Kryptografia

z elementami kryptografii kwantowej

Ryszard Tanaś

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

Wykład 6a

Spis treści

10 Trochę matematyki (c.d.)

10.19 Reszty kwadratowe w $\mathbb{Z}_p^*$

- Oznaczmy przez $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ zbiór reszt modulo p, gdzie $p > 2$ jest nieparzystą liczbą pierwszą; np. $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- Przez $\mathbb{Z}_p^*$ będziemy oznaczali zbiór niezerowych elementów zbioru $\mathbb{Z}_p$, a więc np. $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- W zbiorze $\mathbb{Z}_p^*$ szukamy takich elementów, które są kwadratami innych elementów, tzn. spełniona jest kongruencja $x^2 \equiv a \pmod{p}$, dla $\{x, a\} \in \mathbb{Z}_p^*$.
  Liczby a, które są kwadratami nazywamy resztami kwadratowymi modulo p, zaś pozostałe elementy nazywamy nieresztami.

10 Trochę matematyki (c.d.)

10.19 Reszty kwadratowe w $\mathbb{Z}_p^*$

- Oznaczmy przez $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ zbiór reszt modulo p, gdzie $p > 2$ jest nieparzystą liczbą pierwszą; np. $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- Przez $\mathbb{Z}_p^*$ będziemy oznaczali zbiór niezerowych elementów zbioru $\mathbb{Z}_p$, a więc np. $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- W zbiorze $\mathbb{Z}_p^*$ szukamy takich elementów, które są kwadratami innych elementów, tzn. spełniona jest kongruencja $x^2 \equiv a \pmod{p}$, dla $\{x, a\} \in \mathbb{Z}_p^*$.
  Liczby a, które są kwadratami nazywamy resztami kwadratowymi modulo p, zaś pozostałe elementy nazywamy nieresztami.

10 Trochę matematyki (c.d.)

10.19 Reszty kwadratowe w $\mathbb{Z}_p^*$

- Oznaczmy przez $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ zbiór reszt modulo p, gdzie $p > 2$ jest nieparzystą liczbą pierwszą; np. $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- Przez $\mathbb{Z}_p^*$ będziemy oznaczali zbiór niezerowych elementów zbioru $\mathbb{Z}_p$, a więc np. $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- W zbiorze $\mathbb{Z}_p^*$ szukamy takich elementów, które są kwadratami innych elementów, tzn. spełniona jest kongruencja $x^2 \equiv a \pmod{p}$, dla $\{x, a\} \in \mathbb{Z}_p^*$.
  Liczby a, które są kwadratami nazywamy resztami kwadratowymi modulo p, zaś pozostałe elementy nazywamy nieresztami.

10 Trochę matematyki (c.d.)

10.19 Reszty kwadratowe w $\mathbb{Z}_p^*$

- Oznaczmy przez $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ zbiór reszt modulo p, gdzie $p > 2$ jest nieparzystą liczbą pierwszą; np. $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- Przez $\mathbb{Z}_p^*$ będziemy oznaczali zbiór niezerowych elementów zbioru $\mathbb{Z}_p$, a więc np. $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- W zbiorze $\mathbb{Z}_p^*$ szukamy takich elementów, które są kwadratami innych elementów, tzn. spełniona jest kongruencja $x^2 \equiv a \pmod{p}$, dla $\{x, a\} \in \mathbb{Z}_p^*$.
  Liczby a, które są kwadratami nazywamy resztami kwadratowymi modulo p, zaś pozostałe elementy nazywamy nieresztami.

Przykład:

Weźmy $\mathbb{Z}_{11}^*$ i policzmy $x^2 \pmod{11}$ dla wszystkich x, mamy wtedy

x	1	2	3	4	5	6	7	8	9	10
$a = x^2 \pmod{11}$	1	4	9	5	3	3	5	9	4	1

Przykład:

Weźmy $\mathbb{Z}_{11}^*$ i policzmy $x^2 \pmod{11}$ dla wszystkich x, mamy wtedy

x	1	2	3	4	5	6	7	8	9	10
$a = x^2 \pmod{11}$	1	4	9	5	3	3	5	9	4	1

Resztami kwadratowymi w $\mathbb{Z}_{11}^*$ są więc liczby $\{1, 3, 4, 5, 9\}$, a pozostale liczby $\{2, 6, 7, 8, 10\}$ są nieresztami

10.20 Symbol Legendre'a

Niech a będzie liczbą całkowitą zaś $p > 2$ liczbą pierwszą; symbol Legendre'a definiujemy

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{jeśli } p|a \\ 1, & \text{jeśli } a \text{ jest resztą kwadratową modulo } p \\ -1, & \text{jeśli } a \text{ jest niereszta modulo } p \end{cases}$$

10.20 Symbol Legendre'a

Niech a będzie liczbą całkowitą zaś $p > 2$ liczbą pierwszą; symbol Legendre'a definiujemy

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{jeśli } p|a \\ 1, & \text{jeśli } a \text{ jest resztą kwadratową modulo } p \\ -1, & \text{jeśli } a \text{ jest niereszta modulo } p \end{cases}$$

Twierdzenie:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$$

10.21 Własności symbolu Legendre'a:

(1) $\left(\frac{a}{p}\right)$ zależy tylko od a modulo p

10.21 Własności symbolu Legendre'a:

(1) $\left(\frac{a}{p}\right)$ zależy tylko od a modulo p

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

10.21 Własności symbolu Legendre'a:

(1) $\left(\frac{a}{p}\right)$ zależy tylko od a modulo p

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(3) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$, jeśli $NWD(b,p) = 1$

10.21 Własności symbolu Legendre'a:

(1) $\left(\frac{a}{p}\right)$ zależy tylko od a modulo p

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(3) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$, jeśli $NWD(b,p) = 1$

(4) $\left(\frac{1}{p}\right) = 1$ oraz $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Twierdzenie:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{jeśli } p \equiv \pm 1 \pmod 8 \\ -1, & \text{jeśli } p \equiv \pm 3 \pmod 8 \end{cases}$$

Twierdzenie:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{jeśli } p \equiv \pm 1 \pmod 8 \\ -1, & \text{jeśli } p \equiv \pm 3 \pmod 8 \end{cases}$$

10.22 Prawo wzajemności

Niech p i q będą dwiema nieparzystymi liczbami pierwszymi. Wtedy

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

$$= \begin{cases} -\left(\frac{p}{q}\right), & \text{jeśli } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{p}{q}\right), & \text{w przeciwnym przypadku} \end{cases}$$

Przykład:

$$\left(\frac{91}{167}\right) = \left(\frac{7\cdot 13}{167}\right) = \left(\frac{7}{167}\right)\left(\frac{13}{167}\right)$$

$$= (-1)^{\frac{7-1}{2}\frac{167-1}{2}}\left(\frac{167}{7}\right)(-1)^{\frac{13-1}{2}\frac{167-1}{2}}\left(\frac{167}{13}\right)$$

$$= -\left(\frac{167}{7}\right)\left(\frac{167}{13}\right) = -\left(\frac{6}{7}\right)\left(\frac{11}{13}\right)$$

$$= -\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{11}{13}\right) = -\left(\frac{3}{7}\right)\left(\frac{11}{13}\right)$$

$$-(-1)^{\frac{3-1}{2}\frac{7-1}{2}}\left(\frac{7}{3}\right)(-1)^{\frac{11-1}{2}\frac{13-1}{2}}\left(\frac{13}{11}\right)$$

$$= \left(\frac{1}{3}\right)\left(\frac{2}{11}\right) = 1\cdot(-1) = -1$$

10.23 Pierwiastki kwadratowe modulo p

- Prawo wzajemności pozwala szybko stwierdzić czy a jest resztą kwadratową modulo p, a więc mówi, że istnieje rozwiązanie kongruencji

$$x^2 \equiv a \pmod{p},$$

chociaż nie daje wskazówek jak takie rozwiązanie znaleźć.

- Nie jest znany efektywny deterministyczny algorytm obliczania pierwiastków kwadratowych w $\mathbb{Z}_p^*$. Istnieje natomiast efektywny algorytm probabilistyczny dla obliczania takich pierwiastków jeśli p jest liczbą pierwszą.

10.23 Pierwiastki kwadratowe modulo p

- Prawo wzajemności pozwala szybko stwierdzić czy a jest resztą kwadratową modulo p, a więc mówi, że istnieje rozwiązanie kongruencji

$$x^2 \equiv a \pmod{p},$$

chociaż nie daje wskazówek jak takie rozwiązanie znaleźć.

- Nie jest znany efektywny deterministyczny algorytm obliczania pierwiastków kwadratowych w $\mathbb{Z}_p^*$. Istnieje natomiast efektywny algorytm probabilistyczny dla obliczania takich pierwiastków jeśli p jest liczbą pierwszą.

10.23 Pierwiastki kwadratowe modulo p

- Prawo wzajemności pozwala szybko stwierdzić czy a jest resztą kwadratową modulo p, a więc mówi, że istnieje rozwiązanie kongruencji

$$x^2 \equiv a \pmod{p},$$

chociaż nie daje wskazówek jak takie rozwiązanie znaleźć.

- Nie jest znany efektywny deterministyczny algorytm obliczania pierwiastków kwadratowych w $\mathbb{Z}_p^*$. Istnieje natomiast efektywny algorytm probabilistyczny dla obliczania takich pierwiastków jeśli p jest liczbą pierwszą.

10.24 Reszty kwadratowe w $\mathbb{Z}_n^*$

- Oznaczmy przez $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ zbiór reszt modulo n, gdzie n jest dodatnią liczbą całkowitą; np. $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$
- Przez $\mathbb{Z}_n^*$ będziemy oznaczali podzbiór tych elementów zbioru $\mathbb{Z}_n$, które są względnie pierwsze z n, a więc np. $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Liczba elementów zbioru $\mathbb{Z}_n^*$ jest równa wartości funkcji Eulera $\phi(n)$.
- W zbiorze $\mathbb{Z}_n^*$ szukamy takich elementów, które są kwadratami innych elementów, tzn. spełniona jest kongruencja $x^2 \equiv a \pmod{n}$, dla $\{x, a\} \in \mathbb{Z}_n^*$.

10.24 Reszty kwadratowe w $\mathbb{Z}_n^*$

- Oznaczmy przez $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ zbiór reszt modulo n, gdzie n jest dodatnią liczbą całkowitą; np.
  $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$
- Przez $\mathbb{Z}_n^*$ będziemy oznaczali podzbiór tych elementów zbioru $\mathbb{Z}_n$, które są względnie pierwsze z n, a więc np.
  $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Liczba elementów zbioru $\mathbb{Z}_n^*$ jest równa wartości funkcji Eulera $\phi(n)$.
- W zbiorze $\mathbb{Z}_n^*$ szukamy takich elementów, które są kwadratami innych elementów, tzn. spełniona jest kongruencja $x^2 \equiv a \pmod{n}$, dla $\{x, a\} \in \mathbb{Z}_n^*$.

10.24 Reszty kwadratowe w $\mathbb{Z}_n^*$

- Oznaczmy przez $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ zbiór reszt modulo n, gdzie n jest dodatnią liczbą całkowitą; np. $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$
- Przez $\mathbb{Z}_n^*$ będziemy oznaczali podzbiór tych elementów zbioru $\mathbb{Z}_n$, które są względnie pierwsze z n, a więc np. $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Liczba elementów zbioru $\mathbb{Z}_n^*$ jest równa wartości funkcji Eulera $\phi(n)$.
- W zbiorze $\mathbb{Z}_n^*$ szukamy takich elementów, które są kwadratami innych elementów, tzn. spełniona jest kongruencja $x^2 \equiv a \pmod{n}$, dla $\{x, a\} \in \mathbb{Z}_n^*$.

10.24 Reszty kwadratowe w $\mathbb{Z}_n^*$

- Oznaczmy przez $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ zbiór reszt modulo n, gdzie n jest dodatnią liczbą całkowitą; np. $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$
- Przez $\mathbb{Z}_n^*$ będziemy oznaczali podzbiór tych elementów zbioru $\mathbb{Z}_n$, które są względnie pierwsze z n, a więc np. $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Liczba elementów zbioru $\mathbb{Z}_n^*$ jest równa wartości funkcji Eulera $\phi(n)$.
- W zbiorze $\mathbb{Z}_n^*$ szukamy takich elementów, które są kwadratami innych elementów, tzn. spełniona jest kongruencja $x^2 \equiv a \pmod{n}$, dla $\{x, a\} \in \mathbb{Z}_n^*$.

10.25 Symbol Jacobiego

Niech a będzie liczbą całkowitą i niech n będzie dowolną dodatnią liczbą nieparzystą. Niech $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ będzie rozkładem liczby n na czynniki pierwsze. Wtedy definiujemy symbol Jacobiego (uogólnienie symbolu Legendre'a) jako iloczyn symboli Legendre'a dla dzielników pierwszych n

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{\alpha_r}$$

10.25 Symbol Jacobiego

Niech a będzie liczbą całkowitą i niech n będzie dowolną dodatnią liczbą nieparzystą. Niech $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ będzie rozkładem liczby n na czynniki pierwsze. Wtedy definiujemy symbol Jacobiego (uogólnienie symbolu Legendre'a) jako iloczyn symboli Legendre'a dla dzielników pierwszych n

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{\alpha_r}$$

Twierdzenie:

Dla dowolnej dodatniej liczby nieparzystej n mamy

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

Twierdzenie:

Dla dowolnych dodatnich liczb nieparzystych m i n mamy

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$$

Twierdzenie:

Dla dowolnych dodatnich liczb nieparzystych m i n mamy

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$$

Uwaga:

Jeśli liczba $a \in \mathbb{Z}_n^*$ jest resztą kwadratową to $\left(\frac{a}{n}\right) = 1$.

Jeśli symbol Jacobiego $\left(\frac{a}{n}\right) = 1$ dla liczby złożonej n

to a nie musi być resztą kwadratową!

10.26 Pierwiastki kwadratowe modulo n

- Jeśli $n = pq$ jest iloczynem dwóch dużych, różnych liczb pierwszych, to uważa się, że znajdowanie pierwiastków kwadratowych w $\mathbb{Z}_n^*$ należy do problemów trudnych obliczeniowo!
- Trudność ta jest równoważna trudności z faktoryzacją liczby n. (Faktoryzując n znajdujemy liczby pierwsze p i q, znajdujemy pierwiastki kwadratowe w $\mathbb{Z}_p^*$ oraz $\mathbb{Z}_q^*$, a następnie korzystając z chińskiego twierdzenia o resztach znajdujemy pierwiastki w $\mathbb{Z}_n^*$.)

10.26 Pierwiastki kwadratowe modulo n

- Jeśli $n = pq$ jest iloczynem dwóch dużych, różnych liczb pierwszych, to uważa się, że znajdowanie pierwiastków kwadratowych w $\mathbb{Z}_n^*$ należy do problemów trudnych obliczeniowo!

- Trudność ta jest równoważna trudności z faktoryzacją liczby n. (Faktoryzując n znajdujemy liczby pierwsze p i q, znajdujemy pierwiastki kwadratowe w $\mathbb{Z}_p^*$ oraz $\mathbb{Z}_q^*$, a następnie korzystając z chińskiego twierdzenia o resztach znajdujemy pierwiastki w $\mathbb{Z}_n^*$.)

10.26 Pierwiastki kwadratowe modulo n

- Jeśli $n = pq$ jest iloczynem dwóch dużych, różnych liczb pierwszych, to uważa się, że znajdowanie pierwiastków kwadratowych w $\mathbb{Z}_n^*$ należy do problemów trudnych obliczeniowo!

- Trudność ta jest równoważna trudności z faktoryzacją liczby n. (Faktoryzując n znajdujemy liczby pierwsze p i q, znajdujemy pierwiastki kwadratowe w $\mathbb{Z}_p^*$ oraz $\mathbb{Z}_q^*$, a następnie korzystając z chińskiego twierdzenia o resztach znajdujemy pierwiastki w $\mathbb{Z}_n^*$.)

10.27 Logarytm dyskretny

- Niech p będzie liczbą pierwszą, przez $\mathbb{Z}_p^*$ oznaczamy zbiór liczb $\{1, \ldots, p-1\}$ i niech g będzie generatorem $\mathbb{Z}_p^*$, tzn. takim elementem, że dla każdej liczby $a \in \mathbb{Z}_p^*$ istnieje takie i, że $a \equiv g^i \pmod{p}$ (wszystkie elementy mogą być wygenerowane z g).
- Problem logarytmu dyskretnego polega na znalezieniu dla danej liczby $0 < b < p$ takiej liczby a, że $g^a \equiv b \pmod{p}$.
- Problem znajdowania logarytmu dyskretnego jest problemem trudnym obliczeniowo!

10.27 Logarytm dyskretny

- Niech p będzie liczbą pierwszą, przez $\mathbb{Z}_p^*$ oznaczamy zbiór liczb $\{1, \ldots, p-1\}$ i niech g będzie generatorem $\mathbb{Z}_p^*$, tzn. takim elementem, że dla każdej liczby $a \in \mathbb{Z}_p^*$ istnieje takie i, że $a \equiv g^i \pmod{p}$ (wszystkie elementy mogą być wygenerowane z g).
- Problem logarytmu dyskretnego polega na znalezieniu dla danej liczby $0 < b < p$ takiej liczby a, że $g^a \equiv b \pmod{p}$.
- Problem znajdowania logarytmu dyskretnego jest problemem trudnym obliczeniowo!

10.27 Logarytm dyskretny

- Niech p będzie liczbą pierwszą, przez $\mathbb{Z}_p^*$ oznaczamy zbiór liczb $\{1, \ldots, p-1\}$ i niech g będzie generatorem $\mathbb{Z}_p^*$, tzn. takim elementem, że dla każdej liczby $a \in \mathbb{Z}_p^*$ istnieje takie i, że $a \equiv g^i \pmod{p}$ (wszystkie elementy mogą być wygenerowane z g).
- Problem logarytmu dyskretnego polega na znalezieniu dla danej liczby $0 < b < p$ takiej liczby a, że $g^a \equiv b \pmod{p}$.
- Problem znajdowania logarytmu dyskretnego jest problemem trudnym obliczeniowo!

10.27 Logarytm dyskretny

- Niech p będzie liczbą pierwszą, przez $\mathbb{Z}_p^*$ oznaczamy zbiór liczb $\{1, \ldots, p-1\}$ i niech g będzie generatorem $\mathbb{Z}_p^*$, tzn. takim elementem, że dla każdej liczby $a \in \mathbb{Z}_p^*$ istnieje takie i, że $a \equiv g^i \pmod{p}$ (wszystkie elementy mogą być wygenerowane z g).
- Problem logarytmu dyskretnego polega na znalezieniu dla danej liczby $0 < b < p$ takiej liczby a, że $g^a \equiv b \pmod{p}$.
- Problem znajdowania logarytmu dyskretnego jest problemem trudnym obliczeniowo!

Przykład:

Weźmy $\mathbb{Z}_{19}^*$, czyli zbiór liczb $\{1, \ldots, 18\}$ oraz $g = 2$.

Niech $b = 2^a \pmod{19}$, mamy wtedy

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
b	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Przykład:

Weźmy $\mathbb{Z}_{19}^*$, czyli zbiór liczb $\{1, \ldots, 18\}$ oraz $g = 2$.

Niech $b = 2^a \pmod{19}$, mamy wtedy

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
b	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Tak więc w $\mathbb{Z}_{19}^*$, np.

$$\log_2 13 = 5$$

$$2^5 \equiv 13 \pmod{19}$$

10.28 PARI/GP — teoria liczb na komputerze

```
                GP/PARI CALCULATOR Version 2.1.6 (released)
                     i386 running linux 32-bit version
               (readline v4.3 enabled, extended help available)

                            Copyright (C) 2002 The PARI Group

PARI/GP is free software, covered by the GNU General Public License, and
comes WITHOUT ANY WARRANTY WHATSOEVER.

Type ? for help, \q to quit.
Type ?12 for how to get moral (and possibly technical) support.

   realprecision = 28 significant digits
   seriesprecision = 16 significant terms
   format = g0.28

parisize = 4000000, primelimit = 500000
```

Dzielenie z resztą

```
? divrem(841,160)
%1 = [5, 41]~
? divrem(29876342114321231 23,8765392)
%2 = [340844335476, 5476531]~
```

Algorytm Euklidesa — $NWD(a, b)$

```
? gcd(841,160)
%2 = 1
? gcd(29876342114321231 23,8765392)
%3 = 1
? gcd(73983458723198476321 2876546,497563772132052)
%4 = 6
```

Rozszerzony algorytm Euklidesa

```
? bezout(841,160)
%4 = [-39, 205, 1]
? bezout(29876342114321231 23,8765392)
%5 = [2987931, -101841935614500 6986, 1]
```

Odwrotność modulo n

```
? Mod(160,841)^(-1)
%6 = Mod(205, 841)
? lift(Mod(160,841)^(-1))
%7 = 205

? Mod(8765392,29876342114321231 23)^(-1)
%8 = Mod(19692148552871161 37,29876342114321231 23)
? 29876342114321231 23-101841935614500 6986
%9 = 19692148552871161 37
```

Małe twierdzenie Fermata

```
? isprime(1231)
%10 = 1
? gcd(1231,5871)
%11 = 1
? Mod(5871^1230, 1231)
%12 = Mod(1, 1231)
? Mod(5871,1231)^1230
%13 = Mod(1, 1231)

? Mod(40547201659, 85115991299)^85115991298
%14 = Mod(1, 85115991299)
? Mod(461730729350412, 2461654953439061)^2461654953439060
%15 = Mod(1, 2461654953439061)
```

Chińskie twierdzenie o resztach

```
? a=Mod(1,11)
%16 = Mod(1, 11)
? b=Mod(2,12)
%17 = Mod(2, 12)
? c=Mod(3,13)
%18 = Mod(3, 13)
? d=chinese(a,b)
%19 = Mod(122, 132)
? chinese(c,d)
%20 = Mod(1706, 1716)
```

Funkcja Eulera

```
? eulerphi(841)
%21 = 812
? factorint(841)
%22 =
[29 2]
? eulerphi(1231)
%23 = 1230
? isprime(1231)
%24 = 1
? eulerphi(1000)
%25 = 400
? eulerphi(1200)
%26 = 320
```

Potęgowanie modulo n

```
? lift(Mod(7,1234)^698)
%27 = 287
? Mod(461730729350412,2461654953439061)^2461654953439060
%28 = Mod(1, 2461654953439061)
```

Liczby pierwsze

```
? primes(10)
%31 = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29]
? prime(1000)
%32 = 7919
? nextprime(10^30)
%34 = 1000000000000000000000000057
? nextprime(random(10^30))
%35 = 42517003983368073383237536681
? isprime(%35)
%36 = 1
```

Symbol Jacobiego

```
? kronecker(91,167)
%37 = -1
? kronecker(7,167)
%38 = 1
? for(a=1,167,if(Mod(a,167)^2==7,print1(a, " ")))
72 95
? kronecker(13,167)
%39 = -1
? kronecker(6,7)
%40 = -1
? kronecker(11,13)
%41 = -1


? kronecker(12987616654165515 51,97869853217651987616651 1871)
%42 = 1
```

Logarytm dyskretny

```
? znprimroot(19)
%43 = Mod(2, 19)
? znorder(Mod(2,19))
%44 = 18
? znlog(13,Mod(2,19))
%45 = 5
? znlog(15,Mod(2,19))
%46 = 11


? znprimroot(966099377)
%47 = Mod(3, 966099377)
? znlog(124332,Mod(3, 966099377)
%48 = 120589994
? Mod(3, 966099377)^120589994
%49 = Mod(124332, 966099377)
```

RSA

```
? p=1123;q=1237;n=p*q
%50 = 1389151
? phin=eulerphi(n)
%51 = 1386792
? e=834781
%52 = 834781
? gcd(e,phin)
%53 = 1
? d=lift(Mod(e,phin)^(-1))
%54 = 1087477
? m=983415
%55 = 983415
? c=lift(Mod(m,n)^e)
%56 = 190498
? lift(Mod(c,n)^d)
```

```
%57 = 983415


? p=nextprime(random(10^25))
%60 = 6394410543977819029567513
? q=nextprime(random(10^24))
%61 = 574229193973116022705411
? n=p*q
%62 = 3671857212601577387349834975533584930459534912843
? phin=(p-1)*(q-1)
%63 = 3671857212601577387349828006893846979524482639920
? e=random(10^10)
%64 = 6534579775
? while(gcd(e,phin)!=1,e=e+1)
? e
%65 = 6534579779
? d=lift(Mod(e,phin)^(-1))
%66 = 106908650074747896134819660084538539534981162219
```

```
? m=random(10^30)
%67 = 446763233106745131823069978264
? c=lift(Mod(m,n)^e)
%68 = 366071378740244632828540738063744965348554865640 0
? lift(Mod(c,n)^d)
%69 = 446763233106745131823069978264
```