De ce sunt utile polinoamele?

V-am povestit acum ceva vreme despre importanţa cheilor publice în criptografie. Istoric, prima astfel de cheie a fost furnizată de ideile matematicienilor Diffie şi Hellman. Iddea centrală este furnizată de următorul rezultat din algebră:

Teoremă: Dacă p este un număr prim, atunci grupul $(\mathbb{Z}_p^*, \cdot)$ este ciclic. Cu alte cuvinte, în acest grup există un element de ordin $p-1$.

Schiţa demonstraţiei:

Pasul 1: Fie $(G, \cdot)$ un grup comutativ, finit şi m ordinul maxim al unui element din G. Atunci g^m este e, elementul neutru al grupului G, pentru orice $g \in G$.

Nu voi da demonstraţia completă a acestui rezultat, însă vă voi spune ideea centrală. Trebuie arătat că ordinul lui g divide m, penru orice $g \in G$. Se presupune că nu ar fi adevărat acest lucru şi se construieşte un element din G cu ordinul mai mare decât m. Vă sugerez doar cum se găseşte contradicţia într-un caz concret. Să presupunem că $ord\ g = 12$ şi $ord\ h = 18 = m$. Atunci $ord\ g^3 = \frac{12}{(3,12)} = 4$, $ord\ h^2 = \frac{18}{(2,18)} = 9$ şi

$$ord\ (g^3 \cdot h^2) = ord\ g^3 \cdot ord\ h^2 = 4 \cdot 9 = 36 > 18 = m.$$

Am găsit un element din grup cu ordinul mai mare decât m; contradicţie. Ideea este aceeaşi şi în cazul general.

Pasul 2: Notăm cu m cel mai mare ordin al unui element din grupul $(\mathbb{Z}_p^*, \cdot)$. Evident că m divide $p-1$. Noi trebuie să arătăm că $m = p-1$. Din Pasul 1 ştim că $x^m = \overline{1}$, pentru orice $x \in \mathbb{Z}_p^*$. De aici deducem că polinomul

$$X^m - \overline{1} \in \mathbb{Z}_p[X]$$

are cel puţin $p - 1 = |\mathbb{Z}_p^*|$ rădăcini. Dar numărul rădăcinilor este cel mult gradul polinomului, de unde deducem că

$$p - 1 \leq m.$$

Cum m este divizor al lui $p-1$, rezultă că $m \leq p-1$. Combinând cele două inegalităţi, deducem că $m = p-1$ şi enunţul este demonstrat.

Exerciţiu : Găsiţi acel n pentru care $\overline{2}^n = \overline{31}$ în $\mathbb{Z}_{83}$.

Comentariu: Ordinul lui $\overline{2}$ în grupul $(\mathbb{Z}_{83}^*, \cdot)$ este 82, ceea ce implică existenţa numărului n din exerciţiu. Ordinul lui $\overline{2}$ în grupul menţionat este un divizor al lui 82, deci poate fi 1, 2, 41 sau 82. Cum

$$\overline{2}^{41} = ((\overline{2})^{10})^4\overline{2} = \overline{2} \cdot \overline{28}^4 = \overline{2} \cdot \overline{37}^2 = \overline{2} \cdot \overline{41} = \overline{82},$$

rezultă imediat că ordinul lui $\overline{2}$ în grupul $(\mathbb{Z}_{83}^{*}, \cdot)$ este 82