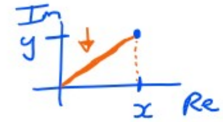
Lec13C

March 2, 2021 1:48 PM

$|x+iy| = \sqrt{x^2+y^2}$



A1Q4. Let $a, b \in \mathbb{Z}[i]$, $b \neq 0$.

$a \div b$: Need $a = bq + r$ with $r=0$ or $v(r) < v(b)$.

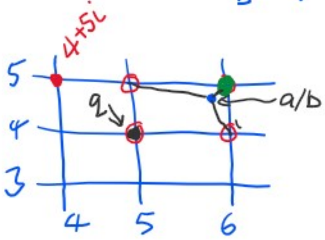
$v(a) = N(a)$ where $N(x+iy) = x^2+y^2 = |x+iy|^2$

$\frac{a}{b} = q + \frac{r}{b} \Rightarrow \left|\frac{a}{b} - q\right| = \left|\frac{r}{b}\right|$

pick q s.t. $\left|\frac{a}{b} - q\right|$ is small

$\Rightarrow \left|\frac{r}{b}\right|$ is small

$\Rightarrow N\left(\frac{r}{b}\right)$ is small.



Pick $q = \text{round}(x) + i\,\text{round}(y)$.

q is the closest $\mathbb{Z}[i]$ to a/b.

Let $\frac{a}{b} = x+iy$

Pick $q = \lfloor x \rfloor + i \lfloor y \rfloor$

$\Rightarrow \left|\frac{a}{b} - q\right| < \sqrt{2}$

$\Rightarrow \left|\frac{r}{b}\right| < \sqrt{2}$

$\Rightarrow N\left(\frac{r}{b}\right) < \sqrt{2}^2 = 2.$

$\Rightarrow \left|\frac{a}{b} - q\right| < \frac{\sqrt{2}}{2}$

$\Rightarrow \left|\frac{r}{b}\right| < \frac{\sqrt{2}}{2}$

$\Rightarrow N\left(\frac{r}{b}\right) < \frac{2}{2^2} = \frac{1}{2}$

$\Rightarrow N(r)/N(b) < \frac{1}{2}$

$\Rightarrow N(r) < \frac{1}{2} N(b) < N(b).$ ✓

$N(a \cdot b) = N(a) \cdot N(b)$.

$\Rightarrow \frac{N(r)}{N(b)} < 2$

$\Rightarrow N(r) < 2 \cdot N(b).$ ✗

Lemma: $N(a/b) = N(a)/N(b)$.

Proof: $N(a \cdot \frac{1}{a}) = N(1) = 1^2 = 1.$
and $N(a \cdot \frac{1}{a}) = N(a) \cdot N(\frac{1}{a}) = 1.$ $\Rightarrow N(\frac{1}{a}) = 1/N(a)$,

so $N(a/b) = N(a \cdot \frac{1}{b}) = N(a) \cdot N(\frac{1}{b}) = N(a) \cdot \frac{1}{N(b)}$

Q1 $a \times b$ in $\mathbb{Z}[x,y]$.

$a = (9y+7)x^1 + (5y^2+12)$ $\quad \|a\|_\infty = 12$

$b = (13y^1+23)x^2 + (2(y^1-11)x + (11y^1-13).$ $\quad \|b\|_\infty = 23.$

$C = a \times b.$

How many evaluation points for interpolating x and y.

$\deg(C) = \deg(a) + \deg(b)$

$\deg(C, x) = 1+2 = 3. \Rightarrow 4$ points. $x = 0,1,2,3$

$\deg(C, y) = 2+1 = 3 \Rightarrow 4$ points $y = 0,1,2,3.$

$\|C\|_\infty < \|a\|_\infty \cdot \|b\|_\infty \cdot \min(\#\text{terms in } a, \#\text{terms in } b)$

$= 12 \cdot 23 \cdot \min(4,6) = 12 \cdot 23 \cdot 4.$

$\prod p_i > 2\|C\|_\infty$ $\quad p_1 = 23,\ p_2 = 29,\ p_3 = 31.$

```
P := [23, 29, 31];            n1  n2  n3

for i to nops(P) do
    p := P[i];
    ai := a mod p;  bi := b mod p;
    for j from 0 to 3 do
```

```
p := P[i];
ai := a mod p;  bi := b mod p;
for j from 0 to 3 do
    aij := Eval(ai, y=j) mod p;
    bij := Eval(bi, y=j) mod p;
    for k from 0 to 3 do
        aijk := Eval(ai, x=k) mod p;
        bijk := Eval(bi, x=k) mod p;
        Cij[k] := aijk * bijk mod p;
    od;
    # interpolate x          [seq( Cij[k], k=0..3)];
    Ci[j] := Interp([0,1,2,3], [Cij[0],Cij[1],Cij[2],Cij[3]], x) mod p;
od;
C[i] := Interp([0,1,2,3], [seq(Ci[j], j=0..3)], y) mod p;
od;
M := P[1] * P[2] * P[3];
C := mods( chrem( [C[1], C[2], C[3]], P ), M);
```

How can we compute a gcd in $\mathbb{Z}_q[t][x]$ if q is small?

E.g. $\gcd(x^4+t^4,\ x^6+t^6) = x^2+t^2$ in $\underline{\mathbb{Z}_2[t][x]}$.

$t=0 \quad \gcd(x^4, x^6) = x^4$

$t=1 \quad \gcd(x^4+1, x^6+1) = x^2+1$

$$\begin{tikzcd}
a,b \in \mathbb{Z}[x] \arrow[r] \arrow[d, "\phi_{p_i}"', "p_i \in \mathbb{Z}"] & g=\gcd(a,b) \\
a_i,b_i \in \mathbb{Z}_{p_i}[x] \arrow[r, "E.A."] & g_i=\gcd(a_i,b_i) \arrow[u, "CRT."']
\end{tikzcd}$$

$$\begin{tikzcd}
a,b \in \underbrace{\mathbb{Z}_2[t]}_{E.D.}[x] \arrow[r] \arrow[d, "\phi_{p_i}"'] & g=\gcd(a,b). \\
a_i,b_i \in \Big(\underbrace{\mathbb{Z}_2[t]/(t^3+t+1)}_{\text{Finite Field with } 8=2^3 \text{ elements}}\Big)[x] \arrow[r, "E.A."', "\text{no expression swell}"'] & g_i=\gcd(a_i,b_i) \arrow[u, bend right, "CRT."']
\end{tikzcd}$$

$p_1 = t \qquad p_4 = t^3+t+1$

$p_2 = t+1 \qquad p_5 = t^3+t^2+1.$

$p_3 = t^2+t+1 \qquad \vdots$

CRT: if $\gcd(p_i,p_j)=1$ in $\mathbb{Z}$ then

$\exists$ a unique $u \in \mathbb{Z}$ s.t.

$0 \le u < M$ and $u \equiv u_i \bmod p_i$

or $-\frac{M}{2} < u < \frac{M}{2}$ where $M = \prod p_i$

CRT $\mathbb{Z}_q[t]$. if $\gcd(p_i,p_j)=1$ in $\mathbb{Z}_q[t]$ then

$\exists$ a unique polynomial $u \in \mathbb{Z}_q[t]$ s.t.

$u=0$ or $\deg(u) < \deg(M)$ and $u \equiv u_i \bmod p_i$.

where $M = \prod p_i$

- We need a source of primes (irreducibles) in $\mathbb{Z}_q[t]$.
  How can we test if a polynomial in $\mathbb{Z}_q[t]$ is irreducible?
  → Ch 8. ✓
- We need a CRA. for $\mathbb{Z}_q[t]$.
- We need to execute the E.A. in $F[x]$ [poly $+, -, \times, \div$]
  where $F = \mathbb{Z}_q[t]/p_i(t)$.
  a finite field.