Def: • $a, b \in \mathbb{Z}$ $\quad b \neq 0$

if $\exists\, m \in \mathbb{Z}$ st. $a = mb$

$\Rightarrow$ a is divisible by b

b - divisor of a.
(factor)

• $p \geq 2$, $p \in \mathbb{N}$ is a prime if only divisors of p are 1 and itself

• $a, b \in \mathbb{Z}$ are relatively prime if they have

1

no common divisor greater than 1.

Sketch of proof

1\. • $|a| = |b|$ or $b = 0$ | assume $|a| = 1$, $m = \text{sign}(a)$ $\quad 1 = ma + 0b$

• $|a| > |b|$ ----> $a \geq b \quad b \geq 0$

ll. • $P(k) =:$ $a, b \in \mathbb{N} \cup \{0\}$, $a + b = k$ a, b relatively prime

$\exists\, m, n \in \mathbb{Z}$ st $ma + nb = 1$

Induction on k

Result $a, b \in \mathbb{Z}$, a, b relatively prime $\Rightarrow \exists\, m, n \in \mathbb{Z}$ st $am + bn = 1$.

Result 2 a, b relatively prime: $a \mid qb \Rightarrow a \mid q$

(Result 1 $\Rightarrow$) $\exists\, m, n \in \mathbb{Z}$ such that $ma + nb = 1$ $\Rightarrow$ $qma + qnb = q$ — (*)

Given:- $\exists\, k \in \mathbb{Z}$ such $qb = ka$ — (**)

Put (**) in (*) to get

$$q = qma + n(ka) = (qm + nk)\,a$$

$u = qm + nk \in \mathbb{Z} \Rightarrow q = ua \Rightarrow a$ divides q. □

(13)

$S = \{ ma + nb : m, n \in \mathbb{Z} \}$

$T = \{ kd \mid k \in \mathbb{Z} \}$

a, b are integers.

d = greatest common divisor of a & b.

Step 0: a, b are s.t. $g.c.d(a,b) = d$

(*) then $\frac{a}{d}$ & b/d are relatively prime.

- $u \in S$ show $u \in T$

$\Rightarrow u = ma + nb$ for some $n, m \in \mathbb{Z}$

(*) $a = kd$ and $b = ld$ for some $k, l \in \mathbb{Z}$.

$\Rightarrow u = m(kd) + n(ld)$

$\Rightarrow u = (mk + nl)d$

as $mk + nl \in \mathbb{Z} \Rightarrow u = zd$ for $z \in \mathbb{Z}$

$\Rightarrow u \in T \Rightarrow S \subseteq T$

$z \in T$ and show $z \in S$

$\Rightarrow \exists\, t \in \mathbb{Z}$ s.t. $z = td$.

from (step 0 & Result 1) $\exists\, r, s \in \mathbb{Z}$

$r\left(\frac{a}{d}\right) + s(b/d) = 1$

$\Rightarrow ra + sb = d$

$\Rightarrow (tr)a + (ts)b = td$. As $tr, ts \in \mathbb{Z}$

$\Rightarrow td \in S \Rightarrow T \subseteq S$.

5.1 Take two positive integers a and b.

1 - If $a < b$ then switch a and b

2 - Find k, r, $0 \leq r < b$, such that $a = kb + r$

3 If $r = 0$, stop and declare $b = \gcd(a,b)$.

If $r \neq 0$, then replace a by b and b by r;

repeat step 2.

Prove

- algorithm terminates
- last iteration of 2 gives $\gcd(a,b)$

E21.