

## Temă pentru acasă - partea C.

14 puncte

**C1. (4 puncte - Las Vegas)** Presupunem că avem un tablou  $x$  cu elemente numere întregi și căutăm în el un întreg,  $a$ , care apare de cel puțin  $k$  ori în acest tablou (care are lungimea  $n$ ).

- (a) **(2 puncte)** Implementați următorul algoritm aleator pentru determinarea unui index al unei apariții a lui  $a$  în  $x$ :

```
found = false;
while (!found) do
    alege uniform  $i \in \{1, 2, \dots, n\}$ ;
    if ( $x[i] = a$ ) then
        return  $i$ ;
    end if
end while
```

- (b) **(2 puncte)** Alegeți un tablou de lungime  $n \geq 200$  în care  $a$  apare de  $k = 10$  ori. Apelați această procedură de  $N = 100$  de ori și determinați numărul mediu de iterații while; comparați rezultatul cu media numărului de iterații while în cazul cel mai nefavorabil care este  $n/k$ .

**C2. (3 puncte - Las Vegas)** Implementați algoritmul aleator pentru determinarea mediei.

**C3. (3 puncte - Monte Carlo)** Se consideră  $f(X)$ ,  $g(X)$  și  $h(X)$  trei polinoame de grade  $n$ ,  $n$  și, respectiv,  $2n$ .

- (a) **(2 puncte)** Implementați următorul algoritm aleator pentru testarea egalității  $f \cdot g = h$ :

```
alege uniform  $p \in \{1, 2, \dots, 3n\}$ ;
if ( $f(p) \cdot g(p) = h(p)$ ) then
    return true;
else
    return false;
end if
```

- (b) **(1 punct)** Să presupunem că această procedură greșește cu o probabilitate de cel mult  $2/3$ . De câte ori trebuie apelată această procedură pentru a reduce probabilitatea de a greși sub 0.0001?

*Indicație. Un polinom de grad  $k$  poate fi reprezentat printr-un tablou de lungime  $k + 1$  al coeficienților.*

**C4. (4 puncte - Monte Carlo)** Implementați următorul algoritm aleator pentru a decide primalitatea unui număr natural (impar) dat,  $n$ :

```
determină  $k, m \in \mathbb{N}$  s. t.  $n - 1 = 2^k m$ ;
alege uniform  $a \in \{2, 3, \dots, n - 2\}$ ;
 $b = a^m \pmod n$ ;
for ( $i = 1, k$ ) do
    if ( $(b \neq 1)$  and  $(b \neq n - 1)$ ) then
        return false;
    else if ( $b = n - 1$ ) then
        return true;
    end if
     $b = b^2 \pmod n$ ;
```

```
end for
if ( $b \neq 1$ ) then
  return false;
else
  return true;
end if
```

Rezolvările acestor exerciții (funcțiile R și apelurile lor) vor fi redactate într-un singur script R.