به نام خدا

نظریه اعداد | امتحان میان ترم | تاریخ پنجشنبه ۱۹ آبان ۱۳۹۰

مدت: ۳ ساعت

---

۱ الف) همه جوابهای صحیح معادله دیوفانتی $6x + 10y + 15z = 1$ را به دست آورید.
ب) اعداد صحیح a، b و c داده شده اند. ثابت کنید اگر معادله دیوفانتی $ax + by = c$ حلپذیر باشد آنگاه جواب (x_0, y_0) از آن وجود دارد به طوری که $0 \leqslant x_0 < |b|$.

۲ الف) باقیمانده تقسیم 5^{2011} را بر 12 و باقیمانده تقسیم $7^{(5^{2011})}$ را بر 36 پیدا کنید.
ب) همه اعداد اول p که طول دوره تناوب بسط اعشاری $\frac{1}{p}$ برابر با 3 باشد را شناسایی کنید.

۳ یك جواب صحیح مثبت معادله $x^2 + x + 1 \equiv 0 \pmod{133}$ را پیدا کنید. (توجه : $133 = 7 \times 19$).

۴ از موارد زیر فقط به دو مورد پاسخ دهید.
الف) کران بالا و پایین مناسبی برای p_n (n امین عدد اول) بیابید.
ب) نشان دهید برای هر $y \geqslant 2$ داریم $\sum_{p \leqslant y} \frac{1}{p} > (\log\log y) - 1$ که در اینجا مجموع روی همه اعداد اول کمتر یا مساوی y بسته شده است.
ج) نشان دهید ثابت c موجود است به طوریکه برای هر $x \geqslant 2$ داریم $\pi(x) \leqslant c\frac{x}{\log x}$. در اینجا $\pi(x)$ تعداد اعداد اول کوچکتر یا مساوی x است.
د) صورت قضیه اعداد اول را به طور دقیق بیان کنید و نشان دهید صحت آن معادل با $\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$ است.

۵ الف) همه جوابهای معادله $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$ را پیدا کنید.
ب) فرض کنید $f(x)$ یک چند جمله ای با ضرایب صحیح، p یک عدد اول و $a \in \mathbb{Z}$ به گونه ای باشد که $f(a) \equiv 0 \pmod{p^j}$ و $f'(a) \not\equiv 0 \pmod{p}$. فرض کنید $\overline{f'(a)}$ عدد صحیحی باشد به طوری که $f'(a)\overline{f'(a)} \equiv 1 \pmod{p^{2j}}$ و قرار دهید $b = a - f(a)\overline{f'(a)}$. نشان دهید $f(b) \equiv 0 \pmod{p^{2j}}$.

۶ الف) فرض کنید p یک عدد اول و d یک عدد صحیح مثبت باشد به طوری که $d|p-1$. نشان دهید معادله $x^d \equiv 1 \pmod{p}$ دقیقا d جواب متمایز به پیمانه p دارد. اگر به جای شرط $d|p-1$ فقط شرط $d \leqslant p-1$ را قرار دهیم آیا این حکم هنوز درست است؟
ب) نشان دهید به پیمانه هر عدد اول p ریشه اولیه وجود دارد.

۷ الف) در روش RSA با کلید عمومی $(n, e) = (22, 7)$ پیام $m = 3$ را رمز کنید. اگر پیام رمز شده $m' = 5$ را دریافت کرده باشیم، پیام اصلی چه بوده است؟
ب) در روش تبادل دیفی هلمن، به کمک عدد اول $p = 13$ و ریشه اولیه $g = 2$، دو نفر اعداد 6 و x را مبادله کرده اند. اگر عدد مشترک انتخاب شده بین آنها 3 باشد، x چه بوده است؟

موفّق باشید