

מועד א.

ועדת המשמעות נזהרה!
נבחן המעביר חומר צד לרעהו
או רמז מילולי יענש בחומרה

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. (30 נק') מצא כל הפתרונות למשוואה $x^3 - 2x^2 + x - 3 \equiv 0 \pmod{3^3}$ לפי שיטת Hensel. נמקו את התשובה.

2. יהיו $n = pq$ כאשר $p, q \equiv 3 \pmod{4}$ ראשוניים שונים ו- $a \in \mathbb{Z}$ ש"ר זרה \pmod{n} (כלומר המשוואה $x^2 \equiv a \pmod{n}$ פתירה ו- $(a, n) = 1$).

(א) (15 נק') הוכיחו ש למשוואה $x^2 \equiv a \pmod{n}$ יש 4 פתרונות שונים.

(ב) (20 נק') הוכיחו ש רק אחד מהפתרונות מסיף (א) הוא ש"ר \pmod{n} .

3. (35 נק') תהי $p > 3$ ראשוני. הוכיחו ש- $\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{6} \\ -1 & p \equiv 5 \pmod{6} \end{cases}$

בהצלחה!

17 ג

$x^2 \equiv a \pmod{p}!$ $x^2 \equiv a \pmod{q}$ א כוונתו \in ה' ג' $x^2 \equiv a \pmod{pq}$ (כ 2

סדר p, q ו 2 ג' p' מ' 3 א 2 x_1, x_2 א $(a, n) = 1 - p$
($x_1 \equiv -x_2$), $x^2 \equiv a \pmod{p}$ - δ ג' x_1, x_2 א

($y_1 \equiv -y_2$), $x^2 \equiv a \pmod{q}$ δ ג' y_1, y_2 !

(*) $\begin{cases} x \equiv x_i \pmod{p} \\ x \equiv y_i \pmod{q} \end{cases}$ א ג' s_k מ' n

$x^2 \equiv a \pmod{pq}$ δ פ' q ג' y מ' n

א $(p, q) = 1 - p$ א x ג' p א n א q א x ג' q א p א n א

$x \equiv y_i \pmod{q}!$ $x \equiv x_i \pmod{p}$ (כ q א' δ)

ג' p א n א x_i א p א n א x_i א p א n א δ

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ $p \equiv 3 \pmod{4} - p$ δ

(*) א' א n א p א q א n א p א q א n א p א q א n א

$s_k \quad p = 6k + 1 \quad p \quad . 3$

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{3k}$

$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{3k} \cdot \left(\frac{p}{3}\right) = (-1)^{3k} \left(\frac{1}{3}\right) = (-1)^{3k}$

$\left(\frac{-1 \cdot 3}{p}\right) = (-1)^{3k} \cdot (-1)^{3k} = (-1)^{6k} = 1.$ \Leftarrow

$p = 6k + 5$ δ ג' p א n א