibility* in NP? in P?

Recall that a decision problem is in NP (resp. coNP) if additional data and a polynomial-time computation can convince you that an instance satisfies (resp. does not satisfy) the problem.

REDUCIBLE

input $f \in \mathbb{Z}[x]$

output YES if f is not irreducible, NO otherwise

REDUCIBLE is in NP. Why?

Do you think reducible is NP-complete?

REDUCIBLE is in coNP (Cantor 1981).

Do you know other problems in NP $\cap$ coNP?

Is *reducibility* in NP? in P?

Recall that a decision problem is in NP (resp. coNP) if additional data and a polynomial-time computation can convince you that an instance satisfies (resp. does not satisfy) the problem.

REDUCIBLE

input $f \in \mathbb{Z}[x]$

output YES if f is not irreducible, NO otherwise

REDUCIBLE is in NP. Why?

Do you think reducible is NP-complete?

REDUCIBLE is in coNP (Cantor 1981).

Do you know other problems in NP $\cap$ coNP?

Computing the irreducible factorization is in P! (A. K. Lenstra, H. W. Lenstra, Lovàsz 1982)
Fantastic breakthrough!

Hensel lifting for factorization (Zassenhaus 1969)

input $f, g, h, u, v \in \mathbb{Z}[x]$ and $N > 0$

precondition $f = gh \pmod{N}$ and $1 = ug + vh \pmod{N}$

output $\tilde{g}, \tilde{h}, \tilde{u}, \tilde{b} \in \mathbb{Z}[x]$

postcondition $\tilde{\bullet} = \bullet \pmod{N}, f = \tilde{g}\tilde{h} \pmod{N^2}$ and $1 = \tilde{u}\tilde{g} + \tilde{v}\tilde{h} \pmod{N^2}$

Hensel lifting for factorization (Zassenhaus 1969)

input $f, g, h, u, v \in \mathbb{Z}[x]$ and $N > 0$

precondition $f = gh \pmod{N}$ and $1 = ug + vh \pmod{N}$

output $\tilde{g}, \tilde{h}, \tilde{u}, \tilde{b} \in \mathbb{Z}[x]$

postcondition $\tilde{\bullet} = \bullet \pmod{N}$, $f = \tilde{g}\tilde{h} \pmod{N^2}$ and $1 = \tilde{u}\tilde{g} + \tilde{v}\tilde{h} \pmod{N^2}$

def *HenselStep*(f, g, h, u, v, N)**:**

$e \leftarrow f - gh$

$q, a \leftarrow \mathrm{QuoRem}(ue, h)$

$b \leftarrow ve + gq$

$\tilde{g} \leftarrow g + b$**;** $\tilde{h} \leftarrow h + a$

$e \leftarrow 1 - ug - vh$

$q, a \leftarrow \mathrm{QuoRem}(ue, h)$

$b \leftarrow ve + gq$

$\tilde{u} \leftarrow u + a$**;** $\tilde{v} \leftarrow v + b$

return $\tilde{g}, \tilde{h}, \tilde{u}, \tilde{v}$

Hensel lifting for factorization (Zassenhaus 1969)

input $f, g, h \in \mathbb{Z}[x]$, p prime and $B > 0$

precondition $f = gh \pmod p$ and f is squarefree mod. p

output $\tilde{g}, \tilde{h} \in \mathbb{Z}[x]$ and $l > 0$

postcondition $\tilde{\bullet} = \bullet \pmod p$, $f = \tilde{g}\tilde{h} \pmod{p^l}$ and $p^l > B$

```
def HenselLift(f, g, h, p, B):
    u, v ← ExtendedEuclideanAlgorithm(g, h)
    l ← 1
    while p^l ≤ B:
        g, h, u, v ← HenselStep(f, g, h, u, v, p^l)
        l ← 2l
    return g, h, l
```

Lifting many factors

input $f \in \mathbb{Z}[X], g_1, \ldots, g_r \in \mathbb{Z}[x]$, p prime and $B > 0$

precondition $f = g_1 \cdots g_r \pmod{p}$ and f is squarefree modulo p

output $\tilde{g}_1, \ldots, \tilde{g}_r \in \mathbb{Z}[x]$ and $l > 0$

postcondition $\tilde{\bullet} = \bullet \pmod{p}, f = \tilde{g}_1 \cdots \tilde{g}_r \pmod{p^l}$ and $p^l > B$

Lifting many factors

input $f \in \mathbb{Z}[X], g_1, \ldots, g_r \in \mathbb{Z}[x]$, p prime and $B > 0$

precondition $f = g_1 \cdots g_r \pmod p$ and f is squarefree modulo p

output $\tilde{g}_1, \ldots, \tilde{g}_r \in \mathbb{Z}[x]$ and $l > 0$

postcondition $\tilde{\bullet} = \bullet \pmod p, f = \tilde{g}_1 \cdots \tilde{g}_r \pmod{p^l}$ and $p^l > B$

def *MultiHenselLift*$(f, (g_i)_{1 \le i \le r}, p, B)$**:**
    if $r = 1$ **then return** f**:**
    else:
        $s \leftarrow \lfloor r/2 \rfloor$
        $L, R \leftarrow$ *HenselLift*$(f, g_1 \cdots g_s, g_{s+1} \cdots g_r, p, B)$
        $g_1, \ldots, g_s \leftarrow$ *MultiHenselLift*$(L, (g_1, \ldots, g_s), p, B)$
        $g_{s+1}, \ldots, g_r \leftarrow$ *MultiHenselLift*$(R, (g_{s+1}, \ldots, g_r), p, B)$
        return $g_1, \ldots, g_r$ **and** l

Recombination is the main issue

The recombination problem

input $f \in \mathbb{Z}[x]$, and $g_1, \ldots, g_r \in \mathbb{Z}/p^l\mathbb{Z}[x]$

precondition f is squarefree modulo p, $p^l \gg 1$ and $f = g_1 \cdots g_r \pmod{p^l}$

problem find a non trivial $S \subseteq [r]$ such that $\prod_{i \in S} g_i$ lifts in $\mathbb{Z}[x]$ into a divisor of f.

⚠ We still have the exponential blowup for the recombination!

Linearizing the problem

$$\text{“}\log f = \log g_1 + \cdots + \log g_r\text{”}$$

$$\frac{f'}{f} = \frac{g_1'}{g_1} + \cdots + \frac{g_r'}{g_r}$$

$$f' = \frac{fg_1'}{g_1} + \cdots + \frac{fg_r'}{g_r}$$

Let $g \in \mathbb{Z}[x]$ be a monic divisor of f. Then $g = \prod_{i \in S} g_i \pmod{p^l}$ for some $S \subseteq [r]$. Moreover

$$\frac{fg'}{g} = \sum_i \delta_{i \in S} \frac{fg_i'}{g_i} + p^l e.$$

More size bounds

Lemma

Let $f \in \mathbb{Z}[x]$ *monic and let* $g \in \mathbb{Z}[x]$ *be a monic divisor.*
Then $\|fg^{-1}g'\|_2 \leq \deg(f)2^{\deg f-1}\|f\|_2$.

More size bounds

Lemma

Let $f \in \mathbb{Z}[x]$ *monic and let* $g \in \mathbb{Z}[x]$ *be a monic divisor.*
Then $\|fg^{-1}g'\|_2 \leq \deg(f)2^{\deg f - 1}\|f\|_2$.

Lemma (Hadamard bound)

Let $f, g \in \mathbb{Z}[x]$. *Then* $|\mathrm{res}(f, g)| \leq \|f\|_2^{\deg g}\|g\|_2^{\deg f}$.

Some Euclidean lattices

Let $f \in \mathbb{Z}[x]$ be a squarefree monic polynomial of degree d and
let $g_1, \ldots, g_r \in \mathbb{Z}/p^l\mathbb{Z}[x]$ be the lifts of the irreducible factors of f modulo p.

Let $E = \mathbb{Z}^r \times \mathbb{Z}[x]_{<d} \simeq \mathbb{Z}^{r+d}$.

Let L be the (full rank) subgroup of $\tilde{E}$ generated by

- $(e_i, f\frac{g_i'}{g_i})$, for $1 \leq i < r$;
- $(0, p^l x^j)$, for $0 \leq j < d$.

Let $B = d2^{d-1}\|f\|_2$. Define the following norm on L: $\|(u, h)\|_2 = \left(d^{-1}B^2\|u\|_2^2 + \|h\|_2^2\right)^{\frac{1}{2}}$.

For $A \geq 0$, let L_A be the subgroup of L generated by elements of norm $\leq A$.

Let W be the subgroup of L generated by the $(\mathbf{n}, f\frac{h'}{h})$, where $h \in \mathbb{Z}[x]$ is a monic divisor of f and $h = \prod_i g_i^{n_i} \pmod p$.

Short vectors

Lemma (van Hoeij 2002)

1. $W \subseteq L_{2B}$
   "divisors yield short vectors"
2. *Let* $C > B$. *If* $p^l > d^{d+1} C^d B^d$, *then* $L_C \subseteq W$.
   "short vectors come from divisors"

In particular, $W = L_{2B} = L_C$.

Short vectors

Lemma (van Hoeij 2002)

1. $W \subseteq L_{2B}$
   "divisors yield short vectors"
2. *Let* $C > B$. *If* $p^l > d^{d+1} C^d B^d$, *then* $L_C \subseteq W$.
   "short vectors come from divisors"

   In particular, $W = L_{2B} = L_C$.

Mind the arbitrary gap between B and C!

Short vectors

Lemma (van Hoeij 2002)

1. $W \subseteq L_{2B}$
   "divisors yield short vectors"
2. *Let* $C > B$. *If* $p^l > d^{d+1} C^d B^d$, *then* $L_C \subseteq W$.
   "short vectors come from divisors"

   In particular, $W = L_{2B} = L_C$.

Mind the arbitrary gap between B and C!

Proof of 1. Come from the bound on $\|f \frac{h'}{h}\|_2$.

M. van Hoeij (Aug. 1, 2002). "Factoring Polynomials and the Knapsack Problem". In: *Journal of Number Theory* 95.2, pp. 167–189. DOI: 10/cnzkv3
K. Belabas, M. van Hoeij, J. Klüners, A. Steel (2009). "Factoring Polynomials over Global Fields". In: *J. Théor. Nombres Bordeaux* 21.1, pp. 15–39. DOI: 10/b28w8q

The core proof

Proof of 2. Let $(\mathbf{n}, q) \in L$ such that $d^{-1}B^2\|\mathbf{n}\|_2^2 + \|q\|_2^2 \leq C^2$.
We say that $i \sim j$ if g_i and g_j are part of the same irreducible factor of f in $\mathbb{Z}[x]$. To prove that $(\mathbf{n}, q) \in W$, it is enough to prove that $i \sim j \Rightarrow n_i = n_j$.

The core proof

Proof of 2. Let $(\mathbf{n}, q) \in L$ such that $d^{-1}B^2\|\mathbf{n}\|_2^2 + \|q\|_2^2 \leq C^2$.
We say that $i \sim j$ if g_i and g_j are part of the same irreducible factor of f in $\mathbb{Z}[x]$. To prove that $(\mathbf{n}, q) \in W$, it is enough to prove that $i \sim j \Rightarrow n_i = n_j$.

NB: $n_i = 0 \Leftrightarrow g_i$ divides q.

The core proof

Proof of 2. Let $(\mathbf{n}, q) \in L$ such that $d^{-1}B^2\|\mathbf{n}\|_2^2 + \|q\|_2^2 \leq C^2$.
We say that $i \sim j$ if g_i and g_j are part of the same irreducible factor of f in $\mathbb{Z}[x]$. To prove that $(\mathbf{n}, q) \in W$, it is enough to prove that $i \sim j \Rightarrow n_i = n_j$.

NB: $n_i = 0 \Leftrightarrow g_i$ divides q.

Let $1 \leq i \leq r$. Let h be the irreducible factor of f containing g_i. Consider $\tilde{q} = q - n_i h$.
Note that $\|\tilde{q}\| \leq (d+1)C$.

The core proof

Proof of 2. Let $(\mathbf{n}, q) \in L$ such that $d^{-1}B^2\|\mathbf{n}\|_2^2 + \|q\|_2^2 \leq C^2$.
We say that $i \sim j$ if g_i and g_j are part of the same irreducible factor of f in $\mathbb{Z}[x]$. To prove that $(\mathbf{n}, q) \in W$, it is enough to prove that $i \sim j \Rightarrow n_i = n_j$.

NB: $n_i = 0 \Leftrightarrow g_i$ divides q.

Let $1 \leq i \leq r$. Let h be the irreducible factor of f containing g_i. Consider $\tilde{q} = q - n_i h$.
Note that $\|\tilde{q}\| \leq (d+1)C$.

In $\mathbb{Z}/p^l\mathbb{Z}[x]$, $\tilde{q}$ is a multiple of g_i. So $\mathrm{res}(h, \tilde{q}) = 0 \pmod{p^l}$.

The core proof

Proof of 2. Let $(\mathbf{n}, q) \in L$ such that $d^{-1}B^2\|\mathbf{n}\|_2^2 + \|q\|_2^2 \leq C^2$.
We say that $i \sim j$ if g_i and g_j are part of the same irreducible factor of f in $\mathbb{Z}[x]$. To prove that $(\mathbf{n}, q) \in W$, it is enough to prove that $i \sim j \Rightarrow n_i = n_j$.

NB: $n_i = 0 \Leftrightarrow g_i$ divides q.

Let $1 \leq i \leq r$. Let h be the irreducible factor of f containing g_i. Consider $\tilde{q} = q - n_i h$.
Note that $\|\tilde{q}\| \leq (d+1)C$.

In $\mathbb{Z}/p^l\mathbb{Z}[x]$, $\tilde{q}$ is a multiple of g_i. So $\mathrm{res}(h, \tilde{q}) = 0 \pmod{p^l}$.

But $|\mathrm{res}(h, \tilde{q})| \leq (d+1)^d C^d B^d < p^l$, so $\mathrm{res}(h, \tilde{q}) = 0$.
Since h is irreducible, it follows that h divides $\tilde{q}$.
It follows that $n_j = 0$ for any $j \sim i$.

Computing short vectors

Computing L_B given a basis of L is, in general, NP-hard.
However...

Computing short vectors

Computing L_B given a basis of L is, in general, NP-hard.
However...

Theorem (A. K. Lenstra, H. W. Lenstra, Lovàsz 1982)

If $L_B = L_{2^d B}$, then we can compute L_B in polynomial time.

The final factorization algorithm

input $f \in \mathbb{Z}[x]$ monic squarefree

output $h_1, \ldots, h_s \in \mathbb{Z}[x]$ the irreducible factors of f

```
def Factor(f):
    p ← a prime number such that disc(f) ≠ 0 (mod p)
    g_1, ..., g_r ← Factor(f mod p)
    d ← deg f; B ← d 2^{d-1} ||f||_2; C ← 2^{r+d} B
    l ← d(log_p(d+1) + log_p C + log_p B)
    g̃_1, ..., g̃_r ← MultiHenselLift(f, (g_1, ..., g_r), p^l)
    L ← Lattice {(e_i, f g_i^{-1} g_i')}_{1≤i≤r} ∪ {(0, p^l x^j)}_{0≤j<d} ⊂ Z^r × Z[x]_{<d}
    F ← basis of L_B    [with LLL, because L_B = L_{2^{r+d} B}]
    {(n_i, r_i)}_{1≤i≤s} ← the row-reduced echelon form of F
    return (Lift_Z(∏_{j=1}^{r} g_j^{n_ij}))_{1≤i≤s}
```

The final complexity result

Theorem (Belabas, van Hoeij, Klüners, Steel 2009)

We can compute the irreducible factors of $f \in \mathbb{Z}[x]$ *in* $\tilde{O}(d^8 + d^6(\log\|f\|_\infty)^2)$.

K. Belabas, M. van Hoeij, J. Klüners, A. Steel (2009). "Factoring Polynomials over Global Fields". In: *J. Théor. Nombres Bordeaux* 21.1, pp. 15–39. DOI: 10/b28w8q