SYSTEMY RESZTOWE

Kongruencje i ich właściwości

Kongruencja, czyli relacja przystawania liczb jest *zwrotna, symetryczna i przechodnia*

$$N \equiv M \bmod w \Leftrightarrow N - M = kw,\ w \in \mathbf{N},\ k \in \mathbf{Z}$$

Liczby *wzajemnie/względnie pierwsze* (ang. *relatively prime*): $NWD(X, Y) = 1$.

Kongruencje są *zachowawcze* (ang. *indifferent*) względem dodawania i mnożenia.

Klasa kongruencji to zbiór przystających liczb całkowitych (naturalnych).

LEMAT:
Jeżeli reszty z dzielenia liczby przez moduły względnie pierwsze są sobie równe, to są one równe reszcie z dzielenia przez iloczyn tych modułów

$$(w_1, w_2) = 1 \;\&\; X \bmod w_1 = X \bmod w_2 = q \Rightarrow X \bmod (w_1 w_2) = q\,.$$

DOWÓD: Jeśli $X \bmod w_1 = q$ i $X \bmod w_2 = q$, to $(X-q) \bmod w_1 = 0$ i $(X-q) \bmod w_2 = 0$.
Zatem $X-q = k_1 w_1$ i $X-q = k_2 w_2$, więc $X-q = k\, w_1 w_2$ oraz $X \bmod w_1 w_2 = q$ ❒

LEMAT: Kongruencje można dzielić obustronnie przez wspólny czynnik:

$$(aX) \bmod (aw) = a(X \bmod w)$$

DOWÓD: $(aX) \bmod (aw) = aX - aw\lfloor aX/aw \rfloor = a(X - w\lfloor X/w \rfloor) = a(X \bmod w)$ ❒

Algorytm Euklidesa

Największy wspólny (po)dzielnik NWD (ang. *greatest common divisor, GCD*)

$$NWD(X,Y) = p \in \mathbf{N} \Leftrightarrow (p \mid X \wedge p \mid Y) \wedge \neg\exists p < q \in \mathbf{N} : q \mid X \wedge q \mid Y$$

Najmniejsza wspólna wielokrotność NWW(ang. *least common multiply, LCM*)

$$NWW(x_1, x_2, ..., x_m) = w \in \mathbf{N} \Leftrightarrow \forall i : x_i \mid w \wedge \neg\exists w > z \in \mathbf{N} : x_i \mid z$$

TWIERDZENIE:

1. Dla dowolnych liczb naturalnych n i m: $NWD(n,m) = NWD(m, n \bmod m)$.
2. Istnieją l. całkowite u, v takie, że $NWD(n,m) = un + vm$ (kombinacja liniowa m n).

DOWÓD:

Jeśli $p = NWD(n,m)$, to $m = k_m p$, $n = k_n p$ oraz $NWD(k_n, k_m) = 1$.

1. Z algorytmu dzielenia mamy $n \bmod m = n - m \cdot n \operatorname{int} m = k_n p - k_m p \cdot (k_n \operatorname{int} k_m) = k_{m,n} p$.

gdzie $NWD(k_{m,n}, k_m) = 1$, bo $NWD(k_n, k_m) = 1$, więc

$$NWD(n,m) = NWD(m, n \bmod m)$$

2. Ponieważ $NWD(k_n, k_m) = 1$, więc każda liczba $u k_n$ dla u=1, 2, …, k_m–1 należy do innej klasy kongruencji modulo k_m–. Istnieje więc takie u, że $uk_n = sk_m + 1$.

Stąd wynika, że $uk_n p = sk_m p + p$, czyli $un + vm = p = NWD(n,m)$, gdzie v=–s. ❐

Odwrotny algorytm Euklidesa

Z twierdzenia Euklidesa wynika rekurencyjna zależność kolejnych reszt:

$$r_{i+1} = r_{i-1} \bmod r_i = r_{i-1} - q_{i+1} r_i$$

gdzie $q_{i+1} = r_{i-1} \operatorname{int} r_i$ – iloraz całkowity, $r_{-1} = n,\ r_0 = m$.
Każda reszta jest więc liniową kombinacją 2 reszt poprzednich, a w konsekwencji:

$$NWD(n,m) = B_i r_{i-1} + A_i r_i$$

Współczynniki skalujące są również powiązane rekurencyjnie:

$$B_i r_{i-1} + A_i r_i = B_i r_{i-1} + A_i (r_{i-2} - q_i r_{i-1}) = A_i r_{i-2} + (B_i - q_i A_i) r_{i-1}$$

skąd widać, że $A_i = B_{i-1}$ i $A_{i-1} = B_i - A_i q_i$, więc $B_{i-2} = B_i - B_{i-1} q_i$ albo $A_{i-1} = A_{i+1} - A_i q_i$

Biorąc $B_i = A_{i+1}$ i $r_{k+1} = 0$, mamy $rk = NWD(n,m) = r_{k-2} - q_k r_{k-1} = A_k r_{k-2} + A_{k-1} r_{k-1}$,
a więc wartości początkowe współczynników (*i*=*k*) to $A_k = 1$ i $A_{k-1} = -q_k$.

Równanie diofantyczne $NWD(n,m) = un + vm$ ma przy tym postać:

$$NWD(n,m) = A_1 r_{-1} + A_0 r_0 = A_1 n + A_0 m$$

WNIOSEK:
Jeśli $NWD(n,m)$=1, to $A_1 = n^{-1} \bmod m$ oraz $A_0 = m^{-1} \bmod n$

Małe twierdzenie Fermata

TWIERDZENIE

Niech p będzie liczbą pierwszą. Jeśli p nie jest podzielnikiem liczby a, to wtedy $a^{p-1} \equiv 1 \pmod{p}$ zaś dla dowolnego a zachodzi $a^p \equiv a \pmod{p}$.

DOWÓD.

Skoro p nie dzieli a, to $\forall 1 \leq i \neq j \leq p-1$: $i \cdot a \neq j \cdot a \bmod p$, więc każda liczba ciągu $1 \cdot a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a$ należy do innej klasy resztowej $\mathbb{Z}_{p:r}$, $r = 1, 2, \ldots, p-1$.

A zatem $[(1 \cdot a)(2 \cdot a)(3 \cdot a)\ldots((p-1) \cdot a)] \bmod p = (p-1)! \bmod p$, czyli

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Ponieważ $NWD(p, a) = 1$, więc $NWD(p, (a^{p-1} - 1) \cdot (p-1)!) = p$, (bowiem $(p-1)!$ nie dzieli się przez p). Stąd wynika, że

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

i ponieważ p nie dzieli a, więc $a \cdot a^{p-1} \equiv a \pmod{p}$, a zatem

$$a^p \equiv a \pmod{p}$$

Jeśli $NWD(p, a) = p$, to ostatnia zależność jest trywialna ($a \bmod p = 0$) ❒

Funkcja Eulera $\varphi(N)$ (totient)

… co druga naturalna jest podzielna przez 2, co trzecia z pozostałych dzieli się przez 3, co piąta z niepodzielnych przez 2 lub 3 dzieli się przez 5, etc.

TWIERDZENIE

Liczb naturalnych mniejszych od $N = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$, $p_i \in \mathbb{P}$ i względnie pierwszych z tą liczbą (ang. *totatives*) jest

$$\varphi(N) = \prod_{i=1}^{i=m} (p_i - 1) p_i^{e_i - 1}, \quad p_i \in \mathbb{P}$$

DOWÓD:

Jeśli p_i jest podzielnikiem N, to w zbiorze $\{1,2,\ldots,N\}$ jest $N{-}N(p_i)^{-1}$ liczb niepodzielnych przez p_i. $[N{-}N(p_i)^{-1}]{-}[N{-}N(p_i)^{-1}]\ (p_j)^{-1}= N\ (1{-}(p_i)^{-1})(1{-}(p_j)^{-1})$ spośród nich nie jest podzielnych przez p_j. (co p_j-ta spośród N i spośród $|p_i$)

Jeśli więc p_i i=1,2,…,m są liczbami pierwszymi, to w zbiorze $\{1,2,\ldots,N\}$ jest $p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m} (1 - p_1^{-1})(1 - p_2^{-1}) \ldots (1 - p_m^{-1}) = p_1^{e_1 - 1} p_2^{e_2 - 1} \ldots p_m^{e_m - 1} (p_1 - 1)(p_2 - 1) \ldots (p_m - 1)$ liczb niepodzielnych przez żadną z nich. ❒

WNIOSEK: Jeśli $NWD(N,M)$=1, to $\varphi(MN) = \varphi(M)\,\varphi(N)$.

$\varphi(N)$ nazywa się *funkcją „fi" Eulera* lub totientem (ang. *Euler's totient function*)

Twierdzenie Eulera

TWIERDZENIE

Jeśli $\varphi(N)$ jest liczbą liczb mniejszych od N i względnie pierwszych z N, to

$$a^{\varphi(N)} \bmod N = 1$$

DOWÓD.

Dla $N=p$ twierdzenie jest prawdziwe, $\varphi(p)=p-1$. Załóżmy, że jest prawdziwe dla $N=p^m$, czyli $a^{p^{m-1}(p-1)} \equiv 1 \bmod p^m$. Stąd wynika, że $a^{p^{m-1}(p-1)} = 1 + kp^m$ oraz $a^{p^m(p-1)} = (1+kp^m)^p = 1 + Kpp^m$, zatem $a^{p^m(p-1)} \equiv 1 \bmod p^{m+1}$. Twierdzenie jest więc prawdziwe dla $N=p^\alpha$, czyli $a^{\varphi(p^m)} \bmod p^m = 1$

Jeśli więc $N = p^a q^b \ldots t^h$, to $a^{\varphi(p^a q^b \ldots t^h)} \bmod p^a = (a^{\varphi(p^a)})^{\varphi(q^b \ldots t^h)} \bmod p^a = 1$ oraz $a^{\varphi(p^a q^b \ldots t^h)} \bmod q^b = (a^{\varphi(q^b)})^{\varphi(p^a \ldots t^h)} \bmod q^b = 1$ itd. Stąd wynika teza twierdzenia:

$a^{\varphi(p^a q^b \ldots w^h)} \bmod (p^a q^b \ldots w^h) = 1$, czyli $a^{\varphi(N)} \bmod N = 1$ ❐

WNIOSKI:

1. Odwrotność można obliczyć przez potęgowanie, bo $a^{\varphi(N)-1} \equiv a^{-1} (\bmod N)$
2. Może istnieć potęga $r<\varphi(N)$ taka, że $a^r \bmod N=1$ ($\varphi(N>2)$ jest parzyste).

Twierdzenie Carmichaela

Najmniejszą potęgę taką, że $a^r \bmod N=1$ nazywa się *rzędem* liczby a modulo N.

TWIERDZENIE (CARMICHAELA)

Maksymalny rząd modulo N elementu a takiego, że $NWD(a,N)=1$, wynosi:

$$\lambda(N)=\lambda(p_1^{e_1}p_2^{e_2}...p_m^{e_m})=NWW(\lambda(p_1^{e_1}),\lambda(p_2^{e_2}),...,\lambda(p_m^{e_m}))\le\varphi(N)$$

gdzie: $\lambda(p)=\varphi(p)=p-1$, $\lambda(p^m)=\varphi(p^m)$ dla $p\geq 3$, $\lambda(2^q)=\varphi(2^{q-1})$ dla $q\geq 3$, $\lambda(4)=2$.

DOWÓD.

Gdy $N=2^m$, to a musi być nieparzyste, $a=2i+1$. Ale $(2i+1)^2=4i(i+1)+1$ a iloczyn $i(i+1)$ jest parzysty, więc $(2i+1)^2 \bmod 2^3=1$, czyli $\lambda(2^3)=2=\varphi(2^{3-1})$. Niech teraz $a^{\lambda(2^q)} \bmod 2^q=1$. Wtedy $a^{\lambda(2^q)}-1=s2^q$, $a^{\lambda(2^q)}+1=s2^q+2$ i $a^{2\lambda(2^q)}-1=ts2^{q+1}$, więc $a^{\lambda(2^{q+1})} \bmod 2^{q+1}=1$, a zatem $\lambda(2^q)=\varphi(2^{q-1})$ dla $q\geq 3$.

A ponieważ dla każdego czynnika p^e rozkładu N liczba $\lambda(p^e)$ dzieli $\lambda(N)$, więc $a^{\lambda(p^e)} \bmod p^e=1$ pociąga za sobą $a^{\lambda(N)} \bmod p^e=1$, a zatem $a^{\lambda(N)} \bmod N=1$.

Dla $N>2$ liczba $\lambda(N)$ jest parzysta i jeśli $a^{\lambda(N)/2}$ jest *nietrywialnym pierwiastkiem kwadratowym* $a^{\lambda(N)} \bmod N$ z jedności, to $\lambda(N)$ jest rzędem elementu a modulo N. W przeciwnym razie $a^{\lambda(N)/2} \bmod N=\pm 1$. Ale $\lambda(N)/2$ może być parzysta, może też mieć podzielnik r taki, że $a^r \bmod N=\pm 1$. ❐

Twierdzenie Carmichaela – wnioski

WNIOSKI:

1. Jeśli odwrotność istnieje, można ją obliczyć przez potęgowanie:

$$a^{-1} \bmod N = a^{\lambda(N)-1} \bmod N.$$

2. W obliczaniu reszt potęgę można redukować modulo $\varphi(p)$ lub $\lambda(p)$:

$$a^x \bmod N = (a^{\lambda(N)})^{[x \operatorname{int} \lambda(N)]} a^{x \bmod \lambda(N)} \bmod N = a^{x \bmod \lambda(N)} \bmod N.$$

Jeśli znana jest binarna reprezentacja $\{\ldots, x_i, x_{i-1}, \ldots, x_1, x_0\}$ liczby naturalnej x, to w obliczeniu reszty potęgi możemy też wykorzystać równość:

$$a^{\sum x_i 2^i} \bmod N = [(a \bmod N)^{x_0}(a^2 \bmod N)^{x_1}(a^{2^2} \bmod N)^{x_2} \ldots] \bmod N$$

Przykład

Obliczmy $7^{32} \bmod 50$. Mamy $\varphi(50)=\varphi(2\cdot 5^2)=\lambda(50)=20$. Stąd wynika, że $7^{32} \equiv 7^{12} \bmod 50$ i $7^{12} \bmod 50 = 7^{4+8} \bmod 50 = 7^0\cdot(7^2)^0\cdot(7^4)^1\cdot(7^8)^1 \bmod 50$. Ale $7^2 \bmod 50 = -1$, więc $7^{12} \bmod 50 = 1$.

Obliczmy $5^{-1} \bmod 39$. Mamy $\varphi(39)=\varphi(13\cdot 3)$, $\lambda(39)=\mathrm{NWW}(2,12)=12$, więc $5^{-1} \equiv 5^{11} \bmod 39$. Jest też $5^2 \bmod 39 = 25$, $5^4 \bmod 39 = 1$, więc $5^{-1} \equiv 5^{11} \bmod 39 = 5\cdot 25\cdot 1 \bmod 39 = 8$.

Chińskie twierdzenie o resztach – system RNS

Niech $\mathbf{W}=\{w_1,w_2,\ldots,w_m\colon \forall i\neq j\colon NWD(w_i,w_j)=1\}$ *zaś* $W=\prod_{i=1}^{m} w_i$ *Reprezentacja*
$\mathbf{X}=\langle x_1,x_2,\ldots,x_m\colon x_i=X \bmod w_i,\ w_i\in\mathbf{W}\rangle$ każdej liczby $0\leq X<W$ *jest unikatowa.*

DOWÓD. Załóżmy, że $\exists 0\leq X,Y<W,\ Y\neq X\colon \forall 1\leq i\leq m\colon Y\equiv X \bmod w_i$. Zatem
$\forall 1\leq i\leq m\colon w_i \mid (Y-X)$, a ponieważ $W=NWW(w_1,w_2,\ldots,w_m)$, to $W\mid(Y-X)$.
Skoro jednak $Y\neq X$, to $Y-X\geq W$, co przeczy założeniu, więc $Y=X$ ❒

System resztowy $RNS(w_1,w_2,\ldots,w_m)$ (*Residue Number System*)

Reprezentacja $\mathbf{X}=\langle x_1 \bmod w_1, x_2 \bmod w_2,\ldots,x_m \bmod w_m\colon\ w_i\in\mathbf{W}\rangle$ w *bazie* $\mathbf{W}$

- $x_i\in\{0,1,\ldots,w_i-1\}$ dla kongruencji w zbiorze $\mathbb{N}$,
- $x_i\in\{-\lfloor w_i/2\rfloor,\ldots,-1,0,1,\ldots,\lfloor w_i/2-1\rfloor\}$ dla kongruencji w zbiorze $\mathbb{Z}$

WNIOSEK: W systemie $RNS(w_1,w_2,\ldots,w_m)$ mamy

$$[\,|\langle q,q,\ldots,q\rangle|\equiv|\langle q\pm w_1,q\pm w_2,\ldots,q\pm w_m\rangle|\equiv q\,] \bmod W,$$

więc $\langle q,q,\ldots,q\rangle$ jest reprezentacją liczby q lub $W-q$, gdy $|q|<w_i$.

Chińskie twierdzenie o resztach – konwersja odwrotna

CHIŃSKIE TWIERDZENIE O RESZTACH (CRT) (*SUN-TZU, III W., QIN JIUSHAO, 1247*)

Niech $\mathbf{W}=\{w_1,w_2,\ldots,w_n:\ \forall i\neq j:\ NWD(w_i,w_j)=1\}$, $W=w_1w_2\ldots w_n$. *Reprezentacja* $\langle x_1,x_2,\ldots,x_n:\ x_i=X \bmod w_i,\ w_i\in\mathbf{W}\rangle$ *każdej liczby* $0\leq X<W$ *jest unikatowa oraz*

$$X=|\mathbf{X}|=\left(\sum_{s=1}^{n}\hat{w}_s(\hat{w}_s^{-1} \bmod w_s)x_s\right) \bmod W$$

gdzie $\hat{w}_s=Ww_s^{-1}$, zaś $\hat{w}_s^{-1} \bmod w_s$ – *odwrotność* $\hat{w}_s$ *względem modułu* w_s.

DOWÓD (*nieformalny szkic dowodu konwersji odwrotnej*).
Ze względu na zachowawczość kongruencji wobec dodawania mamy

$$\langle x_1,x_2,\ldots,x_n\rangle=x_1\cdot\langle 1,0,\ldots,0,0\rangle+x_2\cdot\langle 0,1,\ldots,0,0\rangle+\ldots+x_n\cdot\langle 0,0,\ldots,0,1\rangle.$$

W systemie $RNS(w_1,w_2,\ldots,w_m)$ liczba p_s o reprezentacji $\langle 0,\ldots,0,1_s,0,\ldots,0\rangle$ jest podzielna przez każde w_i oprócz w_s, jest więc $p_s=k\cdot\hat{w}_s$ (liczby p_s istnieją, bo różnych reprezentacji jest dokładnie W). Ponieważ jej reszta względem w_s jest równa 1, więc $k=\hat{w}_s^{-1} \bmod w_s$ jest odwrotnością $\hat{w}_s$ oraz $p_s=\hat{w}_s(\hat{w}_s^{-1} \bmod w_s)$. $\langle x_1,x_2,\ldots,x_n\rangle$ jest więc reprezentacją liczby $(x_1p_1+x_2p_2+\ldots+x_np_n) \bmod W$. ❐

Właściwości systemów resztowych (RNS)

Ponieważ kongruencje są niezmiennicze wobec dodawania i mnożenia, więc:

WNIOSEK 1

Działania można wykonać niezależnie na składowych wektora reprezentacji, dokonując odpowiednio redukcji wyników cząstkowych mod w_i:

$$\{r_1, r_2, \ldots\} \pm \{s_1, s_2, \ldots\} = \{r_1 \pm s_1 \bmod w_1, r_2 \pm s_2 \bmod w_2, \ldots\},$$

$$\{r_1, r_2, \ldots\} * \{s_1, s_2, \ldots\} = \{r_1 * s_1 \bmod w_1, r_2 * s_2 \bmod w_2, \ldots\}.$$

wygodnie jest użyć reszt kongruentnych o małej wartości np. –1 zamiast w_i–1.

WNIOSEK 2

Możliwa jest dekompozycja reprezentacji RNS względem każdego modułu m_i:

$$\{\ldots, r_{i-1}, r_i, r_{i+1}, \ldots\} = \{\ldots, (r_{i-1} - r_i) \bmod w_{i-1}, 0, (r_{i-1} - r_i) \bmod w_{i+1}, \ldots\}$$

$$+ \{\ldots, r_i \bmod w_{i-1}, r_i, r_i \bmod w_{i+1}, \ldots\}$$

Pierwsza liczba jest wielokrotnością modułu w_i, druga ma wartość r_i, więc

$$X = (w_i \cdot X_i + r_i) \bmod W.$$

Wygodnie jest przyjąć, że $w_i = \beta^d$, gdzie β jest podstawą systemu zapisu liczb.

Wybór modułów RNS

Dobór modułów – postulaty

- wystarczający zakres reprezentowanych liczb (iloczyn modułów)
- łatwość i szybkość wykonania działań modulo
- łatwość konwersji na RNS i konwersji odwrotnej

moduły β^k, β^k-1, β^k+1 spełniają powyższe wymagania:

$(\beta^k, \beta^k-1)=1$, $(\beta^k, \beta^k+1)=1$ oraz $(\beta^k-1, \beta^k+1)=1$ (gdy β parzyste)

w systemie dwójkowym

- jeśli $(k,m)=1$, to $(2^k-1,2^m-1)=1$ (liczby Mersenne'a)
- przyśpieszenie dodawania ~ proporcjonalne do log z liczby modułów
- im więcej modułów tym trudniejsza konwersja odwrotna

opcje

$$\mathbf{W}=\{2^k+1, 2^k, 2^k-1\}$$

$$\mathbf{W}=\{2^k+1, 2^k, 2^k-1, 2^k-3\}$$

$$\mathbf{W}=\{2^k, 2^k-1, 2^i-1, \ldots, 2^s-1, \;\; s<\ldots<i<k, \; (s, \ldots, i, k)=1\}$$

Obliczanie reszt w reprezentacji pozycyjnej

Ponieważ dla liczby naturalnej a>3

$$a \bmod a{\pm}1 = -(\pm 1) \Rightarrow a^k \bmod a{\pm}1 = [-(\pm 1)]^k$$

więc dla liczby naturalnej danej w reprezentacji pozycyjnej o podstawie β reszty $\bmod \beta^k{\pm}1$ można obliczyć jako sumy lub różnice liczb k-cyfrowych, utworzonych przez cyfry na pozycjach $jk, jk+1, \ldots, jk+k-1$ ($j=0,1,2,\ldots$):

$$\left(\sum_{i=0}^{n-1} x_i \beta^i\right) \bmod (\beta^k \pm 1) = \left(\sum_{j=0}^{\lceil n/k \rceil} \left(\sum_{i=0}^{k-1} x_{kj+i}\beta^i\right)\beta^{kj}\right) \bmod (\beta^k \pm 1) =$$

$$= \left(\sum_{j=0}^{\lceil n/k \rceil} \left(\sum_{i=0}^{k-1} x_{kj+i}\beta^i\right)(\pm 1)^j\right) \bmod (\beta^k \pm 1)$$

Reszta $\bmod \beta^k$ nie wymaga obliczeń, bo

$$\left(\sum_{i=0}^{n-1} x_i \beta^i\right) \bmod \beta^k = \sum_{i=0}^{k-1} x_i \beta^i$$

Obliczanie wartości jedynek resztowych (CRT)

$p_i=\langle 0,\ldots,1_i,\ldots,0\rangle$ – jedynki resztowe (wagi), $p_i \bmod w_i = 1$ i $p_i \bmod w_{j\neq i} = 0$

Wartością liczby $X<W=\Pi w_i$ o reprezentacji $\langle x_1, x_2, \ldots, x_n\rangle$ jest zatem (CRT)

$$X = (x_1 p_1 + x_2 p_2 + \ldots + x_n p_n) \bmod W,$$

W celu wyznaczenia i-tej jedynki p_i wystarczy wykonać w_i–1 obliczeń. Mamy

$$|\langle 0,\ldots,1_i,\ldots,0\rangle| = k\hat{w}_i = k\prod_{i\neq s} w_s = kw_i^{-1}W, \qquad 1 \leq k = \hat{w}_i^{-1} \bmod w_i \leq w_i - 1,$$

Jedynka jest rozwiązaniem równania $(\hat{w}_i(\hat{w}_i^{-1} \bmod w_i)) \bmod w_i = 1$

- odwrócony algorytm Euklidesa – zapisujemy 1 jako sumę wielokrotności
$$1 = NWD(\hat{w}_i, w_i) = u \cdot \hat{w}_i + v \cdot w_i \Rightarrow u = \hat{w}_i^{-1} \bmod \hat{w}_i$$
- twierdzenie Carmichaela (Eulera): $(\hat{w}_i)^{\lambda(w_i)-1} \equiv (\hat{w}_i \bmod w_i)^{\lambda(w_i)-1} \equiv \hat{w}_i^{-1} (\bmod w_i)$

UWAGA:

1. Warto zauważyć, że $(\hat{w}_i(\hat{w}_i^{-1} \bmod w_i)) \bmod w_i = [(\hat{w}_i \bmod w_i)(\hat{w}_i^{-1} \bmod w_i)] \bmod w_i$
2. Reprezentację *RNS* liczby można dekomponować względem dowolnego modułu, więc wystarczy obliczyć *n*–1 jedynek.

Konwersja z systemu resztowego na system pozycyjny – przykłady

1. Obliczyć X o reprezentacji $\langle r_3, r_2, r_1\rangle$ w systemie RNS(a+1, a, a−1) (a parzyste).

Ponieważ $\langle r_3, r_2, r_1\rangle = \langle r_2, r_2, r_2\rangle + \langle r_3 - r_2, 0, r_1 - r_2\rangle$ wystarczy obliczyć p_3 oraz p_1: Mamy:

$$\hat{w}_3 = w_1 w_2 = (a+1)a, \qquad \hat{w}_3 \bmod w_3 = 2\cdot 1 = 2$$

$$\hat{w}_1 = w_2 w_3 = a(a-1), \qquad \hat{w}_1 \bmod w_1 = (-1)\cdot(-2) = 2$$

oraz ich odwrotności multyplikatywne ($\hat{w}_i^{-1} = \hat{w}_i^{-1} \bmod w_i$)

$$\hat{w}_3^{-1}\hat{w}_3 \bmod w_3 = 2\cdot \hat{w}_3^{-1} \bmod (a-1) = 1 \Rightarrow \hat{w}_3^{-1} \bmod (a-1) = a/2, \text{ więc } \; p_3 = \tfrac{1}{2}(a+1)a^2,$$

$$\hat{w}_1^{-1}\hat{w}_1 \bmod w_1 = 2\cdot \hat{w}_1^{-1} \bmod (a+1) = 1 \Rightarrow \hat{w}_1^{-1} \bmod (a+1) = a/2+1, \; p_1 = a(a-1)(a/2+1)$$

Wartością liczby X o reprezentacji $\langle r_3, r_2, r_1\rangle$ jest więc ($W=(a+1)a(a-1)=(a^3-a)$)

$$X = [(r_3 - r_2)p_3 + r_2 + (r_1 - r_2)p_1] \bmod (a^3 - a)$$

2. W RNS(2^k+1, 2^k, 2^k–1) mamy odpowiednio $W=2^k(2^k+1)(2^k-1)$ oraz:

$$\hat{w}_3^{-1} \bmod (2^k - 1) = 2^{k-1} \Rightarrow p_3 = (2^k+1)\cdot 2^k \cdot 2^{k-1},$$

$$\hat{w}_1^{-1} \bmod (2^k + 1) = -2^{k-1} \Rightarrow p_1 = -(2^k-1)\cdot 2^k \cdot 2^{k-1}$$

zatem wartością liczby X o reprezentacji $\langle r_3, r_2, r_1\rangle$ jest

$$X = [(r_3 - r_2)(2^k+1)\cdot 2^{2k-1} + r_2 - (r_1 - r_2)(2^k-1)\cdot 2^{2k-1}] \bmod (2^{3k} - 2^k).$$

3. W RNS(7,3,2) mamy $\mathbf{X}_{(7,3,2)} = \langle 3,2,1\rangle = \langle -1,-1,-1\rangle + \langle 4,0,0\rangle$ oraz $p_1 = -6$, więc $X = -25 \equiv 17$.

Podzielność liczb

$$\sum_{i=0}^{n-1} x_i\,\beta^i = \sum_{i=0}^{\lceil n/k\rceil-1}\Big(\sum_{s=0}^{k-1} x_{ik+s}\,\beta^s\Big)(\beta^k)^i = \sum_{i=0}^{\lceil n/k\rceil-1} X_i\,\beta^{ki},\quad \text{gdzie } X_i = \sum_{s=0}^{k-1} x_{ik+l}\,\beta^s$$

Ale $\beta^k \operatorname{mod}(\beta^k \pm 1) = \mp 1 \Rightarrow \beta^{kj} \operatorname{mod}(\beta^k \pm 1) = (\mp 1)^j$, a zatem:

$$\left(\sum_{i=0}^{n-1} x_i\beta^i\right)\operatorname{mod}(\beta^k - 1) = \left(\sum_{i=0}^{\lceil n/k\rceil-1} X_i\right)\operatorname{mod}(\beta^k - 1)$$

$$\left(\sum_{i=0}^{n-1} x_i\beta^i\right)\operatorname{mod}(\beta^k + 1) = \left(\sum_{i=0}^{\lceil n/k\rceil-1} (-1)^i X_i\right)\operatorname{mod}(\beta^k + 1)$$

- 4533_{10} mod 101_{10} = 4533_{10} mod $(10^2+1)_{10}$ = (33–45) mod $(10^2+1)_{10}$ = -12_{10}
- 533_{16} mod $0FF_{16}$ = 533_{16} mod $(10^2-1)_{16}$ = $(33+5)_{16}$ mod $(10^2-1)_{16}$ = 38_{16}
- 11011101110_2 mod 77_8 = 2356_8 mod $(10^2-1)_8$ = $(23+56)_8$ mod $(10^2-1)_8$ = 2_8
- $785 \operatorname{mod} 9 = (7+8+5) \operatorname{mod} 9 = 2$, $\quad 785 \operatorname{mod} 11 = (7-8+5) \operatorname{mod} 11 = 4$

Jeśli $\beta=a^k\pm 1$, to $\beta \operatorname{mod} a = \pm 1$ oraz $\beta^k \operatorname{mod} a = (\pm 1)^k$

$\Rightarrow$ reguły podzielności przez a w systemie o podstawie $\beta=a^k\pm 1$

$785 \operatorname{mod} 3 = (7+8+5) \operatorname{mod} 3 = 20 \operatorname{mod} 3 = 2$

Cykliczność reszt

Z właściwości kongruencji wynika, że jeśli $a \bmod w = \pm 1$, to $a^i \bmod w = (\pm 1)^i$.
Zauważmy dalej, że reszty potęg a^i względem $a^k \pm 1$ powtarzają się okresowo:

$$a^k \bmod (a^k \pm 1) = \mp 1 \Rightarrow a^{kj} \bmod (a^k \pm 1) = (\mp 1)^j$$

$$\Rightarrow a^{kj+s} \bmod (a^k \pm 1) = (\mp 1)^j a^s \bmod (a^k \pm 1)$$

Podobnie powtarzają się cyklicznie reszty potęg a^i względem $(a^2 \pm a + 1)$, mamy bowiem $a \bmod (a^2 \pm a + 1) = a$, $a^2 \bmod (a^2 \pm a + 1) = \pm a - 1$, a więc

$$a^3 \bmod (a^2 \pm a + 1) = [a(\mp a - 1)] \bmod (a^2 \pm a + 1) = \pm 1$$

Zauważmy też, że jeśli $NWD(a,w)=1$, to także $NWD(a^i,w)=1$. Ale różnych reszt modulo w jest najwyżej w, więc reszty a^i mod w muszą tworzyć cykle, bo:

$$a^p \bmod w = a^q \bmod w \Rightarrow a^q (a^{p-q} - 1) \bmod w = 0 \;\; w \Rightarrow a^{p-q} \bmod w = 1,$$

czyli istnieje taka potęga a, że a^i mod w $= 1$.

DEFINICJE

Okres (cykl) kongruencji $P(\beta,w)=k \Leftrightarrow \beta^k \equiv 1 \bmod w \;\&\; \forall s < k : \beta^s \bmod w \neq 1.$

Półokres kongruencji $HP(\beta,w)=k \Leftrightarrow \beta^k \equiv -1 \bmod w \;\&\; \forall s < k : \beta^s \bmod w \neq -1.$

System kwadratowo-resztowy QRNS*

– arytmetyka liczb zespolonych (obliczanie transformaty Fouriera):

$$q^2 \bmod w = -1, \Rightarrow q \bmod w = \sqrt{-1} \quad \Rightarrow \text{reprezentacja resztowa } i = \sqrt{-1}:$$

problem: znalezienie modułów, dla których $q^2 \bmod w = -1$ ma rozwiązanie.

DEFINICJA

Liczbę r, pierwszą względem $w \in \mathbf{N}$ i taką, że $x^2 \bmod w = r$ ma rozwiązanie, nazywa się *resztą kwadratową* (*quadratic residue*) względem w. Jeśli $x^2 \bmod w = r$ nie ma rozwiązania, to r nazywa się *nie-resztą kwadratową* (*quadratic nonresidue*) wobec w.

Ponieważ $x^2 \bmod w = (w-x)^2 \bmod w$, więc każde równanie $x^2 \bmod w = r$ ma albo 2 rozwiązania nieprzystające x i $-x$ (a także $w-x$ i $x-w$), albo nie ma rozwiązania. Przy nieparzystym w jest więc $(w-1)/2$ *reszt* oraz $(w-1)/2$ *nie-reszt kwadratowych*.

Na przykład $x^2 \bmod 15=1$ ma rozwiązania –11, –4, 4, 11.

Reszty kwadratowe względem $w = 13$ są rozwiązaniami równania $x^2 \bmod 13 = r$. Metodą przeglądu dla $x = 1, 2, \ldots, 6$ (.$x^2 \equiv (w-x)^2 \bmod w$) znajdujemy: $1^2 \equiv 1 \bmod 13$, $2^2 \equiv 4 \bmod 13$, $3^2 \equiv -4 \bmod 13$, $4^2 \equiv 3 \bmod 13$, $5^2 \equiv -1 \bmod 13$, $6^2 \equiv -3 \bmod 13$, zatem resztami kwadratowymi mod 13 są: –4, –3, –1, 1, 3, 4.

UKŁADY ARYTMETYKI RESZTOWEJ

Sumatory resztowe

Uniwersalny schemat dodawania/odejmowania modulo liczba naturalna może być zrealizowany w trybie multipleksowania dwóch możliwych wyników.

I tak w dodawaniu dwóch liczb $0 \le X < m$ oraz $0 \le Y < m$ modulo m, są 2 możliwości: albo $0 \le X + Y < m$, albo $m \le X + Y$ i wtedy $0 \le X + Y - m < m$.

Podobnie, w odejmowaniu dwóch liczb $0 \le X < m$ oraz $0 \le Y < m$ modulo m, są 2 możliwości: albo $0 \le X - Y < m$, albo $X - Y < 0$ i wtedy $0 \le X - Y + m < m$.

Jeśli jednak argumenty są dane w zapisie pozycyjnym o podstawie β zaś moduł jest postaci $\beta^k - 1$ albo $\beta^k + 1$, to istnieje inne rozwiązanie.

Prefiksowe sumatory resztowe mod $2^k \pm 1$

W realizacji dodawania (i odejmowania) modulo $\beta \pm 1$ argumentów danych w reprezentacji o podstawie β występuje sprzężenie wejścia z wyjściem przeniesienia, co wynika bezpośrednio z reguł arytmetyki:

Wektorowy **operator Brenta-Kunga**:

$$(f,g) = (x,y) \circ (v,z) = (x + yv, yz)$$

jest **obustronnie łączny** lecz nie jest przemienny:

$$[(x,y) \circ (q,r)] \circ (a,b) = (x + yq, yr) \circ (a,b) = (x + yq + yra, yrb)$$

$$(x,y) \circ [(q,r) \circ (a,b)] = (x,y) \circ (q + ra, rb) = (x + yq + yra, yrb)$$

Operator ten ma też właściwość **pochłaniania powtarzalnych czynników**:

$$[(x,y) \circ (q,r)] \circ (x,y) = (x + yq, yr) \circ (x,y) = (x + yq + yrx, yry) = (x + yq, yr) = (x,y) \circ (q,r)$$

Ta właściwość jest bardzo przydatna w konstrukcji niektórych sumatorów

A ponieważ każde przeniesienie zależy od c_0, więc

$$(c_{i+1},0) = (g_i, p_i) \circ \ldots \circ (g_2, p_2) \circ (g_1, p_1) \circ (g_0, p_0) \circ (c_0, 0) = (G_{i:0} + P_{i:0} c_0, 0) =$$

$$= (g_i, p_i) \circ \ldots \circ (g_2, p_2) \circ (g_1, p_1) \circ (g_0 + p_0 c_0, 0) = (G^*_{i:0}, 0)$$