

מרצה: פרופ' א. רזניקוב.
 משך בחינה: 3 שעות (לאחר הארכה).
 חומר עזר מותר בשימוש: מחשבון, דפי הרצאות.

עליהם לענות על כל 3 השאלות הבאות (ציון המקסימאלי הוא 100):

1.
 - (א) (20נק') מצא כל הפתרונות למשוואה $x^3 - 2x^2 + x - 3 \equiv 0 \pmod{3^3}$ לפי שיטת Hensel. נמקו את התשובה.
 - (ב) (20נק') תהי $p > 2$ ראשוני ו $a \in \mathbb{Z}$ כך ש $(a, p) = 1$. הוכיחו ש למשוואה $x^2 \equiv a \pmod{p^n}$ יש אותו מספר פתרונות כמו למשוואה $x^2 \equiv a \pmod{p}$.
2. (20נק') כמה פתרונות יש למשוואה $x^2 \equiv 5 \pmod{2^{13} - 1}$? (מספר $2^{13} - 1$ הינו ראשוני)
3. (40נק') תהי p ראשוני כך ש גם $q = 4p + 1$ הוא ראשוני. הוכיחו ש 2 הינו שורש פרימיטיבי \pmod{q} .
4. (40נק') הוכיחו ש יש אינסוף ראשוניים מהצורה $8n + 3$, $n \in \mathbb{Z}$. (אם P כפל של כל הראשוניים כאלה אזי תתבוננו במחלקים ראשוניים של המספר $P^2 + 2$)

בהצלחה!

$$x_1^{(0)} = 0, x_2^{(0)} = 1 \quad p=3 \quad \text{Hensel's Lemma} : 3 \mid N \quad f(1)$$

$$x_1^{(0)} = 0 \quad p \mid N \quad f'(x) \equiv 3x^2 - 4x + 1 \pmod{3} : \text{Hensel}$$

$$x_2^{(0)} = 1 \quad f'(0) \equiv 1 \pmod{3}$$

$$f(0) \equiv 0 - 3 \equiv -3 \pmod{3^2}, \quad x_1^{(1)} = 0 - \frac{-3}{1} \equiv 3 \pmod{3^2} : \text{Hensel}$$

$$f(3) \equiv 9 \pmod{27}, \quad x_1^{(2)} = 3 - \frac{9}{1} \equiv -6 \pmod{3^3}$$

$$x_1 \equiv -6 \pmod{27}$$

$1, 4, 7 \pmod{9}$: $x \equiv 1 \pmod{3}$ Hensel's Lemma

$$f(7) = 249 \not\equiv 0 \pmod{9}, \quad f(4) = 33 \not\equiv 0 \pmod{9}, \quad f(1) = -3 \not\equiv 0 \pmod{9}$$

$x \equiv 1 \pmod{3}$ Hensel's Lemma

$$x^2 \equiv a \pmod{p} \quad \text{Hensel's Lemma}$$

$$x^2 \equiv a \pmod{p^n} \quad \text{Hensel's Lemma}$$

$$f(x) = x^2 - a, \quad f'(x) = 2x$$

$$(2, p) = (a, p) = 1 \quad f'(a) = 2a \not\equiv 0 \pmod{p}$$

Hensel's Lemma

