

NR PRIME

2	3	5	7	11	13	17	19	23	29	31	41	43	47	53	59	61	67	71	
73	79	83	191	193	197	199	211	223	227	229	233	239	241	251	257	263	269	271	277
179	181	307	311	313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
283	293	419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503	521	541
547	557	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1005	1013	1019	1021	1021	1031	1033	1039	1049	1051	1061	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213	2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181	3187	3191	3203	3209	3217	3221	3229	3251	3257	
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643	3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797	3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889	3907

3911	3917	3919	3923	3929	3931	3943	3947	3967	3989	4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
4073	4079	4091	4093	4099	4111	4127	4129	4133	4139	4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
4241	4243	4253	4259	4261	4271	4273	4283	4289	4297	4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493	4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
4591	4597	4603	4621	4637	4639	4643	4649	4651	4657	4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831	4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003	5009	5011	5021	5023	5039	5051	5059	5077	5081	5087
5099	5101	5107	5113	5119	5147	5153	5167	5171	5179	5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
5281	5297	5303	5309	5323	5333	5347	5351	5381	5387	5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521	5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
5641	5647	5651	5653	5657	5659	5669	5683	5689	5693	5701	5711	5717	5737	5741	5743	5749	5779	5783	5791
5801	5807	5813	5821	5827	5839	5843	5849	5851	5857	5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
5953	5981	5987	6007	6011	6029	6037	6043	6047	6053	6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
6143	6151	6163	6173	6197	6199	6203	6211	6217	6221	6229	6247	6257	6263	6269	6271	6277	6287	6299	6301
6311	6317	6323	6329	6337	6343	6353	6359	6361	6367	6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
6481	6491	6521	6529	6547	6551	6553	6563	6569	6571	6577	6581	6599	6607	6619	6637	6653	6659	6661	6673
6679	6689	6691	6701	6703	6709	6719	6733	6737	6761	6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
6841	6857	6863	6869	6871	6883	6899	6907	6911	6917	6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
7001	7013	7019	7027	7039	7043	7057	7069	7079	7103	7109	7121	7127	7129	7151	7159	7177	7187	7193	7207
7211	7213	7219	7229	7237	7243	7247	7253	7283	7297	7307	7309	7321	7331	7349	7351	7369	7393	7411	
7417	7433	7451	7457	7459	7477	7481	7487	7489	7499	7507	7517	7523	7537	7541	7547	7549	7559	7561	
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643	7649	7669	7673	7681	7687	7691	7699	7703	7717	7723
7727	7741	7753	7757	7759	7789	7793	7817	7823	7829	7841	7853	7867	7873	7877	7879	7883	7901	7907	7919

- 4 numere prime sunt mai mici decât 10,
- 25 de numere prime sunt mai mici decât 100,
- 168 de numere prime sunt mai mici decât 1000,
- 1.229 numere prime sunt mai mici decât 10.000,
- 9.592 numere prime sunt mai mici decât 100.000,
- 17.984 numerele prime sunt mai mici decât 200.000,
- 25.997 numere prime sunt mai mici decât 300.000,

- 33.860 de numere prime sunt mai mici decât 400.000,
 - 41.538 numere prime sunt mai mici decât 500.000,
 - 49.098 numere prime sunt mai mici decât 600.000,
 - 56.543 de numere prime sunt mai mici decât 700.000,
 - 63.951 numere prime sunt mai mici decât 800.000,
 - 71.274 numere prime sunt mai mici decât 900.000,
 - 78.498 numere prime sunt mai mici decât 1.000.000.
- Aceasta întrebare se referă la găsirea unui număr x care să satisfacă ecuația $97x \equiv 1 \pmod{2021}$. Aici, notăm \equiv ca "congruent cu".
- Pentru a rezolva această ecuație, putem folosi teorema lui Euler și teorema micului lui Fermat, având în vedere că $2021 = 43 * 47$ este produsul a două numere prime. Din teorema lui Euler, $97^{\phi(2021)} \equiv 1 \pmod{2021}$, unde ϕ reprezintă funcția phi a lui Euler.
 - Calculând $\phi(2021)$: $\phi(2021) = \phi(43 * 47) = \phi(43) * \phi(47)$ (deoarece 43 și 47 sunt prime) $\phi(2021) = 42 * 46$ (deoarece $\phi(p) = p - 1$ pentru orice număr prim p)
 - Așadar, $\phi(2021) = 1932$.
- Însă, 97 și 2021 nu sunt prime între ele, deci teorema micului lui Fermat nu poate fi aplicată direct. Putem folosi inversul modular pentru a rezolva ecuația.
- Inversul modular al lui 97 în raport cu 2021 poate fi găsit folosind algoritmul extins Euclidean. Voi calcula acest lucru pentru tine. Folosind acest algoritm, găsim că inversul modular al lui 97 $(\text{mod } 2021)$ este 1229.
 - Deci, $x = 1229$ este soluția ecuației $97x \equiv 1 \pmod{2021}$.

Exercițiu

Lucru 1.1 $x = ?$ $x = \overline{0, 2020}$ așt $97 \cdot x \equiv 1 \pmod{2021}$

(1) Abă să găs. inversul lui $\overline{97}$ în $U(\mathbb{Z}_{2021})$, și rezolvare a.c. $97 \cdot x \equiv 1$ în $U(\mathbb{Z}_{2021})$

O să că $(97, 2021) = 1 \Rightarrow \overline{97} \in \text{inversele p.m.r. a.c. } U(\mathbb{Z}_{2021})$

U) $2021 : 97 = \begin{array}{|l|l|}\hline 20 & 81 \\ \hline 1 & 16 \\ \hline\end{array}$ rest

2) $97 : 81 = \begin{array}{|l|l|}\hline 1 & 16 \\ \hline 1 & 1 \\ \hline\end{array}$

3) $81 : 16 = \begin{array}{|l|l|}\hline 5 & 1 \\ \hline 1 & 0 \\ \hline\end{array}$

4) $16 : 1 = \begin{array}{|l|l|}\hline 16 & 1 \\ \hline 0 & 0 \\ \hline\end{array}$

$$\frac{A}{B} = 20 + \frac{1}{1 + \frac{1}{5}} = 20 + \frac{1}{6} = \frac{120 + 1}{6} = \frac{121}{6}$$

$$\frac{2021}{97} = \frac{121}{6} + \frac{(-1)^4}{97 \cdot 6} \Rightarrow \frac{2021 - 97 \cdot 125}{97 \cdot 6} = \frac{1}{97 \cdot 6}$$

$$\Leftrightarrow 121 \cdot 6 - 121 \cdot 125 = 1 \Leftrightarrow 1 \neq 1 \checkmark$$

$$97 \cdot (-1)^4 \cdot 125 = 1 \Rightarrow 97 \cdot \overline{125} = 1 \Rightarrow 97 \cdot \overline{(2021 - 97 \cdot 125)} = 1 \Rightarrow 97 \cdot \overline{1896} = 1 \Rightarrow$$

$$\Rightarrow x = 1896$$

L1.2 x - unic $\in \{0, 1, \dots, 428\}$ așt $x \equiv 2 \pmod{3}$ și $x \equiv 2 \pmod{11}$, $x \equiv 8 \pmod{13}$

$(3, 11, 13) = 1$ sunt coprime

rezolvare ① met. algebraic

→ lemnă clunegă a resturilor

②) sol. generale

$$x \equiv 2 \pmod{3} \Leftrightarrow x = 2 + 3a$$

$$x \equiv 2 \pmod{11} \Leftrightarrow x = 2 + 11b \Leftrightarrow 2 + 3a = 2 + 11b = 8 + 13c$$

$$x \equiv 8 \pmod{13} \Leftrightarrow x = 8 + 13c$$

$$2 + 3a = 2 + 11b \pmod{3}$$

$$2 \equiv 2 + 11b \pmod{3}$$

$$11b \equiv 0 \pmod{3} \Rightarrow 11b \equiv 3j \Rightarrow b \equiv 3k \pmod{11}$$

$$2 + 11 \cdot 3k = 8 + 13c \pmod{13}$$

$$2 + 33k \equiv 8 \pmod{13}$$

$$33k \equiv 6 \pmod{13}$$

$$-6k \equiv 6 \pmod{13}$$

$$-k \equiv 1 \pmod{13}$$

$$k \equiv -1 \equiv 12 \pmod{13} \Rightarrow$$

$$\Rightarrow b = 3 \cdot 12 = 36 \Rightarrow x = 2 + 11 \cdot 36 = 398 \Rightarrow \boxed{x = 398}$$

Ex 2 / Lucr.

verificare: $598 = 3 \cdot 132 + 2 \quad \checkmark$
 $598 = 11 \cdot 56 + 2 \quad \checkmark$
 $598 = 13 \cdot 30 + 8 \quad \checkmark$

② Mă generație:

$$m = 3 \cdot 11 \cdot 13 = 429$$

$$p_1 = 3; p_2 = 11; p_3 = 13$$

$$m_1 = \frac{m}{p_1} = 11 \cdot 13 = 143; m_2 = \frac{m}{p_2} = 3 \cdot 13 = 39; m_3 = \frac{m}{p_3} = 3 \cdot 11 = 33$$

• Mă căreia inversă lui m_{ij} : $\overline{m_{ij}} \cdot \overline{x}_l = \bar{1} \text{ (in } U(\mathbb{Z}_{p_i}))$

$$143 \cdot \overline{2}_1 = \bar{1} \text{ (in } U(\mathbb{Z}_3)) \Rightarrow \bar{2} \cdot \bar{2}_1 = \bar{1} \Rightarrow \bar{2}_1 = \bar{2}$$

$$59 \cdot \overline{2}_2 = \bar{1} \text{ (in } U(\mathbb{Z}_{11})) \Rightarrow \bar{6} \cdot \bar{2}_2 = \bar{1} \Rightarrow \bar{2}_2 = \bar{6}$$

$$33 \cdot \overline{2}_3 = \bar{1} \text{ (in } U(\mathbb{Z}_{13})) \Rightarrow \bar{7} \cdot \bar{2}_3 = \bar{1} \Rightarrow \bar{2}_3 = \bar{7}$$

$$x = \sum m_{ij} \cdot e_j \cdot a_i = 143 \cdot 2 \cdot 2 + 59 \cdot 2 \cdot 2 + 33 \cdot 2 \cdot 8 = 572 + 156 + 328 = 1056 \text{ (mod 429)}$$

$$a_1 = 2; a_2 = 2; a_3 = 8$$

$$\boxed{x = 398}$$

Lucr. 2
d. 2.1 Turbul împărțirii lui 2^{149} la 323 (echivalent: criptare lit.C folos.

RSA cu $n = 323$, $e = 149$ în alfabetul Latin (lit. de 26-litere)

① $n = 323 = 17 \cdot 19 \rightarrow p = 17$
 $q = 19$

$$e = 149$$

$$\varphi(n) = \varphi(323) = (p-1)(q-1) = (17-1)(19-1) = 16 \cdot 18 = 288$$

$$\left| \begin{array}{l} (e, \varphi(323)) \\ \rightarrow (e, \varphi(323)) \end{array} \right. \rightarrow$$

alfabet 26-litere $\Rightarrow 26^k < n \leq 26^{k+1} \Rightarrow 26^k < 323 \leq 26^{k+1}$

$$N = 2 \cdot 26^k = 2 \quad (\text{tacam } N \text{ în baza 26})$$

$$k=0 \Rightarrow 0 < 323 \leq 26^1$$

$$N^e \equiv Q \pmod{323} \Leftrightarrow 2^{149} \equiv Q \pmod{323}$$

- calculăm $2^{149} \equiv Q \pmod{323}$ din aproape în aproape cu ajutorul puterilor

$$2^2 \stackrel{323}{\equiv} 4 \stackrel{323}{\equiv} 4; 2^4 \stackrel{323}{\equiv} 4^2 \stackrel{323}{\equiv} 16; 2^8 \stackrel{323}{\equiv} (16)^2 \stackrel{323}{\equiv} 256; 2^{16} \stackrel{323}{\equiv} (256)^2 \stackrel{323}{\equiv} 290;$$

$$2^{32} \stackrel{323}{\equiv} (290)^2 \stackrel{323}{\equiv} 120; 2^{64} \stackrel{323}{\equiv} (120)^2 \stackrel{323}{\equiv} 188; 2^{128} \stackrel{323}{\equiv} (188)^2 \stackrel{323}{\equiv} 154$$

$$149 = 2^4 + 2^4 + 2^2 + 1 = 128 + 16 + 4 + 1$$

$$2^{149} = 2^{16} \cdot 2^{16} \cdot 2^4 \cdot 2^1 \stackrel{323}{=} 137 \cdot 290 \cdot 16 \cdot 2 \equiv 32 \Rightarrow \boxed{Q = 32}$$

$Q = 32 > 26^0 \Rightarrow Q$ va fi de forma xy

$$Q = (xy)_{26} = x \cdot 26^1 + y \cdot 26^0 = 32 \in 26 + 6 \Leftrightarrow \begin{cases} x = 1 \\ y = 6 \end{cases}$$

dici $C \xrightarrow{\text{RSA}} BG$

Lucrare 2 metul myersonului lui $6^{99} + 3^{99} + 2^{99} \pmod{101}$

$$\text{Obs. că } (6, 101) = 1, (3, 101) = 1, (2, 101) = 1$$

$$\text{din mdcf Fermat: } 6^{100} \equiv 3^{100} \equiv 2^{100} \equiv 1 \pmod{101}$$

notam $m = 6^{99} + 3^{99} + 2^{99}$ și împărțim pe linii cu 101 sau cu multipli de 101

$$6 \nmid 3 \nmid 2 \Rightarrow 6$$

$$6m = 6 \cdot 6^{99} + 2 \cdot 3 \cdot 3^{99} + 3 \cdot 2 \cdot 2^{99} \equiv \underbrace{6^{100}}_1 + \underbrace{2 \cdot 5^{100}}_1 + \underbrace{3 \cdot 2^{100}}_1 \equiv 1 + 2 + 1 + 2 + 1 = 6$$

dici $6m \equiv 6 \pmod{101} \quad | \Rightarrow m \equiv 1 \pmod{101}$ Restul e 1.
 $(6, 101) = 1$

Exercitare 3.1 calc. $\text{ord}(\bar{2})$ în grupul $(U(\mathbb{Z}_{47}), \cdot)$

Lucrare 3 notam $k = \text{ord}(\bar{2})$.

$$\text{P} \circledast \Rightarrow k \mid \text{card}(G)$$

$$\text{card}(G) = \phi(47) \quad | \Rightarrow \phi(47) = 47 - 1 = 46 \Rightarrow k \in \{1, 2, 23\}$$

47 - prim

$$\text{P} \circledast \Rightarrow \bar{2}^k \equiv \bar{1} \pmod{47}$$

$$\bar{2}^1 \neq \bar{1} \pmod{47}$$

$$\bar{2}^2 \neq \bar{1} \pmod{47}$$

$$\Rightarrow \bar{2}^{23} \equiv \bar{1} \pmod{47} \Rightarrow k = \boxed{23 = \text{ord}(\bar{2})}$$

5.9.21

$$\textcircled{1} \quad 17x \equiv 1 \pmod{107}$$

J

$$17x \equiv 1 \mid :17$$

$$102x \equiv 6 \equiv 141$$

$$17x \equiv 1 \mid :17$$

$$x \equiv 119x \equiv 7 \equiv -100 \mid :9$$

$$1 = 108x \equiv 63$$

$$x \equiv 63$$

$$\text{now } \begin{array}{l} 107:17 \leftarrow \boxed{6} \text{ R } 5 \\ 17:5 \leftarrow \boxed{3} \text{ R } 2 \\ 5:2 \leftarrow \boxed{2} \text{ R } 1 \\ 2:1 \equiv 2 \text{ R } 0 \end{array}$$

$$\frac{107}{17} \leftarrow \frac{44}{7} \equiv \frac{(-1)^3}{17 \cdot 7} \text{ cos } 107 \cdot 3 = 13$$

$$17 \cdot \overline{-44} \equiv 1$$

$$\begin{array}{c|cc} 119 & 107 \\ \hline 107 & 1 \\ \hline 2 & \end{array}$$

$$\begin{array}{c|cc} 107 & 107 \\ \hline 107 & 1 \\ \hline 0 & \end{array}$$

$$x \equiv 1 \pmod{3} \Rightarrow 3|x-1 \Rightarrow x \in \{4, 7, 10, \textcircled{13}, 16, 19, 22, 25, \textcircled{28}, 31, \dots\}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 5 \pmod{7}$$

$$13 \equiv 3 \pmod{5}$$

$$28 \not\equiv 3 \pmod{5}$$

$$13 \not\equiv 5 \pmod{7}$$

$$28 \not\equiv 5 \pmod{7}$$

$$t = 3v+1 \equiv 5v+3 \pmod{3}$$

$$5v \equiv -2$$

$$2v \equiv -2$$

$$v \equiv -1 \equiv 2$$

$$x \leq 5 \cdot 2 + 3 = 13$$

$$x \equiv 13 \pmod{15}$$

$$x \equiv 5 \pmod{7}$$

$$\Rightarrow x \equiv 15a + 13 \equiv 7a + 5 \pmod{7}$$

$$1 \equiv 15a \equiv -8 \equiv -1$$

$$a \equiv -1 \equiv 6$$

$$x \equiv 15 \cdot 6 + 13 \equiv 103 \Rightarrow \underline{x \equiv 103}$$

4) $\varphi(n)$ mult. imp. div cu 804?

$$\varphi(n) = \prod_{i=1}^{11} (2, 8, 42, 16, 7, 14, 18, 4, 12, 25, 21) \circ \left(3, 2^7, 3^7 \times 5^4, 12, 36, \dots \right)$$

$$\checkmark \quad \underbrace{(5, 31, 40, 33, 23, 43, 39, 22, 26, 45, 39)}_{11} \circ \left(10, \dots \right)$$

$$\text{nd } \varphi(n) = [1, 11] \subset 11$$

5) $739 \cdot 2^{102} + 1$ este prim

1) primă

$739 \rightarrow$ primă

$$\text{ultima cifră a } 739 \cdot 2^{102} + 1 = 9 \cdot 4 + 1 = 6 + 1 = 7$$

$$p \mid 739 \cdot 2^{102} + 1$$

$$\begin{array}{l} 2^1 = 2 \\ 2^2 = 4 \\ 2^3 = 8 \\ 2^4 = 16 \\ 2^5 = 32 \\ 2^6 = 64 \end{array} \left. \begin{array}{l} \\ \\ \\ \\ \\ \end{array} \right\} 4$$

$$\frac{102}{4} = 25 \text{ r } 2$$

2

ultima cifră

$$\begin{array}{l} \Rightarrow \text{mag le primă} \\ \Downarrow \text{impar} \end{array}$$

$$\begin{array}{l} \text{prime} \\ \text{last} \\ \text{digit} \end{array} \begin{array}{l} 1 \\ 3 \\ 7 \\ 9 \end{array}$$

$$p = 93$$

$$p = 73$$

$$2 \nmid 739 \cdot 2^{102} + 1$$

$$p \mid 2t + 1$$

$$739 \cdot 2^{102} + 1 \stackrel{+3}{=} 9 \cdot 8 + 1 = 73t \Rightarrow 73 \mid 73t$$

Ex. 6 iunie 2021

1) a) $\bar{x} + \bar{y} = \bar{0} (\mathbb{Z}_{100}, +) \Rightarrow \bar{x} = \overline{100 - 8} = \overline{92}$

b) $\bar{x} \cdot \bar{y} = \bar{1} (\mathbb{U}_{103}, \cdot)$

$$\text{c) } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 4 \end{pmatrix} \Rightarrow \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 4 & 2 \end{pmatrix}$$

2) a) $\text{ord } \bar{x} \text{ în } (\mathbb{Z}_{100}, +)$

$$\bar{x}k = \bar{0} = 100 \cdot q \Rightarrow 100 \mid 8k \Leftrightarrow 25 \mid 2k \Rightarrow k = 25 \quad 8 \cdot 25 = 200$$

b) $\text{ord } \bar{x} \text{ în } (\mathbb{U}_{103}, \cdot)$

$$102 = 2 \cdot 3 \cdot 17$$

d) $\text{ord } \bar{x} \mid 102 \Rightarrow d \mid 102 \Rightarrow d \in \{1, 2, 3, 6, 17, 34, 51, 102\}$

(2)

$$g^6 \not\equiv 1$$

b) $g^6 + 512 \not\equiv 100 \pmod{103}$

$$g^6 = g^{6+3} \equiv (100)^2 \equiv 9 \pmod{103}$$

$$g^{18} = g^{6+3+9} \equiv 9^3 \equiv 8 \pmod{103}$$

$$g^{18} + g^{18} + g^{18} \equiv 3 \cdot 13 \equiv 8 \cdot 13 \equiv 104 \equiv 1 \pmod{103} \Rightarrow \boxed{\text{Habt } g \neq 1}$$

de lo (14)

Examen 6 June 2021

(P)

$$\Leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix} \quad \text{und } g \neq ?$$

c) $\zeta = (1, 3, 2, 6, 4, 5) \Rightarrow \text{durchine 6} \Rightarrow \boxed{\text{und } g \neq ?}$

(3) a) Testat Prop. lui Wilson la $\#9$

d) $79 = \text{prim} \stackrel{\text{Wilson}}{\Rightarrow} 78! \equiv -1 \pmod{79}$

$$\frac{78 \cdot 77 \cdot 76 \cdot 75!}{-1 \quad -2 \quad -3} \equiv -1 + \frac{78 \cdot 77 \cdot 76}{-1 \quad -2 \quad -3} \pmod{79}$$

$$-6 \cdot 75! \equiv -1 - 6 = -7 = 72 \quad | \Rightarrow 75! \equiv -12 = 6 \pmod{79}$$

$$(6, 79) = 1$$

b) pt. ca ar-e prim p avem $4^{p-2} + 3^{p-2} + 2^{p-2} \equiv 57 \pmod{p}$?

$$\left. \begin{array}{l} p = \text{prim} \\ p \geq 5 \\ p \geq 3 \\ p \geq 2 \\ p \geq 1 \end{array} \right\} \Rightarrow \begin{array}{l} 4^{p-1} \equiv 1 \pmod{p} \\ 3^{p-1} \equiv 1 \pmod{p} \\ 2^{p-1} \equiv 1 \pmod{p} \end{array}$$

$$4^{p-2} + 3^{p-2} + 2^{p-2} \equiv 57 \pmod{p} \quad | \cdot 4 \cdot 3 \cdot 2$$

$$4^{p-1} \cdot 6 + 3^{p-1} \cdot 8 + 2^{p-1} \cdot 12 \equiv 57 \pmod{p} \quad \left\{ \begin{array}{l} 4 \cdot 3 \cdot 2 = 1368 \\ 1368 \end{array} \right.$$

$$24 \cdot 6 + 8 + 12 \equiv 57 \pmod{p} \quad \Rightarrow \begin{array}{l} 1368 - 24 - 8 - 12 = 1328 \\ 1328 = 2 \cdot 4 \cdot 61 \end{array} \Rightarrow p \in \{2, 3, 61\}$$

testat $p \in \{2, 3, 61\} \Rightarrow p=2 \Rightarrow 4^2 + 3^2 + 2^2 - 3 \equiv 57 \pmod{2} \Leftrightarrow 2 \mid 57-3=54 \quad \checkmark$

testat $p=3 \Rightarrow 4^3 + 3^3 + 2^3 - 3 \equiv 57 \pmod{3} \Leftrightarrow 3 \mid 57-9=48 \quad \checkmark$

testat $p=61 \Rightarrow 4^6 + 3^6 + 2^6 - 3 \equiv 57 \pmod{61} \Leftrightarrow 4^6 - 3 \equiv 28 \quad \times$

$$\Rightarrow X = 398$$

(2)

$$gath, x \in \{0, 1, 2, 3, \dots, 69\} \text{ as}$$

$$\left\{ \begin{array}{l} x \geq 0 \pmod{2} \\ x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{4} \end{array} \right\}$$

$$\text{obj.: } (2, 5) \equiv 1; (2, 4) \equiv 1; (5, 4) \equiv 1$$

$$x \equiv 0 \pmod{2} \Rightarrow x - \text{par}$$

$$x \equiv 1 \pmod{5} \Leftrightarrow x \equiv 5 \cdot 4 + 1$$

$$x \equiv 3 \pmod{4} \Leftrightarrow x \equiv 4 \cdot 4 + 3$$

$$\text{auf: } u = 13 \Rightarrow x \equiv 65 \pmod{2}$$

$$65 \equiv 1 \pmod{2}$$

$$x = 65 < 69 \text{ } \cancel{\text{X}} \text{ } \cancel{\text{X}} \text{ } \cancel{\text{X}}$$

$$u, v \in \mathbb{Z} \Rightarrow 5 \cdot u + 1 = 4 \cdot v + 3 \pmod{4}$$

$$5u + 1 \equiv 3 \pmod{4}$$

$$5u \equiv 2 \pmod{4}$$

$$5u + 1 - \text{par} \Rightarrow 5u - \text{impar}$$

$$18 \cdot u = 13 \Rightarrow 65 \equiv 2 \pmod{4}$$

zăolațire cu algoritm:

$$\text{• se căută nr - le prime cu } p_1 = 2, p_2 = 5, p_3 = 7 \text{ și } n = 2 \cdot 5 \cdot 4 = 40$$

$$\text{• calculează } w_i = \frac{n}{p_i}; w_1 = \frac{40}{2} = 20; w_2 = \frac{40}{5} = 8; w_3 = \frac{40}{7} = 10$$

$$\text{• se obț. că } (p_i > w_i) \Leftrightarrow \text{dec } w_i \text{ este inversabil} \Leftrightarrow \text{calc inversabil } (p_i)$$

$$\text{• algor. Euclid: } \Rightarrow \overline{35}^{-1} (\text{in } U(2)) = \bar{1}, \overline{15}^{-1} (\text{in } U(2_5)) = \bar{4}, \overline{10}^{-1} (\text{in } U(2_4)) = \bar{5} \Rightarrow$$

$$\text{sol. generală: } x = \sum w_i \cdot w_i^{-1} \cdot a_i \equiv 35 \cdot 1 \cdot a_1 + 14 \cdot 4 \cdot a_2 + 10 \cdot 5 \cdot a_3 \pmod{40}$$

$\Rightarrow 0, 20, 0, 2, 1, 0, 3, 2, 3 \Rightarrow x = 35 \cdot 0 + 56 \cdot 1 + 50 \cdot 3 \pmod{40} = 206 \pmod{40} = 66$

rezultat verificat cu sol. $x = 66$ este corect.

$$\widetilde{4u} \equiv -4 \pmod{13}$$

$$(4, 13) = 1 \Rightarrow \text{multiplicarea cu } \frac{1}{4} \Rightarrow u \equiv -1 \pmod{13}$$

$$(U(2_{13}),)$$

$$u \equiv 12 \pmod{13}$$

$$u = 13k + 12$$

$$u = 38(13k+12) + 2$$

$$u = 429k + 334 + 2$$

$$= \underline{\underline{334}}$$

$$\tau(36) \equiv 36 \cdot 3 = 108 \equiv 34 \pmod{37}$$

$$\tau(34) \equiv 34 \cdot 3 = 102 \equiv 28 \pmod{37}$$

$$\tau(28) \equiv 28 \cdot 3 = 84 \equiv 10 \pmod{37}$$

$$\tau(10) \equiv 10 \cdot 3 = 30 \pmod{37}$$

$$\tau(30) \equiv 30 \cdot 3 = 90 \equiv 16 \pmod{37}$$

$$\tau(16) \equiv 16 \cdot 3 = 48 \equiv 11 \pmod{37}$$

$$\tau(11) \equiv 11 \cdot 3 = 33 \pmod{37}$$

$$\tau(33) \equiv 33 \cdot 3 = 99 \equiv 25 \pmod{37}$$

$\tau(25) \equiv 25 \cdot 3 = 75 \equiv 1 \pmod{37} \rightarrow$ s-a inclus ciclul \Rightarrow lungime 18

~~menționam~~ încă m. mult nr. care nu e în ciclul precedent e 2

$$\tau(2) \equiv 3 \cdot 2 = 6 \pmod{37}$$

$$\tau(18) \equiv 18 \cdot 3 = 54 \equiv 17 \pmod{37}$$

$$\tau(6) \equiv 3 \cdot 6 = 18 \pmod{37}$$

$$\tau(17) \equiv 17 \cdot 3 = 51 \equiv 14 \pmod{37}$$

$$\tau(14) \equiv 14 \cdot 3 = 42 \equiv 5 \pmod{37}$$

$$\tau(5) \equiv 5 \cdot 3 = 15 \pmod{37}$$

$$\tau(15) \equiv 15 \cdot 3 = 45 \equiv 8 \pmod{37}$$

$$\tau(8) \equiv 8 \cdot 3 = 24 \pmod{37}$$

$$\tau(24) \equiv 24 \cdot 3 = 72 \equiv 35 \pmod{37}$$

$$\tau(35) \equiv 35 \cdot 3 = 105 \equiv 31 \pmod{37}$$

$$\tau(31) \equiv 31 \cdot 3 = 93 \equiv 19 \pmod{37}$$

$$\tau(19) \equiv 19 \cdot 3 = 57 \equiv 20 \pmod{37}$$

$$\tau(20) \equiv 20 \cdot 3 = 60 \equiv 23 \pmod{37}$$

$$\tau(23) \equiv 23 \cdot 3 = 69 \equiv 32 \pmod{37}$$

$$\tau(32) \equiv 32 \cdot 3 = 96 \equiv 22 \pmod{37}$$

$$\tau(22) \equiv 22 \cdot 3 = 66 \equiv 29 \pmod{37}$$

$$\tau(29) \equiv 29 \cdot 3 = 87 \equiv 13 \pmod{37}$$

$$\tau(13) \equiv 13 \cdot 3 = 39 \equiv 2 \pmod{37} \rightarrow$$
 s-a înlocuit
ciclul

$$\text{ord } \tau(x) = [18, 18] = 18$$

lungime 18

mai se poate da la construirea lui τ după regulile $\tau(x) \equiv 3x \pmod{37}$ (nu ex.

$\tau(10) \equiv 30 \equiv 10 \pmod{37}$ \rightarrow pozi. 10 de pe 1-a linie

($\tau(10) \equiv 30 \equiv 10 \pmod{37}$) și apoi se calc. normal ordinul

(se construiește cicluri disjuncte etc.)

L34 este mai mare ordin al unei permutări din S_{12} .

caz 1: τ -ciclu de lungime 12 $\Rightarrow \text{ord } \tau = [12] = 12$

caz 2: τ -2 cicluri disjuncte, cu lung. $k_1, k_2 \Rightarrow \text{ord } \tau = [k_1, k_2] = 12$

k_1	k_2	$\text{ord } \tau = [k_1, k_2]$
1	11	11
2	10	10
3	9	9
4	8	8
5	7	35
6	6	6

-6 ex -

Eaz 3: $T = 3$ cicluri disjuncte, cu lung. $k_1, k_2 \neq k_3$

k_1	k_2	k_3	ord T	$k_1 + k_2 + k_3 = 12$
10	1	1	10	
9	2	1	18	
8	2	2	8	
8	3	1	24	
7	2	3	$7 \cdot 2 \cdot 3 = 42$	$k_1 = 7$
4	1	1	28	$k_2 = 2$
6	5	1	30	$k_3 = 3$
6	4	2	12	
6	3	3	18	

ord T = 42

pt. $k_1 = 7$

$k_2 = 2$

$k_3 = 3$

J

Eaz 4: $T = 4$ cicluri disjuncte, cu lung. $k_1, k_2, k_3 \neq k_4$

$$12 = 9 + 1 + 1 + 1 = 8 + 1 + 1 + 2 = 7 + 1 + 1 + 3 = 7 + 2 + 1 + 2 = 6 + 1 + 1 + 4 =$$

$$\begin{array}{cccc} \downarrow & \downarrow & \downarrow & \downarrow \\ 9 & 8 & 21 & 14 \\ \end{array}$$

$$= 6 + 2 + 1 + 3$$

$$\begin{array}{cccc} \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 2 & 7 & 12 \\ \end{array}$$

L3.3 cel mai mic factor prim al nr. $2^{24} + 1$

Fie $p \mid 2^{24} + 1$

p -prim

~~$\exists p \in \mathbb{P} \Rightarrow \text{ord } 2 \mid \text{card } U(\mathbb{Z}_p)$~~

$\text{ord } 2 \mid \text{card } U(\mathbb{Z}_p) \Leftrightarrow \text{ord } 2 \mid p - 1$

$\text{card } U(\mathbb{Z}_p) = p - 1$

$$2^{24} + 1 \equiv 0 \pmod{p} \Rightarrow 2^{24} \equiv -1 \pmod{p}$$

$$2^{48} \equiv 1 \pmod{p} \Rightarrow 2^{48} \equiv 1 \Rightarrow$$

$\stackrel{P2}{\Rightarrow} k \mid 48 \Rightarrow k \in \{12, 3, 4, 6, 8, 12, 16, 24, 48\}$

$$2^{24} \equiv -1 \pmod{p} \Rightarrow 2^{24} \not\equiv 1 \pmod{p} \Rightarrow k = \text{ord } 2 \nmid 24 \Rightarrow$$

Ac elimină toti divizorii

lui 24 ($12, 6, 3, 4, 2, 1, 8$) \Rightarrow rămân de verificat 16 și 48

~~sup. $k \mid 24$~~ $\stackrel{Pp. că}{\Rightarrow} k = \text{ord } 2 \mid 24 \Rightarrow 2^{24} = (2^{\text{ord } 2})^{\frac{24}{\text{ord } 2}} \equiv 1^{\frac{24}{\text{ord } 2}} \equiv 1 \pmod{p}$ | \Rightarrow

$1 \pmod{p}$ dar $2^{24} \equiv -1 \pmod{p}$

- 7 ex -

$$\Rightarrow -1 \equiv 1 \pmod{p} \Leftrightarrow p \mid 1 - (-1) = 2 \quad (\Rightarrow p=2) \\ \text{dar } p \mid 2^{24+1} \quad (\text{p este o sa num} \Rightarrow \text{contradicție}) \\ \text{impar}$$

$$\text{cota } k=16 \\ \text{P.e } (2^8)^2 = 2^{16} \equiv 1 \pmod{p}$$

$$\begin{array}{l|l} p \text{ prim} & \Rightarrow p \mid (x-1)(x+1) \Rightarrow p \mid x-1 \text{ sau } p \mid x+1 \\ x^2 \equiv 1 \pmod{p} & x \equiv \pm 1 \pmod{p} \end{array}$$

$$x=2^8 \Rightarrow 2^8 \equiv \pm 1 \pmod{p}$$

$$\text{ord } \bar{z} = 16$$

$$\text{Dacă } 2^8 \equiv 1 \pmod{p} \Rightarrow \text{ord } \bar{z} \mid 8 \text{ contradicție}$$

$$\begin{array}{l|l} 2^{24} + 1 = (2^8)^3 + 1 & \Rightarrow (2^8)^3 + 1 \equiv (-1)^3 + 1 = 0 \pmod{257} \\ 2^8 \equiv -1 \pmod{257} & \downarrow \\ \text{p prime } \neq 257 & \end{array}$$

$$\text{cota } k=48$$

$$\text{ord } \bar{z} = 48 \mid \text{ord } U(\mathbb{Z}_p) = p-1$$

$$p-1 = 48t \Rightarrow p = 48t+1$$

$$t=1 \Rightarrow p=49 - \text{nu e prim}$$

$$t=2 \Rightarrow p=49+48=97 - \text{e prim}$$

$$\bullet \text{ verificare pe } 97: 2^8 = 256 \stackrel{97}{\equiv} 62 \equiv -35$$

$$2^{24} \equiv (2^8)^3 \stackrel{97}{\equiv} (-35)^3 = -35 \cdot 35^2 \stackrel{97}{\equiv} -35 \cdot 61 \stackrel{-1}{\equiv} 1225 \stackrel{97}{\equiv} 61 \stackrel{-1}{\equiv} -2135 \quad (\Leftarrow)$$

$$(2) -2135 \equiv 0 \pmod{97} \text{ și } 2^{24} \equiv -1 \pmod{97} \Rightarrow 97 \mid 2^{24} + 1$$

$$\Rightarrow 97 \mid 2^{24} + 1 \quad (\Leftarrow) \quad 2^{24} \equiv -1 \pmod{97}$$

$97 < 257 \Rightarrow$ cel mai mic factor prim: 97

Ex 4 Pt. ce numere prime p avem $2^{p-2} + 3^{p-2} + 5^{p-2} \equiv 57 \pmod{p}$

Având Fermat: $2^{p-1} \equiv 1 \pmod{p} \Rightarrow 3^{p-1} \equiv 5^{p-1}$, deci $p \neq 3, 2, 5$
 cauzul $p \neq 3, 2, 5$ $\begin{matrix} p \neq 3 \\ p \neq 2 \end{matrix}$

Împărțim cu 30:

$$30m = 15 \cdot \underbrace{2 \cdot 2^{p-2}}_1 + 10 \cdot \underbrace{3 \cdot 3^{p-2}}_1 + 6 \cdot \underbrace{5 \cdot 5^{p-2}}_1 \equiv 1410 \pmod{p} \Rightarrow$$

$$\Rightarrow 31 \equiv 1410 \pmod{p} \Rightarrow p \mid 1410 - 31 = 1379 = 23 \cdot 73 \Rightarrow p \in \{23, 73\}$$

cazul $p \notin \{2, 3, 5\}$

$$p=2 \Rightarrow 2^0 + 3^0 + 5^0 \equiv 3 \equiv 57 \pmod{2}$$

$$p=3 \Rightarrow 2^1 + 3^1 + 5^1 \equiv 10 \not\equiv 57 \pmod{3}$$

$$p=5 \Rightarrow 2^3 + 3^3 + 5^3 \equiv 35 \equiv 0 \not\equiv 57 \pmod{p}$$

$$\Rightarrow p \in \{2, 23, 73\}$$

Ex 4.2 Dacă $x \in \{1, 2, 3, \dots, 58\}$ și $2^x \equiv 29 \pmod{59}$.

- determinăm ord $\bar{2}$ în $(U(\mathbb{Z}_{59}), \cdot)$; 59 - prim

$$k = \text{ord } \bar{2}$$

$$k \mid \varphi(59) = 58 \Rightarrow k \in \{1, 2, 29, 58\}; \text{ dacă } k=58 \Rightarrow x \text{ unic}$$

$$2^1 \not\equiv 1 \pmod{59}$$

$$2^2 \equiv 4 \not\equiv 1 \pmod{59}$$

~~2²⁹~~ - incercăm acum 2^{29} , prin calculul congruenței cu puterile lui 2

$$2^{10} = 1024 \equiv 21 \pmod{59} \quad ; \quad 2^9 = 512 \equiv 40 \pmod{59}$$

x este unic

$$2^{20} = (2^{10})^2 \equiv (21)^2 \equiv 441 \equiv 28 \pmod{59}$$

$$2^{29} = 2^{20} \cdot 2^9 \equiv 28 \cdot 40 \equiv 1120 \equiv 58 \pmod{59} \not\equiv 1 \pmod{59} \Rightarrow \text{ord } \bar{2} < 58$$

$$2^{29} \equiv 58 \pmod{59} \quad \left| \begin{array}{l} \Rightarrow 2^{28} \equiv 29 \pmod{59} \\ (2, 59)=1 \rightarrow \text{putem înmulțifica cu 2} \end{array} \right.$$

$$\bar{2} \in U(\mathbb{Z}_{59})$$

$$X = 28$$

Numai:

$$\bar{2}^X = \bar{2}^9 \cdot \bar{2}$$

$$\bar{2}^{X+1} = \bar{2}^9 \cdot \bar{2} \cdot \bar{2}^2 \Rightarrow \bar{2}^{2X+2} = \bar{1} \quad \left| \begin{array}{l} \text{ord } \bar{2} < 58 \\ \Rightarrow 2X+2 < 58 \Rightarrow 2X < 56 \Rightarrow X < 28 \end{array} \right.$$

- g.e.x -

c) factor prim pt. $2^{83} - 1$

$$\text{d)e } p \mid 2^{83} - 1 \Rightarrow 2^{83} \equiv 1 \pmod{p}$$

prim

$\text{ord } \bar{2} = 83$, căci 83 e prim $\Rightarrow \text{ord } 2 \in \{1, 83\}$

$$\text{ord } \bar{2} + |\langle U(\mathbb{Z}_p) \rangle_2| \mid p-1 \Rightarrow p = 1 + 83 \cdot k$$

$$p \in \{1, 83, 167, 250,$$

\downarrow

prim

$$\underline{p=167} \Rightarrow \text{verificare d.c. } 2^{83} \equiv 1 \pmod{167} \quad \checkmark$$

ex: ult. scrisă ale lui $\overline{723}^{799}$

$$\varphi(1000) = 400 \quad ; \quad (\overline{723}, 1000) = 1$$

$$\overline{723}^{799} = \underbrace{\overline{723}^{400}}_{\equiv 1} \cdot \overline{723}^{399} = \overline{723}^{(399-400)} = \overline{723}^{-1}$$

$\overline{723} \cdot$

$\overline{787}$

$$\overline{723} \cdot \overline{787} = 1$$

$$\begin{array}{r} 5061 \\ 5184 \\ \hline 001 \end{array}$$

$$\Rightarrow u = 8 \cdot \lambda + 5 \Rightarrow x = 63 + 125(8\lambda + 5)$$

$$x = 63 + 125(8\lambda + 5) \stackrel{1000}{\equiv} 125 \cdot 9 + 63 \equiv 625 + 63 \equiv 688$$

Ultimile 3 cifre ale lui x^{999} sunt {688.}

2) L3.2 $a = ?$, $a \in \overline{\mathbb{Z}_{23}}$, $\text{ord}(a) = 22$ în grupul $(U(\mathbb{Z}_{23}), \cdot)$

$$\frac{\text{Lucr}}{3} a \in \{1, 2, 3, \dots, 22\}$$

$$\text{ord}(\bar{a}) = 22 \Rightarrow \bar{a}^{22} = \bar{1} \text{ în } U(\mathbb{Z}_{23})$$

$$\text{ord}(\bar{a}) \mid \text{ord } U(\mathbb{Z}_{23}) \circ \phi(\mathbb{Z}_{23})^{\text{prim}} \stackrel{\text{defn}}{=} 22 \Rightarrow \text{ord}(a) \in \{1, 2, 11, 22\}$$

$$1^k \equiv 1 \pmod{23}$$

$$2^k \equiv 2 \not\equiv 1 \pmod{23}$$

$$2^2 \equiv 4 \not\equiv 1 \pmod{23}$$

$$2^{11} \equiv 2048 \equiv 1 \pmod{23} \Rightarrow \text{ord } \bar{2} = 11$$

$$\text{Obs. că } \overline{-2} \equiv \overline{21} \pmod{23} \text{ și } (-2)^{11} = -2^{11} \equiv -1 \pmod{23}$$

Verificăm pt. $k < 11$ și $\bar{a} \circ \bar{2} \circ \bar{2}^k$:

$$-2^1 = -2 \not\equiv 1 \pmod{23}$$

$$-2^2 = 4 \not\equiv 1 \pmod{23}$$

$$-2^{11} \equiv -1 \not\equiv 1 \pmod{23}$$

$$(-2)^{22} = 2^{22} \equiv (-1)^2 \cdot 1 \pmod{23} \Rightarrow \bar{a} = \bar{21}$$

$$\text{ord } \bar{21} = 22$$

alte multimi: $5, 7, 10, 11, 14, 15, 17, 19, 20, 21$

L2.4 $T \in S_{36}$, $T(x) \in \text{multim } \{1, 2, 3, \dots, 36\}$ și $T(x) \equiv 3x \pmod{37}$.

$$\text{ord}(T) = ?$$

luăm orice vector $T(1) \in \mathbb{Z}_{37}^{36} \Rightarrow \text{ord } T = 37$

$$T(1) \equiv 3(1) \pmod{37} \Rightarrow \text{înmulțim cu } 3 \pmod{37}$$

$$T(3) \equiv 3 \cdot 3 = 9 \pmod{37}$$

$$T(9) \equiv 9 \cdot 3 = 27 \pmod{37}$$

$$T(27) \equiv 27 \cdot 3 = 81 \equiv 4 \pmod{37}$$

$$T(4) \equiv 4 \cdot 3 = 21 \pmod{37}$$

$$T(21) \equiv 21 \cdot 3 = 63 \equiv 26 \pmod{37}$$

$$T(26) \equiv 26 \cdot 3 = 78 \equiv 4 \pmod{37}$$

$$T(4) \equiv 4 \cdot 3 = 12 \pmod{37}$$

$$T(12) \equiv 12 \cdot 3 = 36 \pmod{37}$$

Evidență Matematică - Lecția IV

2) Sunt $x \in \{1, 2, 3, \dots, 58\}$ astfel încât $2^x \equiv 29 \pmod{59}$

$$2^x \equiv 29 \pmod{59} \mid \cdot 2 \quad 58 = 59 - 1$$

$$\text{Deci } 2^{x+1} = 2 \cdot 29 = 58 = 59 - 1 = -1 \pmod{59}$$

$$\Rightarrow 2^{x+1} \equiv -1 \pmod{59}$$

$$\Rightarrow (2^{x+1})^2 \equiv (-1)^2 \equiv 1 \pmod{59}$$

$$\Rightarrow 2^{2x+2} \equiv 1 \pmod{59}$$

\downarrow este elementul neutru de mulțimea și din proprietatea ordinului grupului avem $g^n = e \Rightarrow \boxed{\text{ord}(g) | n}$

În cazul nostru, $e = 1$, $g = 2$, $n = 2x + 2$, avem $2^{2x+2} = 1 \Rightarrow$

$$\Rightarrow \text{ord}(2) | 2x + 2.$$

$x + 1$ nu este ordinul grupului, deci cauzează doar divizorul $2x + 2$. În ceea ce deține de eveneza 2, deci ordinul lui 2 este divisorul par al lui $2x + 2$.

În grupul (\mathbb{Z}_{59}, \cdot) ca cel puțin 1 elevă g , din proprietatea ordinului grupului, avem $\text{ord}(g) | \boxed{\text{ordinal}}$

$$(6, \cdot) \text{ este } (\mathbb{U}(\mathbb{Z}_{59}), \cdot), g = 2 \Rightarrow \text{ord}(2) | |\mathbb{U}(\mathbb{Z}_{59})| \Rightarrow \boxed{\text{ord}(2) | 58}$$

$$\mathbb{U}(\mathbb{Z}_{59}) = 58$$

$$58 = 2 \cdot 29$$

$$d_{58} = \{1, 2, 29, 58\} \xrightarrow{\text{par}} \boxed{-1 \text{ divizor}}$$

Unul dintre divizorii este $\text{ord}(2)$.

$$2^2 \equiv 1 \pmod{59} \neq 1$$

$$\cancel{2^8 \equiv 1 \pmod{59}} \quad \text{ord}(2) = 58 \Rightarrow 58 | (2x+2)$$

$$1 \leq x \leq 58 \Rightarrow 1 \leq 2x+2 \leq 118.$$

$$1 \leq x \leq 58 \Rightarrow 1 \leq 2x+2 \leq 118 \text{ sunt divizori ai } 58 \cdot 2 = 116.$$

Singurul multiplu de 58 între 1 și 118 sunt 58 și $58 \cdot 2 = 116$.
Adică $2x+2 = 58$ sau $2x+2 = 116$

$$2x+2 = 58 \Rightarrow 2x = 56 \Rightarrow \boxed{x = 28}$$

Fără

$$\cancel{2^8 \equiv 29}$$

$$\mathbb{U}(\mathbb{Z}_{59})$$

$$\cancel{2^{x+1} \cdot 29 \cdot 2 = 58 = -1} \Rightarrow \cancel{2^{2x+2} = 1^2} \cancel{2^8} \Rightarrow \boxed{x = 28}$$

Exercice 2 (Méthode du Chiffre)

Quel est le résultat de $m = 2^{39} + 3^{39}$ modulo 41?

$\text{U}(Z_{41})$

Dès que le théorème de Fermat: $\hat{2}^{40} \equiv \hat{3}^{40} \equiv 1$

$$\begin{aligned}\hat{2}^{40} &= \hat{2}^{39} \cdot \hat{2} \stackrel{=} 1 \Rightarrow \hat{2}^{39} \cdot \hat{2} = -\hat{10} \Rightarrow \hat{2}^{39} = -\hat{10}/\hat{2} = -\hat{5} \\ \hat{3}^{40} &= \hat{3}^{39} \cdot \hat{3} \stackrel{=} 1 \Rightarrow \hat{3}^{39} \cdot \hat{3} = \hat{1}\end{aligned}$$

$$m \equiv 2^{39} + 3^{39} \quad | \cdot 6 \Rightarrow \underline{\text{Antidiagonale}}$$

$$6m \equiv 2^{39} \cdot 2 \cdot 3 + 3^{39} \cdot 2 \cdot 3 \Rightarrow$$

$$6m \equiv \hat{2}^{40} \cdot 3 + \hat{3}^{40} \cdot 2 \Rightarrow$$

$$6m \equiv 1 \cdot 3 + 1 \cdot 2 \equiv 5 \equiv -36 \pmod{41} \Rightarrow$$

$$\Rightarrow m \equiv -36/6 \equiv -6 \equiv 35 \Rightarrow$$

$$\boxed{m \equiv 35 \pmod{41}} \quad \underline{\underline{2e_{41}}}$$