

ועדת המשמעת מזהירה!
נבחן המעביר חומר עזר לרעהו
או רמז מילולי יענש בחומרה

(88-576)

תורת המספרים

2012

מועד א.

מרצה: פרופ' א. רזניקוב.

משך בחינה: 3 שעות (כולל הארכה).

חומר עזר מותר בשימוש: מחשבון, דפי הרצאות.

עליך לענות על כל 3 השאלות הבאות:

1. (א) יהיו ראשוני $p \neq 2$ ו- $a_1, \dots, a_p \in \mathbb{Z}$ ו- $b_1, \dots, b_p \in \mathbb{Z}$ שתי מערכות שלמות מודולו p . הוכיחו ש- $a_1 \cdot b_1, \dots, a_p \cdot b_p \in \mathbb{Z}$ איננה מערכות שלמות מודולו p . (10 נק.).
(ב) פתרו את המשוואה: $x^3 + 9x^2 + 2x + 3 \equiv 0 \pmod{3^3}$ לפי שיטת Hensel. (20 נק.)

2. יהי $p \equiv 3 \pmod{4}$ ראשוני. הוכיחו ש- $((p-1)/2)! \equiv (-1)^t \pmod{p}$. כאשר t הוא מספר שלמים $0 < a < p/2$ שאינם שאריות רבועות \pmod{p} . (30 נק.)

3. הוכיחו שקיימים אינסוף ראשוניים מהצורה $5k+4$.
(רמז: הוכיחו שלכל $n > 1$, למספר $N = 5(n!)^2 - 1$ יש מחלק ראשוני $p > n$ מהצורה $5k+4$. תשתמשו בהדדיות ריבועית של Gauss ל- $\left(\frac{p}{5}\right)$. (40 נק. +10 נק. בנוס על פתרון מלא)

בהצלחה!

F 2012

88-576 - פירושון ה' אורח

$i \neq j \quad ! \quad b_j \equiv 0 \pmod{p} \quad ! \quad a_i \equiv 0 \pmod{p}$ or . & 1.

$a_i b_i, a_j b_j \equiv 0$...
 $\{a_k b_k\}_{k=1, \dots, p}$

$a_i \equiv b_i \equiv 0 \pmod{p}$ (or not)

$a_2 \dots a_p \quad ! \quad b_2 \dots b_p$...

$a_2 \dots a_p \equiv b_2 \dots b_p \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \equiv -1 \pmod{p}$ Wilson's th

$(a_2 b_2) \cdot \dots \cdot (a_{p-1} b_{p-1}) \equiv (-1) \cdot (-1) \equiv 1 \pmod{p}$

$\{a_k b_k\}_{k=1, \dots, p} \in (1 \neq -1 \quad p \neq 2 \quad -\dots)$

0, 1, 2 : 3 ...

$f(x) = 3x^2 + 9x + 2$
 $f(x) \equiv 2 \pmod{3}$

$2 \cdot t \equiv -\frac{f(0)}{3} \equiv -1 \pmod{3}$... $x_0 \equiv 0 \pmod{3}$ or
 $x_2 = 0 + 1 \cdot 3 = 3 \pmod{9} \quad t = 1 \quad !$

$2 \cdot t \equiv -\frac{f(3)}{9} \equiv -13 \equiv -1 \pmod{3}$...
 $t \equiv 1 \pmod{3}$

$x_3 = 3 + 1 \cdot 9 \equiv 12 \pmod{27}$...

so $\forall n \in \mathbb{Z} \quad 1 \leq n \leq p-1$ we have $p \equiv 3 \pmod{4}$ s. 2

(...) p is odd $p-1$

$$\binom{p-n}{p} = \binom{-n}{p} = \binom{-1}{p} \binom{n}{p} = -\binom{n}{p} \quad ! \quad \binom{-1}{p} = (-1)^{\frac{p-1}{2}} = -1$$

for $0 < a_i < \frac{p}{2}$ and a_1, \dots, a_t is

for $0 < b_i < \frac{p}{2}$, b_{t+1}, \dots, b_q ! $\forall p \in \mathbb{Z}$

$p \nmid q$ and $q = \frac{p-1}{2}$, $\forall p$

$$\left(\frac{p-1}{2}\right)! = 1 \cdot 2 \cdot \dots \cdot \left(\frac{p-1}{2}\right) \equiv a_1 \cdot a_t \cdot b_{t+1} \cdot \dots \cdot b_q \pmod{p}$$

$\forall p-a_i$! $\frac{p}{2} < p-a_i \leq p-1$ and $p-a_i - 2 \in \mathbb{Z}$

$$(-a_1), \dots, (-a_t), b_{t+1}, \dots, b_q \in p-a_i \neq b_j \pmod{p} \text{ and } \dots$$

$\forall p \nmid q$ is $p \in \mathbb{Z}$ and \dots

$$\left(\frac{p-1}{2}\right)! \equiv a_1 \cdot \dots \cdot a_t \cdot b_{t+1} \cdot \dots \cdot b_q \equiv (-1)^t \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$$

$\forall p \nmid g$ is $p \in \mathbb{Z}$ and \dots

$$\left(\frac{p-1}{2}\right)! \equiv g^2 \cdot g^4 \cdot \dots \cdot g^{p-1} = g^{\frac{(p-1)(p+1)}{2}} = \left(g^{\frac{p-1}{2}}\right)^{p+1} \equiv (-1)^{p+1} \equiv 1 \pmod{p}$$

(...) $\forall p \in \mathbb{Z}$ and g $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^t \cdot 1 \equiv (-1)^t \pmod{p} \Leftarrow$$

$p \equiv 0, 1, 2, 3, 4 \pmod{5}$ $\Rightarrow p \nmid p_k \Rightarrow \delta_5$.3

$p \nmid N = 5(n!)^2 - 1$ \bar{s}_k $p \equiv 0 \pmod{5}$ or

$p \equiv 1 \pmod{5}$ or $p \mid N$ $\nRightarrow p \mid N = 5(n!)^2 - 1$ δ or

or $N \equiv 1 \pmod{5}$ or \bar{s}_k

$p \nmid 5(n!)^2 - 1 \in p \mid n!$ \bar{s}_k $p \leq n$ or

$p \nmid 5(n!)^2 - 1$ \bar{s}_k $p \equiv 2, 3 \pmod{5}$ or $p \leq n$

$5(n!)^2 \equiv 1 \pmod{p}$ \bar{s}_k $p \mid 5(n!)^2 - 1$ or

$\left(\frac{5(n!)^2}{p}\right) = \left(\frac{1}{p}\right) = 1$ Legendre δ $p \nmid n!$ δ_5

\bar{s}_k

$1 = \left(\frac{5(n!)^2}{p}\right) = \left(\frac{5}{p}\right) \left(\frac{(n!)^2}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$

$(n!)^2 \equiv 1 \pmod{p}$ \bar{s}_k $5 \equiv 1 \pmod{4}$ \Rightarrow \bar{s}_k \bar{s}_k

$1, 4 \mid 5 \mid 13 \mid N$ or p

$p \not\equiv 3 \pmod{5} \Leftarrow$

$p > n$ or $p \mid N$ or $p \mid 5(n!)^2 - 1$ $\delta \Leftarrow$

$p \equiv 4 \pmod{5}!$

$n = p_1 \cdots p_k$ δ \bar{s}_k $p_1 \cdots p_k \equiv 4 \pmod{5}$ or $p_i \equiv 4 \pmod{5}$ or $p_i \equiv 1 \pmod{5}$ or $p_i \equiv 2 \pmod{5}$ or $p_i \equiv 3 \pmod{5}$

$p \mid 5(n!)^2 - 1$ $! p_i \neq p \equiv 4 \pmod{5}$ or $p_i \equiv 1 \pmod{5}$ or $p_i \equiv 2 \pmod{5}$ or $p_i \equiv 3 \pmod{5}$

δ or $p_i \equiv 4 \pmod{5}$ or $p_i \equiv 1 \pmod{5}$ or $p_i \equiv 2 \pmod{5}$ or $p_i \equiv 3 \pmod{5}$