

התחילת תוכנית נכונה

נתון $P(x) \in \mathbb{Z}_n[x]$, וסעיף $\alpha \in \mathbb{Z}_n$ - ה- $P(\alpha) \in \mathbb{Z}_n$

$$P(\alpha) \equiv 0 \pmod{n}$$

מכאן $n = p^r$ (כאשר p ראשוני, $r \geq 1$)
 ו- $P(\alpha) \equiv 0 \pmod{p}$

הערה: קודם כעת, מודול p - נרשם $P(\alpha) \equiv 0 \pmod{p}$ כחלק מ- $P(\alpha) \equiv 0 \pmod{p^r}$

הנחה: $P(\alpha) \equiv 0 \pmod{p}$

$$P(\alpha) \equiv 0 \pmod{p}$$

נבחר $\alpha \in \mathbb{Z}_n$ כזה ש- $P(\alpha) \equiv 0 \pmod{p}$

נניח $\alpha \in \mathbb{Z}_n$ ש- $P(\alpha) \equiv 0 \pmod{p}$

$$P(\alpha) \equiv 0 \pmod{p}$$

$$r_2 = r_1 + k \cdot p$$

הכנס α ל- $P(x)$

$$P(r_2) \equiv 0 \pmod{p^2}$$

$$\frac{i!}{s!} = \frac{i!}{s!(i-s)!} = \binom{i}{s}$$

הערה: $\alpha \in \mathbb{Z}_n$

$$P(r+kp) = P(r) + P'(r)kp + \frac{P''(r)}{2}(kp)^2 + \dots$$

$$P(r) \equiv 0 \pmod{p}$$

$$P(x) = \sum_{n=0}^{\deg(P)} a_n x^n$$

הוכחה: $P(\alpha) \equiv 0 \pmod{p}$

$$P(r) = \sum_{n=0}^{\deg(P)} a_n r^n$$

הוכחה: $P(\alpha) \equiv 0 \pmod{p}$

$$r_2 = 7 + 5k$$

נניח $r_1 = 1 + 5k$

$$p'(r_1) \pmod{5}, p(r_1) \pmod{25} = 1, 35$$

$$p(r_1) \equiv 0 \pmod{5}, p'(r_1) \equiv 0 \pmod{5}$$

נניח $r_1 = 1 + 5k$

$$\frac{0}{5} + 0k \equiv 0 \pmod{5}$$

אם k הוא מספר שלם, נגדיר $r_2 = 7 + 5k$

$$r_2 \equiv 7 \pmod{5}$$

$$r = 7 + 5k$$

נניח $r = 7 + 5k$

$$p'(r) \pmod{5}, p(r) \pmod{25}$$

$$p(r) \equiv 5 \pmod{25}$$

$$p'(r) \equiv 0 \pmod{5}$$

נניח $r = 7 + 5k$

$$\frac{5}{5} + 0k \equiv 0 \pmod{5}$$

$$7 \equiv 0 \pmod{5}$$

אין פתרונות.

סה"כ הבעיות מוצאות 25 פתרונות.

$$\begin{cases} r_1 \equiv -1 \pmod{25} \\ r_2 \equiv 7 \pmod{5} \end{cases}$$

נניח $r_1 = -1 + 25k$ ונניח $r_2 = 7 + 5k$

יש 25 פתרונות מוצאות 99

ש/מ 25	7	6
1	7	26
6	106	6
11	36	111
16	141	41
21	71	146
26	99	174

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv -1 \pmod{25} \\ x \pmod{175} \end{cases} \quad (A)$$

$$\begin{cases} x \equiv -1 \pmod{175} \\ x \equiv -1 \pmod{7} \\ x \equiv -1 \pmod{25} \end{cases} \quad (B)$$

$$\begin{cases} x \equiv 1 \pmod{35} \\ x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{5} \end{cases} \quad (C)$$

$$\begin{cases} x \equiv 6 \pmod{35} \\ x \equiv -1 \pmod{7} \\ x \equiv -1 \pmod{5} \end{cases} \quad (D)$$