Dr inż. Robert Wójcik, p. 313, C-3, tel. 320-27-40

Katedra Informatyki Technicznej (K30W04ND03)
Wydział Informatyki i Telekomunikacji (W04N)
Politechnika Wrocławska

E-mail: **robert.wojcik@pwr.edu.pl**
Strona internetowa: google: Wójcik Robert

Ochrona danych

Wykład 3.

3. Matematyczne podstawy kryptografii

3.1. Podzielność liczb, własności, twierdzenia

3.2. Algorytm Euklidesa i rozszerzony algorytm Euklidesa

3.3. Arytmetyka modularna i kongruencje

3.4. Obliczanie odwrotności modularnej

3.5. Chińskie twierdzenie o resztach

3.6. Małe twierdzenie Fermata

3.7. Funkcja Eulera i twierdzenie Eulera

3.8. Testy pierwszości

3.9. Reszty i pierwiastki kwadratowe

3.10. Logarytm dyskretny

Zródła:

Mochnacki W., Kody korekcyjne i kryptografia, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2000.

Wykład z kryptografii: http://zon8.physd.amu.edu.pl/˜tanas

Podzielność liczb

- 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 p, to liczba większa od 1, nie posiadająca innych dzielników dodatnich niż 1 i p.

- Liczba, która ma co najmniej jeden nietrywialny dzielnik jest liczbą złożoną.

Rozkład na czynniki pierwsze

Każda liczba naturalna n może być przedstawiona jednoznacznie (z dokładnością do kolejności czynników), jako iloczyn potęg liczb pierwszych, np. $24 = 8 * 3 = 2^3 * 3^1$.

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(24, 18) = 6

Najmniejsza wspólna wielokrotność — NWW(a, b)

Najmniejsza wspólna wielokrotność, NWW(a, b), to najmniejsza dodatnia liczba całkowita, którą dzielą a i b. Zachodzi:
$NWW(a, b) = a \cdot b / NWD(a, b)$.
Przykład: $NWW(24, 18) = 24 \cdot 18 / NWD(24, 18) = 72$.

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(3, 11) = 1, zatem liczby 3 i 11 są względnie pierwsze.

Własności relacji podzielności

1. Jeśli a|b i c jest dowolną liczbą całkowitą, to a|bc.
2. Jeśli a|b i b|c, to a|c
3. Jeśli a|b i a|c, to a|b ± c
4. Jeśli liczba pierwsza p dzieli ab, to p|a lub p|b
5. Jeśli m|a i n|a oraz m i n nie mają wspólnych dzielników większych od 1, to mn|a.

Algorytm Euklidesa

Algorytm Euklidesa pozwala znaleźć NWD(a,b) w czasie wielomianowym.

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, tj. $b = q_2 r_1 + r_2$.

Postępowanie to kontynuujemy dzieląc kolejne reszty, $r_{i-2} = q_i r_{i-1} + r_i$, aż do momentu, gdy otrzymamy resztę, która dzieli poprzednią resztę.

Ostatnia niezerowa reszta jest równa NWD(a, b).

Przykład. NWD(26,7) = 1, gdyż:

26 = 3*7 + 5,
7 = 1*5 + 2,
5 = 2*2 + 1,
2 = 2*1.

Rozszerzony algorytm Euklidesa

Jeśli d = NWD(a,b), to NWD można przedstawić w postaci kombinacji liniowej liczb a i b ze współczynnikami całkowitymi, to jest d = u a + v b, gdzie u, v – liczby całkowite. Przy czym liczby u, v można znaleźć w czasie wielomianowym.

Korzystając z ciągu równości w algorytmie Euklidesa (idąc w przeciwną stronę) otrzymujemy z rozszerzonego algorytmu

NWD (a,b) = NWD(26,7) = 1 = 5 – 2*2 = 5 – 2*(7 – 1*5) =
(5 + 2*5) – 2*7 = 3*5 – 2*7 = 3*(26 – 3*7) – 2*7 = 3*26 – 11*7.

Ostatecznie: 1 = 3*26 – 11*7, stąd wynika u = 3 oraz v= -11.

Arytmetyka modularna i kongruencje

Dla danych trzech liczb całkowitych a, b i m mówimy, że liczba a przystaje do liczby b modulo m i piszemy a ≡ b (mod m), gdy różnica a − b jest podzielna przez m.

Liczbę m nazywamy modułem kongruencji.

Własności:

1. a ≡ a (mod m);
2. a ≡ b (mod m) wtedy i tylko wtedy, gdy b ≡ a (mod m);
3. Jeśli a ≡ b (mod m) oraz b ≡ c (mod m), to a ≡ c (mod m);

Kongruencje względem tego samego modułu można dodawać, odejmować i mnożyć stronami.

4. Jeśli a ≡ b (mod m) i c ≡ d (mod m),
   to a ± c ≡ b ± d (mod m) oraz ac ≡ bd (mod m);

5. Jeśli a ≡ b (mod m), to a ≡ b (mod d) dla każdego dzielnika d|m;

6. Jeśli a ≡ b (mod m), a ≡ b (mod n), oraz m i n są względnie
   pierwsze, to a ≡ b (mod mn);

Redukcja modularna

Prowadząc obliczenia w arytmetyce modularnej, możemy redukować pośrednie wyniki obliczeń *mod m*, a wynik będzie taki sam jak po redukcji wyniku końcowego.

Jest to szczególnie przydatne, gdy obliczamy potęgi modularne:

$c = m^e \bmod n$.

Podczas obliczeń, po każdym wymnożeniu m * m możemy redukować wynik modulo n, tj.

$c = m^e \bmod n = (\ldots ((m) \bmod n) * m) \bmod n) \ \ldots * m) \bmod n.$

Jeśli reszty zaczną się powtarzać możemy zakończyć obliczenia i wyznaczyć wartość końcową analizując okres reszt.

Np. $2^{17} \bmod 7 =$

$2^1 \bmod 7 = (2) \bmod 7 = 2$
$2^2 \bmod 7 = (2 * 2) \bmod 7 = 4$
$2^3 \bmod 7 = (4 * 2) \bmod 7 = 1$

$2^4 \bmod 7 = (1 * 2) \bmod 7 = 2$ (okres reszt = +3)

$2^7 \bmod 7 = 2$

$2^{10} \bmod 7 = 2$

$2^{13} \bmod 7 = 2$

$2^{16} \bmod 7 = 2$

Ostatecznie: $2^{17} \bmod 7 = 4$.

Kongruencji nie można dzielić stronami. Ale elementy kongruencji można dzielić przez wspólny podzielnik. Dla wszystkich liczb całkowitych a, b i każdej liczby naturalnej m:

jeśli $a \equiv b \pmod m$ i a, b, m mają wspólny podzielnik k, to

$a / k \equiv b / k \pmod{m / k}$

7. Dla ustalonej liczby m, każda liczba całkowita przystaje modulo m do jednej liczby zawartej pomiędzy 0 i m−1.

Np. $7 \equiv 1 \pmod 3$, $7 \equiv -2 \pmod 3$, $6 \equiv 0 \pmod 3$.

Obliczanie odwrotności modularnej

Liczbami a, dla których istnieje liczba u taka, że $a*u \equiv 1 \pmod m$, są dokładnie te liczby a, dla których NWD(a,m) = 1.

Taka liczba odwrotna $u = a^{-1}$ może być znaleziona w czasie wielomianowym z równania: $a*u = v*m + 1$.

Niech a = 26; m = 7, wówczas kongruencja:

$26 *u \equiv 1 \pmod 7$,

ma nieskończenie wiele rozwiązań, gdyż $u = u + k*7 \pmod 7$,
k – liczba całkowita.

Dla celów kryptograficznych potrzebny jest pierwiastek, będący najmniejszą liczbą dodatnią.

Np. NWD(26, 7) = 1 (patrz poprzedni przykład), to istnieje liczba odwrotna $u = 26^{-1} \pmod 7$. Liczbę tę można obliczyć za pomocą rozszerzonego algorytmu Euklidesa. Ponieważ $1 = 3*26 – 11*7$, to

$a*u = 26*3 = 11*7 + 1 = v*m + 1$.

Tak, wiec $u = 3 = a^{-1}$.

Chińskie twierdzenie o resztach

Niech x będzie dowolną liczbą naturalną lub zerem. Dla m naturalnego przez x mod m oznaczamy resztę z dzielenia x przez m.

Zbiór reszt modulo m, czyli {0, 1, …, m-1} oznaczamy Z_m.

Niech liczby

$m_1, m_2, \ldots, m_s$ będą parami względnie pierwsze, tj. $NWD(m_i,m_j)=1$,

liczby $a_1, a_2, \ldots, a_s$, będą dowolnymi liczbami takimi, że $a_i < m_i$.

Wtedy istnieje dokładnie jedna liczba $x < m$, gdzie

$m = m_1 * m_2 * \ldots * m_s$, taka, że dla każdego $i <= s$ zachodzi

$x = a_i \pmod{m_i}$, tj. $x \bmod m_i = a_i$.

Inaczej mówiąc, układ równań

$x = a_1 \pmod{m_1}$,

$x = a_2 \pmod{m_2}$,
…
$x = a_i \pmod{m_i}$,
…
$x = a_s \pmod{m_s}$,

ma wspólne, jednoznaczne rozwiązanie $x < m$, gdzie

$m = m_1 * m_2 * \ldots * m_s$.

Z twierdzenia wynika, że wybierając dowolne $a_i < m_i$ dla $i <= s$ wyznaczamy jednoznacznie liczbę $x \in Z_m$, taką, że $x = a_i \pmod{m_i}$, dla $i <= s$.

Np. $m_1 = 2$; $m_2 = 3$; $m_3 = 5$;

$m = 2*3*5 = 30$;

$a_1 = 1$; $a_2 = 2$; $a_3 = 3$.

Układ równań:

$x = 1 \pmod 2$;
$x = 2 \pmod 3$;
$x = 3 \pmod 5$;

ma dokładnie jedno rozwiązanie x = 23 należące do zbioru
Z_{30} = { 0, 1, …, 29 }.

Małe twierdzenie Fermata

Niech p będzie liczbą pierwszą. Wtedy każda liczba całkowita a spełnia kongruencję

$a^p \equiv a \pmod p$

i każda liczba całkowita a niepodzielna przez p spełnia kongruencję

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

np.
a = 4; p = 2; wariant, gdy a podzielne przez p;

$4^1 \neq 1 \pmod 2$; nie jest spełnione $a^{p-1} \equiv 1 \pmod p$;
$4^2 \equiv 4 \pmod 2$; spełnione $a^p \equiv a \pmod p$;

a = 4; p = 3; wariant, gdy a niepodzielne przez p;

$4^2 \equiv 1 \pmod 3$; spełnione $a^{p-1} \equiv 1 \pmod p$;
$4^3 \equiv 4 \pmod 3$; spełnione $a^p \equiv a \pmod p$;

Funkcja Eulera i twierdzenie Eulera

Dla n ≥ 1, niech φ(n) będzie liczbą tych nieujemnych liczb a mniejszych od n, tj. a $\in$ { 1, 2, ..., n-1}, które są względnie pierwsze z n.

Funkcja φ(n) nazywa się funkcją Eulera.

Funkcja Eulera φ jest „multiplikatywna”, tzn. φ(mn) = φ(m)φ(n), jeśli tylko NWD(m, n) = 1.

Np. φ(8) = 4, gdyż w zbiorze liczb mniejszych od 8 tylko 1, 3, 5, 7 są względnie pierwsze z 8; podobnie φ(7) = 6, gdyż w zbiorze liczb mniejszych od 7 wszystkie liczby są względnie pierwsze z 7.

Generalnie dla liczby pierwszej p jest zawsze φ(p) = p-1.

Np. dla liczb m=8 i n=3, zachodzi NWD(8,3) = 1. Wówczas,

φ(mn) = φ(8*3) = φ(8)φ(3) = 4 * 2 = 8 = φ(24),

1, 5, 7, 11, 13, 17, 19, 23 – liczby względnie pierwsze z x = 24.

Aby znaleźć wartość funkcji Eulera liczby złożonej *n*, rozkładamy ją na iloczyn potęg liczb pierwszych.

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_m^{e_m}$$

Wartość funkcji Eulera dla takiej liczby złożonej wylicza się ze wzoru:

$$\varphi(n) = \prod_{i=1}^{m} p_i^{e_i - 1}(p_i - 1).$$

Obliczenie funkcji Eulera liczby złożonej:

$n = 2646 = 2 \cdot 3^3 \cdot 7^2$, $\varphi(2646) = 1 \cdot 3^2 \cdot 2 \cdot 7 \cdot 6 = 756$.

Funkcję $\varphi(n)$ wykorzystuje się w uogólnieniu Eulera małego twierdzenia Fermata. Jeśli *a* i *n* są względnie pierwsze, to

$$a^{\varphi(n)} \pmod{n} \equiv 1.$$

Funkcja Eulera służy również do obliczania liczb odwrotnych modulo *n*.

Liczbę odwrotną do *a* modulo *n* oznaczamy przez a^{-1}. Liczby te spełniają zależność $a\,a^{-1} \pmod{n} \equiv 1.$

Jeśli *a* i *n* są względnie pierwsze, to liczba odwrotna a^{-1} wynosi

$$a^{-1} \equiv a^{\varphi(n)-1} \pmod{n}.$$

Na przykład, jeśli $a = 4$ i $n = 11$, to $4^{-1} = 4^9 \bmod 11 = 3$.

Testy pierwszości

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

Test Fermata

Testujemy, czy liczba p jest pierwsza. Wybieramy losowo liczbę
$a < p - 1$. Wówczas, na pewno a nie dzieli się przez p.

Obliczamy $r = a^{p-1} \pmod p$, jeśli $r \neq 1$, to p jest liczbą złożoną.

Test przeprowadzamy t-krotnie, $t \geq 1$. Jeśli wszystkie testy wypadną pomyślnie, tzn. dla każdego przypadku jest $r = 1$, to liczbę uznajemy za pierwszą, choć może tak nie być.

Test Millera-Rabina

Testujemy, czy liczba n jest pierwsza.

Zapisujemy $n-1 = 2^s r$, gdzie r jest nieparzyste.

Wybieramy losowo liczbę całkowitą a, z przedziału $1 < a < n - 1$.

Obliczamy $b = a^*r \pmod n$. Jeśli $b \equiv \pm 1 \pmod n$, to uznajemy,
że n jest pierwsza.

W przeciwnym przypadku obliczamy $a^{k*r} \pmod n$, gdzie $k = 2^j$
(k = 2 do potęgi j) dla kolejnych j z przedziału $0 < j < s$.

Jeśli dla pewnego $j < s$ otrzymamy $a^{k*r} \equiv -1 \pmod n$, to uznajemy, że liczba n jest pierwsza.

W przeciwnym przypadku liczba n jest złożona.

Test przeprowadzamy t-krotnie losując różne a.

Np. $n=17$; $n - 1 = 16 = 2^4*1 = 2^s * r$; $s = 4$; $r = 1$;

Niech $a = 3$, będzie losową liczbą z przedziału $1 < 3 < 16$.

Obliczamy $b = a * r \pmod n = 3 * 1 \pmod{17} = 3$.

Liczba b = 3 nie przystaje do ±1 (mod 17).

Wybieramy kolejno j z przedziału $0 < j < 4=s$.

Są to wartości: j=1; j=2; j=3.

Dla j=1 jest k = 2, oraz k*r = 2; stąd $a^{k*r} = 3^2 \equiv 9 \pmod{17}$;
Dla j=2 jest k = 4, oraz k*r = 4; stąd $a^{k*r} = 3^4 \equiv 5 \pmod{17}$;
Dla j=3 jest k = 8, oraz k*r = 8; stąd $a^{k*r} = 3^8 \equiv 16 \equiv -1 \pmod{17}$.

Tak, więc spełniony jest warunek pierwszości liczby n = 17.

Reszty i pierwiastki kwadratowe mod n

Niech dany będzie zbiór reszt $Z_n = \{0, 1, \ldots, n-1\}$.

Mówimy, że liczba całkowita y jest **resztą kwadratową** modulo n,
jeśli istnieje taka liczba całkowita x, że $x^2 = y \pmod{n}$.

W takim przypadku mówimy też, że x jest
pierwiastkiem kwadratowym z y modulo n.

Jeżeli y nie jest resztą kwadratową według modułu n, to y nazywamy niereszta kwadratową.

Reszty kwadratowe są zatem liczbami, dla których istnieją pierwiastki stopnia 2 względem kongruencji modulo n.

W szczególności liczby y=0 i y=1 są resztami kwadratowymi dla dowolnego n naturalnego, gdyż

$0^2 = 0 \bmod n$; x = 0 - pierwiastek kwadratowy modulo n;

$1^2 = 1 \bmod n$; x = 1 - pierwiastek kwadratowy modulo n;

Ponieważ dowolna liczba całkowita x daje mod n jedną z reszt należących do zbioru $Z_n = \{0, 1, \ldots, n-1\}$ wystarczy analizować reszty kwadratowe dla elementów x należących do zbioru reszt Z_n.

Dla elementów x ze zbioru Z_7 = {0, 1, 2, 3, 4, 5, 6 } obliczmy reszty kwadratowe $y = x^2 \pmod 7$:

x=0; $y = 0^2 \pmod 7 = 0$;
x=1; $y = 1^2 \pmod 7 = 1$;
x=2; $y = 2^2 \pmod 7 = 4$;
x=3; $y = 3^2 \pmod 7 = 2$;
x=4; $y = 4^2 \pmod 7 = 2$;
x=5; $y = 5^2 \pmod 7 = 4$;
x=6; $y = 6^2 \pmod 7 = 1$;

Resztami kwadratowymi w Z_7 = { 0, 1, 2, 3, 4, 5, 6 } są liczby {0, 1, 2, 4}, natomiast pozostałe liczby {3, 5, 6} są nieresztami.

Natomiast:

x = 0; - pierwiastek z 0 mod 7;

x=1, x=6 – pierwiastki z 1 modulo 7;

x=2, x=5 – pierwiastki z 4 modulo 7;

x=3, x=4 – pierwiastki z 2 modulo 7.

Niech Z(n) oznacza podzbiór tych niezerowych elementów zbioru reszt Z_n = {0, 1, ..., n-1}, które są względnie pierwsze z n, np. Z(5) = {1, 2, 3, 4}

Liczba elementów zbioru Z(n) jest równa wartości funkcji Eulera φ(n),
np. dla n=5, φ(5)=4.

Prawdziwa jest następująca własność.

Jeśli n = pq jest iloczynem dwóch dużych, różnych liczb pierwszych, to znajdowanie pierwiastków kwadratowych w zbiorze Z(n) należy do problemów trudnych obliczeniowo.

Trudność ta jest równoważna trudności problemu faktoryzacji liczby n: faktoryzując n znajdujemy liczby pierwsze p i q, następnie znajdujemy pierwiastki kwadratowe w Z(p) oraz Z(q), a z kolei korzystając z chińskiego twierdzenia o resztach znajdujemy pierwiastki w Z(n).

Logarytm dyskretny

Niech p będzie liczbą pierwszą, natomiast Zp* oznacza zbiór liczb {1,...,p−1} i niech g będzie generatorem Zp*, tzn. takim elementem, że dla każdej liczby $x \in Zp^*$ istnieje takie $i \in Zp^*$, że

$x \equiv g^i \pmod p$ (wszystkie elementy mogą być wygenerowane z g).

Problem logarytmu dyskretnego polega na znalezieniu dla danej liczby b, gdzie 0 < b < p oraz znanego g, takiej liczby całkowitej i, że

$g^i \equiv b \pmod p$.

Np. Niech p=11, czyli zbiór $Z_{11^*} = \{1, 2, ..., 10\}$, oraz g = 2.

Niech $b = 2^i \bmod 11$, dla kolejnych i należących do zbioru {1, 2, ..., 10} mamy:

i =1; $b = 2^1 \bmod 11 = 2$;
i =2; $b = 2^2 \bmod 11 = 4$;
i =3; $b = 2^3 \bmod 11 = 8$;
i =4; $b = 2^4 \bmod 11 = 5$;
i =5; $b = 2^5 \bmod 11 = 10$;
i =6; $b = 2^6 \bmod 11 = 9$;
i =7; $b = 2^7 \bmod 11 = 7$;
i =8; $b = 2^8 \bmod 11 = 3$;
i =9; $b = 2^9 \bmod 11 = 6$;
i =10; $b = 2^{10} \bmod 11 = 1$;

i =11; $b = 2^{11} \bmod 11 = 2$; istnieje wiele rozwiązań całkowitych.

Stąd, np. $\log_2 10 = 5$, bo $2^5 = 10 \pmod{11}$.

Inne rozwiązania t = 5 + m*(p-1), gdzie p = 11, m – liczba całkowita.

Problem znajdowania logarytmu dyskretnego jest problemem trudnym obliczeniowo (nie jest wielomianowy względem bitów wejścia, np. gdy liczba b jest k-bitowa i jednocześnie $b < 2^k$, to liczba wszystkich możliwych przypadków – wartości (i) może wynieść 2^k; np. dla b <= 10, jest k < 3.5 – sprawdzamy maksymalnie 10 przypadków, tak jak to jest w rozpatrywanym przykładzie, dla p=11 i b=10).