MATH 430 Problem Set 5

Qilin Ye

October 10, 2020

Problem 1

Show that

$$k!(p-1-k)! \equiv (-1)^{k+1} \pmod p$$

where p is any prime and $0 \leqslant k \leqslant p-1$. Hint: use Wilson's Theorem.

Solution

$$\begin{aligned}
k!(p-1-k)! &\equiv \left(\prod_{i=1}^{k} i\right)(p-1-k)! \\
&\equiv \left(\prod_{i=1}^{k} -(p-i)\right)(p-1-k)! && [\text{Since } p-i \equiv -i \pmod p] \\
&\equiv (-1)^k \left(\prod_{i=1}^{k}(p-i)\right)(p-1-k)! \\
&\equiv (-1)^k \left[(p-1)(p-2)\dots(p-k)(p-k-1)!\right] \\
&\equiv (-1)^k(-1) && [\text{By Wilson's Theorem}] \\
&\equiv (-1)^{k+1} \pmod p.
\end{aligned}$$

Problem 2

Let $N = 2^k$ for some $k \geqslant 1$. Find

$$\sum_{d \mid N} (-1)^{N/d} \varphi(d).$$

Solution

Notice that if N is of form 2^k, all its divisors are of form 2^n where $0 \leqslant n \leqslant k$. Therefore we know for all divisors $d \mid N$ except N itself, N/d is even — in particular it is a power of 2 — whereas N/d is odd if $d = N$. Therefore, for $d \mid N$,

$$(-1)^{N/d} = \begin{cases} 1 & \text{if } d \neq N \\ -1 & \text{if } d = N. \end{cases}$$

Also notice that, for some power 2^n with $n \geqslant 1$, $\varphi(2^n) = 2^{n-1}$ since there are precisely 2^{n-1} odd numbers not exceeding 2^n and they are the only numbers coprime to 2^n. We also need to take care of the special case $\varphi(2^0) = \varphi(1) = 1$. Therefore,

$$\begin{aligned} \sum_{d \mid N} (-1)^{N/d} \varphi(d) &= \sum_{i=0}^{k} (-1)^{(2^{k-i})} \varphi(2^i) \\ &= \varphi(1) + \sum_{i=1}^{k} (-1)^{(2^{k-i})} (2^{i-1}) \\ &= 1 + \sum_{i=1}^{k-1} 2^{i-1} - 2^{i-1} \\ &= 1 + (2^{i-1} - 1) - 2^{i-1} \\ &= 0. \end{aligned}$$

Problem 3

Let a, b be two integers and p a prime that does not divide b. Show, without using *Dirichlet's Theorem*, that there exist infinitely many terms which are divisible by p in the sequence

$$(a, a+b, a+2b, \ldots).$$

Solution

If a is a multiple of p then any integer of form $a + kpb$ with $k \in \mathbb{N}$ is a multiple of p and we are done.

On the other hand, if a is not a multiple of p, then $a \equiv (-n) \pmod{p}$ for some $-(p-1) \leqslant (-n) \leqslant -1$. Now look at b. Since $p \nmid b$, we know that $b \in (\mathbb{Z}/p\mathbb{Z})^*$. Therefore there exists an element $m \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $mb \equiv 1 \pmod{p}$. Then $mnb \equiv n \pmod{p}$ and so $a + mnb \equiv (-n) + n \equiv 0 \pmod{p}$ and we have found *one* term in the sequence divisible by p. Once again, anything of form $a + (mn + kp)b$ with $k \in \mathbb{N}$ is a multiple of p. Hence there are infinitely many terms divisible by p. $\square$