Lec18B Handouts, Michael Monagan

March 18, 2021 11:30 AM

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

$$p := 11$$

```
> f := x^8+7*x^7+10*x^6+7*x^5+x^4+3*x^3+3*x^2+3*x+5;
```

$$f := x^8 + 7x^7 + 10x^6 + 7x^5 + x^4 + 3x^3 + 3x^2 + 3x + 5$$

```
> Gcd(f, diff(f,x)) mod p;
```

$$1$$

f has no repeated factor.

```
> g := Gcd( f, x^11-x ) mod p;
```

$$g := x^5 + 7x^4 + 9x^3 + 7x^2 + 8x + 4$$

f has 5 linear factors.

```
> h := Quo( f, g, x ) mod p;
```

$$h := x^3 + x + 4$$

h is irreducible

Note h is irreducible

```
> for alpha from 0 to p-1 do Gcd(g,(x+alpha)^5+1) mod p od;
```

$$x^3 + 4x^2 + 4x + 1$$
$$x^2 + 8$$
$$x^2 + 8$$
$$x^3 + 4x^2 + 7x + 4$$
$$x^3 + 3x + 8$$
$$x^3 + x^2 + 9x + 3$$
$$x + 9$$
$$x^3 + 3x^2 + 9x + 7$$
$$x^3 + 5x^2 + 3x + 10$$
$$x + 1$$
$$x + 8$$

deg h	
0	←
1	III
2	II
3	IIIIII
4	
5	←

```
> g1 := Gcd(g,(x-0)^5+1,'g2') mod p; g2;
```

$$g1 := x^3 + 4x^2 + 4x + 1$$
$$x^2 + 3x + 4$$

$g_2 = g/g_1$

$f = g_1 \cdot g_2$

```
> seq( Gcd(g1,(x-alpha)^5+1) mod p, alpha=0..p-1 );
```

$$x^3 + 4x^2 + 4x + 1, 1, x + 1, x^2 + 10x + 9, x^2 + 6x + 5, x + 9, x + 9, x^2 + 3x + 1, x + 1, x + 5, x + 5$$

Got a split for 9/11 choices of α.

```
> seq( Gcd(g2,(x-alpha)^5+1) mod p, alpha=0..p-1 );
```

$$1, x + 8, 1, x + 6, x + 8, 1, x^2 + 3x + 4, x + 8, x^2 + 3x + 4, x + 6, x + 6$$

Got a split for 6/11 choices for α.

$\text{Prob}(h \neq 1 \text{ and } h \neq g) \geq \frac{4}{9}$

(we get a split)

Algorithm Distinct Degree Factorization 8.8

Input: $a \in \mathbb{Z}_p[x]$, $d = \deg a > 0$, $\gcd(a, a') = 1$.

Output: $g_1, g_2, \dots, g_m$ s.t. $a = \prod g_k$ and g_k is a $\prod$ of irreducibles of degree k.

$k \leftarrow 1$
$w \leftarrow x$
while $k \le \lfloor \deg a / 2 \rfloor$ do

$\deg w < \deg a$ $\quad \underline{w} \leftarrow \mathrm{rem}(w^p, a)$ $\quad = \underline{x^{p^k} \bmod a}$

$O(d^2)$ $\quad g_k \leftarrow \gcd(w - x, a)$ with d, $\le d$, $<d$, d

$O(d^2)$. $\quad a \leftarrow a / g_k$

$k \leftarrow k+1$

od

if $a \ne 1$ then $g_k \leftarrow a$ else $k \leftarrow k-1$

return $g_1, g_2, \dots, g_k$

$w^p = \underbrace{w \cdot w \cdot w \cdots w}$ mod.

$r \leftarrow w$

for i to $p-1$ do $r \leftarrow \mathrm{rem}(r \cdot w, a)$ $\quad O(d^2)$

$w \leftarrow r$

$O(d^2)$. $<d$ $<d$ d

Cost is $(p-1) \cdot O(d^2) = O(pd^2)$.

PowMod(w, p, a, x) mod p

$= w^p \bmod a$.

in $O(d^2 \log p)$.

Maximum number of steps is $\lfloor \frac{d}{2} \rfloor$ when a is irreducible in $\mathbb{Z}_p[x]$.

Cost is $\lfloor d/2 \rfloor \cdot (O(d^2 \log p) + O(d^2) + O(d^2)) = O(d^3 \log p)$ arithmetic ops in $\mathbb{Z}_p$.

POWMOD $\quad$ gcd. $\quad$ a/g_k

Factor A(x) over Z mod 5

```
> A:=x^16+x^15+3*x^14+x^13+4*x^12+2*x^10+4*x^8+3*x^6+3*x^5+3*x^3+3*
  x^2+2;
```

$$A := x^{16} + x^{15} + 3\,x^{14} + x^{13} + 4\,x^{12} + 2\,x^{10} + 4\,x^{8} + 3\,x^{6} + 3\,x^{5} + 3\,x^{3} + 3\,x^{2} + 2$$

Check that A(x) is square-free in $Z_5[x]$.

```
> Gcd(A,diff(A,x)) mod 5;
```

$$1$$

```
> w := x^5;
```

$$w := x^5$$

```
> f1 := Gcd(A,w-x) mod 5;
```

$$f1 := x^3 + 4\,x^2 + x + 4$$

A has 3 linear factors.

There are three linear factors. We are left with

```
> a := Quo(A,f1,x) mod 5;
```

$$a := x^{13} + 2\,x^{12} + 4\,x^{11} + 4\,x^{10} + x^{9} + x^{8} + x^{7} + x^{6} + 4\,x^{3} + 2\,x^{2} + 3\,x + 3$$

Now compute $w = Rem\left(x^{5^2}, a, x\right)$ **mod** $5 = Rem\left(w^5, a, x\right)$ **mod** 5 using Powmod

```
> w := Powmod(w,5,a,x) mod 5;
```

$$w := x^{11} + x^{10} + 3\,x^{9} + 4\,x^{8} + 3\,x^{5} + 4\,x^{4} + 3\,x^{3} + x^{2} + x + 3$$

```
> f2 := Gcd(a,w-x) mod 5;
```

$$f2 := x^2 + x + 2$$

A has 1 quadratic factor

There is one quadratic factor. We are left with

```
> a := Quo(a,f2,x) mod 5;
```

$$a := x^{11} + x^{10} + x^{9} + x^{8} + 3\,x^{7} + x^{6} + 4\,x^{5} + 2\,x^{3} + 3\,x^{2} + 2\,x + 4$$

Now compute $w = Rem\left(x^{5^3}, a, x\right)$ **mod** $5 = Rem\left(w^5, a, x\right)$ **mod** 5 using Powmod

```
> w := Powmod(w,5,a,x) mod 5;
```

$$w := 4\,x^{10} + 4\,x^{9} + 4\,x^{8} + 3\,x^{7} + 3\,x^{5} + x^{3} + 4\,x^{2} + 2\,x$$

```
> f3 := Gcd(a,w-x) mod 5;
```

$$f3 := x^6 + x^5 + x^4 + x^3 + 4\,x^2 + x + 4$$

A has two cubic factors.

There are two cubic factors. We are left with

```
> a := Quo(a,f3,x) mod 5;
```

$$a := x^5 + 4x + 1$$

A has one quintic factor.

which has no linear, quadratic or cubic factors so must be irreducible. Thus the distinct degree factorizaton of A is given by

```
> A = f1*f2*f3*a;
```

$$x^{16} + x^{15} + 3x^{14} + x^{13} + 4x^{12} + 2x^{10} + 4x^8 + 3x^6 + 3x^5 + 3x^3 + 3x^2 + 2 = (x^3 + 4x^2 + x + 4)(x^2 + x + 2)(x^6 + x^5 + x^4 + x^3 + 4x^2 + x + 4)(x^5 + 4x + 1)$$

The three linear factors split as follows: first we try $\alpha = 1$.

```
> w := Powmod( (x+1), 2, f1, x ) mod 5;
```

$$w := x^2 + 2x + 1$$

```
> h := Gcd(f1,w+1) mod 5;
```

$$h := x^2 + 2x + 2$$

$\gcd(f_1 \quad , (x+2)^2+1)$

```
> f1 := Quo(f1,h,x) mod 5;
```

$$f1 := x + 2$$

```
> w := Powmod( (x+2), 2, h, x ) mod 5;
```

$$w := 2x + 2$$

```
> Gcd( h, w+1) mod 5;
```

$$x + 4$$

```
> f1 := f1 * (x+4) * Quo(h,x+4,x) mod 5;
```

$$f1 := (x + 2)(x + 4)(x + 3)$$

It remains to split f3 into two cubic factors.

```
> f3;
```

$$x^6 + x^5 + x^4 + x^3 + 4x^2 + x + 4$$

```
> v := (x^3+x+1);
  w := Powmod(v,(5^3-1)/2,f3,x) mod 5;
  g := Gcd(w+1,f3) mod 5;
```

$\gcd(v^{62}+1, f_3 = g_3)$

both cubic factors are here

$$v := x^3 + x + 1$$

$$w := 4$$

$$g := x^6 + x^5 + x^4 + x^3 + 4x^2 + x + 4$$

This choice $v(x) = x^3 + x + 1$ did not work as we did not split f3. Thus we try another value for v of the form $v(x) = x^3 + \alpha x^2 + \beta x + \gamma$ where α, β, γ are chosen from Z_5.

```
> v := (x^3+x+2);
  w := Powmod(v,(5^3-1)/2,f3,x) mod 5;
```

```
g := Gcd(w+1,f3) mod 5;
```

$$v := x^3 + x + 2$$

$$w := x^4 + 2x^3 + x^2 + x + 2$$

$$g := x^3 + x + 4$$

Lucky.

```
> f3 := g*Quo(f3,g,x) mod 5;
```

$$f3 := (x^3 + x + 4)(x^3 + x^2 + 1)$$

Thus the complete factorization is given by 3 lines, 1 quadratic, 2 cubics, one quintic.

```
> f1*f2*f3*a;
```

$$(x+2)(x+4)(x+3)(x^2+x+2)(x^3+x+4)(x^3+x^2+1)(x^5+4x+1)$$

```
> Factor(A) mod 5;
```

$$(x+2)(x+4)(x+3)(x^2+x+2)(x^3+x+4)(x^3+x^2+1)(x^5+4x+1)$$