

# MAT 311: Number Theory

## Spring 2008

### Solutions to HW3

1. Show that if  $p$  is prime then  $(p-1)! \equiv p-1 \pmod{1+\cdots+p-1}$ .  
Note that  $1+\cdots+p-1 = p \cdot p-1/2$ . SO we need to prove that  $p \cdot p-1/2$  divides  $(p-1)! - (p-1) = (p-1)\{(p-2)! - 1\}$ . But this happens only if  $p$  divides  $(p-2)! - 1$ . But by the proof of Wilson's theorem from HW2, we see that  $(p-2)! \equiv 1 \pmod{p}$ , as required.  $\square$
2. Show that  $7 \mid 3^{2n+1} + 2^{n+2}$ , for every  $n \geq 0$ .  
 $3^{2n+1} \equiv 3 \cdot 9^n \equiv 3 \cdot 2^n \pmod{7}$ . Thus  $3^{2n+1} + 2^{n+2} \equiv 7 \cdot 2^n \equiv 0 \pmod{7}$ .  $\square$
3. Prove that if  $(a, 91) = (n, 91) = 1$ , then  $91 \mid n^{12} - a^{12}$ .  
 $91 = 13 \cdot 7$ . By Fermat's little theorem,  $n^{12} \equiv 1 \pmod{13}$  since  $(n, 13) = 1$ , and  $n^{12} = (n^2)^6 \equiv 1 \pmod{7}$  since  $(n, 7) = 1$  implies  $(n^2, 7) = 1$ . Thus  $n^{12} \equiv 1 \pmod{91}$ . Similarly,  $a^{12} \equiv 1 \pmod{91}$ . Thus  $n^{12} \equiv a^{12} \pmod{91}$ .  $\square$
4. Determine whether  $5x \equiv 1 \pmod{6}$ ,  $4x \equiv 13 \pmod{15}$  has a solution, and find them if exist.  
By multiplying first congruence by 5 and the second by 4, this gives  $x \equiv 4 \pmod{6}$  and  $x \equiv 12 \pmod{15}$ . Second congruence says that  $x$  has to be either 12 or 24 mod 30. First congruence says that  $x$  has to be either 4, 10, 16, 22, 28 mod 30. Thus, the system has no solution.  $\square$
5. Find  $\varphi(p^k)$  for  $p$  prime.  
This number is the number of integers  $n$  with  $1 \leq n \leq p^k$  coprime to  $p^k$ . Note that  $n$  has a common non-trivial factor with  $p^k$  iff it is a multiple of  $p$ . There are  $p^k/p = p^{k-1}$  of them. Thus  $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ .  $\square$
6. Find a homomorphism  $h : (\mathbb{Z}, +) \rightarrow (\mathbb{Q}^*, \cdot)$ .  
The constant map defined by  $h(n) = 1$  for every  $n \in \mathbb{Z}$  is such a homomorphism.  $\square$