Lec11B Handouts

February 23, 2021 11:23 AM

The Modular GCD Algorithm (main idea)

```
> g := x^2-7*x+15;
```

$$g := x^2 - 7x + 15 \quad (1)$$

```
> A := expand( g * (x^2+18*x+5) );
```

$$A := x^4 + 11x^3 - 106x^2 + 235x + 75 \quad (2)$$

```
> B := expand( g * (x^2+x+5) );
```

$$B := x^4 - 6x^3 + 13x^2 - 20x + 75 \quad (3)$$

```
> p1 := 11;
```

$$p1 := 11 \quad (4)$$

```
> g1 := Gcd( A mod p1, B mod p1 ) mod p1;
```

$\mathbb{Z}_{11}[x]$

$$g1 := x^2 + 4x + 4 \quad (5)$$

```
> p2 := 13;
```

$$p2 := 13 \quad (6)$$

```
> g2 := Gcd( A mod p2, B mod p2 ) mod p2;
```

$\mathbb{Z}_{13}[x]$

$$g2 := x^2 + 6x + 2 \quad (7)$$

```
> G := chrem( [g1,g2], [p1,p2] );
```

$$G := x^2 + 136x + 15 \quad (8)$$

Put the coefficient s of G in the symmetric range for the integers modulo M

```
> M := p1*p2;
```

$$M := 143 \quad (9)$$

```
> G := mods(G,M);
```

$$G := x^2 - 7x + 15 \quad (10)$$

```
> gcd(A,B);
```

$$x^2 - 7x + 15 \quad (11)$$

Unlucky Primes

```
> g := x^2-7*x+15;
```

$$g := x^2 - 7\,x + 15 \qquad \textbf{(1)}$$

```
> A := expand( g * (x^2+18*x+5) );
```

$$A := x^4 + 11\,x^3 - 106\,x^2 + 235\,x + 75 \qquad \textbf{(2)}$$

```
> B := expand( g * (x^2+x+5) );
```

$$B := x^4 - 6\,x^3 + 13\,x^2 - 20\,x + 75 \qquad \textbf{(3)}$$

```
> gcd(A,B);
```

$$x^2 - 7\,x + 15 \qquad \textbf{(4)}$$

```
> g1 := Gcd( A, B ) mod 13;
```

$$g1 := x^2 + 6\,x + 2 \qquad \textbf{(5)}$$

```
> g2 := Gcd( A, B ) mod 17;
```

$$g2 := x^4 + 11\,x^3 + 13\,x^2 + 14\,x + 7 \qquad \textbf{(6)}$$

17 is an unlucky prime.

```
> g3 := Gcd( A, B ) mod 19;
```

$$g3 := x^2 + 12\,x + 15 \qquad \textbf{(7)}$$

```
> G := chrem( [g1,g2], [13,17] );
```

$$G := 52\,x^4 + 130\,x^3 + 183\,x^2 + 201\,x + 41 \qquad \textbf{(8)}$$

```
> G := chrem( [g1,g3], [13,19] );
```

$$G := x^2 + 240\,x + 15 \qquad \textbf{(9)}$$

```
> M := 13*19;
  G := mods( G, M );
```

$$M := 247$$

$$G := x^2 - 7\,x + 15 \qquad \textbf{(10)}$$

```
> divide(A,G);
  divide(B,G);
```

$$true$$

$$true \qquad \textbf{(11)}$$

How big can the coefficients of the factors of $x^n - 1$ in $\mathbb{Z}[x]$ be?

```
> f := x^30-1;
```

$$f := x^{30} - 1$$

```
> F := [op(factor(f))];
```

$$F := [x - 1, x^4 + x^3 + x^2 + x + 1, x^2 + x + 1, x^8 - x^7 + x^5 - x^4 + x^3 - x + 1, 1 + x, x^4 - x^3 + x^2 - x + 1, x^2 - x + 1, x^8 + x^7 - x^5 - x^4 - x^3 + x + 1]$$

```
> S := combinat[subsets](F):
> while not S[finished] do
      c := S[nextvalue](S);
      g := expand( mul(h,h=c) );
      if maxnorm(g)>7 then
          divide(f,g,'q');
          print(maxnorm(g),maxnorm(q));
          print(g,q);
      fi;
  od:
```

$$12, 12$$

$$x^{15} + 4x^{14} + 8x^{13} + 10x^{12} + 8x^{11} + 2x^{10} - 6x^9 - 12x^8 - 12x^7 - 6x^6 + 2x^5 + 8x^4 + 10x^3 + 8x^2 + 4x + 1, x^{15} - 4x^{14} + 8x^{13} - 10x^{12} + 8x^{11} - 2x^{10} - 6x^9 + 12x^8 - 12x^7 + 6x^6 + 2x^5 - 8x^4 + 10x^3 - 8x^2 + 4x - 1$$

$$12, 12$$

$$x^{15} - 4x^{14} + 8x^{13} - 10x^{12} + 8x^{11} - 2x^{10} - 6x^9 + 12x^8 - 12x^7 + 6x^6 + 2x^5 - 8x^4 + 10x^3 - 8x^2 + 4x - 1, x^{15} + 4x^{14} + 8x^{13} + 10x^{12} + 8x^{11} + 2x^{10} - 6x^9 - 12x^8 - 12x^7 - 6x^6 + 2x^5 + 8x^4 + 10x^3 + 8x^2 + 4x + 1$$

$$8, 7$$

$$x^{16} - 3x^{15} + 4x^{14} - 2x^{13} - 2x^{12} + 6x^{11} - 8x^{10} + 6x^9 - 6x^7 + 8x^6 - 6x^5 + 2x^4 + 2x^3 - 4x^2 + 3x - 1, x^{14} + 3x^{13} + 5x^{12} + 5x^{11} + 3x^{10} - x^9 - 5x^8 - 7x^7 - 5x^6 - x^5 + 3x^4 + 5x^3 + 5x^2 + 3x + 1$$

$$8, 7$$

$$x^{16} + 3x^{15} + 4x^{14} + 2x^{13} - 2x^{12} - 6x^{11} - 8x^{10} - 6x^9 + 6x^7 + 8x^6 + 6x^5 + 2x^4 - 2x^3 - 4x^2 - 3x - 1, x^{14} - 3x^{13} + 5x^{12} - 5x^{11} + 3x^{10} + x^9 - 5x^8 + 7x^7 - 5x^6 + x^5 + 3x^4 - 5x^3 + 5x^2 - 3x + 1$$

The Modular Gcd Algorithm

Input $\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ Output

$a, b \in \mathbb{Z}[x] \longrightarrow g = \gcd(a,b) \in \mathbb{Z}[x]$

(assume primitive)

if $\bar{g} \mid a$ and $\bar{g} \mid b$ then output $\bar{g}$. otherwise keep going.

$\bar{g} \leftarrow pp(\bar{g})$.

Put $\bar{g}$ in the symmetric range for $\mathbb{Z}_M$.

Mignotte bound.

$p_i \nmid lc(a)$.

ϕ_{p_i} $\qquad M = \prod p_i > 2\|g\|_\infty \cdot \gamma$ $\qquad$ CRT $\qquad$ Solve $\bar{g} \equiv g_i \pmod{p_i}$ for $g \in \mathbb{Z}_M[x]$.

$\gamma = \gcd(lc(a), lc(b))$

$g_i \leftarrow$ $\quad i$ mod p_i

if $g_i = 1$ then output $g = 1$.

$a_i, b_i \in \mathbb{Z}_{p_i}[x] \xrightarrow{\text{Euclidean Algorithm}} g_i = \gcd(a_i, b_i) \in \mathbb{Z}_{p_i}[x]$

$O(n^2)$ operations in $\mathbb{Z}_{p_i}$

This doesn't work: lose too much information about g.

$\phi_{x=\alpha_j}$ $\qquad \alpha_j \in \mathbb{Z}_{p_i}$ $\qquad\qquad$ Interpolate x

field.

$a_{ij}, b_{ij} \in \mathbb{Z}_{p_i} \xrightarrow{\text{Gcd in } \mathbb{Z}_{p_i}} g_{ij} = 1$

How big can $\|g\|_\infty$ be? $\quad g \mid a$ and $g \mid b$.

Can $\|g\|_\infty \geq \|a\|_\infty$ and $\geq \|b\|_\infty$. Yes.

Mignotte bound: Let $f, g \in \mathbb{Z}[x] \setminus \{0\}$. If $g \mid f$ then

$$\|g\|_\infty \leq 2^d \cdot \sqrt{d+1} \cdot \|f\|_\infty \quad \text{where } d = \deg f.$$

So $\|g\|_\infty \leq \min\left(2^{d_a}\sqrt{d_a+1}\,\|a\|_\infty,\ 2^{d_b}\sqrt{d_b+1}\,\|b\|_\infty\right)$ where $d_a = \deg(a)$ and $d_b = \deg b$

The Modular Gcd Algorithm

```
> a := 8*x^4+78*x^3+166*x^2-171*x-360;
  b := 12*x^5+84*x^4+90*x^3-2*x^2-14*x-15;
```

$$a := 8\,x^4 + 78\,x^3 + 166\,x^2 - 171\,x - 360$$

$$b := 12\,x^5 + 84\,x^4 + 90\,x^3 - 2\,x^2 - 14\,x - 15 \qquad (1)$$

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

$$1, 1 \qquad (2)$$

```
> MignotteBound := proc(f,x) local d;
     d := degree(f,x); 2^d*ceil(sqrt(d+1))*maxnorm(f) end:
> B := min( MignotteBound(a,x), MignotteBound(b,x) );
```

$$B := 8640 \qquad (3)$$

```
> M := 23*29*31;
```

$$M := 20677 \qquad (4)$$

```
> gamma := igcd(lcoeff(a),lcoeff(b));
Error, attempting to assign to `gamma` which is protected.  Try
declaring `local gamma`; see ?protect for details.
```

$\gamma = 0.57\ldots$

```
> beta := igcd(lcoeff(a),lcoeff(b));
```

$$\beta := 4 \qquad (5)$$

```
> g1 := Gcd(a,b) mod 23;
  g1 := beta*g1 mod 23;
```

$$g1 := x^2 + 7\,x + 19$$

$$g1 := 4\,x^2 + 5\,x + 7 \qquad (6)$$

```
> g2 := Gcd(a,b) mod 29;
  g2 := beta*g2 mod 29;
```

$$g2 := x^2 + 7\,x + 22$$

$$g2 := 4\,x^2 + 28\,x + 1 \qquad (7)$$

```
> g3 := Gcd(a,b) mod 31;
  g3 := beta*g3 mod 31;
```

$$g3 := x^2 + 7\,x + 23$$

$$g3 := 4\,x^2 + 28\,x + 30 \qquad (8)$$

```
> gbar := mods( chrem([g1,g2,g3],[23,29,31]), M );
```

$$gbar := 4\,x^2 + 28\,x + 30 \qquad (9)$$

```
> g := primpart(gbar);
```

$$g := 2\,x^2 + 14\,x + 15 \qquad (10)$$

```
> divide(a,g), divide(b,g);
```

$$true, true \qquad (11)$$

```
> infolevel[gcd] := 4:
  gcd(a,b);
gcd/gcdchrem1: computing images
gcd/gcdchrem1: combining images
gcd/gcdchrem1: trial division
```

$$2\,x^2 + 14\,x + 15 \qquad (12)$$

Problem: $\underline{\|a\|_\infty}$, $\underline{\|b\|_\infty}$ could be big but
$\|g\|_\infty$ might be small e.g. $\underline{g = 2x-3}$.
Test after each prime whether we have enough primes.

Algorithm ModGcd.

Inputs $a, b \in \mathbb{Z}[x] \setminus \{0\}$, $\operatorname{cont} a = 1$, $\operatorname{cont} b = 1$.
Output $g = \gcd(a,b)$

$\gamma \leftarrow \gcd(\operatorname{lc} a, \operatorname{lc} b) \in \mathbb{Z}$
$G \leftarrow 0$ # CRT applied to previous images g_i
$M \leftarrow 1$ # product of previous primes

Loop: pick a new prime p s.t. $p \nmid \operatorname{lc} a$.
$g_p \leftarrow \gcd(\phi_p(a), \phi_p(b)) \in \mathbb{Z}_p[x]$
if $\deg g_p = 0$ then output 1.
$g_p \leftarrow \phi_p(\gamma) \cdot g_p \bmod p$

Catch unlucky primes.

if $G = 0$ then $G \leftarrow g_p$; $M \leftarrow p$;
elif $\deg g_p > \deg G$ then # p is unlucky
elif $\deg g_p < \deg G$ then # all previous primes
$G \leftarrow g_p$; $M \leftarrow p$; # are unlucky
else

$\deg(g_p) = \deg(G)$.

Solve $\{u \equiv G \bmod M,\ u \equiv g_p \bmod p\}$
for u in the symmetric range mod $M \cdot p$.
if $u = G$ then
$g \leftarrow u / \operatorname{cont}(u)$
if $g \mid a$ and $g \mid b$ then output g. Termination.
$G \leftarrow u$; $M \leftarrow M \cdot p$
end if
go to LOOP.