תורת המספרים — שאלות חזרה

משה קמנסקי

24 בינואר 2021

1. (א) הוכיחו שלכל ראשוני p ולכל $c \in \mathbb{F}_p$ יש $a, b \in \mathbb{F}_p$ כך ש-$a^2 + b^2 = c$

   (ב) הוכיחו שאם n מכפלה של ראשוניים שונים ו-m שלם כלשהו, אז יש שלמים a, b כך ש-$a^2 + b^2 + m$ מתחלק ב-n.

2. הוכיחו שהפתרון היחיד של המשוואה $x^2 = y^3 + y$ בשלמים הוא 0, אבל יש לה פתרון שונה מ-0 ב-$\mathbb{Z}[i]$ (רמז: הוכיחו ראשית ש-a ו-$a^2 + 1$ זרים).

3. הוכיחו שראשוני p הוא מהצורה $n^2 - 2m^2$ אם ורק אם $p = 2$ או שהוא מהצורה $8k \pm 1$

4. נניח ש-p ראשוני אי-זוגי. נסמן ב-S את קבוצת הריבועים ב-${\mathbb{F}_p}^\times$. הוכיחו ש-$\prod S = \left(\frac{-1}{p}\right)$, ושאם $p > 3$ אז $\sum S = 0$.

5. נניח ש-$p = 2^k + 1$ ראשוני. הוכיחו ש-$a \in U_p$ יוצר של החבורה אם ורק אם אינו ריבוע ב-$\mathbb{F}_p$. הסיקו שאם $k > 1$ אז U_p נוצרת על-ידי 3.

6. הוכיחו שאם $\left(\frac{n}{p}\right) = 1$ עבור n שלם ו-p ראשוני, אז n הוא ריבוע ב-$\mathbb{Z}/p^k$ לכל $k > 0$.

7. מיצאו התאמה הפיכה בין זוגות ראשוניים $p, p + 2$ (כלומר, ראשוניים תאומים) למספרים טבעיים n עבורם ל-$n^2 - 1$ יש בדיוק ארבעה מחלקים חיוביים. הוכיחו גם שיש בדיוק ראשוני אחד ששייך לשני זוגות כאלה.

8. הוכיחו שאם $m_0, \dots, m_k$ מספרים חיוביים עוקבים, אז יש חזקה של 2 שמחלקת בדיוק אחד מהם. הסיקו שאם $a_0, \dots, a_k$ אי-זוגיים ו-$k > 0$ אז $\sum_i \frac{a_i}{m_i}$ אינו שלם.

9. הוכיחו שאם $d|m$ אז $\phi(d)|\phi(m)$

10. מיהם הראשוניים p שעבורם $n + 3$ הפכים של $n - 3$ ב-$\mathbb{F}_p$, עבור איזשהו שלם n?

11. הוכיחו שאם ראשוני p מחלק את $n^2 + 1$ ואת $m^2 + 2$ עבור שלמים כלשהם m, n, אז הוא מחלק גם מספר מהצורה $k^4 + 1$ (רמז: חישבו מה קורה ב-$\mathbb{C}$)

12. נניח ש-$f(n)$ פולינום עם מקדמים שלמים (במשתנה אחד).

   (א) הוכיחו שקיימים שני ראשוניים שונים p, q ומספרים שלמים n, m כך ש-$f(m)$ מתחלק ב-p ו-$f(n)$ מתחלק ב-q.

   (ב) הוכיחו שיש אינסוף ראשוניים p כך של-$\bar{f}$ יש שורש ב-$\mathbb{F}_p$ (כאשר $\bar{f}$ הפולינום שמתקבל מ-f על-ידי הפעלת פונקציית השארית על המקדמים)

13. נניח ש-$g \in G$ כאשר G חבורה חילופית סופית. הוכיחו ש-$g^m = e$ אם ורק אם $\chi^m(g) = 1$ לכל $\chi \in \check{G}$, וש-$g = h^m$ לאיזשהו $h \in G$ אם ורק אם $\chi(g) = 1$ לכל $\chi \in \check{G}$ המקיים $\chi^m = 1$.

14. אילו מזוגות התבניות הבאות הן שקולות? (נמקו)

(א) $x^2 + xy + y^2, x^2 - xy + y^2$

(ב) $3x^2 + 6y^2, x^2 + 18y^2$

(ג) $x^2 + 3y^2, 28x^2 + 130xy + 151y^2$

(ד) $x^2 + 3y^2, x^2 + 4xy + y^2$

(ה) $x^2 + 5y^2, 2x^2 + 2xy + 3y^2$

15. הוכיחו שאם g איבר מסדר m בחבורה חילופית מסדר n, אז $\prod_{\chi \in \check{G}}(1 - \chi(g)X) = (1 - X^m)^{\frac{n}{m}}$ (רמז: התחילו מהמקרה $n = m$)

16. נניח ש-$p > 3$ ראשוני. הוכיחו שאם ל--3 יש שורש ריבועי ב-$\mathbb{F}_p$ אז לכל $a \neq 0$ ב-$\mathbb{F}_p$ למשוואה $x^3 = a$ יש שלושה פתרונות או אפס, ואחרת לכל איבר יש שורש שלישי יחיד.

17. נניח ש-H תת-חבורה של חבורה חילופית סופית G (אז $\mathbb{C}[H]$ תת-חוג של $\mathbb{C}[G]$). הוכיחו שלכל $a \in \mathbb{C}[H]$ ולכל $\chi \in \check{G}$ מתקיים $\mathcal{F}_G(a)(\chi) = \mathcal{F}_H(a)(\chi_H)$. הסיקו שלכל $a = \sum_{h \in H} a_h h \in \Bbbk[H]$ כזה $\sum_{\chi \in H^\perp} \mathcal{F}_G(a)(\chi) = |H^\perp| \sum_{h \in H} a_h$ (כאשר $H^\perp = \{\chi \in \check{G} \mid \chi(h) = 1 \forall h \in H\}$)

18. עבור $G = \mathbb{Z}/4$ ועבור $G = \mathbb{Z}/2 \times \mathbb{Z}/2$, חשבו את מטריצת המעבר מהבסיס סטנדרטי של $\mathbb{C}^G$ לבסיס שנתון על-ידי איברי $\check{G}$

19. האם ל-117 יש שורש ביחס ל-3553?

20. נניח ש-$p(x, y)$ תבנית עם דיסקרימיננטה חיובית. הוכיחו שהיא מייצגת גם מספרים חיוביים וגם שליליים.

21. נניח ש-p ראשוני ו-$k > 0$ שלם. חשבו את השארית של $\sum_{i=1}^{p} i^k$ ביחס ל-p (הפרידו בין המקרים ש-k מתחלק ב-$p - 1$ ולא)

22. נזכיר שאם $\Bbbk$ חוג, נגדיר לכל פונקציה $f : \mathbb{N}_+ \to \Bbbk$ פונקציה חדשה $S(f) : \mathbb{N}_+ \to \Bbbk$ על-ידי $S(f)(n) = \sum_{d|n} f(d)$ (כלומר, סכום על כל המחלקים). נזכיר ש-f היא כפלית אם $f(nm) = f(n)f(m)$ לכל n, m זרים.

(א) הוכיח שאם $\Bbbk$ תחום ו-f כפלית ואינה זהותית 0 אז $f(1) = 1$. הראו שזה לא בהכרח נכון אם $\Bbbk$ אינו תחום.

(ב) הוכיחו שאם f כפלית אז גם $S(f)$ כפלית

(ג) הוכיחו ש-$S(\phi)(n) = n$ לכל n (כאשר ϕ פונקציית אוילר)

(ד) נגדיר $\mu(p_1 \dots p_k) = (-1)^k$ אם p_i ראשוניים שונים, ו-$\mu(n) = 0$ לכל n עם ריבוי. חשבו את $S(\mu)$.

23. הוכיחו שחוג השלמים של $\mathbb{Q}(\sqrt{-6})$ אינו תחום פריקות יחידה

24. הוכיחו ש-798 מחלק את $a^{19} - a$ לכל a שלם.

25. נניח ש-p ראשוני, וש-$a_1, \dots, a_p$ ו-$b_1, \dots, b_p$ מערכות נציגים ביחס ל-p (כלומר, $a_i - a_j$ לא מתחלק ב-p עבור $i \neq j$), וגם $a_1 b_1, \dots, a_p b_p$ מערכת נציגים. חשבו את p.

26. נניח ש-n שלם חיובי, ו-a, b שלמים המקיימים $a^2 - nb^2 = 1$. הוכיחו שאם $c + \sqrt{n}d = (a + \sqrt{n}b)^k$ ב-$\mathbb{Q}(\sqrt{n})$ עבור איזשהו n, אז גם $c^2 - nd^2 = 1$. הסיקו שלמשוואה $x^2 - 3y^2 = 1$ יש אינסוף פתרונות שלמים.