

LICZBY PIERWSZE

Jeśli matematyka jest królową nauk, to królową matematyki jest teoria liczb.
C.F. Gauss (1777 - 1855)

14 marzec 2007

Zasadnicze twierdzenie teorii liczb

Twierdzenie

Każdą liczbę naturalną $n > 1$ można przedstawić w postaci iloczynu liczb pierwszych

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k.$$

Przedstawienie to jest jednoznaczne z dokładnością do kolejności czynników.

Ile jest liczb pierwszych?

Twierdzenie

Istnieje nieskończenie wiele liczb pierwszych.

Dowód (Euklides)

- Z1 Przypuśćmy, że zbiór \mathbb{P} wszystkich liczb pierwszych jest skończony, tzn. $\mathbb{P} = \{p_1, p_2, \dots, p_n\}$
- Z2 Niech $a = p_1 p_2 \dots p_n + 1$
- Z3 Żadna liczba ze zbioru \mathbb{P} nie dzieli liczby a
- Z4 Z zasadniczego twierdzenia teorii liczb wynika, że liczba a ma dzielnik pierwszy p
- Z5 Ale $p \notin \mathbb{P}$ - SPRZECZNOŚĆ

Ile jest liczb pierwszych?

Twierdzenie

Istnieje nieskończenie wiele liczb pierwszych.

Dowód (Euklides)

- z1 Przypuśćmy, że zbiór \mathbb{P} wszystkich liczb pierwszych jest skończony, tzn. $\mathbb{P} = \{p_1, p_2, \dots, p_n\}$
- z2 Niech $a = p_1 p_2 \dots p_n + 1$
- z3 Żadna liczba ze zbioru \mathbb{P} nie dzieli liczby a
- z4 Z zasadniczego twierdzenia teorii liczb wynika, że liczba a ma dzielnik pierwszy p
- z5 Ale $p \notin \mathbb{P}$ - SPRZECZNOŚĆ

Ile jest liczb pierwszych?

Twierdzenie

Istnieje nieskończenie wiele liczb pierwszych.

Dowód (Euklides)

- Z1 Przypuśćmy, że zbiór \mathbb{P} wszystkich liczb pierwszych jest skończony, tzn. $\mathbb{P} = \{p_1, p_2, \dots, p_n\}$
- Z2 Niech $a = p_1 p_2 \dots p_n + 1$
- Z3 Żadna liczba ze zbioru \mathbb{P} nie dzieli liczby a
- Z4 Z zasadniczego twierdzenia teorii liczb wynika, że liczba a ma dzielnik pierwszy p
- Z5 Ale $p \notin \mathbb{P}$ - SPRZECZNOŚĆ

Ile jest liczb pierwszych?

Twierdzenie

Istnieje nieskończenie wiele liczb pierwszych.

Dowód (Euklides)

- Z1 Przypuśćmy, że zbiór \mathbb{P} wszystkich liczb pierwszych jest skończony, tzn. $\mathbb{P} = \{p_1, p_2, \dots, p_n\}$
- Z2 Niech $a = p_1 p_2 \dots p_n + 1$
- Z3 Żadna liczba ze zbioru \mathbb{P} nie dzieli liczby a
- Z4 Z zasadniczego twierdzenia teorii liczb wynika, że liczba a ma dzielnik pierwszy p
- Z5 Ale $p \notin \mathbb{P}$ - SPRZECZNOŚĆ

Ile jest liczb pierwszych?

Twierdzenie

Istnieje nieskończenie wiele liczb pierwszych.

Dowód (Euklides)

- Z1 Przypuśćmy, że zbiór \mathbb{P} wszystkich liczb pierwszych jest skończony, tzn. $\mathbb{P} = \{p_1, p_2, \dots, p_n\}$
- Z2 Niech $a = p_1 p_2 \dots p_n + 1$
- Z3 Żadna liczba ze zbioru \mathbb{P} nie dzieli liczby a
- Z4 Z zasadniczego twierdzenia teorii liczb wynika, że liczba a ma dzielnik pierwszy p
- Z5 Ale $p \notin \mathbb{P}$ - SPRZECZNOŚĆ

Ile jest liczb pierwszych?

Twierdzenie

Istnieje nieskończenie wiele liczb pierwszych.

Dowód (Euklides)

- Z1 Przypuśćmy, że zbiór \mathbb{P} wszystkich liczb pierwszych jest skończony, tzn. $\mathbb{P} = \{p_1, p_2, \dots, p_n\}$
- Z2 Niech $a = p_1 p_2 \dots p_n + 1$
- Z3 Żadna liczba ze zbioru \mathbb{P} nie dzieli liczby a
- Z4 Z zasadniczego twierdzenia teorii liczb wynika, że liczba a ma dzielnik pierwszy p
- Z5 Ale $p \notin \mathbb{P}$ - SPRZECZNOŚĆ

Jak rozpoznać, czy dana liczba naturalna jest pierwsza?

SITO ERATOSTENESA

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Jak rozpoznać, czy dana liczba naturalna jest pierwsza?

SITO ERATOSTENESA

	2	3	..	5	..	7	..	9	..
11	..	13	..	15	..	17	..	19	..
21	..	23	..	25	..	27	..	29	..
31	..	33	..	35	..	37	..	39	..
41	..	43	..	45	..	47	..	49	..
51	..	53	..	55	..	57	..	59	..
61	..	63	..	65	..	67	..	69	..
71	..	73	..	75	..	77	..	79	..
81	..	83	..	85	..	87	..	89	..
91	..	93	..	95	..	97	..	99	..

Jak rozpoznać, czy dana liczba naturalna jest pierwsza?

SITO ERATOSTENESA

	2	3	..	5	..	7
11	..	13	17	..	19	..
..	..	23	..	25	29	..
31	35	..	37
41	..	43	47	..	49	..
..	..	53	..	55	59	..
61	65	..	67
71	..	73	77	..	79	..
..	..	83	..	85	89	..
91	95	..	97

Jak rozpoznać, czy dana liczba naturalna jest pierwsza?

SITO ERATOSTENESA

	2	3	..	5	..	7
11	..	13	17	..	19	..
..	..	23	29	..
31	37
41	..	43	47	..	49	..
..	..	53	59	..
61	67
71	..	73	77	..	79	..
..	..	83	89	..
91	97

Jak rozpoznać, czy dana liczba naturalna jest pierwsza?

SITO ERATOSTENESA

	2	3	..	5	..	7
11	..	13	17	..	19	..
..	..	23	29	..
31	37
41	..	43	47
..	..	53	59	..
61	67
71	..	73	79	..
..	..	83	89	..
..	97

Kongruencje

Zapis

$$a \equiv b \pmod{n}$$

oznacza, że reszty z dzielenia liczb całkowitych a i b przez liczbę naturalną n są takie same.

WŁASNOŚCI KONGRUENCJI

$$\text{Z1} \quad a + b \pmod{n} \equiv a \pmod{n} + b \pmod{n}$$

$$\text{Z2} \quad ab \pmod{n} \equiv a \pmod{n} \cdot b \pmod{n}$$

Kongruencje

Zapis

$$a \equiv b \pmod{n}$$

oznacza, że reszty z dzielenia liczb całkowitych a i b przez liczbę naturalną n są takie same.

WŁASNOŚCI KONGRUENCJI

$$\text{Z1} \quad a + b \pmod{n} \equiv a \pmod{n} + b \pmod{n}$$

$$\text{Z2} \quad ab \pmod{n} \equiv a \pmod{n} \cdot b \pmod{n}$$

Kongruencje

Zapis

$$a \equiv b \pmod{n}$$

oznacza, że reszty z dzielenia liczb całkowitych a i b przez liczbę naturalną n są takie same.

WŁASNOŚCI KONGRUENCJI

$$\text{Z1} \quad a + b \pmod{n} \equiv a \pmod{n} + b \pmod{n}$$

$$\text{Z2} \quad ab \pmod{n} \equiv a \pmod{n} \cdot b \pmod{n}$$

Kongruencje

Zapis

$$a \equiv b \pmod{n}$$

oznacza, że reszty z dzielenia liczb całkowitych a i b przez liczbę naturalną n są takie same.

WŁASNOŚCI KONGRUENCJI

$$\text{Z1} \quad a + b \pmod{n} \equiv a \pmod{n} + b \pmod{n}$$

$$\text{Z2} \quad ab \pmod{n} \equiv a \pmod{n} \cdot b \pmod{n}$$

Kongruencje

PRZYKŁAD. Jakie są dwie ostatnie cyfry liczby 2^{200} ?

$$\begin{aligned}2^{200} &\equiv (2^{10})^{20} \equiv 1024^{20} \equiv 24^{20} \equiv (24^2)^{10} \equiv 576^{10} \equiv 76^{10} \equiv \\ &(76^2)^5 \equiv 5776^5 \equiv 76^{2 \cdot 2 + 1} \equiv (76^2)^2 \cdot 76 \equiv 76^2 \cdot 76 \equiv 76 \cdot 76 \equiv \\ &76 \pmod{100}\end{aligned}$$

MAŁE TWIERDZENIE FERMATA

Twierdzenie (Pierre Fermat (1601 - 1665))

Jeśli p jest liczbą pierwszą i p nie dzieli a , to

$$a^{p-1} \equiv 1 \pmod{p}.$$

PRZYKŁAD.

$$2^{705238} \equiv 184796 \pmod{705239},$$

a zatem liczba 705239 NIE JEST PIERWSZA. A oto jej rozkład

$$705239 = 859 \cdot 821$$

MAŁE TWIERDZENIE FERMATA

Twierdzenie (Pierre Fermat (1601 - 1665))

Jeśli p jest liczbą pierwszą i p nie dzieli a , to

$$a^{p-1} \equiv 1 \pmod{p}.$$

PRZYKŁAD.

$$2^{705238} \equiv 184796 \pmod{705239},$$

a zatem liczba 705239 NIE JEST PIERWSZA. A oto jej rozkład

$$705239 = 859 \cdot 821$$

MAŁE TWIERDZENIE FERMATA

Twierdzenie (Pierre Fermat (1601 - 1665))

Jeśli p jest liczbą pierwszą i p nie dzieli a , to

$$a^{p-1} \equiv 1 \pmod{p}.$$

PRZYKŁAD.

$$2^{705238} \equiv 184796 \pmod{705239},$$

a zatem liczba 705239 NIE JEST PIERWSZA. A oto jej rozkład

$$705239 = 859 \cdot 821$$

TWIERDZENIE WILSONA

Twierdzenie (John Wilson -1773)

Jeśli p jest liczbą pierwszą, to

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

Największa liczba pierwsza znana przed epoką komputerów

$p = 170\ 141\ 183\ 460\ 469\ 231\ 731\ 687\ 303\ 715\ 884\ 105\ 727$

TWIERDZENIE WILSONA

Twierdzenie (John Wilson -1773)

Jeśli p jest liczbą pierwszą, to

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

Największa liczba pierwsza znana przed epoką komputerów

$p = 170\ 141\ 183\ 460\ 469\ 231\ 731\ 687\ 303\ 715\ 884\ 105\ 727$

Liczby Fermata:

$$F_n = 2^{2^n} + 1$$

F_0	3	liczba pierwsza	-
F_1	5	liczba pierwsza	-
F_2	17	liczba pierwsza	-
F_3	257	liczba pierwsza	-
F_4	65537	liczba pierwsza	P. Fermat
F_5	641 · 6700417	liczba złożona	L. Euler(1750)
F_6	274177 · 67280421310721	liczba złożona	E. Lucas (1880)

Liczby Fermata:

$$F_n = 2^{2^n} + 1$$

F_0	3	liczba pierwsza	-
F_1	5	liczba pierwsza	-
F_2	17	liczba pierwsza	-
F_3	257	liczba pierwsza	-
F_4	65537	liczba pierwsza	P. Fermat
F_5	641 · 6700417	liczba złożona	L. Euler(1750)
F_6	274177 · 67280421310721	liczba złożona	E. Lucas (1880)

Liczby Fermata:

$$F_n = 2^{2^n} + 1$$

- największą znaną liczbą pierwszą Fermata jest F_5
- największą znaną liczbą Fermata złożoną jest F_{23471}
- znany jest pełny rozkład na czynniki pierwsze tylko następujących liczb Fermata: F_5 , F_6 , F_7 , F_8 , F_9 i F_{11}
- nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Fermata

Liczby Fermata:

$$F_n = 2^{2^n} + 1$$

- największą znaną liczbą pierwszą Fermata jest F_5
- największą znaną liczbą Fermata złożoną jest F_{23471}
- znany jest pełny rozkład na czynniki pierwsze tylko następujących liczb Fermata: F_5 , F_6 , F_7 , F_8 , F_9 i F_{11}
- nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Fermata

Liczby Fermata:

$$F_n = 2^{2^n} + 1$$

- największą znaną liczbą pierwszą Fermata jest F_5
- największą znaną liczbą Fermata złożoną jest F_{23471}
- znany jest pełny rozkład na czynniki pierwsze tylko następujących liczb Fermata: F_5 , F_6 , F_7 , F_8 , F_9 i F_{11}
- nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Fermata

Liczby Fermata:

$$F_n = 2^{2^n} + 1$$

- największą znaną liczbą pierwszą Fermata jest F_5
- największą znaną liczbą Fermata złożoną jest F_{23471}
- znany jest pełny rozkład na czynniki pierwsze tylko następujących liczb Fermata: F_5 , F_6 , F_7 , F_8 , F_9 i F_{11}
- nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Fermata

Liczby Mersenne'a

$$M_q = 2^q - 1$$

M_2	3	liczba pierwsza	-
M_3	7	liczba pierwsza	-
M_5	31	liczba pierwsza	-
M_7	127	liczba pierwsza	-
M_{11}	$23 \cdot 89$	liczba złożona	-
M_{13}	8191	liczba pierwsza	-
M_{17}	131071	liczba pierwsza	P.Cataldi (1588)
M_{31}		liczba pierwsza	L.Euler (1750)
M_{89}		liczba pierwsza	R.Powers (1911)
M_{521}		liczba pierwsza	R.Robinson (1952)
M_{9941}		liczba pierwsza	D. Gillies (1963)
M_{21701}		liczba pierwsza	L.Noll (1978)
M_{132049}		liczba pierwsza	D. Słowiński (1983)
$M_{2976221}$		liczba pierwsza	G. Spence (1997)

Liczby Mersenne'a

$$M_q = 2^q - 1$$

M_2	3	liczba pierwsza	-
M_3	7	liczba pierwsza	-
M_5	31	liczba pierwsza	-
M_7	127	liczba pierwsza	-
M_{11}	$23 \cdot 89$	liczba złożona	-
M_{13}	8191	liczba pierwsza	-
M_{17}	131071	liczba pierwsza	P.Cataldi (1588)
M_{31}		liczba pierwsza	L.Euler (1750)
M_{89}		liczba pierwsza	R.Powers (1911)
M_{521}		liczba pierwsza	R.Robinson (1952)
M_{9941}		liczba pierwsza	D. Gillies (1963)
M_{21701}		liczba pierwsza	L.Noll (1978)
M_{132049}		liczba pierwsza	D. Słowiński (1983)
$M_{2976221}$		liczba pierwsza	G. Spence (1997)

Liczby Mersenne'a

$$M_q = 2^q - 1$$

- znanych jest 36 liczb pierwszych Mersenne'a
- największą znaną liczbą pierwszą Mersenne'a jest $M_{2976221}$ (ma 895932 cyfry) - największa znana liczba pierwsza
- największą znaną liczbą złożoną Mersenne'a, dla której znany jest rozkład na czynniki pierwsze to $M_{3359} = 6719 \cdot P1008$
- nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Mersenne'a.

Liczby Mersenne'a

$$M_q = 2^q - 1$$

- znanych jest 36 liczb pierwszych Mersenne'a
- największą znaną liczbą pierwszą Mersenne'a jest $M_{2976221}$ (ma 895932 cyfry) - największa znana liczba pierwsza
- największą znaną liczbą złożoną Mersenne'a, dla której znany jest rozkład na czynniki pierwsze to $M_{3359} = 6719 \cdot P_{1008}$
- nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Mersenne'a.

Liczby Mersenne'a

$$M_q = 2^q - 1$$

- znanych jest 36 liczb pierwszych Mersenne'a
- największą znaną liczbą pierwszą Mersenne'a jest $M_{2976221}$ (ma 895932 cyfry) - największa znana liczba pierwsza
- największą znaną liczbą złożoną Mersenne'a, dla której znany jest rozkład na czynniki pierwsze to $M_{3359} = 6719 \cdot P1008$
- nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Mersenne'a.

Liczby Mersenne'a

$$M_q = 2^q - 1$$

- znanych jest 36 liczb pierwszych Mersenne'a
- największą znaną liczbą pierwszą Mersenne'a jest $M_{2976221}$ (ma 895932 cyfry) - największa znana liczba pierwsza
- największą znaną liczbą złożoną Mersenne'a, dla której znany jest rozkład na czynniki pierwsze to $M_{3359} = 6719 \cdot P1008$
- nie wiadomo, czy istnieje nieskończenie wiele liczb pierwszych Mersenne'a.

Liczby względnie pierwsze

Definicja

Liczby całkowite m, n nazywamy względnie pierwszymi jeśli
 $NWD(m, n) = 1$

Uwaga

Jeśli p, q są różnymi liczbami pierwszymi, to $NWD(p, q) = 1$

Liczby względnie pierwsze

Definicja

Liczby całkowite m, n nazywamy względnie pierwszymi jeśli $NWD(m, n) = 1$

Uwaga

Jeśli p, q są różnymi liczbami pierwszymi, to $NWD(p, q) = 1$

Chińskie twierdzenie o resztach

Twierdzenie

Jeśli liczby naturalne n_1, \dots, n_k są parami względnie pierwsze, a a_1, \dots, a_k są dowolnymi liczbami całkowitymi, to istnieje taka liczba całkowita a , że

$$\begin{cases} a \equiv a_1 \pmod{n_1} \\ \vdots \\ a \equiv a_k \pmod{n_k} \end{cases} .$$

RÓWNANIA DIOFANTYCZNE

Twierdzenie

Jeśli n, m są względnie pierwszymi liczbami całkowitymi i a dowolną liczbą całkowitą, to równanie

$$nX + mY = a$$

ma rozwiązanie w liczbach całkowitych.

RÓWNANIA DIOFANTYCZNE

Jak przewieźć 200 ton towaru ciężarówkami o ładowności 7 i 11 ton?

$$7X + 11Y = 200$$

ALGORYTM EUKLIDESA:

$$\begin{aligned} 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \end{aligned}$$

ODWRACAMY ALGORYTM EUKLIDESA:

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4) = \\ &= 2 \cdot 4 - 7 = 2 \cdot (11 - 7) - 7 = \\ &= 2 \cdot 11 + (-3) \cdot 7 \end{aligned}$$

Z równości

$$1 = -3 \cdot 7 + 2 \cdot 11$$

mamy

$$200 = -600 \cdot 7 + 400 \cdot 11$$

Stąd odczytujemy rozwiązania całkowite równania:

$$\begin{cases} X = -600 + 11k \\ Y = 400 - 7k \end{cases}$$

Interesują nas nieujemne rozwiązania tego układu nierówności. Otrzymujemy je dla $k \in \{55, 56, 57\}$.

$$k = 55 \Rightarrow \begin{cases} X = 5 \\ Y = 15 \end{cases}$$

$$k = 56 \Rightarrow \begin{cases} X = 16 \\ Y = 8 \end{cases}$$

$$k = 57 \Rightarrow \begin{cases} X = 27 \\ Y = 1 \end{cases}$$

Metody szyfrowania

1 METODY SYMETRYCZNE

NADAWCA

szyfrowanie



klucz prywatny

ODBIORCA

deszyfrowanie

2 METODY ASYMETRYCZNE

NADAWCA

szyfrowanie

klucz publiczny



ODBIORCA

deszyfrowanie

klucz prywatny

Metody szyfrowania

1 METODY SYMETRYCZNE

NADAWCA

szyfrowanie



klucz prywatny

ODBIORCA

deszyfrowanie

2 METODY ASYMETRYCZNE

NADAWCA

szyfrowanie

klucz publiczny



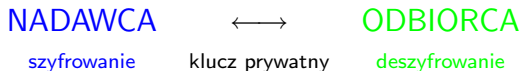
ODBIORCA

deszyfrowanie

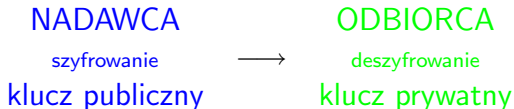
klucz prywatny

Metody szyfrowania

1 METODY SYMETRYCZNE



2 METODY ASYMETRYCZNE



Kryptosystem RSA - R.Rivest, A.Shamir, L. Adleman.

Beata - nadawca

Kamil - odbiorca

Odbiorca wybiera dwie liczby pierwsze p i q oraz liczbę a taką, że $NWD(p - 1, a) = 1$ i $NWD(q - 1, a) = 1$. Wyznacza liczbę $n = p \cdot q$.

KLUCZ PUBLICZNY ODBIORCY TO PARA (n, a) .

Przypuśćmy, że Kamil wybrał $p = 11$, $q = 17$ i $a = 27$. Wtedy klucz publiczny Kamila to para $(187, 27)$.

Szyfrowanie

Nadawca szyfruje wiadomość W obliczając resztę z dzielenia W^a przez n .

Jak to wygląda w praktyce?

Kryptosystem RSA - R.Rivest, A.Shamir, L. Adleman.

Beata - nadawca

Kamil - odbiorca

Odbiorca wybiera dwie liczby pierwsze p i q oraz liczbę a taką, że $NWD(p - 1, a) = 1$ i $NWD(q - 1, a) = 1$. Wyznacza liczbę $n = p \cdot q$.
KLUCZ PUBLICZNY ODBIORCY TO PARA (n, a) .

Przypuśćmy, że Kamil wybrał $p = 11$, $q = 17$ i $a = 27$. Wtedy klucz publiczny Kamila to para $(187, 27)$.

Szyfrowanie

Nadawca szyfruje wiadomość W obliczając resztę z dzielenia W^a przez n .

Jak to wygląda w praktyce?

Kryptosystem RSA - R.Rivest, A.Shamir, L. Adleman.

Beata - nadawca

Kamil - odbiorca

Odbiorca wybiera dwie liczby pierwsze p i q oraz liczbę a taką, że $NWD(p - 1, a) = 1$ i $NWD(q - 1, a) = 1$. Wyznacza liczbę $n = p \cdot q$.
KLUCZ PUBLICZNY ODBIORCY TO PARA (n, a) .

Przyjmijmy, że Kamil wybrał $p = 11$, $q = 17$ i $a = 27$. Wtedy klucz publiczny Kamila to para **$(187, 27)$** .

Szyfrowanie

Nadawca szyfruje wiadomość W obliczając resztę z dzielenia W^a przez n .

Jak to wygląda w praktyce?

Kryptosystem RSA - R.Rivest, A.Shamir, L. Adleman.

Beata - nadawca

Kamil - odbiorca

Odbiorca wybiera dwie liczby pierwsze p i q oraz liczbę a taką, że $NWD(p - 1, a) = 1$ i $NWD(q - 1, a) = 1$. Wyznacza liczbę $n = p \cdot q$.
KLUCZ PUBLICZNY ODBIORCY TO PARA (n, a) .

Przypuśćmy, że Kamil wybrał $p = 11$, $q = 17$ i $a = 27$. Wtedy klucz publiczny Kamila to para $(187, 27)$.

Szyfrowanie

Nadawca szyfruje wiadomość W obliczając resztę z dzielenia W^a przez n .

Jak to wygląda w praktyce?

Kryptosystem RSA - R.Rivest, A.Shamir, L. Adleman.

Beata - nadawca

Kamil - odbiorca

Odbiorca wybiera dwie liczby pierwsze p i q oraz liczbę a taką, że $NWD(p - 1, a) = 1$ i $NWD(q - 1, a) = 1$. Wyznacza liczbę $n = p \cdot q$.
KLUCZ PUBLICZNY ODBIORCY TO PARA (n, a) .

Przypuśćmy, że Kamil wybrał $p = 11$, $q = 17$ i $a = 27$. Wtedy klucz publiczny Kamila to para **$(187, 27)$** .

Szyfrowanie

Nadawca szyfruje wiadomość W obliczając resztę z dzielenia W^a przez n .

Jak to wygląda w praktyce?

Kryptosystem RSA

Beata przesyła Kamilowi pewną wiadomość używając jako alfabetu KODU ASCII.

KOD ASCII

	A	B	C	D	E	F	G	H	I	J	K	L	M
032	065	066	067	068	069	070	071	072	073	074	075	076	077
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	078	079	080	081	082	083	084	085	086	087	088	089	090

Beata zapisuje wiadomość w alfabecie ASCII:

076073067090066089032080073069082087083090069032

Klucz publiczny Kamila to $(187, 27)$. Beata dzieli wiadomość na liczby mniejsze od 187 (każdą z nich traktuje jako oddzielną wiadomość):

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i szyfruje wyznaczając $w_i^{27} \pmod{187}$:

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kryptosystem RSA

Beata przesłała Kamilowi pewną wiadomość używając jako alfabetu KODU ASCII.

KOD ASCII

	A	B	C	D	E	F	G	H	I	J	K	L	M
032	065	066	067	068	069	070	071	072	073	074	075	076	077
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	078	079	080	081	082	083	084	085	086	087	088	089	090

Beata zapisuje wiadomość w alfabecie ASCII:

076073067090066089032080073069082087083090069032

Klucz publiczny Kamila to $(187, 27)$. Beata dzieli wiadomość na liczby mniejsze od 187 (każdą z nich traktuje jako oddzielną wiadomość):

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i szyfruje wyznaczając $w_i^{27} \pmod{187}$:

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kryptosystem RSA

Beata przesyła Kamilowi pewną wiadomość używając jako alfabetu KODU ASCII.

KOD ASCII

	A	B	C	D	E	F	G	H	I	J	K	L	M
032	065	066	067	068	069	070	071	072	073	074	075	076	077
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	078	079	080	081	082	083	084	085	086	087	088	089	090

Beata zapisuje wiadomość w alfabecie ASCII:

076073067090066089032080073069082087083090069032

Klucz publiczny Kamila to $(187, 27)$. Beata dzieli wiadomość na liczby mniejsze od 187 (każdą z nich traktuje jako oddzielną wiadomość):

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i szyfruje wyznaczając $w_i^{27} \pmod{187}$:

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kryptosystem RSA

Beata przesyła Kamilowi pewną wiadomość używając jako alfabetu KODU ASCII.

KOD ASCII

	A	B	C	D	E	F	G	H	I	J	K	L	M
032	065	066	067	068	069	070	071	072	073	074	075	076	077
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	078	079	080	081	082	083	084	085	086	087	088	089	090

Beata zapisuje wiadomość w alfabecie ASCII:

076073067090066089032080073069082087083090069032

Klucz publiczny Kamila to $(187, 27)$. Beata dzieli wiadomość na liczby mniejsze od 187 (każdą z nich traktuje jako oddzielną wiadomość):

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i szyfruje wyznaczając $w_i^{27} \pmod{187}$:

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

stąd

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

stąd

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

stąd

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

stąd

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

stąd

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

stąd

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

stąd

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

stąd

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Do odszyfrowania wiadomości odbiorca używa swojego klucza prywatnego. Jest nim liczba d o własnościach: $da \equiv 1 \pmod{p-1}$ i $da \equiv 1 \pmod{q-1}$. Można ją łatwo wyliczyć korzystając z algorytmu Euklidesa dla pary liczb a i $NWW(p-1, q-1)$.

Jak Kamil odczyta wiadomość Beaty? Jego klucz publiczny to $(187, 27)$, gdzie $187 = 11 \cdot 17$. Kamil wyznacza swój klucz prywatny d :

$$NWW(10, 16) = 80$$

$$80 = 27 \cdot 2 + 26$$

$$27 = 26 \cdot 1 + 1$$

Zatem

$$1 = 27 - 26 = 27 - (80 - 2 \cdot 27) = 3 \cdot 27 - 80,$$

sład

$$3 \cdot 27 \equiv 1 \pmod{80},$$

Czyli dla Kamila $d = 3$

Kryptosystem RSA

Deszyfrowanie

Odbiorca odszyfrowuje wiadomość obliczając $V^d \pmod{n}$.

Przypomnijmy, że wiadomość od Beaty, to

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kamil wyznacza dla każdego słowa v_i wartość $v_i^3 \pmod{187}$:

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i odczytuje wiadomość korzystając z kodu ASCII:

076	073	067	090	066	089	032	080	073	069	082	087	083	090	069
L	I	C	Z	B	Y		P	I	E	R	W	S	Z	E

Kryptosystem RSA

Deszyfrowanie

Odbiorca odszyfrowuje wiadomość obliczając $V^d \pmod{n}$.

Przypomnijmy, że wiadomość od Beaty, to

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kamil wyznacza dla każdego słowa v_i wartość $v_i^3 \pmod{187}$:

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i odczytuje wiadomość korzystając z kodu ASCII:

076	073	067	090	066	089	032	080	073	069	082	087	083	090	069
L	I	C	Z	B	Y		P	I	E	R	W	S	Z	E

Kryptosystem RSA

Deszyfrowanie

Odbiorca odszyfrowuje wiadomość obliczając $V^d \pmod{n}$.

Przypomnijmy, że wiadomość od Beaty, to

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kamil wyznacza dla każdego słowa v_i wartość $v_i^3 \pmod{187}$:

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i odczytuje wiadomość korzystając z kodu ASCII:

076	073	067	090	066	089	032	080	073	069	082	087	083	090	069
L	I	C	Z	B	Y	L	P	I	E	R	W	S	Z	E

Kryptosystem RSA

Deszyfrowanie

Odbiorca odszyfrowuje wiadomość obliczając $V^d \pmod{n}$.

Przypomnijmy, że wiadomość od Beaty, to

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kamil wyznacza dla każdego słowa v_i wartość $v_i^3 \pmod{187}$:

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i odczytuje wiadomość korzystając z kodu ASCII:

076	073	067	090	066	089	032	080	073	069	082	087	083	090	069
L	I	C	Z	B	Y	L	P	I	E	R	W	S	Z	E

Kryptosystem RSA

Deszyfrowanie

Odbiorca odszyfrowuje wiadomość obliczając $V^d \pmod{n}$.

Przypomnijmy, że wiadomość od Beaty, to

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kamil wyznacza dla każdego słowa v_i wartość $v_i^3 \pmod{187}$:

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i odczytuje wiadomość korzystając z kodu ASCII:

076	073	067	090	066	089	032	080	073	069	082	087	083	090	069
L	I	C	Z	B	Y	L	P	I	E	R	W	S	Z	E

Kryptosystem RSA

Deszyfrowanie

Odbiorca odszyfrowuje wiadomość obliczając $V^d \pmod{n}$.

Przypomnijmy, że wiadomość od Beaty, to

116 168 28 107 93 62 107 168 166 75 92 108 116 123 86 2 92 76 2 123 62 107 62 43

Kamil wyznacza dla każdego słowa v_i wartość $v_i^3 \pmod{187}$:

07 60 73 06 70 90 06 60 89 03 20 80 07 30 69 08 20 87 08 30 90 06 90 32

i odczytuje wiadomość korzystając z kodu ASCII:

076	073	067	090	066	089	032	080	073	069	082	087	083	090	069
L	I	C	Z	B	Y		P	I	E	R	W	S	Z	E

Kryptosystem RSA

Henryk przejął zaszyfowaną wiadomość Beaty. Zna również klucz publiczny Kamila ($n = 187, a = 27$).

Co powstrzyma Henryka, przed odszyfrowaniem wiadomości?

NIC, no chyba że...Kamil wybierze inny klucz publiczny np $n =$

```
2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440
6918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014
9718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822
1686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067
4810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350
7787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103
97122822120720357
```

(RSA - 2048)

Kryptosystem RSA

Henryk przejął zaszyfowaną wiadomość Beaty. Zna również klucz publiczny Kamila ($n = 187, a = 27$).

Co powstrzyma Henryka, przed odszyfrowaniem wiadomości?

NIC, no chyba że...Kamil wybierze inny klucz publiczny np $n =$

```
2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440
6918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014
9718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822
1686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067
4810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350
7787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103
97122822120720357
```

(RSA - 2048)

Kryptosystem RSA

Henryk przejął zaszyfowaną wiadomość Beaty. Zna również klucz publiczny Kamila ($n = 187, a = 27$).

Co powstrzyma Henryka, przed odszyfrowaniem wiadomości?

NIC, no chyba że....Kamil wybierze inny klucz publiczny np $n =$

```
2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440
6918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014
9718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822
1686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067
4810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350
7787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103
97122822120720357
```

(RSA - 2048)

Kryptosystem RSA

Henryk przejął zaszyfowaną wiadomość Beaty. Zna również klucz publiczny Kamila ($n = 187, a = 27$).

Co powstrzyma Henryka, przed odszyfrowaniem wiadomości?

NIC, no chyba że....Kamil wybierze inny klucz publiczny np $n =$

```
2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440
6918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014
9718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822
1686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067
4810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350
7787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103
97122822120720357
```

(RSA - 2048)

Kryptosystem RSA

Henryk przejął zaszyfowaną wiadomość Beaty. Zna również klucz publiczny Kamila ($n = 187, a = 27$).

Co powstrzyma Henryka, przed odszyfrowaniem wiadomości?

NIC, no chyba że....Kamil wybierze inny klucz publiczny np $n =$

2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440
6918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014
9718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822
1686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067
4810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350
7787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103
97122822120720357

(RSA - 2048)

Kryptosystem RSA

Ile czasu potrzebuje komputer aby rozłożyć na czynniki duże liczby n ?

n	1986	1996	2006
10^{50}	90 s	3 s	90 ms
10^{70}	5 h	10 min	17 s
10^{100}	172 dni	5 h	3,5 h
10^{120}	26 lat	300 dni	10 dni
10^{140}	10^3 lat	35 lat	400 dni
10^{160}	10^4 lat	400 lat	26 lat

Czy potrafisz odszyfrować tę wiadomość?

4061 0321 0779 1279 1954 0050 1878 1954 3833 4118 0321 4061
0321 2924 0050 0490 0321 1279 1172 0490 0321 1279 0969 0589
1172

Wiadomość została zapisana w alfabecie ASCII i zakodowana kluczem publicznym:

$$(n = 4223, a = 583)$$

Literatura

- 1 Paulo Ribenboim *Mała księga wielkich liczb pierwszych*, WNT Warszawa 1994;
- 2 Neal Koblitz *Algebraiczne aspekty kryptografii*, WNT Warszawa 2000;
- 3 <http://www.rsa.com/rsalabs>