Divizibilitate

Motto : Un număr divizibil este ca o dreaptă paralelă sau un informatician nematematician

I. Câteva probleme simple şi cunoscute

1) Găsiți toate numerele X de n cifre ($n \le 10000$) cu proprietatea că X este divizibil cu produsul cifrelor şi X+1 este de asemenea divizibil cu produsul cifrelor sale.

2) Calculați $1+a+a2+a3+\ldots+ab \bmod 9901$ ($a,b \le 50000000$)

3) Descompuneți numărul natural n într-o sumă de numere naturale $n=x_1+x_2+\ldots+x_p$ astfel ca cel mai mic multiplu comun al numerelor $x_1, x_2, \ldots x_p$ să fie maxim ($n \le 1000$)

4) Găsiți cel mai mic număr natural, format numai din cifre de 1, divizibil cu $n \le 1000000$.

Presupun că toată lumea a întâlnit aceste probleme.

Comentarii:
1) Un număr nenul nu e divizibil cu 0, deci pentru $X=\overline{c_1 \cdot c_2 \cdot c_3 \cdot \ldots \cdot c_n}$, avem $x_n \neq 0$, dar şi $x_n \neq 9$. Conform unei proprietăți simple (vezi mai jos), dacă X e divizibil cu $c_1 \cdot c_2 \cdot \ldots \cdot c_n$ şi X+1 e divizibil cu $\overline{c_1 \cdot c_2 \cdot \ldots \cdot (c_n+1)}$, atunci diferența lor e divizibilă cu $c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1}$, deci numerele sunt de forma $\overline{111\ldots111c_n}$.

2) Dacă a e divizibil cu 9901 rezultatul e 1, altfel resturile lui $a^k : 9901$ se repetă ($a^{9900} : 9901$ dă restul 1 – vezi tot mai jos). Deci trebuie să calculăm doar $1+a+a^2+\ldots+a^{9899} \bmod 9901$, apoi să înmulțim rezultatul cu [b/9900], să mai adunăm $1+a+a^2+\ldots+a^{b \bmod 9900}$ şi să luăm restul.

3) Numerele x_i vor fi de forma $x_i=p_i^{ei}$, cu p_i număr prim, iar exponentul e_i destul de mic. Dacă un termen x_i ar avea 2 divizori primi între ei, $x_i=u \cdot v$, cum $u+v<u \cdot v$ am putea lua $n=x_1+\ldots+x_{i-1}+u+v+x_{i+1}+\ldots+x_p+$rest, iar noul cmmmc ar fi cel puțin egal cu cel inițial. Se poate vedea că termenii vor fi puteri ale numerelor prime mai mici ca 100, mai mult, doar 2,3,5 şi 7 pot fi la puteri mai mari ca 1 (11^2 ar putea fi înlocuit cu 11+101, care ar da cmmmc mai mare). Avem o descompunere optimă de forma $2^a+3^b+5^c+7^d+11e+13e'+\ldots+97e"$, unde e,e',e" sunt 0 sau 1; se poate găsi uşor cel mai mare termen al sumei.(de ex. 97 nu apare de loc)

4) Dacă n e divizibil cu 2 sau 5 (divizorii lui 10) nu există un astfel de multiplu.
Altfel căutăm :

```
r=1 ; k=1
cât timp r mod n≠0
              {r=(r*10+1) mod n ;
               n=n+1;}
```

Dar dacă am fi luat $n \le 10^9$, de exemplu n=987654321, metoda nu pare prea eficientă. Vezi continuarea.

II. Puțină teorie

A. Proprietăți simple

- dacă a şi b sunt divizibile cu n atunci şi ax+by este divizibil cu n, oricare ar fi x,y∈ **Z** (de altfel peste tot va fi vorba numai de numere întregi).

- dacă a este divizor al lui b avem (x mod b) mod a = x mod a

- dacă p este prim şi a nu e divizibil cu p mulțimea {a mod p, 2a mod p,…,(p–1)a mod p} = {1,2,3,…,p–1}- adică numerele ka dau resturi diferite la împărțirea la p, pentru k=1,2,..p–1

- dacă $N=p_1^{a1}\cdot p_2^{a2}\cdot\ldots\cdot p_k^{ak}$ este descompunerea lui N în factori primi, numărul divizorilor (pozitivi) ai lui N este $(a1+1)\cdot(a2+1)\cdot\ldots\cdot(ak+1)$

- suma divizorilor pozitivi ai lui N este $(1+p_1+p_1^2+\ldots+p_1^{a1})\cdot\ldots\cdot(1+p_k+p_k^2+\ldots+p_k^{ak})$, sumele progresiilor geometrice din paranteze pot fi scrise mai scurt.

- numărul numerelor prime mai mici ca n este ≈ n/ln n

- numărul numerelor prime cu N şi mai mici ca N (indicatorul φ(N) a lui Euler) este $N\cdot(1-1/p_1)\cdot(1-1/p_2)\cdot\ldots\cdot(1-1/p_k)$

- (p–1) !+1 este divizibil cu p dacă şi numai dacă p este număr prim

- n! este aproximativ egal cu $(n/e)^n\cdot\sqrt{2\pi n}$, de aici obținem ln n !=ln 1+ln 2+…+ln n ≈ n·(ln n –1)+1/2·(ln n + 6.28) cu o eroare foarte mică pentru n>20.

B. Proprietăți legate de cmmdc

- $cmmdc(a_1,a_2,\ldots,a_n)=cmmdc(cmmdc(a_1,a_2,\ldots,a_{n-1}), a_n)$ (acelaşi lucru este valabil şi pentru cmmmc)

- cmmdc(a,b)·cmmmc(a,b)=a·b (nu mai e valabil pentru $cmmdc(a_1,a_2,a_3)$!)

- dacă cmmdc(a,b)=d există x,y∈Z astfel ca d=ax+by, numerele x şi y pot fi calculate tot prin algoritmul lui Euclid (forma extinsă) :

- analog pentru n numere: $cmmdc(a_1,a_2,\ldots,a_n)=a_1x_1+a_2x_2+\ldots+a_nx_n$, cmmdc fiind cel mai mic număr natural nenul care poate fi scris ca o combinație liniară a numerelor $a_1,\ldots a_n$

- $cmmdc(F_m, F_n) = F_{cmmdc(m,n)}$, F_i fiind al i-lea termen al şirului lui Fibonacci

- calculul cmmdc(a,b) cu algoritmul lui Euclid are complexitatea O(lg min(a,b))

C. Proprietăți legate de puteri

- Teorema (mică) a lui Fermat : dacă p este prim şi a nu e divizibil cu p atunci a^{p-1} mod p=1. Resturile a mod p, a^2 mod p,…a^{p-1} mod p nu sunt însă neapărat distincte

- dacă a^x mod p=1 şi x e cel mai mic exponent pentru care obținem restul 1, avem a^y mod p=1 dacă şi numai dacă y e divizibil cu x

- $cmmdc(a^x-1, a^y-1) = a^{cmmdc(x,y)}-1$

- $a^{\varphi(n)}$ mod n = 1, dacă a nu e divizibil cu n (teorema lui Euler, generalizarea micii teoreme a lui Fermat)

- dacă n este de forma p^k, cu p prim impar şi k≥1 (dar şi în alte cazuri, de ex. n=2,4 sau $2p^k$) există m,1<m<n astfel ca m, m^2, m^3, …, m^{n-1} să dea resturi diferite prin împărțirea la n (se zice că m este o rădăcină primitivă în $\mathbf{Z}_n$).

III. Algoritmi elementari de teoria numerelor

1. Algoritmul Euclid extins(a,b)

Să se determine d=cmmdc(a,b) şi x,y∈ **Z** pentru care ax+by=d :

```
Euclid extins(a,b)
dacă b=0 returnează (a,1,0)
altfel (d',x',y')=Euclid extins(b, a mod b)
          returnează (d',y',x'-[a/b]·y')
```

2. Determinarea ordinului unui număr

ord(a)=cel mai mic număr nenul pentru care $a^{ord(a)}$ mod p = 1, sau a invesului lui a modulo p :

```
calculează q=φ(p)
pentru i=2, q/2
   dacă q divizibil cu i
      calculează R=ai mod p
      dacă R mod p=1 returnează i
returnează q
```

3. Rezolvarea ecuației ax mod n = b

```
Rezolv(a,b,n)
      (d,x,y) = Euclid-extins(a,n)
      dacă d mod b=0
         x0=x·b/d mod n
         pentru i=0, d-1
            scrie x0+i·n/d
      altfel
        scrie "fără soluţie"
```

4. Teorema chineză a resturilor

Fie n_1, n_2, …, n_k k numere naturale prime două câte două. Atunci sistemul : x mod $n_1=b_1$, x mod $n_2=b_2$,…, x mod $n_k=b_k$, are soluție unică modulo $n_1 \cdot n_2 \cdot \ldots \cdot n_k$. Soluția este $b_1 \cdot q_1^{\varphi(n1)} + b_2 \cdot q_2^{\varphi(n2)} + \ldots + b_k \cdot q_k^{\varphi(nk)}$ mod $(n_1 \cdot n_2 \cdot \ldots \cdot n_k)$, unde $q_i=(n_1 \cdot n_2 \cdot \ldots \cdot n_k)/n_i$, iar φ este indicatorul lui Euler.

```
Algoritm chinez(b1,b2,n1,n2) - pentru k=2
          n=n1·n2
         a=(n2-n1) mod n
         dacă a<0   a=a+n
         b=(n2·b1-n1·b2) mod n
        dacă b<0   b=b+n
 rezolv(a,b,n);
```

5. Testul de primalitate Miller-Rabin

```
Prim(n,s)
(bk,bk-1,…,b0) = reprezentarea binară a lui n-1
pentru j=1,s
  a=random(n)
  d=1
  pentru i=k,0,-1
    x=d; d=d·d mod n
    dacă d=1 şi x≠1 şi x≠n-1
      returnează COMPUS
    dacă bi=1  d=d·a mod n
  sf.
  dacă d≠1 returnează COMPUS
sf.
returnează PRIM (aproape sigur, cu probabilitate > 1-2-s )
```

IV. Câteva probleme mai necunoscute

1. Divizor şi multiplu

Se citesc n+1 numere naturale $x_1, x_2,\ldots,x_{n+1}$, $1\le x_i\le 2n$. Găsiți j,k∈ **N**, $1\le j,k\le n+1$, $j\ne k$, astfel ca x_j să fie divizibil cu x_k. Dacă nu există astfel de numere afişaţi 0 0. Dacă există mai multe soluții posibile afişaţi cele mai mari numere posibile. Restricție : n≤60000.
Exemplu ; pentru n=5 şi 4,6,7,8,9,10 se afişează 4 8

Rezolvare : Se ordonează şirul în ordine crescătoare a părții impare a termenilor (numim parte impară a lui x factorul y din descompunerea în factori $x=2^k\cdot y$, y impar). Parcurgând şirul ordonat trebuie să găsim doi termeni cu aceeaşi parte impară (pentru numere între 1 şi 2n sunt posibile n părți impare). (Sau o încercare în O(n) – se face un heap, verificăm vârful, e 2n?)

2. Submulțime

Se dă un şir de 2n–1 numere naturale; alegeți n numere a căror sumă să fie divizibilă cu n ($n<10^6$). Dacă nu există soluție afişaţi n cifre de 0, dacă sunt mai multe soluții afişati una oarecare.
Exemplu : Pentru n=5 şi 3,4,5,7,8,9,11,12,13 se poate afişa 4,5,7,8,11

Rezolvare : E suficient să arătăm cu se găseşte soluție pentru n prim, pentru că dacă ştim să găsim soluție pentru n_1 şi n_2, putem găsi o soluție şi pentru $n=n_1\cdot n_2$. Problema va avea deci întotdeauna soluție.

3. Bancnote curioase

Avem bancnote de p şi q lei. Câte valori din intervalul [a,b] nu se pot plăti cu astfel de bancnote? ($1\le p,q\le 1000$; $1<a<b<1000000$)
Exemplu : pentru bancnote de 3 şi 5 lei şi intervalul [5,15] se va afişa 10.

Rezolvare : dacă cmmdc(p,q)>1 evident nu se pot plăti sume nedivizibile cu d, reducem acest caz la cel cu p şi q prime între ele luând intervalul [[a/d]+1, [b/d]] şi bancnote de valori p/d şi q/d. În acest caz se ştie că orice număr t poate fi scris t=px+qy, unde x sau y pot fi negativi. dar pentru t>pq–p–q există o scriere cu x şi y pozitivi, rămâne să verificăm numerele mai mici ca pq–p–q.

4. Fracții raționale

Se citesc din fişierul de intrare numerele n şi m. Aflați câte fracții raționale ireductibile de forma a/b, cu $0\le a\le n$ şi $0<b\le n$ există. Afişaţi un sfert din aceste fracții, în ordine crescătoare, începând cu a m-a fracție şi mergând din 4 în 4. ($1<m<n\le 500$).
Exemplu : Pentru n=5, m=2 se va afişa : 11 şi 1/3 1/2 2/3 4/5

Rezolvare : Se construieşte şirul cerut pornind cu şirul 0/1 1/1, apoi între fiecare doi termeni se scrie fracția obținută adunând numărătorii, respectiv numitorii termenilor respectivi; se obține succesiv : 0/1 1/2 1/1, apoi 0/1 1/3 1/2 2/3 1/1, etc. Se pot da şi formule de recurență pentru fracțiile şirului obținut după n paşi, observând că $x_{k+1}\cdot y_k - x_k\cdot y_{k+1}=1$: $x_0=0$, $x_1=y_0=1$, $y_1=n$, $x_{k+2}=[(y_k+n)/y_{k+1}]\cdot x_{k+1}-x_k$, $y_{k+2}=[(y_k+n)/y_{k+1}]\cdot y_{k+1}-y_k$.

5. Se dau numerele m şi n. Calculați F_m mod n ($m,n\le 10^9$).
Exemplu m=5, n=3, se va afişa 2

Rezolvare: Considerăm matricea $M=\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$. Matricele M^2, M^3, conțin termenii şirului lui Fibonacci şi se poate calcula M^m folosind reprezentarea binară a lui m. Evident, de fiecare dată luăm valorile modulo n, ceea ce evită calculele cu numere mari.

V. Probleme deschise

1. Numere congruente
Se dă n natural. Aflați dacă există un triunghi dreptunghic de arie n, cu laturile de lungimi raționale, adică există numerele naturale a,b,c,d,e,f astfel ca $(a/b)^2+(c/d)^2=(e/f)^2$ şi n=ac/2bd.

2. Fracții egiptene
Se consideră fracția a/b, ($1 \le a < b \le 1000$). Găsiți numărul minim de întregi pozitivi n_1, n_2,…, n_k distincți astfel ca $a/b=1/n_1+1/n_2+\ldots+1/n_k$.

3. Conjectura lui Catalan
Găsiți două puteri consecutive, adică numere naturale a,b>1 şi p,q>1 astfel ca $a^p-b^q=1$ (în afară de soluția $3^2-2^3=1$).

4. Spargerea codurilor
Se dă un număr X. Găsiți $a,b \in \mathbf{N}$, a,b>1 astfel ca $a \cdot b=X$

VI Problemă de baraj

Se consideră n becuri aşezate în formă de cerc, unele aprinse altele stinse. Singura operație posibilă cu aceste becuri este schimbarea stării a k becuri consecutive (din aprins în stins şi invers).

Cerință
Dându-se două configurații de becuri să se precizeze dacă se poate trece din prima configurație în a doua prin mai multe astfel de operații

Date de intrare
Fişierul becuri.in conține pe prima linie numerele n şi k, pe linia a doua n cifre de 0 sau 1 reprezentând starea inițială a becurilor iar pe linia a treia alt şir de 0 şi 1, starea finală. Numerele de pe aceeaşi linie sunt separate de câte un spațiu.

Date de ieşire
Fişierul de ieşire becuri.out va conține, dacă nu e posibilă trecerea din prima stare în a doua numărul 0. Dacă e posibilă se va scrie numărul de operații pe prima linie, iar pe următoarele linii operațiile precizate prin numărul de ordine al celui mai mic bec din secvența de k becuri care-şi schimbă starea.

Exemplu

becuri.in	becuri.out
10 3 1 0 0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0	2 1 3

Restricții
$1 \le k < n \le 100000$.

Comentariu
Dacă avem k mic, rezolvarea e cunoscută, dar aşa încercăm un algoritm de pattern matching? Algoritmul comisiei e liniar, dar prea savant (dar e în temă). Se asociază fiecărei configurații un şir de 0 şi 1, care ne arată dacă două şiruri sunt echivalente.

VII. Bibliografie

1. E. Morozova, I. Petrov, V. Skvorțov – Olimpiadele internaționale de matematică, Ed. Tehnică Bucureşti 1978
2. H. Banea – Probleme de matematică traduse din revista sovietică Kvant, Ed. Didactică şi Pedagogică Bucureşti 1983
3. T. Cormen, C. Leiserson, R. Rivest – Introducere în algoritmi, Ed. Agora Cluj 2000
4. D. Knuth – Tratat de programare a calculatoarelor. Algoritmi seminumerici, Ed. Tehnică Bucureşti 1983
5. Gazeta matematică seria B, 1980 –2000
6. GInfo 1998 - 2002