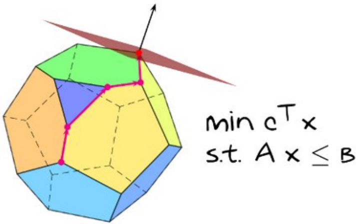
The Euclidean algorithm

- The greatest common divisor
- Analysis of the Euclidean algorithm



Example: The Euclidean algorithm

- For $a, b \in \mathbb{Z}$, $b \neq 0$ we say b *divides* a if there exists an $x \in \mathbb{Z}$ such that $a = b \cdot x$. We write $b \mid a$.

example: $\underset{b}{5} \mid \underset{a}{30}$, $5 \cdot \underset{x}{6} = 30$

Example: The Euclidean algorithm

- For $a, b \in \mathbb{Z}$, $b \neq 0$ we say b *divides* a if there exists an $x \in \mathbb{Z}$ such that $a = b \cdot x$. We write $b \mid a$.
- For $a, b, c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then c is a *common divisor* of a and b.

$a = 60$, $b = 42$ $3 \mid 60$ and $3 \mid 42$

3 common divisor of 60 and 42

Example: The Euclidean algorithm

- For $a, b \in \mathbb{Z}$, $b \neq 0$ we say b *divides* a if there exists an $x \in \mathbb{Z}$ such that $a = b \cdot x$. We write $b \mid a$.
- For $a, b, c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then c is a *common divisor* of a and b.
- If at least one of the two integers a and b is non-zero, then there exists a *greatest common divisor* of a and b. It is denoted by $\gcd(a, b)$.

$$\gcd(60, 42) = \boxed{6}$$

Example: The Euclidean algorithm

- For $a, b \in \mathbb{Z}$, $b \neq 0$ we say b *divides* a if there exists an $x \in \mathbb{Z}$ such that $a = b \cdot x$. We write $b \mid a$.
- For $a, b, c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then c is a *common divisor* of a and b.
- If at least one of the two integers a and b is non-zero, then there exists a *greatest common divisor* of a and b. It is denoted by $\gcd(a, b)$.
- For $a, b \in \mathbb{Z}$ with $b > 0$ there exist unique integers $q, r \in \mathbb{Z}$ with

$$a = q \cdot b + r, \text{ and } 0 \leqslant r < b. \qquad \textit{(Division with remainder)}$$

$$60 = \underset{q}{1} \cdot 42 + \underset{r}{18}$$

Example: The Euclidean algorithm

- For $a, b \in \mathbb{Z}$, $b \neq 0$ we say b *divides* a if there exists an $x \in \mathbb{Z}$ such that $a = b \cdot x$. We write $b \mid a$.
- For $a, b, c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then c is a *common divisor* of a and b.
- If at least one of the two integers a and b is non-zero, then there exists a *greatest common divisor* of a and b. It is denoted by $\gcd(a, b)$.
- For $a, b \in \mathbb{Z}$ with $b > 0$ there exist unique integers $q, r \in \mathbb{Z}$ with

$$a = q \cdot b + r, \text{ and } 0 \leqslant r < b. \qquad \textit{(Division with remainder)}$$

Q: $a > 0$, $b = 0$ $\quad \gcd(a,b) = \boxed{a}$

- For $a, b \in \mathbb{Z}$ with $b > 0$ and $q, r \in \mathbb{Z}$ as above one has $\gcd(a, b) = \gcd(b, r)$.

$d \mid a$, $d \mid b$ $\quad a = x_1 \cdot d$, $b = x_2 \cdot d$ $\Rightarrow r = x_1 \cdot d - q \cdot x_2 \cdot d$

$= (x_1 - q \cdot x_2) \cdot d \Rightarrow d \mid r$

$d \mid r$, $d \mid b$ $\quad b = x_1 \cdot d$, $r = x_2 \cdot d$

$a = q \cdot x_1 \cdot d + x_2 \cdot d = (q \cdot x_1 + x_2) \cdot d \Rightarrow d \mid a$

Example: The Euclidean algorithm (cont.)

```
# Condition a>=b>=0, not both equal to 0
def Euclid(a,b):
    if b == 0:
        return a
    else:
        r = a%b
        return Euclid(b,r)
```

$a = \overset{\geq 1}{q} \cdot b + r \qquad 0 \leq r < b$

- $r \leqslant a/2$
- First parameter halved every second iteration
- Number of iterations: $O(\log a) = O(\text{size}(a))$
- Linear time algorithm

$a \geq b > r$

if $r > a/2$:

$a \geq 1 \cdot \underbrace{b}_{>a/2} + \underbrace{r}_{>a/2} > a$ ↯