PROBLEM OF THE WEEK

Solution of Problem No. 7 (Fall 2003 Series)

Problem: Given a prime number p, prove that the polynomial congruence $(x+y)^n \equiv x^n + y^n \pmod p$ is true if and only if n is a power of p.

Solution (by the Panel)

Let $P(x,y) = (x+y)^n - x^n - y^n = \displaystyle\sum_{k=1}^{n-1} \binom{n}{k} x^k y^{n-k}$.

(a) If $n = p^a$, then all the coefficients of P are divisible by p.

Proof: For $1 \le j \le p^a - 1$, $\binom{p^a}{j} = \dfrac{p^a}{j}\dbinom{p^a-1}{j-1}$. If $j = rp^b$ where $(r,p) = 1$, then $\dfrac{p^a}{j} = \dfrac{p^{a-b}}{r}$ where $a - b \ge 1$ (since $j < p^a$). Thus r must divide $\binom{p^a-1}{j-1}$ (since $\binom{p^a}{j}$ is an integer), and $\binom{p^a}{j}$ is divisible by p^{a-b}.

(b) If n is not a power of p then not all $\binom{n}{j}$ are divisible by p.

Proof: For $p^a < n < p^{a+1}$, let $c = n - p^a$ so $0 < c < p^a(p-1)$. Then $\binom{n}{c} = \binom{p^a+c}{c} = \displaystyle\prod_{j=1}^{c} \frac{p^a+j}{j}$. If $j = rp^b$ where $(r,p) = 1$ and $b < a$, then $\dfrac{p^a+j}{j} = \dfrac{p^{a-b}+r}{r}$. From this $\binom{n}{c}$ equals a product of fractions none of whose numerators is a multiple of p.

Remark. Prof. Landy thought to have given a counter example to part (a). However, the assertion $f(x,y) = (x+y)^n - x^n - y^n \equiv 0$ is not meant as $f(x,y) \equiv 0$ for all integers x, y, but that every coefficient of the polynomial $f(x,y)$ is congruent to zero $\pmod p$.

Also solved by:

Undergraduates: Michael Chun Chang (So. Bio/Chem), Jignesh V. Mehta (So. Phys)

Graduates: Jianguang Guo (Phys)

Faculty: Steven Landy (Physics at IUPUI)

Six incorrect solutions were received.

Jason Anema (Jr. MA) submitted a late correct solution of Problem 5.