9.03.2016

ALGEBRĂ

SEMINAR 2

Alfabet

A B C D ... Z ␣ . ? \$ 0 1 2

0 1 2 3 ...

$n = 2047$

$e = \cancel{179}$ Decriptați BH␣ | A␣2 | AUC | AJE | ARO

$\underbrace{\text{BH␣}}_{\text{SE}}$ | A␣2

$2047 = 23 \cdot 89$

I $n = p \cdot q$

II $e \cdot d \equiv 1 \pmod{\varphi(n)}$

III $Q^d \pmod n$

$$\varphi(n) = n \prod_{\substack{p \text{ prim} \\ p \mid n}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(2047) = 23 \cdot 89 \left(1 - \frac{1}{23}\right)\left(1 - \frac{1}{89}\right) = 22 \cdot 88 = 1936$$

$$179 d \equiv 1 \ (1936)$$

$(a, b) = 1 \qquad ax \equiv 1 \pmod b$

$a = b q_1 + r_1$

$b = r_1 q_2 + r_2$

$\vdots$

$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$ $\quad r_{n-1} = (a, b) = 1.$

$r_{n-2} = r_{n-1} \cdot q_n$

$$\frac{A}{B} = q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_{n-1}}}$$

$$\frac{a}{b} - \frac{A}{B} = \frac{(-1)^{n}}{bB}$$ $n \to$ nr op. alg Eucl.

$aB - bA = (-1)^n$

$a \cdot B \equiv (-1)^n \pmod b$

$$x \overset{b}{\equiv} \begin{cases} B & \text{dacă } n \text{ par} \\ -B & \text{dacă } n \text{ impar} \end{cases}$$

$1936 = 179 \cdot \boxed{10} + 146$

$179 = 146 \cdot \boxed{1} + 33$

$146 = 33 \cdot \boxed{4} + 14$

$33 = 14 \cdot \boxed{2} + 5$

$14 = 5 \cdot \boxed{2} + 4$

$5 = 4 \cdot \boxed{1} + 1$

$4 = 1 \cdot 4.$

$$\frac{A}{B} = 10 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2 + 1 \ddots}}} =$$

$1936 \cdot 38 - 411 \cdot 179 = -1$

$179 \cdot 411 \equiv 1 (1936)$

$f = 411$

$A \_ 2$ $\quad Q = 0 \cdot 40^2 + 26 \cdot 40 + 32 = 1072.$

IV $1072^{411} \overset{2047}{\equiv}$

$Q^f \overset{23}{\equiv} 1072^{411} \overset{23}{\equiv} 14^{411} = (14^{22})^{18} \cdot 14^{15} \overset{23}{\equiv} 14^{15}$

$14^2 = 196 \overset{23}{\equiv} 12.$

$14^4 \overset{23}{\equiv} 12^2 = 144 \equiv 6$

$14^8 \equiv 36 \overset{23}{\equiv} 13$

$14^{16} \equiv 13^2 = 169 \equiv 8$

$14 \cdot 14^{15} \equiv 8 (23)$

$7 \cdot 14^{15} \overset{23}{\equiv} 4 \mid \cdot 3$

$21 \cdot 14^{15} \overset{23}{\equiv} 12.$

$-2 \cdot 14^{15} \equiv 12$

$14^{15} \equiv -6 \equiv 17.$

$Q^f \overset{23}{\equiv} 17$

$$Q^f \overset{89}{\equiv} 1072^{411} \equiv 4^{411} = 2^{822} = (2^{88})^9 \cdot 2^{30} \qquad 2^{30} = (2^{10})^3 \equiv 45^3$$

$$= 45^2 \cdot 45 \overset{89}{\equiv} 67 \cdot 45 \overset{89}{\equiv}$$

$$Q^f \overset{89}{\equiv} 78$$

$$Q^f = 89t + 78 \overset{23}{\equiv} 17$$

$$-3t \equiv 17 - 78 \equiv 17 - 9 = 8$$

$$3t \overset{23}{\equiv} \qquad t = 5 (23)$$

$$Q^f = 89t + 78 = 89(23s + 5) + 78.$$

$$Q^f = 1072^{411} \overset{2047}{\equiv} 89 \cdot 5 + 78 = 523 = 40 \cdot 13 + 3$$

ND.

Polinoame

1) $x^2 + \bar{1} \in \mathbb{Z}_{107}[x]$

2) $x^2 + \bar{1} \in \mathbb{Z}_{113}[x]$

Au rădăcini aceste polinoame?

$x^2 + \bar{1} = (x + \bar{1})^2$ în $\mathbb{Z}_2$

$113 = 64 + 49$ patr. perf.

$$8^2 \equiv -7^2 (113) \mid u^2$$

$$7u = 1 (113)$$

$$7u \equiv -112 (113)$$

$$u = -16$$

$$15^2 \overset{113}{\equiv} 128^2 = (8 \cdot 16)^2 \equiv -1 (113)$$

$x^2 + \bar{1}$ are răd $\overline{15}$ și $\overline{98}$ (care e -15)

p prim , $p = 4k+1$

$\exists\, a, b$ a.î. $p = a^2 + b^2$

Presupun că $\exists\, x \in \mathbb{Z}_{107}$ a.î. $x^2 = -\hat{1}$

$\rightarrow \hat{1} = x^{106} = \hat{1} = (-\hat{1})^{53} = -\hat{1} \Rightarrow 107 / 2.$ ab.

mica th. Fermat.

$(x^2)^{53} = (-\hat{1})^{53}$

$(x^2)^{\frac{p-1}{2}} = (-\hat{1})^{\frac{p-1}{2}} = -\hat{1}$

$\hat{1} = x^{p-1}$

$p = 4k+3$ $\qquad p/2 \Rightarrow p = 2$ ab.

$p - 1 = 4k+2.$

$\frac{p-1}{2} = 2k+1 =$ impar

$x^2+1 \in \mathbb{Z}_{107}[x]$

$x^4 + \hat{1} \in \mathbb{Z}_{107}[x]$

$\rightarrow$ se desc în prod. de polin. neconstante.

$x^4 + \hat{1} = (x^2 + \hat{a}x + \hat{b})(x^2 + \hat{c}x + \hat{d})$

$$\begin{cases} 0 = \hat{a} + \hat{c} & (\text{coef lui } x^3) \Rightarrow \boxed{\hat{c} = -\hat{a}} \\ 0 = \widehat{ac} + \hat{b} + \hat{d} & (\text{coef } x^2) \\ 0 = \widehat{ad + bc} & (\text{coef } x) \\ \hat{1} = \widehat{bd} & (\text{coef } 1) \end{cases}$$

$\Rightarrow 0 = \hat{a}(\hat{d} - \hat{b}) \Rightarrow \hat{a} = 0$ sau $\hat{d} = \hat{b}$

Dacă $a = \hat{0} \Rightarrow \hat{c} = 0$ $\begin{cases} \widehat{b+d} = \hat{0} \quad / \cdot \hat{b} \\ \widehat{b \cdot d} = 1 \end{cases} \Rightarrow \hat{b}^2 + 1 = \hat{0}$ NU.

$\bar{a} \neq \bar{0}$

$\bar{b}^2 = \bar{1}$

$(\bar{b} - \bar{1})(\bar{b} + \bar{1}) = \bar{0}$

corp: $\Rightarrow \bar{b} - \bar{1} = 0 \qquad \bar{b} = \bar{1}$

sau $\bar{b} + \bar{1} = 0 \Rightarrow \bar{b} = -\bar{1}$

$\bar{b} = \bar{1}$

$\Rightarrow \bar{a}^2 = \bar{2}\bar{b} = \bar{2}$

$$\begin{array}{r|l} 441 & 107 \\ 428 & 4 \\ \hline 13 & \end{array}$$

$\bar{1} = \bar{a}^{106} = (\bar{a}^2)^{53} = \bar{2}^{53} = -\bar{1}$ ↯

$\bar{b} = \bar{d} = -1$ e obligatoriu.

$\bar{a}^2 = -\bar{2}$ în $\mathbb{Z}_{107}$

$14^2 = 196 \overset{107}{\equiv} -18$

$14^2 \equiv -2 \cdot 3^2 \ (107)$

$3u \equiv 1 (107)$

$3u \equiv 108 (107)$

$u \equiv 36 (107)$

$(14 \cdot 36)^2 \equiv -2 (107)$

$(x^2 + \overline{76}x - \bar{1})(x^2 + \overline{31}x - \bar{1})$

$$\begin{array}{r} 31 \\ 31 \\ \hline 31 \\ 93 \\ \hline 961 \end{array}$$

$x^4 + 1 \in \mathbb{Q}[x]$ (nu se scrie ca prod de 2 pol. necont cu coef în $\mathbb{Q}$)

ireductibil. $\quad x^4 + 1 \in \mathbb{R}[x]$

$(x^4+1)^2 = (x^2+1)^2 - 2x^2 =$

$= (x^2+1)^2 - (\sqrt{2}x)^2 = (x^2 + 1 + \sqrt{2}x)(x^2 + 1 - \sqrt{2}x)$

$$x^4+1=(x^2+ax+b)(x^2+cx+d)$$

$$\begin{cases} 0=a+c \\ 0=b+d+ac \\ 0=ad+bc=a(d-b) \\ 1=bd \end{cases}$$

$c=-a$.

$a\neq 0$, $b=d \Rightarrow b=\pm 1$.

$\pm 2=2b=-ac=a^2 \Rightarrow a^2=\pm 2$ ok

12