دانشگاه صنعتی شریف

نظریه اعداد | امتحان میان‌ترم | تاریخ پنجشنبه ۲۴ آبان ۱۳۸۶

مدت: ۳ ساعت

---

۱ الف) ب م م 2007 و 1386 را به صورت ترکیب خطی این دو عدد بیان کنید. (۴ نمره)

ب) ثابت کنید تعداد تقسیم‌های لازم در الگوریتم اقلیدس برای محاسبه ب م م دو عدد حداکثر به‌اندازه پنج برابر تعداد ارقام کوچکترین این دو عدد است. (۶ نمره)

ج) نشان دهید برای هر n ، n عدد صحیح متوالی وجود دارند که هیچ‌یک اول نیستند. (۳ نمره)

۲ الف) اگر p_n نمایش دهنده n امین عدد اول باشد آنگاه $p_n \leqslant 2^{2^n}$. (۴ نمره)

ب) نشان دهید سری $\Sigma \frac{1}{p}$ (که مجموع روی همه اعداد اول p گرفته شده است) واگراست. (۶ نمره)

ج) صورت قضیه اعداد اول را بیان کنید. با استفاده از آن ثابت کنید وقتی‌که x به بی‌نهایت میل می‌کند $\pi(ax)/\pi(bx)$ به a/b میل می‌کند که در اینجا a و b دو عدد مثبت هستند. (۵ نمره)

۳ الف) برای $a = 2^2 \times 7^2 \times 19^2 \times 23^2 \times 91^2$ مقدار $\tau(a)$ را پیدا کنید. (۳ نمره)

ب) نشان دهید $\sigma(n)$ فرد است اگر و تنها اگر n یک مربع کامل یا دو برابر یک مربع کامل باشد. (۴ نمره)

ج) f یک تابع حسابی است و $F(n) = \Sigma_{d|n} f(d)$. نشان دهید f نیز ضربی است اگر و تنها اگر F چنین باشد. (۶ نمره)

د) نشان دهید برای هر m, n تساوی $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$ برقرار است که در اینجا d ب م م m و n است. (۴ نمره)

۴ الف) کوچکترین جواب صحیح مثبت دستگاه معادلات همنهشتی $\begin{cases} x \equiv 1 \mod 8 \\ x \equiv 9 \mod 13 \\ x \equiv 10 \mod 19 \end{cases}$ را پیدا کنید. (۵ نمره)

ب) یکی از آزمونهای بخشپذیری بر 7 را با ذکر اثبات بیان کنید. (۴ نمره)

ج) نشان دهید n اول است اگر و تنها اگر $(n-1)! \equiv -1 \mod n$. (۶ نمره)

د) a و b دو عدد نسبت به هم اول هستند. اگر دوره تناوب کسر $\frac{a}{b}$ چهار باشد در مورد a و b چه می‌توان گفت؟ (۴ نمره)

۵ الف) اگر $k \geqslant 3$ آنگاه ریشه اولیه به پیمانه 2^k وجود ندارد. (۶ نمره)

ب) یک ریشه اولیه به پیمانه اعداد 11 ، 121 و 22 پیدا کنید. (۵ نمره)

ج) جدول اندیس را در مبنای ریشه اولیه‌ای که در قسمت (ب) برای 22 به‌دست آورده‌اید تشکیل دهید. (۴ نمره)

د) همه جوابهای معادله $3x^{17} \equiv 2 \mod 22$ را در صورت وجود به‌دست آورید. (۴ نمره)

۶ الف) با ذکر یک مثال روش RSA و چگونگی به‌کار بردن آن برای رمزنگاری و رمزگشایی را توضیح دهید. (۴ نمره)

ب) توضیح دهید چرا امنیت این روش در صورت پیدا شدن یک الگوریتم سریع برای تجزیه به خطر می‌افتد. (۳ نمره)

موفق باشید