دانشگاه صنعتی شریف

نظریه اعداد | امتحان پایان‌ترم | تاریخ سه‌شنبه ۲ بهمن ۱۳۸۶

مدت: ۳ ساعت

---

۱ الف) فرض کنید a یک عدد صحیح و p یک عدد اول فرد باشد و $p \nmid a$. فرض کنید μ تعداد اعضای مجموعه $S = \{a, 2a, \cdots, \frac{p-1}{2}a\}$ باشد که باقیمانده تقسیم‌شان بر p از $\frac{p}{2}$ بیشتر باشد. آنگاه $(\frac{a}{p}) = (-1)^{\mu}$. (۸ نمره)

ب) فرض کنید p و $4p+1$ هردو اول باشند. ثابت کنید 2 یک ریشه اولیه به پیمانه $4p+1$ است. (۸ نمره)

ج) کوچکترین عدد اول q را پیدا کنید به‌طوری‌که $(\frac{-1}{q}) = (\frac{-2}{q}) = (\frac{-3}{q}) = 1$. (۷ نمره)

۲ الف) فرض کنید $\zeta = e^{\frac{2\pi i}{p}}$ که در اینجا p یک عدد اول فرد است. قرار می‌دهیم $g_a = \sum_{t=0}^{p-1} (\frac{t}{p})\zeta^{at}$. نشان دهید $g_a = (\frac{a}{p})g_1$ و $g_1^2 = (-1)^{\frac{p-1}{2}}p$. (۸ نمره)

ب) برای $p = 11$ و $p = 13$ حاصل مجموع‌های $S_p = \sum_{a=1}^{p-1} g_a$ و $T_p = \sum_{1 \leqslant a < b \leqslant p-1} g_a g_b$ را به‌طور صریح به‌دست آورید. (۸ نمره)

۳ الف) عدد اول p را در نظر می‌گیریم. تساوی‌های زیر را ثابت کنید:

$$\prod_{\alpha \in \mathbb{Z}_{/p}} (x - \alpha) = (x^p - x) \in \mathbb{Z}_{/p}[x]$$
$$\prod_{\alpha \in \mathbb{Z}_{/p}} (x^p - x - \alpha) = (x^{2p} - 2x^p + x) \in \mathbb{Z}_{/p}[x]$$

(۷ نمره)

ب) ثابت کنید تعداد چندجمله‌ای‌های تکین تحویل‌ناپذیر از درجه n روی $\mathbb{Z}_{/p}$ برابر است با $\frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})p^d$ است. (۸ نمره)

۴ الف) ثابت کنید $\mathbb{Z}[\sqrt{-2}]$ یک دامنه اقلیدسی است. (۷ نمره)

ب) نشان دهید هر عدد اول به‌صورت $p = 8k+1$ یا $p = 8k+3$ را می‌توان به‌صورت $x^2 + 2y^2$ نوشت. برای $p = 41$ و $p = 43$ این نمایش را به‌طور صریح ارائه کنید. (۸ نمره)

ج) همه جواب‌های صحیح معادله $y^2 = x^3 - 2$ را پیدا کنید. (۷ نمره)

۵ الف) فرض کنید $\alpha = 28i$ و $\beta = 5 + 5i$. چند زوج $(q, r) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ وجود دارد به‌طوری‌که $\alpha = \beta q + r$ و $N(r) < N(\beta)$ ؟ همه این زوج‌ها را پیدا کنید. (۷ نمره)

ب) ب م م α و β را به‌صورت ترکیب خطی این دو عدد بیان کنید. (۷ نمره)

۶ (سؤال اختیاری) ثابت کنید برای هر عدد اول p ، چندجمله‌ای $x^4 + 1$ روی $\mathbb{Z}_{/p}$ تحویل‌پذیر است.

موفق باشید