תרגול 12

נגדיר נגזרת של פולינום מעל שדה כלשהו.

הגדרה: $f\in R[x]$, R חוג.

$$f(x)=a_nx^n+\dots+a_1x+a_0$$
$$f'(x)=na_nx^{n-1}+\dots+a_1$$
$$f^{(k)}(x)=(f^{(k-1)})'(x)$$

טענה: $f,g\in R[x]$ יהי, אזי $(f+g)'=f'+g'$, $\forall c\in R\ (cf)'=cf'$

$$(f+g)^{(k)}=f^{(k)}+g^{(k)},\quad (cf)^{(k)}=cf^{(k)}$$

הוכחה מהגדרה.

לשים לב: אזי $f(x)=x^m$ $f^{(k)}(x)=m(m-1)\cdots(m-k+1)x^{m-k}$

משפט-שארית הקטן: יהי $f\in\mathbb{Z}[x]$, $k\in\mathbb{Z}$, $k\neq 2$. p ראשוני כשהוא (כולל 2).

יהי a פתרון שלם יחיד ל-$f(x)\equiv 0\pmod p$. אזי: (הנקודה נמצאת מ-a פחות פעמים $f(a)\equiv 0\pmod{p^2}$)

(א) אזי $f'(a)\not\equiv 0\pmod p$ אז $f(a+tp)\equiv f(a)\pmod{p^2}$ $\forall t\in\mathbb{Z}$ יחיד

(ב) אזי $f'(a)\equiv 0\pmod p$ ו $f(a)\equiv 0\pmod{p^2}$ אז $f(a+tp)\equiv f(a)\pmod{p^2}$ $\forall t\in\mathbb{Z}$

(ג) אזי $f'(a)\equiv 0\pmod p$ ו $f(a)\not\equiv 0\pmod{p^2}$ אין פתרונות עבור x מודולו p^2

$$x=a+tp$$

דוגמה מהשורה: מקרה א': הנגזרת לא מתאפסת

מקרה ב': הנגזרת כן מתאפסת

מקרה ג': אין הנגזרת

$$\left.\begin{array}{l}\text{שם הפתרון (מ-}\bmod p^{k-1}\text{ ל-}\bmod p^k\text{)}\\ \text{תסביר למה הקרן הנגזרת}\end{array}\right\}$$

משפט (הנוסחה של טיילור): $f\in\mathbb{Z}[x]$. f מתפצל עם הינתי n. אזי $\forall a\in\mathbb{Z}$

$$f(x+a)=f(a)+f'(a)x+\frac{1}{2!}f''(a)x^2+\dots+\frac{1}{n!}f^{(n)}(a)x^n$$

כאשר המקדמים מהנגזרת $\frac{1}{n!}f^{(n)}(a)$ הם שלמים.

הוכחה: מספיק לטפל במקרה $f=x^m$, $m\geq n$.

$$(x+a)^m=\sum_{j=0}^{m}\binom{m}{j}x^{m-j}a^j=\sum_{j=0}^{m}\frac{1}{j!}\frac{m!}{(m-j)!}x^{m-j}a^j=\sum_{j=0}^{m}\frac{1}{j!}f^{(j)}(a)x^j$$

הוכחת שארית הקסם:

אזי a מספיק $f(x)\equiv 0 \pmod{p}$ כך ש r קיים $r\equiv a \pmod{p-1}$

מהנתון שתקיים $a^{p-1}+tp=r$. $t\in\mathbb{Z}$

מה שהיינו צריכים להוכיח $f(x)\equiv 0 \pmod{p}$ כאשר x המקיים את f הוא שורש

$$\Leftarrow \quad f(x)\equiv 0 \pmod{p} \quad \text{כי} \quad \sum_{i=0}^{n} \frac{1}{i!} f^{(i)}(x)\cdot(a^{p-1}+tp)^i = f(a^{p-1}+tp) \equiv 0 \pmod{p}$$

(שארית ב- p של $f^{(i)}(x)$ כאשר $i\geq 1$ מתאפסת)

$\Rightarrow$ $f(x)\equiv 0 \pmod{p}$. אזי בוודאי ש- $a^{p-1}+tp \mid f(x)$ ולכן

$t\cdot a^{p-1}+tp \mid a^{p-1}+f(x)$ נקבל $t+\frac{f(x)}{a^{p-1}} \mid a^{p-1}+\frac{f(x)}{a^{p-1}}\cdot a^{p-1}$

ולכן בוודאי $a^{p-1}\mid f(x)$ קיבלנו g עליה מדובר שכזה $f(x)-\frac{a^{p-1}}{f(x)}=g(x)$.

מסקנה 1: אזי $a^{p-1}\mid f(x)$ וזה $f(x)\not\equiv 0 \pmod{p}$ אז קיים x שהוא פתרון ☑

מסקנה 2: $f(x)\equiv 0 \pmod{p}$ וזה $f(x)\not\equiv 0 \pmod{p^2}$ ונקבל כי x הינו פתרון.

מסקנה 3: אזי $f(x)\equiv 0 \pmod{p}$ יש פתרון, תהי הינו $\widetilde{f(x)}\cdot\frac{a^{p-1}}{f(x)}=x$.

ולכן בוודאי $g(x)\equiv -\frac{a^{p-1}}{f(x)} \pmod{p}$ הקבע g עליה מדובר שכזה $f(x)$.

מסקנה: יהי r_1 השורש פתרון של $f(x)\equiv 0 \pmod{p}$, p כאשר.

$f(r_1)\equiv 0 \pmod{p^2}$, אזי קיים r_2 מהצורה r_1+tp הקבע g- r_1 מהצורה p $(k=2,3,4,\dots)$

$$\boxed{\widetilde{f'(r_1)}\cdot f(r_{k-1}) - r_{k-1} = r_k \pmod{p}}$$

הוכחה: $f'(r_1)\not\equiv 0 \pmod{p}$, אזי קיים r_2 מהצורה r_1+tp הקבע g- r_1 מהצורה p.

$tp+r_1=r_2$, $\widetilde{f'(r_1)}\cdot\frac{f(r_1)}{p}=t$ אזי $\widetilde{f'(r_1)}\cdot f(r_1)-r_1=r_2$

צ"ל: $\widetilde{f'(r_2)}\cdot f(r_2)-r_2=r_3$, אם $\widetilde{f'(r_1)}=\widetilde{f'(r_2)}$ ומספיק $\widetilde{f'(r_2)}\equiv\widetilde{f'(r_1)}$

מאינדוקציה קיים r_k הנקבע $\widetilde{f'(r_{k-1})}\cdot(f(r_{k-1})-r_{k-1})=r_k$ ☑

דוגמא: $f(x)=x^2+x+1$. $f(2)\equiv 0$

$p=3$: מהצורה 3 : $f(x)\equiv 0$. $x=1$: $f'(x)=2x+1 \Rightarrow f'(1)=3$

נפרוק: $f(1)=3\equiv 0$, $f'(1)=3\equiv 0$, $f(4)=21\equiv 0$ ← מקיים כי!

אזי $x=1,4,7$ מהצורה 3^2. יכן $x=3t+1$ כשהוא פתרון. נציב $t=0,1,2$ ונקבע

מהצורה 27: פתרונות $f(1)\not\equiv 0$, $f'(1)\equiv 0$ ⇐ מקיים $f(27)$ אין הרמה!

$x=4+9t$, $t=0,1,2$ יכן $f(4)\equiv 0$, $f'(4)\equiv 0$ ⇐ מקיים כי, הרמה יש אז:

$x=4,13,22$

מהצורה 27 הם $x\equiv 4,13,22 \pmod{27}$ ☑

המשך תרגול 3

שאלה: אם p ראשוני אי זוגי אז לפחות $x^2 \equiv a \pmod{p}$ (*) פתירה.

הוכחה: $\Leftarrow$ נניח ש- x_0 פתרון של (*). כלומר $f(x) = x^2 - a$. אם $x_1 \in$ פתרון של (*) אז $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ כי $x_1 \not\equiv 0 \pmod{p}$

כי $a \not\equiv 0 \pmod{p}$ אין אף מחלקה x_i שהיא גם הפכי.

$\Rightarrow$ יהי x_1 פתרון של (*) אז $x_1^2 \equiv a \pmod{p}$ כלומר $\left(\frac{a}{p}\right) = 1$ (לפי הגדרת שארית ריבועית)

שאלה: אם p ראשוני אי זוגי אז לפחות $x^2 \equiv a \pmod{p}$ (*) פתירה.

הוכחה: $\Leftarrow$ נניח ש- x_0 פתרון של (*). כלומר $f(x) = x^2 - a$. אם $x_1 \in$ פתרון של (*) אז $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ כי $x_1 \not\equiv 0 \pmod{p}$

כי $a \not\equiv 0 \pmod{p}$ אין אף מחלקה x_i שהיא גם הפכי.

$\Rightarrow$ יהי x_1 פתרון של (*) אז $x_1^2 \equiv a \pmod{p}$ כלומר $\left(\frac{a}{p}\right) = 1$ (לפי הגדרת שארית ריבועית)

שאלה: אם p ראשוני אי זוגי אז לפחות $x^2 \equiv a \pmod{p}$ (*) פתירה.

הוכחה: $\Leftarrow$ נניח ש- x_0 פתרון של (*). כלומר $f(x) = x^2 - a$. אם $x_1 \in$ פתרון של (*) אז $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ כי $x_1 \not\equiv 0 \pmod{p}$

כי $a \not\equiv 0 \pmod{p}$ אין אף מחלקה x_i שהיא גם הפכי.

$\Rightarrow$ יהי x_1 פתרון של (*) אז $x_1^2 \equiv a \pmod{p}$ כלומר $\left(\frac{a}{p}\right) = 1$ (לפי הגדרת שארית ריבועית)

שאלה: אם p ראשוני אי זוגי אז לפחות $x^2 \equiv a \pmod{p}$ (*) פתירה.

הוכחה: $\Leftarrow$ נניח ש- x_0 פתרון של (*). כלומר $f(x) = x^2 - a$. אם $x_1 \in$ פתרון של (*) אז $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ כי $x_1 \not\equiv 0 \pmod{p}$

כי $a \not\equiv 0 \pmod{p}$ אין אף מחלקה x_i שהיא גם הפכי.

$\Rightarrow$ יהי x_1 פתרון של (*) אז $x_1^2 \equiv a \pmod{p}$ כלומר $\left(\frac{a}{p}\right) = 1$ (לפי הגדרת שארית ריבועית)

שאלה: אם p ראשוני אי זוגי אז לפחות $x^2 \equiv a \pmod{p}$ (*) פתירה.

הוכחה: $\Leftarrow$ נניח ש- x_0 פתרון של (*). כלומר $f(x) = x^2 - a$. אם $x_1 \in$ פתרון של (*) אז $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ כי $x_1 \not\equiv 0 \pmod{p}$

כי $a \not\equiv 0 \pmod{p}$ אין אף מחלקה x_i שהיא גם הפכי.

$\Rightarrow$ יהי x_1 פתרון של (*) אז $x_1^2 \equiv a \pmod{p}$ כלומר $\left(\frac{a}{p}\right) = 1$ (לפי הגדרת שארית ריבועית)

שאלה: אם p ראשוני אי זוגי אז לפחות $x^2 \equiv a \pmod{p}$ (*) פתירה.

הוכחה: $\Leftarrow$ נניח ש- x_0 פתרון של (*). כלומר $f(x) = x^2 - a$. אם $x_1 \in$ פתרון של (*) אז $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ כי $x_1 \not\equiv 0 \pmod{p}$

כי $a \not\equiv 0 \pmod{p}$ אין אף מחלקה x_i שהיא גם הפכי.

$\Rightarrow$ יהי x_1 פתרון של (*) אז $x_1^2 \equiv a \pmod{p}$ כלומר $\left(\frac{a}{p}\right) = 1$ (לפי הגדרת שארית ריבועית)

שאלה: אם p ראשוני אי זוגי אז לפחות $x^2 \equiv a \pmod{p}$ (*) פתירה.

הוכחה: $\Leftarrow$ נניח ש- x_0 פתרון של (*). כלומר $f(x) = x^2 - a$. אם $x_1 \in$ פתרון של (*) אז $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ כי $x_1 \not\equiv 0 \pmod{p}$

כי $a \not\equiv 0 \pmod{p}$ אין אף מחלקה x_i שהיא גם הפכי.

$\Rightarrow$ יהי x_1 פתרון של (*) אז $x_1^2 \equiv a \pmod{p}$ כלומר $\left(\frac{a}{p}\right) = 1$ (לפי הגדרת שארית ריבועית)

שאלה: אם p ראשוני אי זוגי אז לפחות $x^2 \equiv a \pmod{p}$ (*) פתירה.

הוכחה: $\Leftarrow$ נניח ש- x_0 פתרון של (*). כלומר $f(x) = x^2 - a$. אם $x_1 \in$ פתרון של (*) אז $f'(x_1) = 2x_1 \not\equiv 0 \pmod{p}$ כי $x_1 \not\equiv 0 \pmod{p}$

כי $a \not\equiv 0 \pmod{p}$ אין אף מחלקה x_i שהיא גם הפכי.

$\Rightarrow$ יהי x_1 פתרון של (*) אז $x_1^2 \equiv a \pmod{p}$ כלומר $\left(\frac{a}{p}\right) = 1$ (לפי הגדרת שארית ריבועית)