# 1'st tutorial: Eukleidian algorithm

Př: Find $\gcd(260, 84)$

Brute force: $a = 260 = 2^2 \cdot 5 \cdot 13$
$b = 84 = 2^2 \cdot 3 \cdot 7$ $\rightarrow \gcd(a,b) = 2^2 = 4$

Eukleid: $a = qr + b$

$$260 = 3 \cdot 84 + 8$$
$$84 = 10 \cdot 8 + \boxed{4}$$
$$8 = 2 \cdot \boxed{4} + 0$$

$\gcd(260, 84) = 4$

Shortly:

| | |
|---|---|
| | $a$ |
| $=$ | $q \cdot b$ |
| $+$ | $r$ |

| | |
|---|---|
| | 260 |
| $3 \cdot$ | 84 |
| $10 \cdot$ | 8 |
| $2 \cdot$ | $\boxed{4}$ |
| | 0 |

Př: Find $\gcd(114, 156)$ and kombine it in $\mathbb{Z}$ from $a = 156$, $b = 114$

Bezout's theorem: $\gcd(a,b) = s \cdot a + t \cdot b$ for some $s, t \in \mathbb{Z}$

Extended Eukleid:

$156 = 1 \cdot 114 + 42$ $\qquad 42 = a - b$

$114 = 2 \cdot 42 + 30$ $\qquad 30 = 114 - 2 \cdot 42 = b - 2(a-b) = -2a + 3b$

$42 = 1 \cdot 30 + 12$ $\qquad 12 = 42 - 30 = (a-b) - (-2a+3b) = 3a - 4b$

$30 = 2 \cdot 12 + 6$ $\qquad 6 = 30 - 2 \cdot 12 = (-2a+3b) - 2(3a-4b) = -8a + 11b$

$12 = 2 \cdot 6 + 0$ $\qquad 0 = 12 - 2 \cdot 6 = (3a-4b) - 2(-8a+11b) = 19a - 26b$

$\gcd(156, 114) = 6 = -8 \cdot 156 + 11 \cdot 114$

Př: Solve in $\mathbb{Z}$ $\quad 156x + 114y = 18$ (Diofantine equation)

$\gcd(156, 114) = 6$, $6 \mid 18$ $\rightarrow$ there exists solution in $\mathbb{Z}$.

part. solution – Extended Eukleid. algorithm (see above)

$$6 = -8 \cdot 156 + 11 \cdot 114 \quad / \cdot 3$$
$$18 = \underbrace{-24}_{x_p} \cdot 156 + \underbrace{33}_{y_p} \cdot 114$$

relatively prime solution of the homog. equation:

$$156x + 114y = 0 \quad / : \gcd = 6$$
$$26x + 19y = 0 \quad \rightarrow x_0 = 19, \; y_0 = -26$$

All sol. in $\mathbb{Z}$: $(x, y) = (x_p, y_p) + k(x_0, y_0)$
$= (-24, 33) + k(19, -26)$, $k \in \mathbb{Z}$

Note: We can get this relatively prime solution from Eukleid. algor., in case we combine also 0 (zero) from $a, b$ in the last equation.

Př: Solve in $\mathbb{Z}_{45}$ : $12x = 6$

in $\mathbb{Z}$ : $12x + 45y = 6$

Extended Eukleid alg: $a = 12$, $n = 45$

$$
\begin{array}{lll}
45 = 3\cdot 12 + 9 & 9 = n - 3a & \\
12 = 1\cdot 9 + 3 & 3 = a - (n-3a) = -n + 4a & /\cdot 2 \\
9 = 3\cdot 3 + 0 & 0 = (n-3a) - 3(-n+4a) = 4n - 15a & /\cdot k\in\mathbb{Z}
\end{array}
$$

$$6 = \underbrace{(-2+4k)}_{y}\, n + \underbrace{(8-15k)}_{x}\, a$$

in $\mathbb{Z}_{45}$ there will be $\gcd(12,45) = 3$ solutions in $\mathbb{Z}_{45}$

$$x = 8 - 15k = 8 + 30k \in \{8, 38, 23\}$$

## Extended Eukleid - a matrix notation

- Let's denote $r_0 = a$, $r_1 = b$, $i$'th equation from Eukleid's alg. is : $r_{i-1} = q_i r_i + r_{i+1}$.

Each two next equations from Ext. Eukleid

$$r_i = s_i a + t_i b$$
$$r_{i+1} = s_{i+1} a + t_{i+1} b$$

make a system of linear equations with solutions $a, b$

We shall start from $\begin{matrix} 1a = a \\ 1b = b \end{matrix}$ , we shall make ekvivalent modifications in $\mathbb{Z}$,

where steps of modification are lead by Eukleidian algorithm

$$\begin{pmatrix} R_1 \\ R_2 \end{pmatrix} \underset{r_{i-1} = q_i r_i + r_{i+1}}{\sim} \begin{pmatrix} R_2 \\ R_1 - q_i R_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \cdot \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

we can simulate row modifications by multiplying with a suitable matrix from the left side

Each modified system has got solutions $a, b$.

We want to obtain last two equations from Ext. Eukleid,

especially : $\left(\begin{array}{cc|c} s & t & d \\ u & v & 0 \end{array}\right)$ , where again $a, b$ are the solutions.

From this system we have the coef. of Bezout's theorem : $sa + tb = d = \gcd(a,b)$ $\Leftrightarrow (x_p, y_p) = (s,t)$

and the relatively prime solutions of homog. equat. $ua + vb = 0$ $\to (x_0, y_0) = (u, v)$

- Why are $u, v$ relatively prime?

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_\lambda \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\det \begin{pmatrix} s & t \\ u & v \end{pmatrix} = sv - tu = (-1)^\lambda \cdot 1 = (-1)^\lambda$$

so $\gcd(u,v) \mid \pm 1$ , thus $\gcd(u,v) = 1$

as well as $\gcd(s,t) = 1$

- All this will work only if we use just modifications invertable in $\mathbb{Z}$, namely
  - changing of the order of rows (it'll change a sign of determinant)
  - adding/subtracting of a multiple of one row to another row (it'll not change the determinant)
  - multiplying of a row by $\alpha = \pm 1$; here $\alpha$ must be invertable in $\mathbb{Z}$ (it'll change the det $\alpha$-times, so only $\pm 1$-times ✓)

In case we use only these modifications to transform systems

from $\left(\begin{array}{cc|c} 1 & 0 & a \\ 0 & 1 & b \end{array}\right)$ into $\left(\begin{array}{cc|c} s & t & d \\ u & v & 0 \end{array}\right)$, where $d \geq 0$,

it will hold: $\det\begin{pmatrix} s & t \\ u & v \end{pmatrix} = sv - tu = (\pm 1)$, so $\gcd(u,v) = 1$, $\gcd(s,t) = 1$

$d = \gcd(a,b)$, because modifications will not change the gcd of right sides

$R_i \leftrightarrow R_j$ $\left(\begin{array}{c|c} & a \\ & b \end{array}\right) \sim \left(\begin{array}{c|c} & b \\ & a \end{array}\right)$

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

$R_i := R_i - qR_j$ $\left(\begin{array}{c|c} & a \\ & b \end{array}\right) \sim \left(\begin{array}{c|c} & a-qb \\ & b \end{array}\right)$ $= r$

$\gcd(a,b) = \gcd(b,r)$

$R_i := -R_i$ $\left(\begin{array}{c|c} & a \\ & b \end{array}\right) \sim \left(\begin{array}{c|c} & -a \\ & b \end{array}\right)$

$\gcd(a,b) = \gcd(-a,b)$

Note: A modification $R_i := \alpha R_i$, $\alpha \neq \pm 1$, can loose relatively primeness of $u,v$ and change $d = \gcd(a,b)$, of right sides. Thus it is forbiden!

Pr: Solve $12x + 45y = 6$ in $\mathbb{Z}$ (once again).

$$\left(\begin{array}{cc|c} 1 & 0 & 12 \\ 0 & 1 & 45 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 12 \\ -4 & 1 & -3 \end{array}\right)_{R_2 - R_1} \sim \left(\begin{array}{cc|c} 4 & -1 & 3 \\ -15 & 4 & 0 \end{array}\right)\begin{array}{l} -R_2 \\ R_1 + 4R_2 \end{array}$$

$a = 12,\ n = 45$

$4a - n = 3 \quad /\cdot 2$

$-15a + 4n = 0 \quad /\cdot k \in \mathbb{Z}$

$$\underbrace{(8 - 15k)}_{x} \cdot 12 + \underbrace{(-2 + 4k)}_{y} \cdot 45 = 6$$

Pr: Solve in $\mathbb{Z}$ $9x + 6y = 42$

$\gcd(9,6) = 3$, $3 \mid 42$ → there exists a solution in $\mathbb{Z}$

$$\left(\begin{array}{cc|c} 1 & 0 & 9 \\ 0 & 1 & 6 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & -1 & 3 \\ 0 & 1 & 6 \end{array}\right)^{R_1 - R_2} \sim \left(\begin{array}{cc|c} 1 & -1 & 3 \\ -2 & 3 & 0 \end{array}\right)_{R_2 - 2R_1}$$

$a = 9,\ b = 6$

$42 : 3 = 14$, $14R_1 + kR_2$

$$\underbrace{(14 - 2k)}_{x} \cdot 9 + \underbrace{(-14 + 3k)}_{y} \cdot 6 = 42$$

Pr: $9x + 6y = 2$ in $\mathbb{Z}$.

$\gcd(9,6) = 3$, $3 \nmid 2$ → no solutions in $\mathbb{Z}$.

Př: Find $51^{-1}$ in $\mathbb{Z}_{73}$

We sould solve $\quad 51x = 1 \quad v \quad \mathbb{Z}_{73}$

$\quad 51x + 73y = 1 \quad v \quad \mathbb{Z}$

$$\left(\begin{array}{cc|c} 1 & 0 & 51 \\ 0 & 1 & 73 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 51 \\ -1 & 1 & 22 \end{array}\right) \begin{array}{l} \\ R_2 - R_1 \end{array} \sim \left(\begin{array}{cc|c} 3 & -2 & 7 \\ -10 & 7 & 1 \end{array}\right) \begin{array}{l} R_1 - 2R_2 = \check{R}_1 \\ R_2 - 3\check{R}_1 \end{array} \sim$$

$$\sim \left(\begin{array}{cc|c} -10 & 7 & 1 \\ & & 0 \end{array}\right) \begin{array}{l} R_2 \\ R_1 - 7R_2 \end{array}$$

A part. solution is enough to find: $\quad x_p = -10 = 63$

$$\underbrace{-10}_{x_p} \cdot 51 + 7 \cdot 73 = 1$$

$51^{-1} = 63$ in $\mathbb{Z}_{73}$

Pozn: Analogiously, the $\gcd(a_1, .., a_k)$ can be defined.

A generalization of Bezout's theorem: There exist $t_1, .., t_k \in \mathbb{Z}$ such that

$$\gcd(a_1, .., a_k) = t_1 a_1 + .. + t_k a_k .$$

To find coefitients ~~oef~~ $t_1, .., t_k \in \mathbb{Z}$ we can use our matrix notation.

PF: Find and combine: $\quad \gcd(18, 21, 45)$ from $a = 18,\ b = 21,\ c = 45$.

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 18 \\ 0 & 1 & 0 & 21 \\ 0 & 0 & 1 & 45 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & -1 & 0 & -3 \\ 0 & 1 & 0 & 21 \\ 0 & -2 & 1 & 3 \end{array}\right) \begin{array}{l} R_1 - R_2 \\ \\ R_3 - 2R_2 \end{array} \sim \left(\begin{array}{ccc|c} -1 & 1 & 0 & 3 \\ 7 & -6 & 0 & 0 \\ 1 & -3 & 1 & 0 \end{array}\right) \begin{array}{l} -R_1 \\ R_2 + 7R_1 \\ R_3 + R_1 \end{array}$$

a, b, c solves the system $\qquad\qquad$ a, b, c solve the system

$$(-1 + 7k + \ell) \cdot 18 + (1 - 6k - 3\ell) \cdot 21 + \ell \cdot 45 = 3$$

for $k, \ell \in \mathbb{Z}$

Homework:

1) In $\mathbb{Z}_{267}$ solve $\quad 114x = 15$.

[ Here $\quad x \in \{54, 143, 232\}$. ]

2) Find $\quad 5^{-1}, \quad 21^{-1}$ in $\mathbb{Z}_{27}$.

[ $5^{-1} = 11$ in $\mathbb{Z}_{27}$, $\quad 21^{-1}$ doesn't exist in $\mathbb{Z}_{27}$ ]

3) Prove: If $a / n$, $b / n$, $\gcd(a, b) = 1$, then $ab / n$.

4) Prove: If $a \equiv b \pmod{n}$, $n' / n$, then $a \equiv b \pmod{n'}$.