

# Department of Mathematics

## MTL 145: Number Theory

### PROBLEMS ON CONGRUENCES

These problems are taken from *An Introduction to the Theory of Numbers* by NIVEN, ZUCKERMAN & MONTGOMERY with minor changes.

1. Show that  $7 \mid (3^{2n+1} + 2^{n+2})$  for all  $n \in \mathbb{N}$ .
2. Find all integers  $a_1, \dots, a_5$  such that every integer  $x$  satisfies at least one of the congruences  $x \equiv a_1 \pmod{2}$ ,  $x \equiv a_2 \pmod{3}$ ,  $x \equiv a_3 \pmod{4}$ ,  $x \equiv a_4 \pmod{6}$ ,  $x \equiv a_5 \pmod{12}$ .
3. Show that if  $p$  is *prime* and  $p \equiv 3 \pmod{4}$ , then  $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$ .
4. Show that if  $(ab, 91) = 1$ , then  $91 \mid (a^{12} - b^{12})$ .
5. Show that the product of three consecutive integers is always divisible by 504 if the middle term is a cube.
6. Prove that  $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$  is an integer whenever  $n$  is an integer.
7. What are the last two digits of  $3^{400}$ ?
8. If  $p$  is a *prime*, prove that  $(p-1)! + 1$  is a power of  $p$  if and only if  $p \in \{2, 3, 5\}$ .
9. Show that there are *infinitely* many  $n$  such that  $n! + 1$  is divisible by at least two *distinct* primes.
10. Prove that there are infinitely many primes of the form  $4k + 1$ .
11. Find all triples  $a, b, c$  of nonzero integers such that  $a \equiv b \pmod{|c|}$ ,  $b \equiv c \pmod{|a|}$ ,  $c \equiv a \pmod{|b|}$ .
12. If  $p$  is an odd prime, prove that

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \equiv 2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2$$

modulo  $p$ .

13. Show that if  $p$  is *prime* and  $0 \leq k \leq p-1$ , then  $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ .
14. Prove that if  $p$  is *prime* and  $a^p \equiv b^p \pmod{p}$ , then  $a^p \equiv b^p \pmod{p^2}$ .
15. If  $r_1, \dots, r_p$  and  $r'_1, \dots, r'_p$  are any two complete residue systems modulo a prime  $p > 2$ , prove that  $r_1 r'_1, \dots, r_p r'_p$  *cannot* be a complete residue system modulo  $p$ .
16. If  $p$  is a *prime*,  $p \neq 2, 5$ , prove that  $p$  divides *infinitely* many of the integers  $1, 11, 111, \dots$
17. For each positive integer  $n$ , prove that there is a multiple of  $n$  that contains only the digits 0 and 1. Prove that the role played by the pair of digits 0, 1 may only be replaced by one of the pairs  $\{0, 2\}$ ,  $\{0, 3\}$ ,  $\dots$ ,  $\{0, 9\}$ .
18. Use the factorization  $561 = 3 \cdot 11 \cdot 17$  to show that  $n^{561} \equiv n \pmod{561}$  holds for all  $n \in \mathbb{Z}$ .
19. Suppose that  $m_1, \dots, m_r$  are pairwise relatively prime positive integers. For each  $i$ , let  $\mathcal{C}(m_i)$  denote a complete system of residues modulo  $m_i$ . Show that the integers  $c_1 + c_2 m_1 + c_3 m_1 m_2 + \cdots + c_r m_1 \cdots m_{r-1}$ ,  $c_i \in \mathcal{C}(m_i)$ , form a complete system of residues modulo  $m = m_1 \cdots m_r$ .

20. If  $P$  denotes the product of the primes common to  $m$  and  $n$ , prove that  $\phi(mn) = P\phi(m)\phi(n)/\phi(P)$ .
21. If  $\phi(mn) = \phi(m)$  and  $n > 1$ , prove that  $n = 2$  and  $m$  is odd.
22. Let  $(a, b) = 1$  and  $c > 0$ . Prove that there is an integer  $n$  such that  $(a + bn, c) = 1$ .
23. Prove that the sum of all positive integers  $< n$  and relatively prime to  $n$  is  $\frac{1}{2}n\phi(n)$  if  $n > 1$ .
24. Find all positive integers  $n$  such that  $\phi(n) \mid n$ .
25. If  $d \mid n$  and  $0 < d < n$ , prove that  $n - \phi(n) > d - \phi(d)$ .
26. Prove that  $a^m \equiv a^{m-\phi(m)} \pmod{m}$  for all  $a \in \mathbb{Z}$ .
27. Suppose that  $m$  is square-free, and that  $k$  and  $\bar{k}$  are positive integers such that  $k\bar{k} \equiv 1 \pmod{\phi(m)}$ . Show that  $a^{k\bar{k}} \equiv a \pmod{m}$  for all  $a \in \mathbb{Z}$ .
28. Suppose  $m$  is positive and *not* square-free. Show that there exist integers  $a$  and  $b$  such that  $a \not\equiv b \pmod{m}$  but  $a^n \equiv b^n \pmod{m}$  for  $n > 1$ .
29. Let  $p$  be a *prime*,  $p \geq 5$ . For  $1 \leq r \leq p-1$ , let  $\sigma_r$  denote the sum of all products of  $r$  distinct integers from the set  $\{1, \dots, p-1\}$ . Prove that  $\sigma_{p-2} \equiv p\sigma_{p-3} \pmod{p^3}$ .
30. Let  $p$  be a *prime*,  $p \geq 5$ , and let  $m \in \mathbb{N}$ . Prove that  $\binom{mp-1}{p-1} \equiv 1 \pmod{p^3}$ .
31. Let  $p$  be a *prime*,  $p \geq 5$ , and let  $m \in \mathbb{N}$ . Prove that  $(mp)! \equiv m! \cdot (p!)^m \pmod{p^{m+3}}$ .