

## NUMBER THEORY: HOMEWORK 4

TO BE HANDED IN BY THURSDAY 13TH FEBRUARY 2025 BY 6PM

1. (i) Find solutions of  $x^2 \equiv -1 \pmod{5}$  and  $x^2 \equiv -1 \pmod{17}$ . Hence, applying the Chinese Remainder Theorem, obtain a solution of  $x^2 \equiv -1 \pmod{85}$ .  
(ii) How many solutions does  $x^2 \equiv -1 \pmod{85}$  possess?
2. (i) Let  $p$  be a prime number. By applying Fermat's Little Theorem, or otherwise, show that the congruence  $x^p - x + 1 \equiv 0 \pmod{p}$  has no solution.  
(ii) How many solutions does the congruence  $x^{16} - x + 3 \equiv 0 \pmod{40}$  possess? Explain your answer.
3. By considering the prime factorisation of the integer 561, prove that whenever  $(a, 561) = 1$ , one has  $a^{80} \equiv 1 \pmod{561}$ . Hence prove that  $a^{560} \equiv 1 \pmod{561}$  whenever  $(a, 561) = 1$ .
4. Let  $f(x) = x^2 + x$  throughout.  
(a) Show that for every prime number  $p$  and every positive integer  $k$ , the congruence  $f(x) \equiv 0 \pmod{p^k}$  has precisely 2 solutions.  
(b) Let  $m$  be a natural number, and let  $r$  denote the number of distinct prime numbers dividing  $m$ . Show that the congruence  $f(x) \equiv 0 \pmod{m}$  has precisely  $2^r$  solutions.
5. (a) Prove that if  $p$  is prime,  $(a, p) = 1$  and  $(n, p - 1) = 1$ , then  $x^n \equiv a \pmod{p}$  has exactly one solution.  
(b) Show that when  $(n, p - 1) = d$ , then  $x^n \equiv 1 \pmod{p}$  has precisely  $d$  solutions.

©Trevor D. Wooley, Purdue University 2025. This material is copyright of Trevor D. Wooley at Purdue University unless explicitly stated otherwise. It is provided exclusively for educational purposes at Purdue University, and is to be downloaded or copied for your private study only.