Kryptografia

z elementami kryptografii kwantowej

Ryszard Tanaś

http://zon8.physd.amu.edu.pl/~tanas

Wykład 6

Spis treści

10 Trochę matematyki

10.1 Podzielność liczb

- Zbiór liczb całkowitych zwykle oznaczamy

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

- a zbiór liczb naturalnych

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

- Dla danych liczb całkowitych a i b mówimy, że liczba b jest podzielna przez a lub, że liczba a dzieli liczbę b, jeżeli istnieje taka liczba całkowita d, że $b = ad$. Liczbę a nazywamy dzielnikiem liczby b, a fakt ten zapisujemy $a|b$.

10 Trochę matematyki

10.1 Podzielność liczb

- Zbiór liczb całkowitych zwykle oznaczamy

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

- a zbiór liczb naturalnych

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

- Dla danych liczb całkowitych a i b mówimy, że liczba b jest podzielna przez a lub, że liczba a dzieli liczbę b, jeżeli istnieje taka liczba całkowita d, że $b = ad$. Liczbę a nazywamy dzielnikiem liczby b, a fakt ten zapisujemy $a|b$.

10 Trochę matematyki

10.1 Podzielność liczb

- Zbiór liczb całkowitych zwykle oznaczamy

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

- a zbiór liczb naturalnych

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

- Dla danych liczb całkowitych a i b mówimy, że liczba b jest podzielna przez a lub, że liczba a dzieli liczbę b, jeżeli istnieje taka liczba całkowita d, że $b = ad$. Liczbę a nazywamy dzielnikiem liczby b, a fakt ten zapisujemy $a|b$.

10 Trochę matematyki

10.1 Podzielność liczb

- Zbiór liczb całkowitych zwykle oznaczamy

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

- a zbiór liczb naturalnych

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

- Dla danych liczb całkowitych a i b mówimy, że liczba b jest podzielna przez a lub, że liczba a dzieli liczbę b, jeżeli istnieje taka liczba całkowita d, że $b = ad$. Liczbę a nazywamy dzielnikiem liczby b, a fakt ten zapisujemy $a|b$.

- Każda liczba $b > 1$ ma co najmniej dwa dzielniki dodatnie: 1 i b.
- Dzielnikiem nietrywialnym liczby b nazywamy dzielnik dodatni różny od 1 i b.
- Liczba pierwsza to liczba większa od 1 nie mająca innych dzielników dodatnich niż 1 i ona sama.
- Liczba mająca co najmniej jeden nietrywialny dzielnik jest liczbą złożoną.

- Każda liczba $b > 1$ ma co najmniej dwa dzielniki dodatnie: 1 i b.
- Dzielnikiem nietrywialnym liczby b nazywamy dzielnik dodatni różny od 1 i b.
- Liczba pierwsza to liczba większa od 1 nie mająca innych dzielników dodatnich niż 1 i ona sama.
- Liczba mająca co najmniej jeden nietrywialny dzielnik jest liczbą złożoną.

- Każda liczba $b > 1$ ma co najmniej dwa dzielniki dodatnie: 1 i b.
- Dzielnikiem nietrywialnym liczby b nazywamy dzielnik dodatni różny od 1 i b.
- Liczba pierwsza to liczba większa od 1 nie mająca innych dzielników dodatnich niż 1 i ona sama.
- Liczba mająca co najmniej jeden nietrywialny dzielnik jest liczbą złożoną.

- Każda liczba $b > 1$ ma co najmniej dwa dzielniki dodatnie: 1 i b.
- Dzielnikiem nietrywialnym liczby b nazywamy dzielnik dodatni różny od 1 i b.
- Liczba pierwsza to liczba większa od 1 nie mająca innych dzielników dodatnich niż 1 i ona sama.
- Liczba mająca co najmniej jeden nietrywialny dzielnik jest liczbą złożoną.

10.2 Twierdzenie o rozkładzie na czynniki pierwsze

Każda liczba naturalna n może być przedstawiona jednoznacznie (z dokładnością do kolejności czynników) jako iloczyn liczb pierwszych.

10.2 Twierdzenie o rozkładzie na czynniki pierwsze

Każda liczba naturalna n może być przedstawiona jednoznacznie (z dokładnością do kolejności czynników) jako iloczyn liczb pierwszych.

Zwykle taki rozkład zapisujemy jako iloczyn odpowiednich potęg różnych liczb pierwszych, np.

$$6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$$

10.3 Własności relacji podzielności

- Jeśli $a|b$ i c jest dowolną liczbą całkowitą, to $a|bc$.
- Jeśli $a|b$ i $b|c$, to $a|c$
- Jeśli $a|b$ i $a|c$, to $a|b \pm c$
- Jeśli liczba pierwsza p dzieli ab, to $p|a$ lub $p|b$
- Jeśli $m|a$ i $n|a$ oraz m i n nie mają wspólnych dzielników większych od 1, to $mn|a$

10.3 Własności relacji podzielności

- Jeśli $a|b$ i c jest dowolną liczbą całkowitą, to $a|bc$.
- Jeśli $a|b$ i $b|c$, to $a|c$
- Jeśli $a|b$ i $a|c$, to $a|b \pm c$
- Jeśli liczba pierwsza p dzieli ab, to $p|a$ lub $p|b$
- Jeśli $m|a$ i $n|a$ oraz m i n nie mają wspólnych dzielników większych od 1, to $mn|a$

10.3 Własności relacji podzielności

- Jeśli $a|b$ i c jest dowolną liczbą całkowitą, to $a|bc$.
- Jeśli $a|b$ i $b|c$, to $a|c$
- Jeśli $a|b$ i $a|c$, to $a|b \pm c$
- Jeśli liczba pierwsza p dzieli ab, to $p|a$ lub $p|b$
- Jeśli $m|a$ i $n|a$ oraz m i n nie mają wspólnych dzielników większych od 1, to $mn|a$

10.3 Własności relacji podzielności

- Jeśli $a|b$ i c jest dowolną liczbą całkowitą, to $a|bc$.
- Jeśli $a|b$ i $b|c$, to $a|c$
- Jeśli $a|b$ i $a|c$, to $a|b \pm c$
- Jeśli liczba pierwsza p dzieli ab, to $p|a$ lub $p|b$
- Jeśli $m|a$ i $n|a$ oraz m i n nie mają wspólnych dzielników większych od 1, to $mn|a$

10.3 Własności relacji podzielności

- Jeśli $a|b$ i c jest dowolną liczbą całkowitą, to $a|bc$.
- Jeśli $a|b$ i $b|c$, to $a|c$
- Jeśli $a|b$ i $a|c$, to $a|b \pm c$
- Jeśli liczba pierwsza p dzieli ab, to $p|a$ lub $p|b$
- Jeśli $m|a$ i $n|a$ oraz m i n nie mają wspólnych dzielników większych od 1, to $mn|a$

10.3 Własności relacji podzielności

- Jeśli $a|b$ i c jest dowolną liczbą całkowitą, to $a|bc$.
- Jeśli $a|b$ i $b|c$, to $a|c$
- Jeśli $a|b$ i $a|c$, to $a|b \pm c$
- Jeśli liczba pierwsza p dzieli ab, to $p|a$ lub $p|b$
- Jeśli $m|a$ i $n|a$ oraz m i n nie mają wspólnych dzielników większych od 1, to $mn|a$

10.4 Największy wspólny dzielnik — $NWD(a, b)$

Największy wspólny dzielnik, $NWD(a, b)$, dla danych dwóch liczb całkowitych (nie będących jednocześnie zerami), to największa liczba całkowita d będąca dzielnikiem zarówno a, jak i b.

Przykład:

$$NWD(12, 18) = NWD(2^2 \cdot 3, 2 \cdot 3^2) = 6$$

10.4 Największy wspólny dzielnik — $NWD(a, b)$

Największy wspólny dzielnik, $NWD(a, b)$, dla danych dwóch liczb całkowitych (nie będących jednocześnie zerami), to największa liczba całkowita d będąca dzielnikiem zarówno a, jak i b.

Przykład:

$$NWD(12, 18) = NWD(2^2 \cdot 3, 2 \cdot 3^2) = 6$$

10.4 Największy wspólny dzielnik — $NWD(a, b)$

Największy wspólny dzielnik, $NWD(a, b)$, dla danych dwóch liczb całkowitych (nie będących jednocześnie zerami), to największa liczba całkowita d będąca dzielnikiem zarówno a, jak i b.

Przykład:

$$NWD(12, 18) = NWD(2^2 \cdot 3, 2 \cdot 3^2) = 6$$

10.5 Najmniejsza wspólna wielokrotność — $NWW(a, b)$

Najmniejsza wspólna wielokrotność, $NWW(a, b)$, to najmniejsza dodatnia liczba całkowita, którą dzielą a i b.
$NWW(a, b) = a \cdot b / NWD(a, b)$

Przykład:

$$NWW(12, 18) = 36 = 12 \cdot 18 / NWD(12, 18)$$

10.5 Najmniejsza wspólna wielokrotność — $NWW(a, b)$

Najmniejsza wspólna wielokrotność, $NWW(a, b)$, to najmniejsza dodatnia liczba całkowita, którą dzielą a i b.

$NWW(a, b) = a \cdot b / NWD(a, b)$

Przykład:

$$NWW(12, 18) = 36 = 12 \cdot 18 / NWD(12, 18)$$

10.5 Najmniejsza wspólna wielokrotność — $NWW(a, b)$

Najmniejsza wspólna wielokrotność, $NWW(a, b)$, to najmniejsza dodatnia liczba całkowita, którą dzielą a i b.
$NWW(a, b) = a \cdot b / NWD(a, b)$

Przykład:

$$NWW(12, 18) = 36 = 12 \cdot 18 / NWD(12, 18)$$

10.6 Liczby względnie pierwsze

Liczby a i b są względnie pierwsze jeżeli $NWD(a, b) = 1$, tzn. liczby a i b nie mają wspólnego dzielnika większego od 1.

Przykład:

$$NWD(841, 160) = 1$$

zatem liczby 841 i 160 są względnie pierwsze

10.6 Liczby względnie pierwsze

Liczby a i b są względnie pierwsze jeżeli $NWD(a, b) = 1$, tzn. liczby a i b nie mają wspólnego dzielnika większego od 1.

Przykład:

$$NWD(841, 160) = 1$$

zatem liczby 841 i 160 są względnie pierwsze

10.6 Liczby względnie pierwsze

Liczby a i b są względnie pierwsze jeżeli $NWD(a, b) = 1$, tzn. liczby a i b nie mają wspólnego dzielnika większego od 1.

Przykład:

$$NWD(841, 160) = 1$$

zatem liczby 841 i 160 są względnie pierwsze

10.7 Algorytm Euklidesa

- Dla $a > b$, dzielimy a przez b otrzymując iloraz q_1 i resztę r_1, tzn.
  $a = q_1 b + r_1$,
- w następnym kroku b gra rolę a, zaś r_1 gra rolę b:
  $b = q_2 r_1 + r_2$.
- Postępowanie to kontynuujemy dzieląc kolejne reszty,
  $r_{i-2} = q_i r_{i-1} + r_i$,
  aż do momentu kiedy otrzymamy resztę, która dzieli poprzednią resztę.
- Ostatnia niezerowa reszta jest $NWD(a, b)$.

10.7 Algorytm Euklidesa

- Dla $a > b$, dzielimy a przez b otrzymując iloraz q_1 i resztę r_1, tzn.

  $a = q_1 b + r_1$,

- w następnym kroku b gra rolę a, zaś r_1 gra rolę b:

  $b = q_2 r_1 + r_2$.

- Postępowanie to kontynuujemy dzieląc kolejne reszty,

  $r_{i-2} = q_i r_{i-1} + r_i$,

  aż do momentu kiedy otrzymamy resztę, która dzieli poprzednią resztę.

- Ostatnia niezerowa reszta jest $NWD(a, b)$.

10.7 Algorytm Euklidesa

- Dla $a > b$, dzielimy a przez b otrzymując iloraz q_1 i resztę r_1, tzn.

  $a = q_1 b + r_1$,

- w następnym kroku b gra rolę a, zaś r_1 gra rolę b:

  $b = q_2 r_1 + r_2$.

- Postępowanie to kontynuujemy dzieląc kolejne reszty,

  $r_{i-2} = q_i r_{i-1} + r_i$,

  aż do momentu kiedy otrzymamy resztę, która dzieli poprzednią resztę.

- Ostatnia niezerowa reszta jest $NWD(a, b)$.

10.7 Algorytm Euklidesa

- Dla $a > b$, dzielimy a przez b otrzymując iloraz q_1 i resztę r_1, tzn.

  $a = q_1 b + r_1$,

- w następnym kroku b gra rolę a, zaś r_1 gra rolę b:

  $b = q_2 r_1 + r_2$.

- Postępowanie to kontynuujemy dzieląc kolejne reszty,

  $r_{i-2} = q_i r_{i-1} + r_i$,

  aż do momentu kiedy otrzymamy resztę, która dzieli poprzednią resztę.

- Ostatnia niezerowa reszta jest $NWD(a, b)$.

10.7 Algorytm Euklidesa

- Dla $a > b$, dzielimy a przez b otrzymując iloraz q_1 i resztę r_1, tzn.
  $a = q_1 b + r_1$,
- w następnym kroku b gra rolę a, zaś r_1 gra rolę b:
  $b = q_2 r_1 + r_2$.
- Postępowanie to kontynuujemy dzieląc kolejne reszty,
  $r_{i-2} = q_i r_{i-1} + r_i$,
  aż do momentu kiedy otrzymamy resztę, która dzieli poprzednią resztę.
- Ostatnia niezerowa reszta jest $NWD(a, b)$.

Przykład:

Obliczmy $NWD(841, 160)$

Przykład:

Obliczmy $NWD(841, 160)$

a		q		b		r
841	$=$	5	$\cdot$	160	$+$	41

Przykład:

Obliczmy $NWD(841, 160)$

a		q		b		r
841	$=$	5	$\cdot$	160	$+$	41
160	$=$	3	$\cdot$	41	$+$	37

Przykład:

Obliczmy $NWD(841, 160)$

a		q		b		r
841	$=$	5	$\cdot$	160	$+$	41
160	$=$	3	$\cdot$	41	$+$	37
41	$=$	1	$\cdot$	37	$+$	4

Przykład:

Obliczmy $NWD(841, 160)$

a		q		b		r
841	$=$	5	$\cdot$	160	$+$	41
160	$=$	3	$\cdot$	41	$+$	37
41	$=$	1	$\cdot$	37	$+$	4
37	$=$	9	$\cdot$	4	$+$	1

Przykład:

Obliczmy $NWD(841, 160)$

a		q		b		r
841	$=$	5	$\cdot$	160	$+$	41
160	$=$	3	$\cdot$	41	$+$	37
41	$=$	1	$\cdot$	37	$+$	4
37	$=$	9	$\cdot$	4	$+$	1
4	$=$	4	$\cdot$	1	$+$	0

Przykład:

Obliczmy $NWD(841, 160)$

a		q		b		r
841	$=$	5	$\cdot$	160	$+$	41
160	$=$	3	$\cdot$	41	$+$	37
41	$=$	1	$\cdot$	37	$+$	4
37	$=$	9	$\cdot$	4	$+$	1
4	$=$	4	$\cdot$	1	$+$	0

Ponieważ $NWD(841, 160) = 1$, to liczby 841 i 160 są względnie pierwsze.

Przykład:

Obliczmy $NWD(841, 160)$

a		q		b		r
841	$=$	5	$\cdot$	160	$+$	41
160	$=$	3	$\cdot$	41	$+$	37
41	$=$	1	$\cdot$	37	$+$	4
37	$=$	9	$\cdot$	4	$+$	1
4	$=$	4	$\cdot$	1	$+$	0

Ponieważ $NWD(841, 160) = 1$, to liczby 841 i 160 są względnie pierwsze.

Algorytm Euklidesa pozwala znaleźć $NWD(a, b)$ w czasie wielomianowym (dla $a > b$, $O(\ln^2(a))$)

10.8 Twierdzenie o superpozycji

Największy wspólny dzielnik dwóch liczb może być przedstawiony w postaci kombinacji liniowej tych liczb ze współczynnikami całkowitymi:

$$NWD(a, b) = xa + yb$$

przy czym liczby x i y można znaleźć w czasie $O(\ln^2(a))$.

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

$$1 = 37 - 9 \cdot 4$$

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

$$1 = 37 - 9 \cdot 4 = 37 - 9(41 - 1 \cdot 37)$$

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

$$\begin{aligned} 1 &= 37 - 9 \cdot 4 = 37 - 9(41 - 1 \cdot 37) \\ &= 10 \cdot 37 - 9 \cdot 41 \end{aligned}$$

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

$$\begin{aligned} 1 &= 37 - 9 \cdot 4 = 37 - 9(41 - 1 \cdot 37) \\ &= 10 \cdot 37 - 9 \cdot 41 = 10(160 - 3 \cdot 41) - 9 \cdot 41 \end{aligned}$$

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

$$
\begin{aligned}
1 &= 37 - 9 \cdot 4 = 37 - 9(41 - 1 \cdot 37) \\
&= 10 \cdot 37 - 9 \cdot 41 = 10(160 - 3 \cdot 41) - 9 \cdot 41 \\
&= 10 \cdot 160 - 39 \cdot 41
\end{aligned}
$$

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

$$
\begin{aligned}
1 &= 37 - 9 \cdot 4 = 37 - 9(41 - 1 \cdot 37) \\
&= 10 \cdot 37 - 9 \cdot 41 = 10(160 - 3 \cdot 41) - 9 \cdot 41 \\
&= 10 \cdot 160 - 39 \cdot 41 = 10 \cdot 160 - 39 \cdot (841 - 5 \cdot 160)
\end{aligned}
$$

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

$$
\begin{aligned}
1 &= 37 - 9 \cdot 4 = 37 - 9(41 - 1 \cdot 37) \\
&= 10 \cdot 37 - 9 \cdot 41 = 10(160 - 3 \cdot 41) - 9 \cdot 41 \\
&= 10 \cdot 160 - 39 \cdot 41 = 10 \cdot 160 - 39 \cdot (841 - 5 \cdot 160) \\
&= -39 \cdot 841 + 205 \cdot 160
\end{aligned}
$$

W poprzednim przykładzie $NWD(841, 160) = 1$. Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy

$$
\begin{aligned}
1 &= 37 - 9 \cdot 4 = 37 - 9(41 - 1 \cdot 37) \\
&= 10 \cdot 37 - 9 \cdot 41 = 10(160 - 3 \cdot 41) - 9 \cdot 41 \\
&= 10 \cdot 160 - 39 \cdot 41 = 10 \cdot 160 - 39 \cdot (841 - 5 \cdot 160) \\
&= -39 \cdot 841 + 205 \cdot 160
\end{aligned}
$$

Zatem: $x = -39$, $y = 205$

10.9 Rozszerzony algorytm Euklidesa

Rozszerzony algorytm Euklidesa znajduje zarówno największy wspólny dzielnik $NWD(a, b)$ liczb a i b jak i liczby x i y będące współczynnikami kombinacji liniowej

$$NWD(a, b) = xa + yb$$

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5									

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41								

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160							

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41						

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1					

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0				

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1			

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5		

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5	1	

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5	1	-5

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5	1	-5
3									

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5	1	-5
3	37								

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5	1	-5
3	37	41							

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5	1	-5
3	37	41	37						

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5	1	-5
3	37	41	37	-3					

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1				

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	-5	1	-5
3	37	41	37	-3	1	-3			

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16		

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1									

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4								

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37							

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4						

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4					

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3				

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4			

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21		

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9									

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1								

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4							

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4	1						

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4	1	−39					

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4	1	−39	4				

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4	1	−39	4	−39			

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4	1	−39	4	−39	205		

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4	1	−39	4	−39	205	−21	

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4	1	−39	4	−39	205	−21	205

Przyporządkowania w algorytmie:

$$q = \lfloor a/b \rfloor, \quad r \leftarrow a - qb, \quad a \leftarrow b, \quad b \leftarrow r,$$

$$x \leftarrow x_2 - qx_1, \quad x_2 \leftarrow x_1, \quad x_1 \leftarrow x,$$

$$y \leftarrow y_2 - qy_1, \quad y_2 \leftarrow y_1, \quad y_1 \leftarrow y$$

q	r	a	b	x	x_2	x_1	y	y_2	y_1
—	—	841	160	—	1	0	—	0	1
5	41	160	41	1	0	1	−5	1	−5
3	37	41	37	−3	1	−3	16	−5	16
1	4	37	4	4	−3	4	−21	16	−21
9	1	4	1	−39	4	−39	205	−21	205

Z ostatniego wiersza odczytujemy:

$$NWD(841, 160) = 1 = -39 \cdot 841 + 205 \cdot 160$$

10.10 Kongruencje

Dla danych trzech liczb całkowitych a, b i m mówimy, że liczba a przystaje do liczby b modulo m i piszemy $a \equiv b \pmod{m}$, gdy różnica $a - b$ jest podzielna przez m. Liczbę m nazywamy modułem kongruencji.

10.10 Kongruencje

Dla danych trzech liczb całkowitych a, b i m mówimy, że liczba a przystaje do liczby b modulo m i piszemy $a \equiv b \pmod{m}$, gdy różnica $a - b$ jest podzielna przez m. Liczbę m nazywamy modułem kongruencji.

Przykłady:

$27 \equiv 7 \pmod{5}$ bo $27 - 7 = 4 \cdot 5$

$27 \equiv 2 \pmod{5}$ bo $27 - 2 = 5 \cdot 5$

$-8 \equiv 7 \pmod{5}$ bo $-8 - 7 = -3 \cdot 5$

Własności kongruencji:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m}$ wtedy i tylko wtedy, gdy $b \equiv a \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$ oraz $ac \equiv bd \pmod{m}$
  Kongruencje względem tego samego modułu można dodawać, odejmować i mnożyć stronami.
- Jeśli $a \equiv b \pmod{m}$, to $a \equiv b \pmod{d}$ dla każdego dzielnika $d|m$

Własności kongruencji:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m}$ wtedy i tylko wtedy, gdy $b \equiv a \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$ oraz $ac \equiv bd \pmod{m}$
  Kongruencje względem tego samego modułu można dodawać, odejmować i mnożyć stronami.
- Jeśli $a \equiv b \pmod{m}$, to $a \equiv b \pmod{d}$ dla każdego dzielnika $d|m$

Własności kongruencji:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m}$ wtedy i tylko wtedy, gdy $b \equiv a \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$ oraz $ac \equiv bd \pmod{m}$
  Kongruencje względem tego samego modułu można dodawać, odejmować i mnożyć stronami.
- Jeśli $a \equiv b \pmod{m}$, to $a \equiv b \pmod{d}$ dla każdego dzielnika $d|m$

Własności kongruencji:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m}$ wtedy i tylko wtedy, gdy $b \equiv a \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$ oraz $ac \equiv bd \pmod{m}$
  Kongruencje względem tego samego modułu można dodawać, odejmować i mnożyć stronami.
- Jeśli $a \equiv b \pmod{m}$, to $a \equiv b \pmod{d}$ dla każdego dzielnika $d|m$

Własności kongruencji:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m}$ wtedy i tylko wtedy, gdy $b \equiv a \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$ oraz $ac \equiv bd \pmod{m}$
  Kongruencje względem tego samego modułu można dodawać, odejmować i mnożyć stronami.
- Jeśli $a \equiv b \pmod{m}$, to $a \equiv b \pmod{d}$ dla każdego dzielnika $d|m$

Własności kongruencji:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m}$ wtedy i tylko wtedy, gdy $b \equiv a \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$
- Jeśli $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$ oraz $ac \equiv bd \pmod{m}$
  Kongruencje względem tego samego modułu można dodawać, odejmować i mnożyć stronami.
- Jeśli $a \equiv b \pmod{m}$, to $a \equiv b \pmod{d}$ dla każdego dzielnika $d|m$

- Jeśli $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$, oraz m i n są względnie pierwsze, to $a \equiv b \pmod{mn}$
- Dla ustalonej liczby m, każda liczba przystaje modulo m do jednej liczby zawartej pomiędzy 0 i $m-1$.

- Jeśli $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$, oraz m i n są względnie pierwsze, to $a \equiv b \pmod{mn}$
- Dla ustalonej liczby m, każda liczba przystaje modulo m do jednej liczby zawartej pomiędzy 0 i $m - 1$.

10.11 Twierdzenie o odwrotności

Liczbami a, dla których istnieje liczba b taka, że $ab \equiv 1 \pmod{m}$, są dokładnie te liczby a, dla których $NWD(a, m) = 1$. Taka liczba odwrotna $b = a^{-1}$ może być znaleziona w czasie $O(\ln^2(m))$.

10.11 Twierdzenie o odwrotności

Liczbami a, dla których istnieje liczba b taka, że $ab \equiv 1 \pmod{m}$, są dokładnie te liczby a, dla których $NWD(a, m) = 1$. Taka liczba odwrotna $b = a^{-1}$ może być znaleziona w czasie $O(\ln^2(m))$.

Przykład:

Ponieważ $NWD(841, 160) = 1$, to istnieje liczba $160^{-1} \pmod{841}$.

10.11 Twierdzenie o odwrotności

Liczbami a, dla których istnieje liczba b taka, że $ab \equiv 1 \pmod{m}$, są dokładnie te liczby a, dla których $NWD(a, m) = 1$. Taka liczba odwrotna $b = a^{-1}$ może być znaleziona w czasie $O(\ln^2(m))$.

Przykład:

Ponieważ $NWD(841, 160) = 1$, to istnieje liczba $160^{-1} \pmod{841}$.

Liczbę tę można obliczyć za pomocą rozszerzonego algorytmu Euklidesa.

10.11 Twierdzenie o odwrotności

Liczbami a, dla których istnieje liczba b taka, że $ab \equiv 1 \pmod{m}$, są dokładnie te liczby a, dla których $NWD(a, m) = 1$. Taka liczba odwrotna $b = a^{-1}$ może być znaleziona w czasie $O(\ln^2(m))$.

Przykład:

Ponieważ $NWD(841, 160) = 1$, to istnieje liczba $160^{-1} \pmod{841}$.

Liczbę tę można obliczyć za pomocą rozszerzonego algorytmu Euklidesa.

Ponieważ

$1 = -39 \cdot 841 + 205 \cdot 160$, to $205 \cdot 160 \equiv 1 \pmod{841}$,

a więc $160^{-1} \pmod{841} = 205$.

10.12 Małe twierdzenie Fermata

Niech p będzie liczbą pierwszą. Wtedy każda liczba a spełnia kongruencję $a^p \equiv a \pmod{p}$ i każda liczba a niepodzielna przez p spełnia kongruencję
$a^{p-1} \equiv 1 \pmod{p}$.

10.12 Małe twierdzenie Fermata

Niech p będzie liczbą pierwszą. Wtedy każda liczba a spełnia kongruencję $a^p \equiv a \pmod{p}$ i każda liczba a niepodzielna przez p spełnia kongruencję
$a^{p-1} \equiv 1 \pmod{p}$.

Liczba 1231 jest liczbą pierwszą i $NWD(1231, 5871) = 1$, więc
$5871^{1230} \equiv \quad 1 \pmod{1231}$

10.13 Chińskie twierdzenie o resztach

Jeśli liczby $m_1, m_2, \ldots, m_k$ są parami względnie pierwsze, tzn. $NWD(m_i, m_j) = 1$ dla $i \neq j$, wtedy układ kongruencji

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ \ldots & \quad \ldots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

ma wspólne rozwiązanie modulo $m = m_1 m_2 \ldots m_k$.

Przykład:

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 2 \pmod{12} \\ x &\equiv 3 \pmod{13} \end{aligned}$$

Przykład:

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 2 \pmod{12} \\ x &\equiv 3 \pmod{13} \end{aligned}$$

Niech $M_i = m/m_i$ będzie iloczynem wszystkich modułów z wyjątkiem i-tego. Wtedy $NWD(m_i, M_i) = 1$, a więc istnieje taka liczba N_i, że $M_i N_i \equiv 1 \pmod{m_i}$, wtedy wspólnym rozwiązaniem modulo m jest $x = \sum_i a_i M_i N_i$. Dla każdego i wszystkie składniki sumy poza i-tym są podzielne przez m_i, gdyż $m_i | M_j$ dla $j \neq i$ zatem dla każdego i mamy $x \equiv a_i M_i N_i \equiv a_i \pmod{m_i}$.

W naszym przykładzie mamy:

$a_1 = 1$, $a_2 = 2$, $a_3 = 3$,

$m_1 = 11$, $m_2 = 12$, $m_3 = 13$, $\quad m = 1716$,

$M_1 = 156$, $M_2 = 143$, $M_3 = 132$.

W naszym przykładzie mamy:

$a_1 = 1$, $a_2 = 2$, $a_3 = 3$,

$m_1 = 11$, $m_2 = 12$, $m_3 = 13$, $\quad m = 1716$,

$M_1 = 156$, $M_2 = 143$, $M_3 = 132$.

Aby znaleźć wspólne rozwiązanie tego układu kongruencji należy znaleźć liczby N_i będące odwrotnościami liczb M_i modulo m_i. W tym celu możemy użyć algorytmu Euklidesa. W wyniku otrzymujemy liczby:

$N_1 = 6$, $N_2 = 11$ i $N_3 = 7$.

Zatem wspólnym rozwiązaniem jest

$$x \equiv 1 \cdot 6 \cdot 156 + 2 \cdot 11 \cdot 143 + 3 \cdot 7 \cdot 132 \pmod{1716}$$
$$\equiv 1706 \pmod{1716}.$$

W naszym przykładzie mamy:

$a_1 = 1$, $a_2 = 2$, $a_3 = 3$,

$m_1 = 11$, $m_2 = 12$, $m_3 = 13$, $\quad m = 1716$,

$M_1 = 156$, $M_2 = 143$, $M_3 = 132$.

Aby znaleźć wspólne rozwiązanie tego układu kongruencji należy znaleźć liczby N_i będące odwrotnościami liczb M_i modulo m_i. W tym celu możemy użyć algorytmu Euklidesa. W wyniku otrzymujemy liczby:

$N_1 = 6$, $N_2 = 11$ i $N_3 = 7$.

Zatem wspólnym rozwiązaniem jest

$$x \equiv 1 \cdot 6 \cdot 156 + 2 \cdot 11 \cdot 143 + 3 \cdot 7 \cdot 132 \pmod{1716}$$
$$\equiv 1706 \pmod{1716}.$$

W tym przykładzie widać, że liczba -10 daje takie reszty zatem

$x = -10 + 1716$.

10.14 Funkcja Eulera

Dla $n \geq 1$, niech $\phi(n)$ będzie liczbą tych nieujemnych liczb b mniejszych od n, które są względnie pierwsze z n. Funkcja $\phi(n)$ nazywa się funkcją Eulera.

10.14 Funkcja Eulera

Dla $n \geq 1$, niech $\phi(n)$ będzie liczbą tych nieujemnych liczb b mniejszych od n, które są względnie pierwsze z n. Funkcja $\phi(n)$ nazywa się funkcją Eulera.

Funkcja Eulera ϕ jest „multiplikatywna", tzn. $\phi(mn) = \phi(m)\phi(n)$, jeśli tylko $NWD(m, n) = 1$.

10.14 Funkcja Eulera

Dla $n \geq 1$, niech $\phi(n)$ będzie liczbą tych nieujemnych liczb b mniejszych od n, które są względnie pierwsze z n. Funkcja $\phi(n)$ nazywa się funkcją Eulera.

Funkcja Eulera ϕ jest „multiplikatywna", tzn. $\phi(mn) = \phi(m)\phi(n)$, jeśli tylko $NWD(m, n) = 1$.

10.15 Twierdzenie Eulera

Jeśli $NWD(a, m) = 1$, to $a^{\phi(m)} \equiv 1 \pmod{m}$.

10.14 Funkcja Eulera

Dla $n \geq 1$, niech $\phi(n)$ będzie liczbą tych nieujemnych liczb b mniejszych od n, które są względnie pierwsze z n. Funkcja $\phi(n)$ nazywa się funkcją Eulera.

Funkcja Eulera ϕ jest „multiplikatywna", tzn. $\phi(mn) = \phi(m)\phi(n)$, jeśli tylko $NWD(m, n) = 1$.

10.15 Twierdzenie Eulera

Jeśli $NWD(a, m) = 1$, to $a^{\phi(m)} \equiv 1 \pmod{m}$.

Wniosek

Jeśli $NWD(a, m) = 1$ i jeśli n' jest resztą z dzielenia n przez $\phi(m)$, to $a^n \equiv a^{n'} \pmod{m}$

10.16 Potęgowanie modulo metodą iterowanego podnoszenia do kwadratu

Podstawowym działaniem w kryptografii jest obliczanie $a^n \pmod{m}$, gdzie m i n są bardzo dużymi liczbami.

10.16 Potęgowanie modulo metodą iterowanego podnoszenia do kwadratu

Podstawowym działaniem w kryptografii jest obliczanie $a^n \pmod{m}$, gdzie m i n są bardzo dużymi liczbami. Zauważmy, że rozwinięcie dwójkowe liczby n ma postać

$$n = \sum_{i=0}^{k-1} n_i 2^i = n_0 + 2n_1 + 4n_2 + \cdots + 2^{k-1} n_{k-1}$$

gdzie $n_i \in \{0, 1\}$ są cyframi rozwinięcia dwójkowego.

10.16 Potęgowanie modulo metodą iterowanego podnoszenia do kwadratu

Podstawowym działaniem w kryptografii jest obliczanie $a^n \pmod{m}$, gdzie m i n są bardzo dużymi liczbami. Zauważmy, że rozwinięcie dwójkowe liczby n ma postać

$$n = \sum_{i=0}^{k-1} n_i 2^i = n_0 + 2n_1 + 4n_2 + \cdots + 2^{k-1} n_{k-1}$$

gdzie $n_i \in \{0, 1\}$ są cyframi rozwinięcia dwójkowego. Zatem

$$a^n = \prod_{i=0}^{k-1} a^{n_i 2^i} = \left(a^{2^0}\right)^{n_0} \left(a^{2^1}\right)^{n_1} \ldots \left(a^{2^{k-1}}\right)^{n_{k-1}}$$

- Załóżmy, że $a < m$ oraz przyjmijmy, że przez b będziemy oznaczali częściowe iloczyny. Na początku $b = 1$.
- Jeżeli $n_0 = 1$ to zastępujemy b przez a, w przeciwnym przypadku nadal $b = 1$.
- Następnie liczymy $a_1 \equiv a^2 \pmod{m}$. Jeśli $n_1 = 1$, to mnożymy b przez a_1 i redukujemy modulo m, zaś jeśli $n_1 = 0$ nie zmieniamy b.
- Następnie liczymy $a_2 \equiv a_1^2 \pmod{m}$. Znowu, jeśli $n_2 = 1$, to mnożymy b przez a_2; w przeciwnym przypadku nie zmieniamy b.

- Załóżmy, że $a < m$ oraz przyjmijmy, że przez b będziemy oznaczali częściowe iloczyny. Na początku $b = 1$.
- Jeżeli $n_0 = 1$ to zastępujemy b przez a, w przeciwnym przypadku nadal $b = 1$.
- Następnie liczymy $a_1 \equiv a^2 \pmod{m}$. Jeśli $n_1 = 1$, to mnożymy b przez a_1 i redukujemy modulo m, zaś jeśli $n_1 = 0$ nie zmieniamy b.
- Następnie liczymy $a_2 \equiv a_1^2 \pmod{m}$. Znowu, jeśli $n_2 = 1$, to mnożymy b przez a_2; w przeciwnym przypadku nie zmieniamy b.

- Załóżmy, że $a < m$ oraz przyjmijmy, że przez b będziemy oznaczali częściowe iloczyny. Na początku $b = 1$.
- Jeżeli $n_0 = 1$ to zastępujemy b przez a, w przeciwnym przypadku nadal $b = 1$.
- Następnie liczymy $a_1 \equiv a^2 \pmod{m}$. Jeśli $n_1 = 1$, to mnożymy b przez a_1 i redukujemy modulo m, zaś jeśli $n_1 = 0$ nie zmieniamy b.
- Następnie liczymy $a_2 \equiv a_1^2 \pmod{m}$. Znowu, jeśli $n_2 = 1$, to mnożymy b przez a_2; w przeciwnym przypadku nie zmieniamy b.

- Załóżmy, że $a < m$ oraz przyjmijmy, że przez b będziemy oznaczali częściowe iloczyny. Na początku $b = 1$.
- Jeżeli $n_0 = 1$ to zastępujemy b przez a, w przeciwnym przypadku nadal $b = 1$.
- Następnie liczymy $a_1 \equiv a^2 \pmod{m}$. Jeśli $n_1 = 1$, to mnożymy b przez a_1 i redukujemy modulo m, zaś jeśli $n_1 = 0$ nie zmieniamy b.
- Następnie liczymy $a_2 \equiv a_1^2 \pmod{m}$. Znowu, jeśli $n_2 = 1$, to mnożymy b przez a_2; w przeciwnym przypadku nie zmieniamy b.

- Postępując dalej w ten sposób, w j-tym kroku mamy obliczoną potęgę $a_j \equiv a^{2^j} \pmod{m}$. Jeśli $n_j = 1$ to włączamy a_j do iloczynu b, jeśli $n_j = 0$ to b się nie zmienia.
- Po $k-1$ krokach otrzymamy $b \equiv a^n \pmod{m}$.

- Postępując dalej w ten sposób, w j-tym kroku mamy obliczoną potęgę $a_j \equiv a^{2^j} \pmod{m}$. Jeśli $n_j = 1$ to włączamy a_j do iloczynu b, jeśli $n_j = 0$ to b się nie zmienia.
- Po $k-1$ krokach otrzymamy $b \equiv a^n \pmod{m}$.

- Postępując dalej w ten sposób, w j-tym kroku mamy obliczoną potęgę $a_j \equiv a^{2^j} \pmod{m}$. Jeśli $n_j = 1$ to włączamy a_j do iloczynu b, jeśli $n_j = 0$ to b się nie zmienia.
- Po $k-1$ krokach otrzymamy $b \equiv a^n \pmod{m}$.

Przykład:

Obliczmy $7^{698} \pmod{1234} = 287$

i	0	1	2	3	4	5	6	7	8	9
n_i	0	1	0	1	1	1	0	1	0	1
a_i	7	49	1167	787	1135	1163	105	1153	391	1099
b	1	49	49	309	259	121	121	71	71	287

10.17 Czy wystarczy liczb pierwszych?

Twierdzenie

Niech $\pi(x)$ oznacza liczbę liczb pierwszych $\leq x$. Wtedy

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

10.17 Czy wystarczy liczb pierwszych?

Twierdzenie

Niech $\pi(x)$ oznacza liczbę liczb pierwszych $\leq x$. Wtedy

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

Dla $x \geq 17$

$$\pi(x) > \frac{x}{\ln x}$$

Dla przykładu, dla $x = 10^{10}$, $\pi(x) = 455052511$, natomiast $\lfloor x/\ln x \rfloor = 434294481$.

10.18 Testy pierwszości

Istnieją probabilistyczne testy pierwszości liczb, które pozwalają z dużym prawdopodobieństwem w skończonym czasie dać odpowiedź czy dana liczba jest pierwsza.

10.18.1 Test Fermata

- Testujemy czy liczba n jest pierwsza
- Wybieramy losowo liczbę $a < n - 1$, obliczamy $r = a^{n-1} \pmod{n}$, jeśli $r \neq 1$ to n jest liczbą złożoną
- Test przeprowadzamy t-krotnie, $t \geq 1$. Jeśli wszystkie testy wypadną pomyślnie, tzn. $r = 1$, to liczbę uznajemy za pierwszą, choć może tak nie być

10.18.1 Test Fermata

- Testujemy czy liczba n jest pierwsza
- Wybieramy losowo liczbę $a < n - 1$, obliczamy $r = a^{n-1} \pmod{n}$, jeśli $r \neq 1$ to n jest liczbą złożoną
- Test przeprowadzamy t-krotnie, $t \geq 1$. Jeśli wszystkie testy wypadną pomyślnie, tzn. $r = 1$, to liczbę uznajemy za pierwszą, choć może tak nie być

10.18.1 Test Fermata

- Testujemy czy liczba n jest pierwsza
- Wybieramy losowo liczbę $a < n - 1$, obliczamy $r = a^{n-1} \pmod{n}$, jeśli $r \neq 1$ to n jest liczbą złożoną
- Test przeprowadzamy t-krotnie, $t \geq 1$. Jeśli wszystkie testy wypadną pomyślnie, tzn. $r = 1$, to liczbę uznajemy za pierwszą, choć może tak nie być

10.18.1 Test Fermata

- Testujemy czy liczba n jest pierwsza
- Wybieramy losowo liczbę $a < n - 1$, obliczamy $r = a^{n-1} \pmod{n}$, jeśli $r \neq 1$ to n jest liczbą złożoną
- Test przeprowadzamy t-krotnie, $t \geq 1$. Jeśli wszystkie testy wypadną pomyślnie, tzn. $r = 1$, to liczbę uznajemy za pierwszą, choć może tak nie być

10.18.2 Test Millera-Rabina

- Testujemy czy liczba n jest pierwsza
- Piszemy $n - 1 = 2^s r$, gdzie r jest nieparzyste
- Wybieramy losowo liczbę a, $1 < a < n - 1$. Obliczamy $b = a^r \pmod{n}$. Jeśli $b \equiv \pm 1 \pmod{n}$ to uznajemy, że n jest liczbą pierwszą.
- W przeciwnym przypadku obliczamy $a^{2^j r} \pmod{n}$ dla $0 < j < s$.

  Jeśli dla pewnego $j < s$ otrzymamy $a^{2^j r} \equiv -1 \pmod{n}$ to uznajemy, że n jest pierwsza.
- W przeciwnym przypadku liczba n jest złożona.
- Test przeprowadzamy t-krotnie dla różnych a.

10.18.2 Test Millera-Rabina

- Testujemy czy liczba n jest pierwsza
- Piszemy $n - 1 = 2^s r$, gdzie r jest nieparzyste
- Wybieramy losowo liczbę a, $1 < a < n - 1$. Obliczamy $b = a^r \pmod{n}$. Jeśli $b \equiv \pm 1 \pmod{n}$ to uznajemy, że n jest liczbą pierwszą.
- W przeciwnym przypadku obliczamy $a^{2^j r} \pmod{n}$ dla $0 < j < s$.
  Jeśli dla pewnego $j < s$ otrzymamy $a^{2^j r} \equiv -1 \pmod{n}$ to uznajemy, że n jest pierwsza.
- W przeciwnym przypadku liczba n jest złożona.
- Test przeprowadzamy t-krotnie dla różnych a.

10.18.2 Test Millera-Rabina

- Testujemy czy liczba n jest pierwsza
- Piszemy $n - 1 = 2^s r$, gdzie r jest nieparzyste
- Wybieramy losowo liczbę a, $1 < a < n - 1$. Obliczamy $b = a^r \pmod{n}$. Jeśli $b \equiv \pm 1 \pmod{n}$ to uznajemy, że n jest liczbą pierwszą.
- W przeciwnym przypadku obliczamy $a^{2^j r} \pmod{n}$ dla $0 < j < s$.
  Jeśli dla pewnego $j < s$ otrzymamy $a^{2^j r} \equiv -1 \pmod{n}$ to uznajemy, że n jest pierwsza.
- W przeciwnym przypadku liczba n jest złożona.
- Test przeprowadzamy t-krotnie dla różnych a.

10.18.2 Test Millera-Rabina

- Testujemy czy liczba n jest pierwsza
- Piszemy $n - 1 = 2^s r$, gdzie r jest nieparzyste
- Wybieramy losowo liczbę a, $1 < a < n - 1$. Obliczamy $b = a^r \pmod{n}$. Jeśli $b \equiv \pm 1 \pmod{n}$ to uznajemy, że n jest liczbą pierwszą.
- W przeciwnym przypadku obliczamy $a^{2^j r} \pmod{n}$ dla $0 < j < s$.
  Jeśli dla pewnego $j < s$ otrzymamy $a^{2^j r} \equiv -1 \pmod{n}$ to uznajemy, że n jest pierwsza.
- W przeciwnym przypadku liczba n jest złożona.
- Test przeprowadzamy t-krotnie dla różnych a.

10.18.2 Test Millera-Rabina

- Testujemy czy liczba n jest pierwsza
- Piszemy $n - 1 = 2^s r$, gdzie r jest nieparzyste
- Wybieramy losowo liczbę a, $1 < a < n - 1$. Obliczamy $b = a^r \pmod{n}$. Jeśli $b \equiv \pm 1 \pmod{n}$ to uznajemy, że n jest liczbą pierwszą.
- W przeciwnym przypadku obliczamy $a^{2^j r} \pmod{n}$ dla $0 < j < s$.
  Jeśli dla pewnego $j < s$ otrzymamy $a^{2^j r} \equiv -1 \pmod{n}$ to uznajemy, że n jest pierwsza.
- W przeciwnym przypadku liczba n jest złożona.
- Test przeprowadzamy t-krotnie dla różnych a.

10.18.2 Test Millera-Rabina

- Testujemy czy liczba n jest pierwsza
- Piszemy $n-1=2^s r$, gdzie r jest nieparzyste
- Wybieramy losowo liczbę a, $1<a<n-1$. Obliczamy $b=a^r \pmod{n}$. Jeśli $b \equiv \pm 1 \pmod{n}$ to uznajemy, że n jest liczbą pierwszą.
- W przeciwnym przypadku obliczamy $a^{2^j r} \pmod{n}$ dla $0<j<s$.
  Jeśli dla pewnego $j<s$ otrzymamy $a^{2^j r} \equiv -1 \pmod{n}$ to uznajemy, że n jest pierwsza.
- W przeciwnym przypadku liczba n jest złożona.
- Test przeprowadzamy t-krotnie dla różnych a.

10.18.2 Test Millera-Rabina

- Testujemy czy liczba n jest pierwsza
- Piszemy $n - 1 = 2^s r$, gdzie r jest nieparzyste
- Wybieramy losowo liczbę a, $1 < a < n - 1$. Obliczamy $b = a^r \pmod{n}$. Jeśli $b \equiv \pm 1 \pmod{n}$ to uznajemy, że n jest liczbą pierwszą.
- W przeciwnym przypadku obliczamy $a^{2^j r} \pmod{n}$ dla $0 < j < s$.
  Jeśli dla pewnego $j < s$ otrzymamy $a^{2^j r} \equiv -1 \pmod{n}$ to uznajemy, że n jest pierwsza.
- W przeciwnym przypadku liczba n jest złożona.
- Test przeprowadzamy t-krotnie dla różnych a.