TEORIA NUMERELOR

Problema nr. 1

Un număr este perfect dacă este egal cu suma divizorilor săi, în afara lui însuşi. Exemplu: 6 = 1+2+3 sau 28 = 1+2+4+7+14. Explicaţi de ce $2^{k-1}(2^k-1)$ este număr perfect dacă (2^k-1) este număr prim.

Problema nr. 2

Să se demonstreze următoarea teoremă:

Teoremă: Dacă cmmdc(a,b) = 1, atunci cmmdc(a+b, a-b) =1 sau 2.

Problema nr. 3

Dacă a şi b sunt două numere întregi atunci cmmdc al celor două numere are următoarea proprietate (printre altele):

cmmdc(a,b) = cmmdc(b, a mod b)

unde a mod b este restul împărţirii numărului a la b. Aplicarea repetată a acestei proprietăţi atât timp cât obţinem un rest diferit de zero constituie algoritmul lui Euclid de determinare a cmmdc.

Folosind proprietatea indicată mai sus să se calculeze cmmdc(1147, 899)

Problema nr. 4

Algoritmul lui Euclid ne permite calcularea valorii celui mai mare divizor comun a două numere a şi b. Ne interesează şi combinaţia liniară corespunzătore. Pentru determinarea acesteia vom face apel la algoritmul extins al lui Euclid.

Teorema împărţirii afirmă că: oricare ar fi două numere întregi **a** şi **b**, există o pereche unică (q_0, r_0) de numere întregi asociată numerelor **a** şi **b** astfel încât:

$$a=q_0b+r_0 \rightarrow r_0=a-q_0b$$

q_0 se numeşte câtul, iar r_0 este restul împărţirii lui a la b. Se observă că putem exprima restul împărţirii ca o combinaţie liniară a numerelor considerate (a şi b).

Aplicăm algoritmul lui Euclid de determinare a cmmdc şi obţinem în continuare:

$$b = q_1r_0 + r_1 \rightarrow r_1 = b - q_1r_0 =$$
$$= b - q_1(a - q_0b) =$$
$$= -q_1a + (1+q_1q_0)b$$

Se observă că şi acest al doilea rest a putut fi exprimat ca o combinaţie liniară a celor două numere luate în discuţie.

Procedeul se continuă până se obţine un rest egal cu zero. Cmmdc este atunci ultimul rest nenul pentru care putem determina şi combinaţia liniară corespunzătoare a numerelor iniţiale.

Exemplu:

Să se calculeze cmmdc şi combinaţia liniară corespunzătoare pentru numerele 259 şi 70.

Se notează x = a = 259 şi y = b = 70.

Se construieşte următorul tabel:

x	y	x mod y	= x - qb
259	70	49	= 259 – 3 · 70

70	49	21	=70 – 1 · 49 = 70 – 1·(259–3·70) = =-1·259 + 4·70
49	21	**7**	=49-2·21 = (1·259-3·70)–2(-1·259+4·70) = =**3·259 - 11·70**
21	7	0	

Putem scrie cmmdc(259, 70) = 7 = **3·259 - 11·70**

Constatăm că acest algoritm ne permite calcularea combinaţiei liniare întregi asociate celui mai mare divizor comun.

Aplicaţii ale algoritmului extins al lui Euclid. Rezolvarea unei clase de ecuaţii diofantice.

Putem folosi acest algoritm la rezolvarea ecuaţiilor diofantice liniare. Acestea sunt ecuaţii de forma:

$$ax + by = c \qquad (1)$$

Ecuaţiile de acest tip au soluţii numai dacă c este un multiplu al cmmdc al numerelor a şi b. Deducem de aici o condiţie de existenţă a soluţiilor ecuaţiei (1).

De exemplu, ecuaţia

$$259x + 70y = 7$$

are ca soluţii valorile x = 3 şi y = -11, adică tocmai coeficienţii combinaţiei liniare corespunzătoare cmmdc(259, 70).

În cazul general, dacă cmmdc(a,b) = d, atunci rezolvarea ecuaţiei diofantice (1) are mai multe etape:

a) Verificarea existenţei soluţiei ecuaţiei
b) determinarea soluţiei ecuaţiei
$$ax + by = d \qquad (2)$$
c) o soluţie a ecuaţiei (2) este se notează cu x_0^d şi y_0^d
d) o soluţie a ecuaţiei (1) este atunci
$$x_0 = x_0^d \cdot \frac{c}{d} \qquad y_0 = y_0^d \cdot \frac{c}{d} \qquad (3)$$
e) ecuaţia (1) nu are o singură soluţie, ci o mulţime de soluţii. Mulţimea soluţiilor ecuaţiei (1) este dată de relaţiile:
$$x = x_0 + \frac{b}{d} \cdot t$$
$$y = y_0 - \frac{a}{d} \cdot t$$

unde **t** este un număr întreg.

Să găsească soluţiile ecuaţiilor

a) 23x+29y=7
b) 3456x+246y=73
c) 436x-393y=5

Problema nr. 5

În bucătărie nu există ceas, dar ştiu că:

a) robinetul picură o dată la 54 s după ce l-am închis.

b) prăjitorul de pâine dă o felie de pâine prăjită la fiecare 84 s.

Trebuie să prăjesc un ou exact 141 secunde. Mi-am propus să pun prăjitorul în priză şi să închid robinetul exact în acelaşi timp. Voi începe prăjitul oului când din robinet picură picătura *D* şi să închei prăjitul când prăjitorul aruncă felia *P*. Care sunt valorile lui *D* şi *P* necesare pentru ca acest plan să funcţioneze?

Problema nr. 6

În grădină am un lac. în interiorul lacului sunt **n** pietre aranjate în cerc. O broască stă pe una din pietre. Oricum ar sări broasca, ea aterizează la **k** pietre mai departe, în sensul acelor de ceasornic, de piatra pe care se află (0<k<n). Masa broaştei, un vierme gustos, stă pe o piatră aflată chiar lângă piatra pe care stă broasca, în sensul acelor de ceasornic.

a) Descrieţi o situaţie în care broasca nu poate ajunge la vierme.

b) În situaţia în care broasca poate ajunge la vierme, explicaţi cum putem utiliza algoritmul extins al lui Euclid pentru a afla câte sărituri trebuie să facă broasca pentru a ajunge la vierme.

c) Calculaţi numărul de sărituri dacă n = 50 şi k = 21. Este un rezultat credibil?

Problema nr. 7

Să se demonstreze că: dacă a|b şi a|c atunci a|(sb+tc), oricare ar fi s, t numere întregi.

Problema nr. 8

a) Să se folosească Algoritmul extins al lui Euclid pentru a determina întregii *s* şi *t* astfel incât 135s+59t = cmmdc(135, 59).

b) Să se folosească punctul a0 pentru a determina inversul lui 59 modulo 135 din domeniul {1, 2, ..., 135}.

Problema nr. 9 RSA

a) Alegeţi două numere prime *p* şi *q* relativ mici (în intervalul 5 – 15, de exemplu p = 7 şi q = 11). (În realitatea p şi q vor fi numere foarte mari).

b) Calculaţi n = pq. Acest număr va fi folosit pentru criptarea şi decriptarea mesajelor.

c) Determinaţi un e>1 astfel încât cmmdc(e, (p-1)(q-1)) = 1. Perechea (e,n) este cheia publică care va fi făcută cunoscută.

d) Determinaţi un d astfel încât $de \equiv 1(\mathrm{mod}(p-1)(q-1))$. Sepoate utiliza Algoritmul extins al lui Euclid sau teorema lui Fermat. Perechea (d,n) va fi cheia secretă.

Alegeţi un mesaj format din câteva litere şi criptaţi-l folosind cheia publică. Un alt coleg trebuie sa-l decripteze.

Elemente de codare a mesajelor

Invers multiplicativ

Inversul multiplicativ al unui număr *x* este un alt număr x^{-1} astfel incât:

$$x \cdot x^{-1} = 1$$

În general, invers multiplicativ există pentru fiecare număr real (cu excepţia numărul 0). De exemplu, inversul multiplicativ al lui 3 este $\frac{1}{3}$ pentru că:

$$3 \cdot \frac{1}{3} = 3 \cdot 3^{-1} = 1$$

Pe de altă parte, în mulţimea numerelor întregi nu există invers multiplicativ. De exemplu, 11 nu poate fi înmulţit cu un alt număr întreg astfel încât rezultatul să fie egal cu 1.

Totuşi, invers multiplicativ există atunci când lucrăm *modulo un număr prim* (când folosim relaţia de congruenţă corespunzătoare unui număr prim). De exemplu, dacă lucrăm modulo 5, atunci 3 este un invers multiplicativ al lui 7 pentru că:

$$7 \cdot 3 \equiv 1 (\mathrm{mod}\, 5)$$

Observaţie: toate numerele congruente cu 3 modulo 5 sunt de asemenea invers multiplicativ pentru 7. De exemplu: $7 \cdot 8 \equiv 1 (\mathrm{mod}\, 5))$. Singura excepţie sunt acele numere care sunt congruente cu 0 modulo 5 (adică multiplii lui 5) care nu au invers multiplicativ aşa cum 0 nu are invers în mulţimea numerelor reale.

Lemma 1. *Dacă p este număr prim şi k nu este un multiplu al lui p, atunci k are un invers multiplicativ modulo p*.

Demonstraţie. deoarece *p* este număr prim, el are numai doi divizori: 1 şi *p*. Pentru că *k* nu este un multiplu al lui *p*, trebuie să avem cmmdc(p,k) = 1. De aici rezultă că există o combinaţie liniară de *p* şi *k* egală cu 1:

$$sp + tk = 1$$

Rearanjând termenii vom avea:

$$sp = 1 - tk$$

Rezultă că $p \mid (1 - tk)$ (din definiţia divizibilităţii) şi astfel

$$tk \equiv 1 (\mathrm{mod}\, p)$$

prin definiţia congruenţei. Astfel, *t* este inversul multiplicativ al lui *k*.

Simplificare

Tot în mulţimea numerelor reale putem simplifica termenii într-o înmulţire. Cu alte cuvinte, dacă ştim că $m_1 k = m_2 k$ atunci putem simplifica prin *k* şi concluziona că $m_1 = m_2$ (în condiţiile în care $k \neq 0$). în general simplificarea nu este validă în aritmetica modulară. De exemplu,

$$2 \cdot 3 \equiv 4 \cdot 3 (\mathrm{mod}\, 6)$$

dar simplificarea cu 3 conduce la concluzia falsă că $2 \equiv 4 (\mathrm{mod}\, 6)$. Faptul că termenii multiplicativi nu pot fi simplificaţi este cea mai semnificativă diferenţă între congruenţă şi egalitatea obişnuită. Totuşi, această diferenţă dispare dacă lucrăm cu o relaţie de congruenţă modulo *p*, în care *p* este număr prim şi, în acest caz, simplificarea este validă.

Lemma 2. Fie *p* un număr prim şi *k* un număr care nu este multiplu al lui *p*. Atunci

$$ak \equiv bk (\mathrm{mod}\, p) \text{ implică } a \equiv b (\mathrm{mod}\, p).$$

Demonstraţiei. Multiplicăm ambii termeni ai congruenţei cu inversul multiplicativ k^{-1}.

Corolar. Presupunem că *p* este un număr prim şi *k* nu este multiplu al lui *p*. Atunci secvenţa:

$$rem((1 \cdot k), p), rem((2 \cdot k), p), \ldots, rem((1 \cdot k), p)$$

este o permutare a secvenţei:

$$1, 2, \ldots, (p-1)$$

Demonstraţie. Secvenţa de resturi conţine $p-1$ numere. Pentru că $i \cdot k$ nu este divizibil cu p pentru i = 1, 2, ..., p – 1, toate aceste resturi sunt din mulţimea {1, 2, ..., p-1} prin definiţia restului împărţirii. Mai mult, toate resturile sunt diferite: nu există două numere din această mulţime care să fie congruente modulo p şi aplicând Lemma 2 ($i \cdot k \equiv j \cdot k (\mathrm{mod}\, p) \leftrightarrow i \equiv j (\mathrm{mod}\, p)$). Astfel, secvenţa de resturi trebuie să conţină *toate* numerele de la 1 la p-1 într-o ordine oarecare.

Exemplu, p = 5 şi k = 3. Atunci secvenţa:

$$\underbrace{rem((1 \cdot 3),5)}_{=3}, \underbrace{rem((2 \cdot 3),5)}_{=1}, \underbrace{rem((3 \cdot 3),5)}_{=4}, \underbrace{rem((4 \cdot 3),5)}_{=2}$$

este o permutare a secvenţei 1, 2, 3, 4.

Mica teoremă a lui Fermat

O altă cale de a determina inversul multiplicativ al unui număr întreg porneşte de la mica teoremă a lui Fermat.

Fie p un număr prim şi k un număr care nu este multiplu al lui p. Atunci:

$$k^{p-1} \equiv 1 (\mathrm{mod}\, p)$$

Putem acum determina inversul multiplicativ folosind mica teoremă a lui Fermat. Presupunem că p este un număr prim şi considerăm un număr k care nu este multiplu al numărului p. Atunci, prin mica teoremă a lui Fermat, putem scrie:

$$k^{p-2} \cdot k \equiv 1 (\mathrm{mod}\, p)$$

Astfel k^{p-2} trebuie să fie inversul multiplicativ al lui k. De exemplu, presupunem că dorim să calculăm inversul multiplicativ al lui 6 modulo 17. Trebuie să calculăm pentru aceasta $rem(6^{15},17)$ şi vom folosi proprietăţile relaţiei de congruenţă modulo 17 astfel (toate congruenţele de mai jos sunt considerate a fi modulo 17):

$$6^2 \equiv 36 \equiv 2$$
$$6^4 \equiv (6^2)^2 \equiv 2^2 \equiv 4$$
$$6^8 \equiv (6^4)^2 \equiv 4^2 \equiv 16$$
$$6^{15} \equiv 6^8 \cdot 6^4 \cdot 6^2 \cdot 6 \equiv 16 \cdot 4 \cdot 2 \cdot 6 \equiv 3$$

Deci, $6^{15} \equiv 3 (\mathrm{mod}\, 17)$, adică $rem(6^{15},17) = 3$. Deci 3 este inversul multiplicativ al lui 6 modulo 17 întrucât

$$3 \cdot 6 \equiv 1 (\mathrm{mod} 17)$$

În general, dacă lucrăm cu relaţia de congruenţă modulo p, unde p este un număr prim, găsirea unui invers multiplicativ încercând fiecare valoare între 1 şi *p-1* necesită aproape p operaţii. Cu toate acestea, abordarea de mai sus cere numai $2\log(p)$ operaţii.

În cazul în care se cunosc atât mesajul original (m), cât şi mesajul criptat, folosind a doua variantă a codului Turing, (m^*) în care:

- la codare avem

$$m^* \equiv mk (\mathrm{mod}\, p)$$

- la decodare avem:

$$m = rem(m^* k^{-1}, p)$$

Dacă avem ambele mesaje la dispoziţie se poate calcula:

$$m^{p-2} \cdot m^* \equiv m^{p-2} \cdot rem(mk, p) \equiv m^{p-2} \cdot mk \pmod{p} \equiv m^{p-1} \cdot k \pmod{p} \equiv k \pmod{p}$$

Astfel se poate determin valoarea lui *k* şi se poate decripta orice mesaj.

RSA (MIT – 1977)

Destinatarul are atât o cheie secretă, pe care o păstrează la el, cât şi o cheie publică pe care o distribuie cât mai mult posibil. Transmiţătorul criptează mesajul folosind cheia publică, apoi se decriptează mesajul folosind cheia privată. RSA nu lucrează modulo un număr prim, ci modulo produsul a două numere foarte mari.

Definiţie. Două numere întregi *a* şi *b* sunt prime între ele (relativ prime) dacă şi numai dacă au cel mai mare divizor comun al lor egal cu 1 (cmmdc(a,b) = 1).

Rezultatele descrise în Lemma 1 şi Lemma 2 (care lucrează cu numere prime) pot fi extinse şi pentru numere prime între ele.

Lemma 3. *Fie n un întreg pozitiv. Dacă numărul k este prim cu n, atunci există un întreg* k^{-1} *astfel încât:*

$$k \cdot k^{-1} \equiv 1 \pmod{n}$$

Corolar. *Fie n un întreg pozitiv şi k un număr prim cu n. Dacă*

$$ak \equiv bk \pmod{n}$$

atunci

$$a \equiv b \pmod{n}$$