תרגול 10 :

(כלומר ש- $a\in\mathbb{Z}$ הוא שורש פרימיטיבי מודולו m אם $\bar{a}$ הוא יוצר של $(\mathbb{Z}/m\mathbb{Z})^\times$).

$\gcd(a,m)=1$. צ"ל: $\exists$ שלם חיובי k כך ש $a^k\equiv 1 \pmod m$.

$k=\varphi(m)$ נבחר 2 אינו שלם חיובי k.

⚠ הכוונה כי בכל קבוצה קיים שורש פרימיטיבי! (השאלה שאלה)

$m=8$ כאשר בשאלה שקבר כי אין שלם.

$m=91$ כי שלם חיובי מ"ו הוא k חיובי קטן ביותר אין שלם ל- 91.

נכון: עבור a^n, $n\geq 3$, אין שורש פרימיטיבי!

$n\in\mathbb{N}$, $n>1$. באיזה יש שלם חיובי k? $n=p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_t^{a_t}$

$$(\mathbb{Z}/n\mathbb{Z})^\cap \simeq (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\cap\times\ldots\times(\mathbb{Z}/p_t^{a_t}\mathbb{Z})^\cap$$

האם $(\mathbb{Z}/p^a\mathbb{Z})^\cap$ חבורה?

$\leftarrow$ אם $p=2$ ו $a\geq 3$ $\hat{g}$- $\{\pm 1\}=(\mathbb{Z}/2\mathbb{Z})^\cap$ חבורה טריוויאלית

$*$ $\{\bar{1},\bar{-1}\}=(\mathbb{Z}/4\mathbb{Z})^\cap$ חבורה (1- יוצר)

$*$ $a>2$ $(\mathbb{Z}/2^a\mathbb{Z})^\cap$ עבור חבורה!

טענה: אם $p>2$ ראשוני אזי $(\mathbb{Z}/p^a\mathbb{Z})^\times$ היא חבורה

טענה: אם p ראשוני, $p>k\geq 1$ אזי $\binom{k}{p}$ מתחלק ב- p

הוכחה: $\binom{p}{k}\cdot k!(k-p)!=p! \Rightarrow \binom{p}{k}\cdot\frac{k!(k-p)!}{p!}=\binom{p}{k}$

$\checkmark$ $p\mid\binom{p}{k}\Rightarrow p\mid k!$ או $p\mid(k-p)!$

טענה 3: אם $p>1$, $a,b\in\mathbb{Z}$, $p\mid a-b$ אזי $p^{l+1}\mid a^p-b^p$

הוכחה: מהנתון $a=b+c\cdot p^l$ עבור c מתאים (קיים בראשית)

$$a^p=b^p+\binom{p}{1}b^{p-1}cp^{l+1}+A \quad A=\sum_{k=2}^{p}\binom{p}{k}c^k p^{lk}b^{p-k}$$

מתקיים $p^{l+2}\mid A$, $l+1<2l \leftarrow p^{l+1}\mid A$ ו $p^{l+1}\mid b^{p-1}\cdot c\cdot p^{l+1}$

אזי $a^p\equiv b^p \pmod{p^{l+1}}$

מסקנה 1: אם $l>1$, $p\neq 2$ ראשוני אזי עבור $a\in\mathbb{Z}$ מתקיים

$$(1+ap)^{p^{l-2}}\equiv 1+ap^{l-1} \pmod{p^l}$$

מספיק להוכיח שיש $g^k \equiv -1 \pmod{p^{e-1}}$ כאשר $k \mid p^{e-1}(p-1)$.

ראשי משפט אוילר $g^{\varphi(p^e)} = g^{p^{e-1}(p-1)} \equiv 1 \pmod{p^e}$.

אז סדרן של g הוא שורש פרימיטיבי $\bmod p^e$. מתקיים: $\varphi(p^e) = p^{e-1}(p-1)$

לכן אפשר להניח שיש שם מודולו p לא $-1 \pmod{p^e}$ (כלומר g כך ש $g+p$ שם זה)

אבל $g^{p^{e-2}(p-1)} \neq -1 \pmod{p^e}$ כנ"ל.

$$g^{p^{e-2}(p-1)} + 1 \equiv$$

אם $g^{p^{e-1}} \equiv -1 \pmod{p^e}$ אז $g^{p^{e-2}(p-1)} + p^{e-1} \equiv -1 \pmod{p^e}$ (הכינוס)

צ"ל $g+p$ שם מודולו p. אין סדרן g לא $g^{p^{e-1}} \neq -1 \pmod{p^e}$

אלא יודעים שיש שם מודולו p (כלומר g).

הוכחה:

משפט: אם $p \neq 2$ אז $\mathbb{Z}/p^e\mathbb{Z}^\times$ היא **ציקלית**, כלומר יש שם מ- p^e לא A.

הוכחה:

$(p) \quad g^{p^{e-1}} \equiv 1 \pmod{p^e}$, אחרת $g^{p^{e-2}} \not\equiv 1 \pmod{p^e}$ ✓

שנקרא $p^{e-2}(p-1)$ וכיוון שאחד מהחזקות 1 אכן כזה).

(אם ה"מ מתוך שם p^{e-2} שהוא הסדר (כמעט) שמקיים $g^{p^{e-2}(p-1)} \equiv 1 \pmod{p^e}$ מהגדרת p אז

אז: $p^{e-1} \mid (ab+1)^{p^{e-2}}$ מספיק להוכיח $g^{p^{e-2}} \not\equiv 1 \pmod{p^e}$

לכן: $(p) \quad g^{p^{e-1}} \equiv 1 \pmod{p^e}$

הוכחה שם מקדם:

$$(1+ap)^{p^{e-1}} \equiv 1 + ap^e \quad (p^{e+1})$$

טענה 2: אם $p \neq 2$, אז כל a כזה ש $ap+1$ מודולו p הוא $\neq p^{e-1}$

הוכחה: באינדוקציה על e:

$$(p^{e+1}) \quad (1+ap)^{p^{e-1}} \equiv 1 + ap^e$$

בסיס: $e=1$ ברור.

מעבר: נניח עבור e ונוכיח עבור $e+1$:

$$(1+ap)^{p^e} = \left((1+ap)^{p^{e-1}}\right)^p \equiv (1+ap^e)^p \pmod{p^{e+1}}$$

$$= 1 + \binom{p}{1} ap^e + \sum_{k=2}^{p} \binom{p}{k} a^k p^{k(e-1)}$$

לפי הבינום של ניוטון:

אם $p \geq 3$ אז כמעט $p^{e+1} \mid p^{2e-1}$ כי $2e-1 \geq e+1$

$$\equiv 1 + ap^e \pmod{p^{e+1}}$$

$$(1+ap)^{p^{e-1}} \equiv 1 + ap^e \pmod{p^{e+1}}$$

הוכחה: ✓

הוכחה: $p \neq 2$ אז $p^{e-1} \mid p-1$ כי $p-1$ זוגי.

$$(1+ap)^{p^{e-1}} \equiv 1 + ap^e \pmod{p^{e+1}}$$

$$(1+ap)^{p^{e-2}} \equiv 1 + ap^{e-1} \pmod{p^e}$$

$$a^p \equiv (1+ap^{e-1})^p \equiv 1 + ap^e \pmod{p^{e+1}}$$

$$(1+a^p) \quad a^{p^{e-1}} \equiv (1+ap^{e-1})^{p^{e-2}} \equiv 1 + ap^e \pmod{p^{e+1}}$$

נניח $a \not\equiv 1 \pmod{p}$ כלשהו זר ל- p. אז $a^{p^{e-1}} \not\equiv 1 \pmod{p^e}$

הוכחה: אם $e=1$ טריוויאלי.

נ.ט $a \not\equiv 1 \pmod{p}$ כלשהו זר ל- p. אז $a^{p^{e-1}} \not\equiv 1 \pmod{p^e}$

הוכחה: באינדוקציה על e: $e=1$ טריוויאלי.

המשך הוכחת משפט 6.3

המשך ההוכחה:

אבחן את g^{p-1}: $g^{p-1} \not\equiv 1 \pmod{p^2}$, $g^{p-1} \equiv 1 \pmod{p}$ — ברור

↓

אזי קיים a כך ש $g^{p-1} = 1+ap$ $p \nmid a$

לפי טענה 2 בשורה 3: $\operatorname{ord}_{p^e}(1+ap) = p^{e-1}$

לכן: $(1+ap)^n = (g^{p-1})^n \pmod{p^e}$

$\equiv (g^k)^{p-1} \equiv 1^{p-1} \equiv 1 \pmod{p^e}$

אבל הסדר של $1+ap$ מודולו p^e הוא p^{e-1} לכן $p^{e-1} \mid n$