Lec17C Berlekamp-Hensel. Michael Monagan

March 16, 2021 12:35 PM

The Berlekamp-Hensel Procedure
(Hans Zassenhaus ~1972)

Input $A \in \mathbb{Z}[x]$ s.t.
$d > 1$
$A = a_d x^d + \dots + a_0$
$\mathrm{cont}(A) = 1$
$\gcd(A, A') = 1$

$\longrightarrow$

Output $f_1, f_2, \dots, f_m \in \mathbb{Z}[x]$ s.t.
f_i irreducible over $\mathbb{Q}$
$A = f_1 f_2 \cdot \dots \cdot f_m$

ϕ_p

① Pick p s.t.
$p \nmid \mathrm{lc}\, A = a_d$
$\gcd(A, A') = 1$ in $\mathbb{Z}_p[x]$

$A \in \mathbb{Z}_p[x]$

② Factor $A \in \mathbb{Z}_p[x]$
Cantor-Zassenhaus
$O(d^3 \log^3 p)$

$A \equiv a_d \cdot g_1 g_2 \cdots g_\ell$, $\ell \geq m$
$g_i \in \mathbb{Z}_p[x]$, monic, irreducible

③ For $j = 1, 2, \dots, \ell$ Hensel lift g_j
using $u_0 = g_j$, $w_0 = a_d \cdot \prod_{i \neq j} g_i$ until
$p^n > 2 a_d \cdot \|f_i\|_\infty$ to obtain
$A \equiv a_d \, g_1^{(n)} \cdot g_2^{(n)} \cdots g_\ell^{(n)} \pmod{p^n}$

monic.

④ Test if $pp(a_d \cdot g_i^{(n)} \bmod p^n) \mid A \;\; \forall i$
Test if $pp(\underbrace{a_d \cdot g_i^{(n)} \cdot g_j^{(n)}}_{\text{expand}} \bmod p^n) \mid A \;\; \forall i \neq j$
etc.

attaching $\mathrm{lc}(A)$.

① Choose one large prime $p > 2 a_d \|f\|_\infty$ to avoid H.L.?
This increases the cost of step ②.

② Choose many small primes p_i and apply CRT.?
This results in too many combinations.

③ Factor mod ~ ln deg a primes and use the factorization
with the least # of factors for the H.L.

④ In 2002 Mark van Hoeij solved the combinatorial search
for factors in step ④.

Factor the following polynomial over $\mathbb{Z}$ by first factoring it modulo a suitably chosen prime p and employing linear Hensel lifting.

```
> a := 35*x^4+77*x^2+51*x-15*x^3-36;
```

$$a := 35\,x^4 - 15\,x^3 + 77\,x^2 + 51\,x - 36$$

```
> gcd(a,diff(a,x));
```

$$1$$

```
> content(a,x);
```

$$1$$

```
> `mod` := mods;
```

$$mod := mods$$

```
> Factor(a) mod 2;
```

$$x\,(x+1)^3$$

NOT SQRFREE

```
> Factor(a) mod 3;
```

$$-x^2\,(x^2+1)$$

```
> Factor(a) mod 11;
```

$$2\,(x+4)\,(x^2-4\,x+5)\,(x-2)$$

```
> Factor(a) mod 13;
```

$$-4\,(x+3)\,(x^2-3\,x+6)\,(x-6)$$

We cannot use p=2 nor p=3 since the polynomial is not square-free modulo those primes.
Let us use p=11 noting that the factorization modulo 11 is square-free hence is assured.

```
> p := 11;
```

$$p := 11$$

```
> alpha := lcoeff(a,x);
```

$$\alpha := 35$$

The Mignotte bound on the the biggest coefficient of any factor of a(x)

```
> d := degree(a,x):
  B := ceil( alpha*maxnorm(a)*2^degree(a,x)*sqrt(d+1) );
```

$$B := 96420$$

```
> p^4-B, p^5-B;
```

$$-81779,\ 64631$$

```
> DiophantSolve := proc(a,b,c,x,p)
  local g,sigma,tau,q,s,t;
      g := Gcdex(a,b,x,'s','t') mod p;
      if g <> 1 then error "a and b are not relatively prime!" fi;
      sigma := Rem(c*s,b,x,'q') mod p;
      # c s a = b (aq) + sigma a
      tau := Expand(c*t+q*a) mod p;
      return( sigma,tau );
  end:
```

Let us lift the first factor $x - 2$ up to the bound Lift u_0

```
> u[0] := x-2 mod p;
```

$$u_0 := x - 2$$

```
> w[0] := Expand( alpha*(x+4)*(x^2-4*x+5) ) mod 11;
```

$$w_0 := 2 x^3 - 4$$

```
> U := u[0];
W := w[0];
for k while p^k < 2*B do
    e[k] := expand( a-U*W );
    if k=1 then print(evaln(e[k])=e[k]); fi;
    if e[k]=0 then break; fi;
    c[k] := (e[k]/p^k) mod p;
    u[k], w[k] := DiophantSolve( w[0], u[0], c[k], x, p );
    U := U + u[k]*p^k;
    W := W + w[k]*p^k;
od:
```

$$U := x - 2$$

$$W := 2 x^3 - 4$$

$$e_1 = 33 x^4 - 11 x^3 + 77 x^2 + 55 x - 44$$

```
> 'U' = U, 'W' = W;
```

$$U = x + 759240,\ W = 35 x^3 + 77 x + 84$$

Check that we have $a - U \cdot W = 0$ **mod** p^k .

```
> Expand( a - U*W ) mod p^k;
```

$$0$$

In principal we would lift the other factors but perhaps we have a real factor already.

Notice U is monic and lc(W) = α = 35 .

```
> f := alpha*U mod p^k;
```

$$f := 35 x - 15$$

cont(f)=5

```
> f := primpart(f);
```

$$f := 7 x - 3$$

```
> divide(a,f,'g');
```

$$true$$

Thus we have found the factorization

```
> a = f*g;
```

$$35 x^4 - 15 x^3 + 77 x^2 + 51 x - 36 = (7 x - 3) \left(5 x^3 + 11 x + 12\right)$$

But we do not know that g is irreducible because it has a non-trivial factorization modulo p .

```
> Factor(g) mod p;
```

$$\underbrace{5\left(x^2-4x+5\right)}^{w_0}\ \overbrace{(x+4)}^{u_0}$$

Let us lift $x+4$ the other linear factor with a/(x+4).

```
> u[0] := x+4 mod p;
```

$$u_0 := x+4$$

```
> w[0] := Quo( a, u[0], x ) mod p;
```

$$w_0 := 2x^3-x^2+4x+2$$

```
> U := u[0];
  W := w[0];
  for k while p^k < 2*B do
      e[k] := expand( a-U*W );
      if e[k]=0 then break; fi;
      c[k] := (e[k]/p^k) mod p;
      u[k], w[k] := DiophantSolve( w[0], u[0], c[k], x, p );
      U := U + u[k]*p^k;
      W := W + w[k]*p^k;
  od:
  'U'=U; 'W'=W;
```

$$U := x+4$$

$$W := 2x^3-x^2+4x+2$$

$$U = x-159661$$

$$W = 35x^3+273437x^2+647211x-797608$$

```
> h := alpha*U mod p^k;
```

$$h := 35x-273452$$

```
> h := primpart(h);
```

$$h := 35x-273452$$

```
> divide(a,h);
```

false

Therefore since there are no linear factors dividing the factor g determined earlier g must be irreducible (over $\mathbb{Z}$) hence

```
> a = f*g;
```

$$35x^4-15x^3+77x^2+51x-36 = (7x-3)\left(5x^3+11x+12\right)$$

```
> factor(a);
```

$$(7x-3)\left(5x^3+11x+12\right)$$