Kongruencja liniowa

Zadania 1-3 liczymy ręcznie.

1. Rozwiązać kongruencję liniową $24x \equiv_{66} 138$.
2. Korzystając z tabelki poniżej zaszyfrować tekst **ŁĄKA** szyfrem afinicznym o kluczu a=7, b=13.

A	Ą	B	C	Ć	D	E	Ę	F	G	H	I	J	K	L	Ł	M	N	Ń	O	Ó	P	R	S	Ś	T	U	W	Y	Z	Ź	Ż
0	1	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

3. Wyznaczyć wzór funkcji deszyfrującej i odczytać tekst z szyfrogramu **ĆKL.**

4. Napisać algorytm, który rozwiązuje kongruencję liniową $ax \equiv_n c$.

We: a, c, n – całkowite, a różne od zera, n dodatnie

Wy: wszystkie rozwiązania kongruencji modulo n

Jeżeli $d = NWD(a, n)$ nie dzieli c, to brak rozwiązań,

w.p.p. jest d różnych rozwiązań, które otrzymujemy rozwiązując liniowe równanie diofantyczne $ax + ny = c$.

Rozwiązaniem kongruencji są liczby $x_t \equiv_n x_0 + tn$', gdzie $t = 0,1, \dots, d-1$

5. Napisać algorytm wyznaczający odwrotność liczby a modulo n. Sprowadza się to do zadania rozwiązania kongruencji liniowej $ax \equiv_n 1$

We: a, n – całkowite, a różne od zera, n dodatnie

Wy: odwrotność liczby a modulo n

Jeżeli $d = NWD(a, n) \neq 1$, to brak rozwiązań,

w.p.p. jest 1 rozwiązanie $x \equiv_n x0$

6. Szyfr afiniczny

a) Szyfrowanie WE: n – liczba znaków w alfabecie, klucz a,b – całkowite różne od zera, z - znak do zaszyfrowania = liczba od zera do n-1

WY: szyfrogram – s = zaszyfrowany znak z, tzn. $s \equiv_n az + b$

W pierwszym kroku sprawdzamy poprawność klucza – a musi być odwracalne modulo n, b – dowolne, poprawność z – musi być liczbą od zera do n-1. Potem wyliczamy s.

b) Deszyfrowanie

WE: n – liczba znaków w alfabecie, klucz a,b – całkowite różne od zera, s – szyfrogram do odszyfrowania – liczba od zera do n-1

WY: znak z tzn. $z \equiv_n a^{-1}(s - b)$

Poprawny klucz powinien być wzięty z algorytmu szyfrowania. Do znalezienia odwrotności bierzemy algorytm z zadania5.