RELACJE

Przypomnienie

Iloczyn (produkt) kartezjański zbiorów A i B:

$$A \times B = \{(a, b) : a \in A,\ \ b \in B\}$$

Określenie relacji:

Relacja R jest zbiorem par uporządkowanych, czyli podzbiorem iloczynu kartezjańskiego dwóch zbiorów: A (dziedzina relacji) i B (przeciwdziedzina relacji):

$$R \subseteq A \times B.$$

Zamiast pisać $(a, b) \in R$ piszemy zazwyczaj $a\,R\,b$. W sytuacji, gdy dziedzina i przeciwdziedzina relacji są tym samym zbiorem ($A = B$), to mówimy o relacji określonej na zbiorze A:

$$R \subseteq A \times A.$$

Przykład

Niech $X = \{1, 4, 5\}$, $Y = \{2, 3\}$.
Wówczas $X \times Y = \{(1, 2), (4, 2), (5, 2), (1, 3), (4, 3), (5, 3)\}$.
Jeśli $R = \{(x, y) : x + y \text{ jest liczbą parzystą}\}$,
to $R = \{(4, 2), (1, 3), (5, 3)\}$.

Własności relacji

Mówimy, że relacja R na zbiorze A jest:

- zwrotna, jeśli $(\forall a \in A)(a\,R\,a)$;
- przeciwzwrotna, jeśli $(\forall a \in A)\,\neg(a\,R\,a)$;
- przechodnia, jeśli $(\forall a, b, c \in A)\,[((a\,R\,b) \ \wedge\ (b\,R\,c)) \ \Rightarrow\ (a\,R\,c)]$;
- symetryczna, jeśli $(\forall a, b \in A)\,[(a\,R\,b) \ \Rightarrow\ (b\,R\,a)]$;
- przeciwsymetryczna, jeśli $(\forall a, b \in A)\,[(a\,R\,b) \ \Rightarrow\ \neg(b\,R\,a)]$;
- antysymetryczna, jeśli $(\forall a, b \in A)\,[((a\,R\,b) \ \wedge\ (b\,R\,a)) \ \Rightarrow\ a = b]$.

Relacje równoważności

Relację R na zbiorze A nazywamy relacją równoważności, gdy R jest:

- zwrotna,
- symetryczna,
- przechodnia.

Przykład 1

Niech X = zbiór wszystkich ludzi. Dla $x, y \in X$ określamy relację R w następujący sposób:

$$x\,R\,y \;\Leftrightarrow\; x \text{ jest tej samej płci co } y.$$

- zwrotność

  Zawsze człowiek x jest tej samej płci co x, tzn. $x\,R\,x$, więc relacja jest zwrotna.
- symetria

  Jeśli człowiek x jest tej samej płci co y, to również na odwrót, y jest tej samej płci co x. Zatem relacja R jest symetryczna.
- przechodniość

  Załóżmy, że człowiek x jest tej samej płci co y oraz że y jest tej samej płci co z. Wówczas wszyscy x, y i z są mają tą samą płeć, w szczególności x jest tej samej płci co z. Zatem relacja R jest przechodnia.

R jest więc relacją równoważności.

Przykład 2

Niech X = zbiór wszystkich ludzi. Dla $x, y \in X$ określamy relację R w następujący sposób:

$$x\,R\,y \;\Leftrightarrow\; x \text{ jest tego samego wzrostu co } y.$$

- zwrotność

  Człowiek x jest tego samego wzrostu co x, tzn. $x\,R\,x$.
- symetria

  Jeśli człowiek x jest tego samego wzrostu co y, to również na odwrót, y jest tego samego wzrostu co x.
- przechodniość

  Załóżmy, że człowiek x jest tego samego wzrostu co y oraz że y jest tego samego wzrostu co z. Wówczas wszyscy x, y i z są tego samego wzrostu, w szczególności x ma ten sam wzrost co z.

R jest więc relacją równoważności.

Przykład 3

Niech X = zbiór wszystkich ludzi. Dla $x, y \in X$ określamy relację R w następujący sposób:

$$x\,R\,y \;\Leftrightarrow\; x \text{ jest niższy niż } y.$$

- zwrotność

  Żaden człowiek nie jest niższy od samego siebie, więc ta relacja nie jest zwrotna.
- symetria

  Jeśli człowiek x jest niższy od y, to nie na odwrót: y nie jest niższy od x. Zatem relacja R nie jest symetryczna.
- przechodniość

  Załóżmy, że człowiek x jest niższy od y oraz że y jest niższy od z. Wówczas x jest niższy od z i widać, że relacja jest przechodnia.

Relacja R nie jest relacją równoważności.

Zauważmy, że w **Przykładzie 1** relacja R dzieli wszystkich ludzi na kobiety i mężczyzn. Formalnie zbiór X został podzielony na dwa podzbiory: podzbiór X_1 kobiet oraz podzbiór X_2 mężczyzn. Podzbiory te mają dwie istotne własności:

- $X_1 \cap X_2 = \emptyset$, czyli są one rozłączne,
- $X_1 \cup X_2 = X$, czyli w sumie dają cały zbiór X.

Mówimy, że rodzina $\{X_1, X_2, \dots\}$ (niekoniecznie skończona) podzbiorów zbioru X jest podziałem, gdy $X = X_1 \cup X_2 \cup \dots$ oraz $X_i \cap X_j = \emptyset$ dla $i \neq j$, czyli gdy w sumie daje cały zbiór X oraz elementy rodziny są parami rozłączne.

W przypadku relacji równoważności mówimy czasem, że x przystaje do y, zamiast mówić, że x jest w relacji z y. Podkreślamy w ten sposób, że x i y są dla tej relacji nierozróżnialne.

Każda relacja równoważności R na zbiorze X wyznacza jednoznacznie podział zbioru X na parami rozłączne podzbiory, które w sumie dają X. Podzbiory te nazywamy <u>klasy abstrakcji</u> (<u>klasy równoważności</u>). Elementy w jednej klasie abstrakcji przystają do siebie, tj. są ze sobą w relacji R. Elementy z różnych klas abstrakcji nie są w relacji R. Zauważmy, że dana klasa abstrakcji jest jednoznacznie wyznaczona przez dowolny element z tej klasy.

Podsumowując, relacja równoważności wprowadza podział zbioru A na klasy abstrakcji. Przez $[a]_R$ oznaczamy klasę abstrakcji relacji R o reprezentancie $a \in A$. Mamy zatem:

$$[a]_R = \{b \in A : a\, R\, b\}$$
$$(\forall a, b \in A)\,([a]_R = [b]_R \,\vee\, [a]_R \cap [b]_R = \emptyset)$$
$$\bigcup_{a \in A} [a]_R = A$$

Macierze boolowskie relacji

Niech $A = \{a_1, a_2, \ldots, a_n\}$, $\quad R \subseteq A \times A$, $\quad I_n = \{1, 2, \ldots, n\}$.

Macierzą boolowską M reprezentującą relację R nazywamy odwzorowanie

$$M : I_n \times I_n \mapsto \{0, 1\}$$

takie, że

$$M_{i,j} = M(i,j) = \begin{cases} 1 & \Leftrightarrow \; a_i\, R\, a_j \\ 0 & \Leftrightarrow \; \neg\,(a_i\, R\, a_j). \end{cases}$$

Przykład

$$A = \{a_1, a_2, a_3\}, \quad R = \{(a_1, a_3), (a_2, a_3), (a_3, a_2)\},$$

$$M = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Niech R' i R'' będą relacjami i niech macierz M' reprezentuje R' oraz niech M'' reprezentuje R''.

Niech R będzie sumą teoriomnogościową R' i R'':

$$R = R' \cup R'', \quad a_1\, R\, a_2 \;\Leftrightarrow\; a_1\, R'\, a_2 \;\vee\; a_1\, R''\, a_2.$$

Wówczas

$$M = M' \vee M''$$
$$M_{i,j} = \begin{cases} 1 & \Leftrightarrow \; M'_{i,j} = 1 \vee M''_{i,j} = 1 \\ 0 & \Leftrightarrow \; M'_{i,j} = 0 \wedge M''_{i,j} = 0. \end{cases}$$

Niech teraz R będzie złożeniem R' z R'':

$$R = R' \circ R'', \quad a_1\, R\, a_2 \;\Leftrightarrow\; (\exists a \in A)\,(a_1\, R''\, a \;\vee\; a\, R'\, a_2).$$

Wówczas

$$M = M' \cdot M''$$
$$M_{i,j} = \bigvee_{k=1}^{n} M'_{i,k} \wedge M''_{k,j}$$
$$M'_{i,k} \wedge M''_{k,j} = \begin{cases} 1 & \Leftrightarrow \; M'_{i,k} = 1 \wedge M''_{k,j} = 1 \\ 0 & \Leftrightarrow \; M'_{i,k} = 0 \vee M''_{k,j} = 0. \end{cases}$$

Przykład

$$A=\{a,b\},\quad R'=\{(a,a),(a,b),(b,b)\},\quad R''=\{(a,b),(b,a)\},$$

$$M'=\left[\begin{array}{cc}1&1\\0&1\end{array}\right],\quad M''=\left[\begin{array}{cc}0&1\\1&0\end{array}\right],$$

$$M_1=M'\vee M''=\left[\begin{array}{cc}1&1\\0&1\end{array}\right]\vee\left[\begin{array}{cc}0&1\\1&0\end{array}\right]=\left[\begin{array}{cc}1&1\\1&1\end{array}\right],$$

$$R_1=R'\cup R''=\{(a,a),(a,b),(b,a),(b,b)\},$$

$$M_2=M'\cdot M''=\left[\begin{array}{cc}1&1\\0&1\end{array}\right]\cdot\left[\begin{array}{cc}0&1\\1&0\end{array}\right]=\left[\begin{array}{cc}1&1\\1&0\end{array}\right],$$

$$R_2=R'\circ R''=\{(a,a),(a,b),(b,a),(b,b)\}.$$

Relacje porządkujące

Relację porządkującą oznaczamy zazwyczaj symbolem $\leq$.
Relację porządkującą na X spełniającą aksjomaty:

P1. $(\forall x\in X)\,(x\leq x)$

P2. $(\forall x,y\in X)\,[(x\leq y)\wedge(x\leq y)\Rightarrow x=y]$

P3. $(\forall x,y,z\in X)\,[(x\leq y)\wedge(y\leq z)\Rightarrow x\leq z]$

nazywamy częściowym porządkiem, zaś parę $(X,\leq)$ nazywamy zbiorem częściowo uporządkowanym lub po prostu zbiorem uporządkowanym.

Jeśli dodatkowo zachodzi:

P4. $(\forall x,y\in X)\,[(x\leq y)\vee(y\leq x)]$,

to relację nazywamy porządkiem liniowym, a parę $(X,\leq)$ zbiorem uporządkowanym liniowo.

Jeśli $x\leq y$ i $x\neq y$, to piszemy $x<y$. Zapis $x\geq y$ oznacza, że $y\leq x$.

Przykłady:

1. Niech M będzie dowolnym zbiorem, $X=P(M)$, gdzie $P(M)$ oznacza zbiór wszystkich podzbiorów zbioru M. Określamy:

   $$A\leq B\ \Leftrightarrow\ A\subseteq B.$$

   Jest to porządek, ale nie liniowy.
2. $X=\mathbb{N}$, $m\leq n\ \Leftrightarrow\ m$ jest mniejsze lub równe n.
3. $X=\mathbb{N}$, $m\leq n\ \Leftrightarrow\ m|n$.

Relacje porządkujące w zbiorze skończonym X można przedstawiać graficznie za pomocą diagramów Hassego, tj. grafów $G = (X, E)$, gdzie:

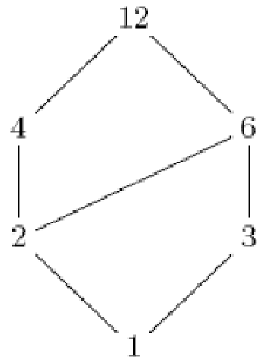
- X zbiór wierzchołków
- E zbiór krawędzi (bezpośrednich połączeń)

$$E = \{(x, y) \in X \times X : x \leq y \wedge \neg (\exists z \in X)(x < z < y)\}.$$

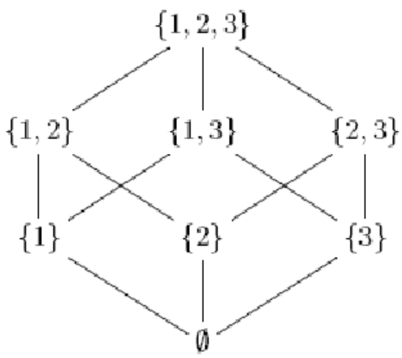
Jeżeli $(x, y) \in E$, to na diagramie rysujemy y wyżej niż x.

Przykłady:

1. $X = \{1, 2, 3, 4, 6, 12\}$, relacja podzielności.



2. $X = P(\{1, 2, 3\})$, relacja inkluzji.



Przechodnie domknięcie relacji

k-ty stopień R^k relacji R na zbiorze A określamy następująco:

$$\begin{aligned} a\,R^0\,b &\Leftrightarrow a = b \\ a\,R^1\,b &\Leftrightarrow a\,R\,b \\ &\vdots \\ a\,R^k\,b &\Leftrightarrow (\exists\, c \in A)\,(a\,R\,c \ \wedge \ c\,R^{k-1}\,b), \end{aligned}$$

czyli np.

$$a\,R^2\,b \Leftrightarrow (\exists\, c \in A)\,(a\,R\,c \ \wedge \ c\,R\,b),$$

$$a\,R^3\,b \;\Leftrightarrow\; (\exists\, c_1, c_2 \in A)\,(a\,R\,c_1 \;\wedge\; c_1\,R\,c_2 \;\wedge\; c_2\,R\,b).$$

Przechodnie domknięcie R^+ relacji R na zbiorze A definiujemy następująco:

$$a\,R^+\,b \;\Leftrightarrow\; (a,b) \in \bigcup_{k=1}^{\infty} R^k \;\Leftrightarrow\; (\exists\, k \geqslant 1)\,(a\,R^k\,b).$$

Przykład:

$\mathbb{N} = \{0, 1, 2, \dots\}$ zbiór liczb naturalnych (z zerem), $R \subseteq \mathbb{N} \times \mathbb{N}$

$$n\,R\,m \;\Leftrightarrow\; n = m + 2$$

$n\,R^2\,m \;\Leftrightarrow\; (\exists\, p \in \mathbb{N})\,(n = p + 2, p = m + 2) \;\Leftrightarrow\; n = m + 4$

$n\,R^3\,m \;\Leftrightarrow\; (\exists\, p_1, p_2 \in \mathbb{N})\,(n = p_1 + 2,\, p_1 = p_2 + 2,\, p_2 = m + 2) \;\Leftrightarrow$
$\Leftrightarrow\; n = m + 6,$

np. $(8,6) \in R, \quad (8,4) \in R^2, \quad (8,2) \in R^3.$

Widać, że

$(n,m) \in R^+ \;\Leftrightarrow\; n - m$ jest niezerową parzystą liczbą naturalną.

KONGRUENCJE

Niech n będzie dodatnią liczba całkowitą, natomiast a i b dowolnymi liczbami całkowitymi. Liczby a i b nazywamy *przystającymi* (*kongruentnymi*) modulo n i piszemy

$$a \equiv b \,(\mathrm{mod}\, n) \text{ lub } a \equiv_n b,$$

jeżeli różnica $a - b$ jest podzielna przez n, tj.

$$n \,|\, a - b \;\Leftrightarrow\; (\exists\, k \in \mathbb{Z})\,(a - b = kn).$$

Na przykład:

$$3 \equiv 24 \,(\mathrm{mod}\, 7), \quad -31 \equiv 11 \,(\mathrm{mod}\, 7), \quad -15 \equiv -64 \,(\mathrm{mod}\, 7),$$

bo mamy:

$$3 - 24 = 21 = 3 \cdot 7, \quad -31 - 11 = -42 = -6 \cdot 7, \quad -15 - (-64) = 49 = 7 \cdot 7.$$

Analogicznie, mamy liczby, które *nie są przystające* modulo n

$$a \not\equiv b \,(\mathrm{mod}\, n),$$

Na przykład $6 \not\equiv 12 \,(\mathrm{mod}\, 7)$, bo $6 - 12 = -6$ nie dzieli się przez 7.

Własności kongruencji

Warunkiem koniecznym i wystarczającym, aby $a \equiv b \,(\mathrm{mod}\, n)$, jest równość reszt z dzielenia a i b przez n. Na przykład:

$$\begin{aligned} -56 &\equiv -11 (\mathrm{mod}\, 9), \text{bo} \\ -56 &= (-7) \cdot 9 + 7, \\ -11 &= (-2) \cdot 9 + 7. \end{aligned}$$

Każde dwie liczby całkowite a i b przystają do siebie modulo 1 oraz modulo -1. Mamy więc $a \equiv b \,(\mathrm{mod}\, 1)$ i $a \equiv b \,(\mathrm{mod}\, (-1))$. Dlatego nie warto rozważać kongruencji o module 1.

Ponieważ $a \equiv b \,(\mathrm{mod}\, m)$ implikuje $a \equiv b \,(\mathrm{mod}\, (-m))$, to rozważamy tylko dodatnie moduły.

Kongruencja albo przystawanie liczb całkowitych okazuje się mieć podobne własności w stosunku do operacji dodawania, mnożenia i potęgowania jak zwykła relacja równości.

1. $a \equiv a \,(\mathrm{mod}\, n)$
2. $a \equiv b \,(\mathrm{mod}\, n) \;\Rightarrow\; b \equiv a \,(\mathrm{mod}\, n)$

3. $[\, a \equiv b \,(\mathrm{mod}\, n)$ i $b \equiv c \,(\mathrm{mod}\, n)\,] \;\Rightarrow\; a \equiv c \,(\mathrm{mod}\, n)$

4. $a \equiv b \,(\mathrm{mod}\, n) \;\Rightarrow\; \begin{cases} a + c \equiv b + c \,(\mathrm{mod}\, n) \\ a \cdot c \equiv b \cdot c \,(\mathrm{mod}\, n) \end{cases}$

5. $[\, a \equiv b \,(\mathrm{mod}\, n)$ i $c \equiv d \,(\mathrm{mod}\, n)\,] \;\Rightarrow\; \begin{cases} a + c \equiv b + d \,(\mathrm{mod}\, n) \\ a \cdot c \equiv b \cdot d \,(\mathrm{mod}\, n) \end{cases}$

6. $a \equiv b \,(\mathrm{mod}\, n) \;\Rightarrow\; a^k \equiv b^k \,(\mathrm{mod}\, n)$

7. $[\, a \cdot c \equiv b \cdot c \,(\mathrm{mod}\, n)$ i $\mathrm{NWD}(c, n) = 1] \;\Rightarrow\; a \equiv b \,(\mathrm{mod}\, n)$

Przykład. Czemu jest równe $2^{32} \,(\mathrm{mod}\, 17)$?

Zauważmy, że $2^4 \equiv -1 \,(\mathrm{mod}\, 17)$.

Stąd $(2^4)^8 \equiv (-1)^8 \,(\mathrm{mod}\, 17)$.

Zatem $2^{32} \,(\mathrm{mod}\, 17) = 1$.

Klasy reszt modulo m

Kiedy liczba całkowita a zostaje podzielona przez inna liczbę całkowitą m, to

$$a = km + r, \text{ gdzie } k \in \mathbb{Z},\; 0 \leqslant r < m,$$

a zatem każda liczba całkowita przystaje modulo m do jednej z liczb

$$0, 1, \ldots, m - 1.$$

Żadne dwie liczby tego zbioru nie przystają do siebie modulo m.

Mówimy, że zbiór $\{0, 1, \ldots, m - 1\}$ tworzy pełny układ reszt modulo m. Liczby, które przy dzieleniu przez m dają tą samą resztę r tworzą daną klasę reszt modulo m. Klas takich jest m.

Dla danej reszty r klasa reszt, do której ta należy składa się z liczb

$$r, r \pm m, r \pm 2m, \ldots$$

Nowa definicja kongruencji:

$a \equiv b \,(\mathrm{mod}\, m)$ oznacza, że a i b należą do tej samej klasy reszt modulo m.

Ustalmy teraz liczbę m i zdefiniujmy na zbiorze $\mathbb{Z}$ relację R następująco:

$$a \, R \, b \;\Leftrightarrow\; a \equiv b \,(\mathrm{mod}\, m).$$

Twierdzenie. Relacja R jest relacją równoważności.

Klasy abstrakcji tej relacji tworzą zbiór reszt modulo m.

Zbiór ilorazowy relacji R oznaczamy przez $\mathbb{Z}_m$. Zatem $\mathbb{Z}_5$ składa się z następujących zbiorów:

$$\begin{aligned}
[0] &= \{\dots, -10, -5, 0, 5, 10, 15, \dots\}, \\
[1] &= \{\dots, -9, -4, 1, 6, 11, 16, \dots\}, \\
[2] &= \{\dots, -8, -3, 2, 7, 12, 17, \dots\}, \\
[3] &= \{\dots, -7, -2, 3, 8, 13, 18, \dots\}, \\
[4] &= \{\dots, -6, -1, 4, 9, 14, 19, \dots\},
\end{aligned}$$

Zazwyczaj utożsamiamy elementy $0, 1, 2, 3, 4$ z klasami abstrakcji, które są przez nie reprezentowane. Piszemy więc $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Każde wyrażenie algebraiczne, w konstrukcji którego są użyte operacje dodawania, odejmowania i mnożenia, musi dać "ten sam" (w sensie przystawania) wynik, jeżeli podstawimy za zmienna wartości kongruentne. Na przykład wielomian

$$W(x) = x^3 - 8x + 6$$

da wartości kongruentne modulo 5 jeżeli za x podstawić $x = -2$ i $x = 3$, bo $-2 \equiv 3 \pmod 5$. Rzeczywiście

$$W(-2) = 14 \equiv 9 = W(3) \pmod 5.$$

Małe Twierdzenie Fermata (MTF)

Dla dowolnej liczby pierwszej p i liczby naturalnej a zachodzi

$$a^p \equiv_p a.$$

Równoważnie (stosując regułę skracania), jeśli p nie dzieli a, to

$$a^{p-1} \equiv_p 1.$$

Zastosowania MTF

Przykład 1. Pokażemy, że $2^{50} + 3^{50}$ jest podzielne przez 13.

Ponieważ $50 = 4 \cdot 12 + 2$, to z MTF mamy dla $a \in \{2, 3\}$
$a^{12} \equiv_{13} 1$. Następnie
$a^{48} \equiv_{13} 1$ (po podniesieniu stronami do 4-ej potęgi),
$a^{50} \equiv_{13} a^2$ (po pomnożeniu stronami przez a^2).

Stąd $2^{50} + 3^{50} \equiv_{13} 2^2 + 3^2 = 13 \equiv_{13} 0$, więc $13 \mid 2^{50} + 3^{50}$.

Przykład 2. Pokażemy, że 7 nie dzieli $n^2 + 1$ dla żadnego $n \in \mathbb{N}$.

Istotnie, gdyby $n^2 + 1 \equiv_7 0$, to wówczas (odejmując stronami 1)
$n^2 \equiv_7 -1$. Stąd, po podniesieniu do 3-ej potęgi.
$n^6 \equiv_7 -1 \not\equiv_7 1$, wbrew MTF (z założenia nie wprost wynika, że $7 \not| n$).

Ponieważ $2^{340} \pmod{341}$ oraz $341 = 11 \cdot 31$, więc twierdzenie odwrotne do MTF nie jest prawdziwe. Liczby p, które spełniają tezę MTF, ale nie są liczbami pierwszymi nazywamy liczbami *pseudopierwszymi.*

Funkcja φ Eulera

$$\varphi(n) = |\{1 \leqslant a < n : \mathrm{NWD}(a, n) = 1\}|$$

W szczególności $\varphi(p) = p - 1$ dla dowolnej liczby pierwszej p.

Uwaga.

Jeśli n ma rozkład na czynniki pierwsze postaci $\prod\limits_{i=1}^{k} p_i^{\alpha_i}$, to

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Przykład.

$$\varphi(5^2 \cdot 29) = 5^2 \cdot 29 \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{29}\right) = 560.$$

Twierdzenie Eulera

Dla liczb naturalnych a i n takich, że NWD $(a, n) = 1$, zachodzi

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

Rozwiązywanie równań modularnych (kongruencji)

Niech $a, b \in \mathbb{Z}$ i $a \neq 0$. Równanie modularne

$$ax \equiv_n b$$

ma rozwiązanie wtedy i tylko wtedy, gdy $d \,|\, b$, gdzie $d = \text{NWD}\,(a, n)$.

W przypadku rozwiązywalnego równania modularnego:

- gdy $d = 1$, to równanie ma nieskończenie wiele rozwiązań postaci

  $$x = x_0 + kn,\;\; k \in \mathbb{Z},$$

  gdzie x_0 jest szczególnym rozwiązaniem równania;
- gdy $d > 1$, to jego rozwiązania są identyczne z rozwiązaniami równania

  $$\frac{a}{d}x \equiv_{\frac{n}{d}} \frac{b}{d}, \text{ w którym NWD}\left(\frac{a}{d}, \frac{n}{d}\right) = 1.$$

Przykłady:

1. $3x \equiv_7 4$

   NWD$(3, 7) = 1$, więc równanie ma nieskończenie wiele rozwiązań.

   $$3x - 4 = 7s \;\;\Rightarrow\;\; x_0 = -1 \text{ dla } s = -1.$$

   Zbiorem rozwiązań jest więc $\{7k - 1 : k \in \mathbb{Z}\}$.
2. $3x \equiv_{12} 4$

   NWD$(3, 12) = 4$, ale 3 nie dzieli bez reszty 4, więc równanie nie ma rozwiązań.
3. $15x \equiv_{24} 12$

   NWD$(15, 24) = 3 \,|\, 12$, więc równanie to ma te same rozwiązania, co

   $$\frac{15}{3}x \equiv_{\frac{24}{3}} \frac{12}{3}, \text{ tj. } 5x \equiv_8 4.$$

   Ponieważ $x_0 = 4$ jest jednym z rozwiązań tego równania, to zbiorem wszystkich jego rozwiązań jest zbiór

   $$\{8k + 4 : k \in \mathbb{Z}\}.$$

Chińskie Twierdzenie o Resztach

Kiedy dowódca chciał zliczyć swoje wojsko, kazał ustawiać się żołnierzom w dwuszeregu, następnie w trzyszeregu, potem w pięcioszeregu itd. Liczba niesparowanych żołnierzy w każdym z tych ustawień (czyli reszty z dzielenia ogólnej liczby żołnierzy przez $2, 3, 5, \ldots$) pozwalały ustalić liczbę wszystkich żołnierzy.

Przykład.

Po ustawieniu całego wojska w 3, 5 i 7-szeregu dostaliśmy, odpowiednio 2, 1 oraz 6 niesparowanych żołnierzy. Jaka jest liczebność oddziału, jeżeli wiadomo, że żołnierzy jest mniej niż 100?

Rozwiązanie:

Niech x będzie liczbą żołnierzy. Zatem reszty z dzielenia x przez 3, 5 oraz 7, to odpowiednio 2, 1 i 6. Stąd

$$x \equiv 2 \pmod 3, \tag{1}$$
$$x \equiv 1 \pmod 5, \tag{2}$$
$$x \equiv 6 \pmod 7. \tag{3}$$

Z kongruencji (1) mamy $x = 3k + 2$. Podstawiając do (2), mamy

$$3k + 2 \equiv 1 \pmod 5, \text{ czyli } 3k \equiv -1 \pmod 5.$$

Ponieważ 2 jest liczbę odwrotną do 3 modulo 5 (tzn. jest elementem odwrotnym do 3 w $\mathbb{Z}_5$), to mnożąc stronami przez 2 ostatnią kongruencję, otrzymujemy

$$k \equiv -2 \pmod 5.$$

Zatem

$$k = 5r - 2 \text{ oraz } x = 3 \cdot (5r - 2) + 2 = 15r - 4.$$

Podstawiając tę postać x do (3), otrzymujemy

$$15r - 4 \equiv 6 \pmod 7 \;\Leftrightarrow\; 15r \equiv 10 \pmod 7 \;\Leftrightarrow\; 3r \equiv 2 \pmod 7,$$

gdzie w ostatniej równoważności stosujemy regułę skracania (można, bo $\mathrm{NWD}(5, 7) = 1$). Ponieważ $3^{-1} \equiv 5 (\mathrm{mod}\, 7)$, to mnożąc stronami ostatnie dwie kongruencje, dostajemy

$$r \equiv 10 \equiv 3 \pmod 7.$$

Stąd mamy

$$r = 7s + 3, \text{ czyli } x = 15 \cdot (7s + 3) - 4 = 105s + 41.$$

Zatem wszystkich żołnierzy jest 41 (następna możliwość to 146, ale jak zaznaczyliśmy, żołnierzy jest mniej niż 100).

Chińskie Twierdzenie o Resztach

Wówczas układ kongruencji

$$(*) \qquad \begin{cases} x & \equiv_{m_1} a_1, \\ x & \equiv_{m_2} a_2, \\ & \vdots \\ x & \equiv_{m_k} a_k, \end{cases}$$

ma jednoznaczne rozwiązanie modulo $M = m_1 \cdot m_2 \cdot \ \ldots \ \cdot m_k$.

Konstrukcja rozwiązania.

Najpierw wyznaczamy $s_1, s_2, \ldots s_k$ takie, że

$$\begin{gathered} \frac{M}{m_1} s_1 \equiv_{m_1} 1, \\ \frac{M}{m_2} s_2 \equiv_{m_2} 1, \\ \vdots \\ \frac{M}{m_k} s_k \equiv_{m_k} 1. \end{gathered}$$

Wówczas układ kongruencji $(*)$ ma dokładnie jedno rozwiązanie x_0 modulo M dane wzorem:

$$x_0 = \frac{M}{m_1} s_1 \cdot a_1 + \frac{M}{m_2} s_2 \cdot a_2 + \cdots + \frac{M}{m_k} s_k \cdot a_k \pmod{M}.$$

Przykład. Wyznaczyć najmniejsze dodatnie rozwiązanie układu kongruencji

$$\begin{cases} x & \equiv_3 2, \\ x & \equiv_7 4, \\ x & \equiv_{10} 6. \end{cases}$$

Rozwiązanie:

Mamy $M = 3 \cdot 7 \cdot 10 = 210$ oraz

$$\begin{array}{ccc} m_1 = 3, & m_2 = 7, & m_3 = 10, \\ a_1 = 2, & a_2 = 4, & a_3 = 6. \end{array}$$

Wyznaczamy $s_i \pmod{m_i} = \left(\frac{M}{m_i}\right)^{-1} \pmod{m_i}$ dla $i = 1, 2, 3$:

$$\begin{aligned} \frac{210}{3} s_1 \equiv_3 70 s_1 \equiv_3 s_1 \equiv_3 1 \qquad & \Rightarrow \ s_1 = 1, \\ \frac{210}{7} s_1 \equiv_7 30 s_2 \equiv_7 2 s_2 \equiv_7 1 \qquad & \Rightarrow \ s_2 = 4, \\ \frac{210}{10} s_1 \equiv_{10} 21 s_3 \equiv_{10} s_3 \equiv_{10} 1 \qquad & \Rightarrow \ s_3 = 1. \end{aligned}$$

Wobec tego

$$x \equiv_{210} \frac{3 \cdot 7 \cdot 10}{3} \cdot 1 \cdot 2 + \frac{3 \cdot 7 \cdot 10}{7} \cdot 4 \cdot 4 + \frac{3 \cdot 7 \cdot 10}{10} \cdot 1 \cdot 6$$
$$x \equiv_{210} 140 + 480 + 126 \equiv_{210} -70 + 60 + 126 \;\Rightarrow\; x = 116.$$

Algorytm szyfrowania RSA

Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman

Metoda polega na wybraniu trzech liczb n, e i d:

- n, która jest iloczynem dwóch liczb pierwszych (w praktyce n musi mieć ponad 200 cyfr),
- e oraz d, które dobieramy w odpowiedni sposób w zależności od wspomnianych liczb pierwszych.

  Liczby e i d nazywamy kluczami. Algorytm doboru e i d jest znany w literaturze.
- n i e są jawne.
- Klucz d posiada jedynie odbiorca wiadomości.

Przykład. Dla uproszczenia nasze n, e, d będą małe:

$$n = 85 = 5 \cdot 17, \quad e = 5, \quad d = 13.$$

Szyfrujemy uproszczoną wiadomość w postaci litery $x = 24$ (x jest 24-tą literą alfabetu) w następujący sposób:

$$24^5 = 7962624 \equiv 79 \pmod{85}.$$

Przy użyciu klucza $d = 13$ rozszyfrowujemy wiadomość:

$$79^{13} \pmod{85} = 24 \pmod{85} = x.$$
