Euclid's GCD

- Given $a, b \in \mathbb{N}$ in bits; compute (a,b).
  largest $c \in \mathbb{N}$ s.t. $c|a$ & $c|b$
- Eg. $(100, 1001) = (100, 100 \times 10 + 1) = (100, 1) = 1$
  ↖ coprime
- Euclid gives an algo. to compute gcd in his book Elements (300BC).
- The key step is based on the fact:

$$a = bq + r \quad ; \quad -\frac{b}{2} \leq r \leq b/2$$

$(a,b) = (b,r)$ ← halving!

Algorithm: Use this repeatedly to compute (a,b).
[It stops in $\leq |b|$ many steps.]

Analysis: First step — $\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ r_1 \end{pmatrix}$

[$a = q_1 b + r_1$; $b =: r_0$ & $a =: r_{-1}$]

Next step: $\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \cdot \begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$

[$\underline{b} - q_2 \underline{r_1} = r_2$]

▷ Do this for $\leq \lceil (\lg b) \rceil$ rounds!

Base case [halt condition]:

$$r_i = 0 .$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} (a,b) \\ 0 \end{pmatrix} \quad \text{--- (1)}$$

▷ $r_{j-2} = q_j r_{j-1} + r_j$

$r_{-1} = a \; ; \; r_0 = b$

Overall time complexity:

$$\sum_{j=1}^{i+1} O(\ell g|q_j| \cdot \ell g|r_{j-1}|)$$

$$\leq (\ell g|b|) \cdot O\left(\sum_j \ell g|q_j|\right)$$

$$\leq \ell g|b| \cdot O\left(\sum_j \ell g|r_{j-2}| - \ell g|r_{j-1}|\right) \leq O(\ell g|b| \cdot \ell g|a|)$$

Theorem: 1) Integer $\gcd(a,b)$ is computable in $O(\lg|a| \cdot \lg|b|)$ time.

2) Moreover, the algo. yields $u_1, u_2 \in \mathbb{Z}$:

(Bézout) $u_1 a + u_2 b = (a,b)$

$|u_1| < b$ & $|u_2| < a$.

$|u_2'| < a$

▷ $\langle a,b \rangle_{\mathbb{Z}} = \langle (a,b) \rangle_{\mathbb{Z}}$

u_2' ⇑

Pf of (2): • In eqn(1), multiply the matrices.

• Say $u_1 \geq b$: $u_1 = qb + u_1'$ $[|u_1'| < b]$

$\Rightarrow (qb+u_1')a + u_2 b = (a,b) \Rightarrow u_1' a + (u_2 + qa) b = (a,b)$

Corollary: Given coprime integers a, b; we can compute $a^{-1} \bmod b$ in $O(\lg|a| \cdot \lg|b|)$-time.

Pf: $u_1 a + u_2 b = (a,b) = 1$.

$\Rightarrow u_1 = (a^{-1} \bmod b)$. □

▷ Similary, $\mathrm{lcm}(a,b)$.

Pf: $\mathrm{lcm} \times \gcd = a \times b$. □

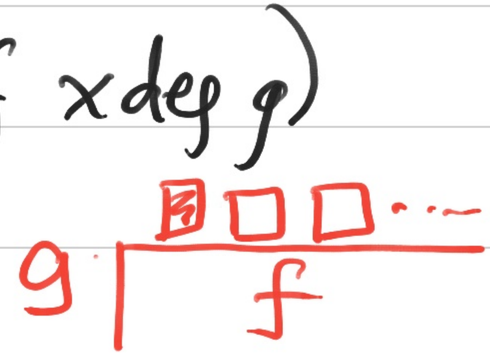
— Arithmetic problems in polynomial rings also get solved similarly.

One measures complexity differently.

Polynomial arithmetic in $R[x]$:

▷ $f \pm g$ can be computed in $O(\deg f + \deg g)$ many R-additions.

▷ $f \cdot g$ can be computed in $O(\deg f \times \deg g)$ many R-operations.



▷ $f = \underline{q} \cdot g + \underline{r}$ $[\deg r < \deg g]$ can be computed in $O(\deg q \cdot \deg g)$ many R-operations.

▷ If g is monic, then r exists $\forall R$.

▷ Similarly, $\gcd(f,g)$ & $f^{-1} \bmod g$ (if it exists for R, f, g.)

[Safe: R is field: $\forall f, g$.]

- It's useful to factor rings; when doing ring arithmetic.
- For rings R_1, R_2 we define $\underline{R_1 \times R_2} := (\{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\}, +, \times)$ is a ring.

coordinate-wise

- The most basic result is:
Chinese Remainder Theorem (CRT)
(~500 AD)

Theorem [CRT]: $a, b \in \mathbb{Z}$ are coprime $\Rightarrow$

$$\mathbb{Z}/\langle a \rangle \times \mathbb{Z}/\langle b \rangle \cong \mathbb{Z}/\langle ab \rangle$$

Moreover, the isomorphism is computable in $O(\lg|a| \cdot \lg|b|)$ time.

- Ex. $\mathbb{Z}/\langle 4 \rangle \not\cong \mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$

Witness: 1 $\qquad$ $(1, 1)$

Pf: $\mathbb{Z}/\langle a\rangle \times \mathbb{Z}/\langle b\rangle \longrightarrow \mathbb{Z}/\langle ab\rangle$

$\varphi : (x_1, x_2) \longmapsto x_1 u_1 b + x_2 u_2 a$

$u_1 := b^{-1} \bmod a$
$u_2 := a^{-1} \bmod b$

▷ $\varphi(x_1, x_2) \equiv x_1 \bmod a$

$\equiv x_2 \bmod b$

1) φ is a homomorphism ?

2) φ is injective ?

$\Rightarrow \varphi$ is isomorphism !

□

$[(x_1 u_1 b + x_2 u_2 a)\cdot(x_1' u_1 b + x_2' u_2 a)$

$\equiv_{ab} x_1 x_1' \cdot (u_1 b)^2 + x_2 x_2' (u_2 a)^2$

$u_1 b$ // , // $u_2 a$

$= \varphi(x_1 x_1', x_2 x_2')$]

CRT for polynomials: If $f, g \in \mathbb{F}[x]$ are coprime polynomials, then

$$\mathbb{F}[x]/\langle f \rangle \times \mathbb{F}[x]/\langle g \rangle \cong \mathbb{F}[x]/\langle fg \rangle .$$

Moreover, the isomorphism is computable in $O(\deg f \cdot \deg g)$ many $\mathbb{F}$-operations.

→ CRT reduces rings to fields; in proofs & in algorithms.