1. Utilizând Teorema Chineză a Resturilor, să se rezolve sistemul de ecuaţii:

$$\begin{cases} x & \equiv & 2 \ mod \ 3 \\ x & \equiv & 3 \ mod \ 4 \\ x & \equiv & 4 \ mod \ 7 \end{cases}$$

(25p)

Soluţie:
Numerele 3, 4, 7 sunt coprime două câte două, deci se poate aplica Teorema Chineză a Resturilor.

(I) Se calculează $m = 3 \cdot 4 \cdot 7 = 84$, $c_1 = \frac{m}{3} = 28$, $c_2 = \frac{m}{4} = 21$, $c_3 = \frac{m}{7} = 12$;

(II) Se rezolvă ecuaţiile

- $28x \equiv 2 \ mod \ 3 \Leftrightarrow x \equiv 2 \ mod \ 3 \Rightarrow x_1 = 2$;
- $21x \equiv 3 \ mod \ 4 \Leftrightarrow x \equiv 3 \ mod \ 4 \Rightarrow x_2 = 3$;
- $12x \equiv 4 \ mod \ 7 \Leftrightarrow 5x \equiv 4 \ mod \ 7 \Rightarrow x_3 = 5$;

(III) Soluţia sistemului se obţine astfel:

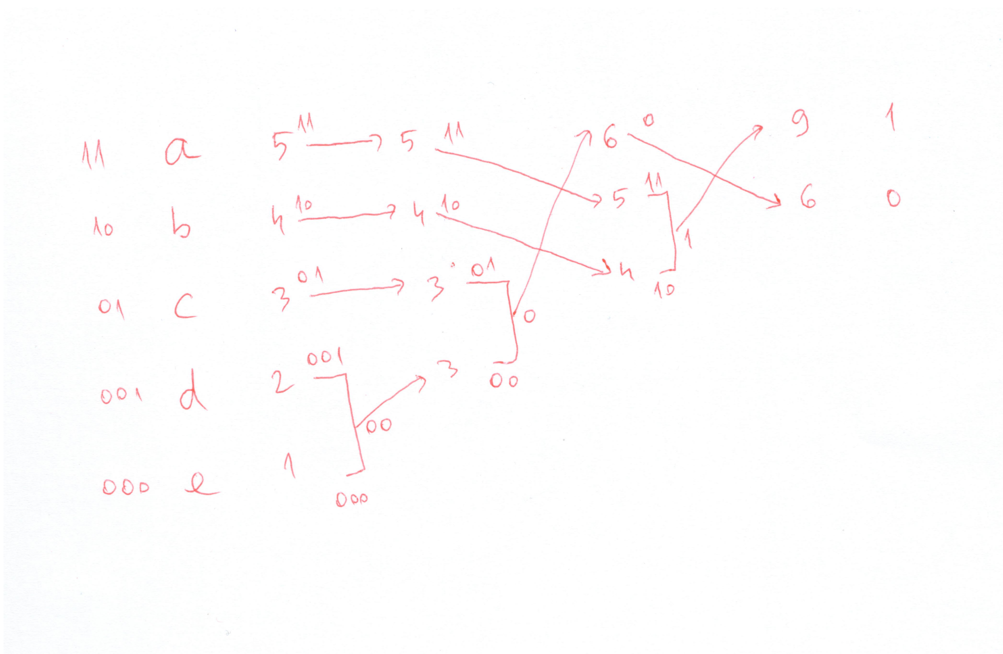
$$\begin{aligned} x_0 &= (c_1x_1 + c_2x_2 + c_3x_3) \ mod \ m \\ &= (28 \cdot 2 + 21 \cdot 3 + 12 \cdot 5) \ mod \ 84 \\ &= 179 \ mod \ 84 \\ &= \mathbf{11} \end{aligned}$$

2. Codificaţi şirul *aababcabcdabcde* folosind varianta clasică a algoritmului Huffman. (25p)

Soluţie:
Sursa de informaţii ataşată şirului este:

A	a	b	c	d	e
π	5	4	3	2	1

Aplicând algoritmul Huffman obţinem:



Astfel, codificarea finală va fi:

$$111110111001111001001111001001000$$

3. Definiţi ordinul unui element într-un grup finit şi demonstraţi următoarele proprietăţi ale acestuia:

   Fie $\mathbf{G}$ un grup finit şi $a \in \mathbf{G}$.

   (a) Dacă $a^k = e$ atunci $ord_{\mathbf{G}}(a) \mid k$, pentru orice număr întreg k. Justificaţi faptul că $ord_{\mathbf{G}}(a) \mid |\mathbf{G}|$;

   (b) Pentru orice număr întreg k, are loc proprietatea

$$ord_{\mathbf{G}}(a^k) = \frac{ord_{\mathbf{G}}(a)}{(ord_{\mathbf{G}}(a), k)}.$$

(25p)

Soluţie:

$$ord_{\mathbf{G}}(a) = |<a>_{\mathbf{G}}| = min(\{n \in \mathbf{N}^* | a^n = e\})$$

(a) Conform Teoremei Împărţirii cu Rest, avem $k = q \cdot ord_{\mathbf{G}}(a) + r$, unde $0 \leq r < ord_{\mathbf{G}}(a)$. Vom obţine

$$\begin{aligned} e &= a^{q \cdot ord_{\mathbf{G}}(a) + r} \\ &= \left(a^{ord_{\mathbf{G}}(a)}\right)^q \cdot a^r \\ &= a^r \end{aligned}$$

Rezultă că $r = 0$ (altfel, s-ar contrazice minimalitatea lui $ord_{\mathbf{G}}(a)$) şi, în final, că $ord_{\mathbf{G}}(a) \mid k$.

Relaţia $ord_{\mathbf{G}}(a) \mid |\mathbf{G}|$ rezultă din Teorema lui Lagrange (ordinul subgrupului indus de a divide ordinul grupului).

(b) Notăm $m = \frac{ord_{\mathbf{G}}(a)}{(ord_{\mathbf{G}}(a),k)}$. Trebuie să demonstrăm că m este cel mai mic număr natural nenul cu proprietatea $\left(a^k\right)^m = e$.

- $\left(a^k\right)^m = \left(a^k\right)^{\frac{ord_{\mathbf{G}}(a)}{(ord_{\mathbf{G}}(a),k)}} = \left(a^{ord_{\mathbf{G}}(a)}\right)^{\frac{k}{(ord_{\mathbf{G}}(a),k)}} = e$ (am folosit faptul că $a^{ord_{\mathbf{G}}(a)} = e$);
- Presupunem, prin reducere la absurd, că există $0 < n < m$ astfel încât $(a^k)^n = e$. Obţinem $a^{kn} = e$, ceea ce implică, conform punctului (a), că $ord_{\mathbf{G}}(a) \mid kn$, sau, echivalent, $m \mid \frac{k}{(ord_{\mathbf{G}}(a),k)} n$ (am împărţit cu $(ord_{\mathbf{G}}(a), k)$). Deoarece m şi $\frac{k}{(ord_{\mathbf{G}}(a),k)}$ sunt coprime, rezultă că $m \mid n$, ceea ce constituie o contradicţie (deoarece am considerat $0 < n < m$). Astfel rezultă şi minimalitatea lui m.

4. Determinaţi semantica programului S, sub interpretarea uzuală pe $\mathbf{N}$:

$$(S) \qquad z := 0;\ \texttt{while}\ \neg(x = 0)\ \texttt{do}\ (z := z + y;\ x := x - 1)$$

(25p)

Soluţie:

Vom nota

$$\begin{array}{lcl} S_1 & = & z := 0 \\ S_2 & = & \texttt{while}\ \neg(x = 0)\ \texttt{do}\ S_3 \\ S_3 & = & z := z + y;\ x := x - 1 \end{array}$$

Fie γ o asignare (stare) arbitrară. Dacă $\gamma = \perp$ atunci $\phi_{\mathcal{I}}(S)(\gamma) = \perp$. Altfel

$$\begin{array}{lcl} \phi_{\mathcal{I}}(S)(\gamma) & = & \phi_{\mathcal{I}}(S_1; S_2)(\gamma) \\ & = & \phi_{\mathcal{I}}(S_2)(\phi_{\mathcal{I}}(S_1)(\gamma)) \\ & = & \phi_{\mathcal{I}}(S_2)(\phi_{\mathcal{I}}(z := 0)(\gamma)) \\ & = & \phi_{\mathcal{I}}(S_2)(\gamma[z/\mathcal{I}_0(0)]) \\ & = & \phi_{\mathcal{I}}(S_2)(\gamma[z/0]) \end{array}$$

Vom evalua mai departe $\phi_{\mathcal{I}}(S_2)(\gamma')$, pentru o asignare (stare) arbitrară γ':

$$\begin{array}{lcl} \phi_{\mathcal{I}}(S_2)(\gamma') & = & \phi_{\mathcal{I}}(\texttt{while}\ \neg(x = 0)\ \texttt{do}\ S_3)(\gamma') \\ & = & \begin{cases} \gamma', & \text{dacă } \mathcal{I}(\neg(x = 0))(\gamma') = 0, \\ \phi_{\mathcal{I}}(\texttt{while}\ \neg(x = 0)\ \texttt{do}\ S_3)(\phi_{\mathcal{I}}(S_3)(\gamma')), & \text{dacă } \mathcal{I}(\neg(x = 0))(\gamma') = 1 \end{cases} \\ & = & \mu(F)(\gamma'), \quad \text{unde} \\ F(f)(\gamma') & = & \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ f(\phi_{\mathcal{I}}(z := z + y;\ x := x - 1)(\gamma')), & \text{dacă } \gamma'(x) \neq 0 \end{cases} \end{array}$$

Cel mai mic punct fix al funcţiei F va fi determinat folosind construcţia din Teorema de Punct Fix:

$$\mu(F) = sup(\{\underbrace{F^i(\perp)}_{f_i} | i \in \mathbf{N}\}).$$

Mai exact, vom avea $f_0(\gamma') = \perp$ şi $f_{i+1}(\gamma') = F(f_i)(\gamma')$, pentru orice asignare (stare) γ'.

Vom determina mai întâi câteva elemente ale acestui lanţ. Pentru a uşura notaţia, vom introduce un şir de asignări definit recursiv după cum urmează:

$$\begin{array}{lcl} \gamma'_{modif(0)} & = & \gamma', \\ \gamma'_{modif(i+1)} & = & \gamma'_{modif(i)}[z/(\gamma'_{modif(i)}(z) + \gamma'_{modif(i)}(y))][x/(\gamma'_{modif(i)}(x) - 1)], \forall i \geq 0. \end{array}$$

Vom nota $\gamma'_{modif(1)}$ şi prin γ'_{modif}.

Se poate demonstra uşor prin inducţie că au loc relaţiile:

$$\begin{array}{lcl} \gamma'_{modif(i)}(x) & = & \gamma'(x) - i, \\ \gamma'_{modif(i)}(y) & = & \gamma'(y), \\ \gamma'_{modif(i)}(z) & = & \gamma'(z) + i \cdot \gamma'(y), \end{array}$$

pentru $\forall 1 \leq i \leq \gamma'(x)$.

Vom obţine

$$\begin{array}{lcl} f_1(\gamma') & = & F(f_0)(\gamma') \\ & = & \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ \perp, & \text{dacă } \gamma'(x) \neq 0, \end{cases} \end{array}$$

$$\begin{array}{lcl} f_2(\gamma') & = & F(f_1)(\gamma') \\ & = & \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ f_1(\gamma'_{modif}), & \text{dacă } \gamma'(x) \neq 0, \end{cases} \\ & = & \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ \gamma'_{modif}, & \text{dacă } \gamma'_{modif}(x) = 0, \\ \perp, & \text{altfel} \end{cases} \\ & = & \begin{cases} \gamma'_{modif(0)}, & \text{dacă } \gamma'(x) = 0, \\ \gamma'_{modif(1)}, & \text{dacă } \gamma'(x) = 1, \\ \perp, & \text{altfel} \end{cases} \end{array}$$

$$
\begin{aligned}
f_3(\gamma') &= F(f_2)(\gamma') \\
&= \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ f_2(\gamma'_{modif}), & \text{dacă } \gamma'(x) \neq 0, \end{cases} \\
&= \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ \gamma'_{modif}, & \text{dacă } \gamma'_{modif}(x) = 0, \\ (\gamma'_{modif})_{modif}, & \text{dacă } \gamma'_{modif}(x) = 1, \\ \perp, & \text{altfel} \end{cases} \\
&= \begin{cases} \gamma'_{modif(0)}, & \text{dacă } \gamma'(x) = 0, \\ \gamma'_{modif(1)}, & \text{dacă } \gamma'(x) = 1, \\ \gamma'_{modif(2)}, & \text{dacă } \gamma'(x) = 2, \\ \perp, & \text{altfel} \end{cases}
\end{aligned}
$$

Vom demonstra prin inducţie că, oricare ar fi $i \geq 0$, are loc relaţia

$$
f_i(\gamma') = \begin{cases} \gamma'_{modif(j)}, & \text{dacă } \gamma'(x) = j,\ 0 \leq j \leq i-1, \\ \perp, & \text{altfel} \end{cases}
$$

- pasul de bază - simplă verificare;
- pasul inductiv - fie $i \geq 0$ arbitrar - presupunem că f_i are forma propusă. Pentru a demonstra că şi f_{i+1} are forma corespunzătoare vom folosi relaţia de recurenţă:

$$
\begin{aligned}
f_{i+1}(\gamma') &= F(f_i)(\gamma') \\
&= \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ f_i(\gamma'_{modif}), & \text{dacă } \gamma'(x) \neq 0, \end{cases}
\end{aligned}
$$

$$
\begin{aligned}
&= \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ (\gamma'_{modif})_{modif(j)}, & \text{dacă } \gamma'_{modif}(x) = j,\ 0 \leq j \leq i-1, \\ \perp, & \text{altfel} \end{cases} \\
&= \begin{cases} \gamma', & \text{dacă } \gamma'(x) = 0, \\ \gamma'_{modif(j+1)}, & \text{dacă } \gamma'(x) = j+1,\ 0 \leq j \leq i-1, \\ \perp, & \text{altfel} \end{cases} \\
&= \begin{cases} \gamma'_{modif(j)}, & \text{dacă } \gamma'(x) = j,\ 0 \leq j \leq (i+1)-1, \\ \perp, & \text{altfel} \end{cases}
\end{aligned}
$$

q.e.d.

Fie $\gamma(x) = n$. Vom obţine:

$$\begin{array}{rcl}\phi_{\mathcal{I}}(S)(\gamma) & = & \phi_{\mathcal{I}}(S_2)(\gamma'),\ \text{unde}\ \gamma' = \gamma[z/0] \\ & = & \mu(F)(\gamma') \\ & = & (sup(\{f_i | i \in \mathbf{N}\}))(\gamma') \\ & = & sup(\{f_i(\gamma') | i \in \mathbf{N}\}) \\ & = & \gamma'_{modif(n)},\end{array}$$

ceea ce va conduce în final la $\phi_{\mathcal{I}}(S)(\gamma) = \gamma[x/0][z/\gamma(x) \cdot \gamma(y)]$, pentru orice asignare (stare) γ.