به نام خدا

نظریه اعداد | امتحان پایان ترم | تاریخ یکشنبه ۲۹ دی ۱۳۸۷

مدت: ۳ ساعت

---

۱ الف) محک اویلر: اگر p یک عدد اول فرد و a یک عدد صحیح که نسبت به p اول باشد ثابت کنید $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \mod p$.
(۶ نمره)

ب) مقدار سمبل ژاکوبی $(\frac{123}{917})$ را محاسبه کنید. (۶ نمره)

۲ الف) اگر p یک عدد اول فرد باشد ثابت کنید $\sum_{a=1}^{p-1}(\frac{a}{p}) = 0$. (۶ نمره)

ب) فرض کنید p یک عدد اول فرد و g یک ریشه اولیه به پیمانه p باشد. نشان دهید $g-$ یک ریشه اولیه به پیمانه p است اگر و تنها اگر $p \equiv 1 \mod 4$. (۶ نمره)

ج) یک ریشه اولیه به پیمانه هر کدام از اعداد 7، 14 و 7^3 بیابید. (۶ نمره)

۳ الف) p یک عدد اول بزرگتر از 3 است. نشان دهید $(\frac{-3}{p}) = 1$ اگر و تنها اگر p به صورت $3k+1$ باشد. (۶ نمره)

ب) ثابت کنید نامتناهی تا عدد اول به صورت $3k+1$ وجود دارد. (۶ نمره)

۴ الف) نشان دهید $\sqrt{-6}$ در $\mathbb{Z}[\sqrt{-6}]$ اول نیست. (۶ نمره)

ب) نشان دهید $\sqrt{-6}$ در $\mathbb{Z}[\sqrt{-6}]$ تحویل ناپذیر است. (۶ نمره)

۵ الف) همه جواب های صحیح معادله سیاله $x^3 = y^2 + 1$ را بیابید. (۶ نمره)

ب) کدام یک از اعداد گاوسی i، $2i$، $3+4i$، -17، 19 و $-2+5i$ اول هستند؟ (۶ نمره)

ج) دو عدد گاوسی $a = 10i$ و $b = 4+3i$ را در نظر می گیریم. چند زوج $(q,r) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ وجود دارند به طوری که $a = bq + r$ و $N(r) < N(b)$؟ همه این زوج ها را پیدا کنید. (۶ نمره)

۶ الف) تعداد چند جمله ای های تکین تحویل ناپذیر درجه 3 را روی $\mathbb{F}_3$ به دست آورید؟ یکی از این نوع چند جمله ای ها را پیدا کنید. (۶ نمره)

ب) چند عضو اولیه در $\mathbb{F}_9$ وجود دارد؟ یکی از آنها را پیدا کنید. (۶ نمره)

ج) وزن کد خطی 0000, 0121, 0212, 1022, 1110, 1201, 2011, 2102, 2220 (روی $\mathbb{F}_3$) را پیدا کنید. این کد چند خطا را می تواند تصحیح و چند خطا را می تواند تشخیص دهد؟ (۶ نمره)

موفّق باشید