$m, n \in \mathbb{N} \quad m > n$

$NWD(m,n) = ?$

$d \in \mathbb{N} \quad d \mid m \wedge d \mid n \Rightarrow d \mid m-n \wedge d \mid n$

$d \mid m-n \wedge d \mid n \Rightarrow d \mid m \wedge d \mid n$

$\Downarrow \qquad\qquad \Downarrow$

$m-n = k \cdot d \qquad n = l \cdot d$

$m = k \cdot d + n = k \cdot d + l \cdot d = (k+l)d$

$$\boxed{d \mid m \wedge d \mid n \Leftrightarrow d \mid m-n \wedge d \mid n}$$

$\Downarrow$

$NWD(m,n) = NWD(m-n, n)$

Algorytm Euklidesa

Twierdzenie

Jeżeli $m, n \in \mathbb{N}$, *to*

$$\mathrm{NWD}(m,n) = \mathrm{NWD}(n, m \bmod n).$$

$$m = q \cdot n + \underbrace{r}_{= \, m \bmod n}$$

$$\mathrm{NWD}(m,n) = \mathrm{NWD}(q \cdot n + r, n) = \mathrm{NWD}((q-1)n + r, n) =$$

$$= \mathrm{NWD}((q-2)n + r) = \ldots = \mathrm{NWD}(r, n) = \mathrm{NWD}(n, r) =$$

$$= \mathrm{NWD}(n, m \bmod n)$$

Algorytm Euklidesa

$$\boxed{NWD(m,n) = NWD(n,\ m \bmod n)}$$

$$NWD(17017,\ 6783) = NWD(6783,\ 3451) =$$
$$= NWD(3451,\ 3332) = NWD(3332,\ 119) =$$
$$= NWD(119,\ 0) = \boxed{119}$$

$$6783 \cdot 2 = 13566$$

3434
17
3451

119 · 3 = 387

119 · 28 = 952 + 238 = 3332

Algorytm Euklidesa

input: $m, n \in \mathbb{N} \cup \{0\},\ m + n > 0$
output: $d = \mathrm{NWD}(m, n)$
$d \leftarrow m$
$k \leftarrow n$
while $k \neq 0$ **do**
  $(d, k) \leftarrow (k, d \bmod k)$
end while

NIEZMIENNIK: $\mathrm{NWD}(d, k) = \mathrm{NWD}(m, n)$

$\mathrm{NWD}(m, n) = \mathrm{NWD}(n, m \bmod n)$

$(d, k) \rightsquigarrow (d', k')$

$0 \leq \text{nowe}(k) = k' = d \bmod k < k$

Tw. o niezmiennikach $\Rightarrow$ po zakończeniu:

$\neg(k \neq 0) \wedge \mathrm{NWD}(d, k) = \mathrm{NWD}(m, n)$

$\Leftrightarrow k = 0 \wedge \mathrm{NWD}(d, 0) = d = \mathrm{NWD}(m, n)$

Algorytm Euklidesa

$m = 45,\ n = 12$	$m = 20,\ n = 63$	$m = 17017,\ n = 6783$
(d, k)	(d, k)	(d, k)
$(45, 12)$	$(20, 63)$	$(17017, 6783)$
$(12, 9)$	$(63, 20)$	$(6783, 3451)$
$(9, 3)$	$(20, 3)$	$(3451, 3332)$
$(\mathbf{3}, 0)$	$(3, 2)$	$(3332, 119)$
	$(2, 1)$	$(\mathbf{119}, 0)$
	$(\mathbf{1}, 0)$	

NWD(20, 63) = NWD(63, 20)

Algorytm Euklidesa: złożoność

1: $d \leftarrow m$
2: $k \leftarrow n$
3: **while** $k \neq 0$ **do**
4: $\quad (d, k) \leftarrow (k, d \bmod k)$ ← ILE RAZY TA INSTRUKCJA SIĘ WYKONA?
5: **end while**

- i = liczba obrotów pętli.
- $i \leqslant n$, $\quad i \leqslant \min\{m, n\} + 1$ ŹLE!

  $m, n \sim 2^{100}$ $\quad i \leqslant 2^{100} + 1$

  $\boxed{d > k}$
- $(d, k) \rightsquigarrow (d', k') = (k, d \bmod k)$
  - $k' = d \bmod k < k$
  - $\boxed{d} = q \cdot k + (d \bmod k) \geqslant k + d \bmod k > \boxed{2(d \bmod k)}$

$\Longrightarrow \boxed{d' \cdot k'} = k \cdot (d \bmod k) < k \cdot \frac{d}{2} = \boxed{\frac{1}{2} d \cdot k}$

Algorytm Euklidesa: złożoność

Twierdzenie

Algorytm Euklidesa dla $m, n \in \mathbb{N}$ wykonuje co najwyżej

$$\log_2 m + \log_2 n + 1$$

przebiegów pętli.

$d' \cdot l' < \frac{1}{2} d \cdot l$

pierwsze 0

i obrotów do zakończenia

$(m, n) \to (\, , \,) \to (\, , \,) \to (\, , \,) \to \dots \to (\, , \,) \to (\, , \,) \to (\, , 0)$

$< \frac{1}{2} m \cdot n$ $\quad$ $< \frac{1}{2} m \cdot n$ $\quad$ i $\quad$ $< \frac{1}{2} \cdot \dots$

$< \frac{1}{2} \cdot \frac{1}{2} \cdot m \cdot n = \frac{1}{4} m \cdot n$ $\qquad$ $< \frac{1}{2^i} m \cdot n$

$$\frac{1}{2^i} m \cdot n \geq 1 \Rightarrow m \cdot n \geq 2^i \Rightarrow \log_2 m + \log_2 n \geq i$$

$m, n \sim 2^{100}$ $\qquad$ $\log_2 2^{1000} + \log_2 2^{1000} + 1 = 2001$

Rozszerzony algorytm Euklidesa

$m = 17017, \ n = 6783$

$(17017, \ 6783)$

$(6783, 3451)$

$(3451, 3332)$

$(3332, 119)$

$(119, 0)$

$$3451 = 17017 - 2 \cdot 6783$$
$$3332 = 6783 - 1 \cdot 3451$$
$$119 = 3451 - 1 \cdot 3332$$
$$0 = 3332 - 28 \cdot 119$$

$$119 = 3451 - 3332 = 3451 - (6783 - 1 \cdot 3451) =$$
$$= 2 \cdot 3451 - 6783 = 2 \cdot (17017 - 2 \cdot 6783) - 6783 =$$
$$= 2 \cdot \boxed{17017} - 5 \cdot \boxed{6783}$$

$$119 = s \cdot 17017 - t \cdot 6783$$

Rozszerzony algorytm Euklidesa

$d \leftarrow m$

$k \leftarrow n$

while $k \neq 0$ **do**

  ~~$(d, k) \leftarrow (k, d \bmod k)$~~

end while

$d \bmod k = d - (d \operatorname{div} k) \cdot k$

$d \operatorname{div} k \to q$

$(d, k) \leftarrow (k, d - (d \operatorname{div} k) \cdot k)$

Rozszerzony algorytm Euklidesa

$d \leftarrow m$

$k \leftarrow n$

while $k \neq 0$ **do**

  $q \leftarrow d \text{ div } k$

  $(d, k) \leftarrow (k, d - qk)$

end while

d mod k

Rozszerzony algorytm Euklidesa

$d \leftarrow m$
$k \leftarrow n$
while $k \neq 0$ **do**
  $q \leftarrow d \operatorname{div} k$
  $(d, k) \leftarrow (k, d - qk)$
end while

$d = 17017$	q	$k = 6783$
$d = 6783$	2	$k = 17017 - 2 \cdot 6783$
$d = 3451$	1	$k = 6783 - 1 \cdot 3451$
$d = 3332$	1	$k = 3451 - 1 \cdot 3332$
$d = 119$	28	$k = 3332 - 28 \cdot 119$

Rozszerzony algorytm Euklidesa

Twierdzenie (Lemat Bezout'a)

Dla dowolnych liczb $m, n \in \mathbb{N}_0$, które nie są jednocześnie równe zero, istnieją takie liczby całkowite s i t, że

$$\mathrm{NWD}(m, n) = s \cdot m + t \cdot n.$$

Rozszerzony algorytm Euklidesa

$d \leftarrow m$
$k \leftarrow n$
while $k \neq 0$ **do**
    $q \leftarrow d \text{ div } k$
    $(d, k) \leftarrow (k, d - qk)$
end while

$d' = k$

Rozszerzony algorytm Euklidesa

$d \leftarrow m$
$d' \leftarrow n$
while $d' \neq 0$ **do**
    $q \leftarrow d \operatorname{div} d'$
    $(d, d') \leftarrow (d', d - qd')$
end while

Rozszerzony algorytm Euklidesa

$d \leftarrow m$
$d' \leftarrow n$
while $d' \neq 0$ **do**
  $q \leftarrow d \operatorname{div} d'$
  $(d, d') \leftarrow (d', d - qd')$
end while

d	d'	q
$d_0 = 135$	$d_1 = 40$	

Rozszerzony algorytm Euklidesa

$d \leftarrow m$
$d' \leftarrow n$
while $d' \neq 0$ **do**
  $q \leftarrow d \text{ div } d'$
  $(d, d') \leftarrow (d', d - qd')$
end while

d	d'	q
$d_0 = 135$	$d_1 = 40$	
$d_1 = 40$	$d_2 = 135 - 3 \cdot 40$	$q_1 = 3$
$d_2 = 15$	$d_3 = 40 - 2 \cdot 15$	$q_2 = 2$
$d_3 = 10$	$d_4 = 15 - 1 \cdot 10$	$q_3 = 1$
$d_4 = 5$	$d_5 = 10 - 2 \cdot 5$	$q_4 = 2$

Rozszerzony algorytm Euklidesa

d_0 $\quad NWD(m,n) = d = s \cdot m + t \cdot n$

$$d = m = 1 \cdot m + 0 \cdot n = s_0 \cdot m + t_0 \cdot n$$

$s_0 = 1$, $t_0 = 0$

$$d' = n = 0 \cdot m + 1 \cdot n = s_1 \cdot m + t_1 \cdot n$$

$d' = d_1$, $s_1 = 0$, $t_1 = 1$

$$d_2 = d_0 - q \cdot d_1 = (s_0 \cdot m + t_0 \cdot n) - q(s_1 \cdot m + t_1 \cdot n)$$

$$= \underbrace{(s_0 - q s_1)} m + \underbrace{(t_0 - q t_1)} n$$

$$\to \quad d_{i+1} = d_{i-1} - q d_i = (s_{i-1} - q_i s_i) m + (t_{i-1} - q_i t_i) n$$

Rozszerzony algorytm Euklidesa

input: $m, n \in \mathbb{N} \cup \{0\},\ m + n > 0$
output: $d = \mathrm{NWD}(m, n)$
$d \leftarrow m$
$d' \leftarrow n$

$(s, s') \leftarrow (1, 0)$
$(t, t') \leftarrow (0, 1)$

while $d' \neq 0$ **do**
    $(d, d') \leftarrow (d', d - qd')$
end while

Rozszerzony algorytm Euklidesa

input: $m, n \in \mathbb{N} \cup \{0\},\ m + n > 0$
output: $d = \mathrm{NWD}(m, n) = sm + tn$
$(d, d') \leftarrow (m, n)$
$(s, s') \leftarrow (1, 0)$
$(t, t') \leftarrow (0, 1)$
while $d' \neq 0$ **do**
    $q \leftarrow d \text{ div } d'$
    $(d, d') \leftarrow (d', d - qd')$
    $(s, s') \leftarrow \boxed{(s', s - qs')}$
    $(t, t') \leftarrow \boxed{(d', t - qt')}$
end while

$$d = \boxed{s} \cdot m + \boxed{t} \cdot n$$

Rozszerzony algorytm Euklidesa

input: $m, n \in \mathbb{N} \cup \{0\},\ m + n > 0$
output: $d = \mathrm{NWD}(m, n) = sm + tn$
$(d, d') \leftarrow (m, n)$
$(s, s') \leftarrow (1, 0)$
$(t, t') \leftarrow (0, 1)$
while $d' \neq 0$ **do**
    $q \leftarrow d \text{ div } d'$
    $(d, d') \leftarrow (d', d - qd')$
    $(s, s') \leftarrow (s', s - qs')$
    $(t, t') \leftarrow (d', t - qt')$
end while

i	d_i	q_i	s_i	t_i

Rozszerzony algorytm Euklidesa

input: $m, n \in \mathbb{N} \cup \{0\},\ m + n > 0$

output: $d = \mathrm{NWD}(m, n) = sm + tn$

$(d, d') \leftarrow (m, n)$

$(s, s') \leftarrow (1, 0)$

$(t, t') \leftarrow (0, 1)$

while $d' \neq 0$ **do**

  $q \leftarrow d \text{ div } d'$

  $(d, d') \leftarrow (d', d - qd')$

  $(s, s') \leftarrow (s', s - qs')$

  $(t, t') \leftarrow (d', t - qt')$

end while

i	d_i	q_i	s_i	t_i
0	135		1	0
1	40	3	0	1
2	15	2	1	-3
3	10	1	-2	7
4	5	2	3	-10
5	0			