

Math 364 - Chapters 3 and 4
Fall 2008

47. (Problem 3.11) Prove and extend *or* disprove and salvage: For a prime number $p > 5$ the number $p^2 - 1$ is a multiple of 12.
48. (Problem 3.12) Prove and extend *or* disprove and salvage: Let m and n be integers. Suppose p is a prime number such that $p \mid mn$. Then either $p \mid m$ or $p \mid n$.
49. (Problem 3.13) Prove the Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be expressed as a finite product of prime numbers. Moreover, that product is unique, except for possible reorderings of the factors.
50. (Problem 3.14) Prove and extend *or* disprove and salvage: If m and n are integers with $m > 1$ and $m \mid n$ then $m \mid n + 1$.
51. (Problem 3.15) Prove: There are infinitely many prime numbers.
52. (Problem 4.1) Using the definition of congruence, verify that the notion of congruence gives rise to an equivalence relation; that is verify the following properties for all integers a, b, c and all $m > 1$:
 - (a) Reflexive: $a \equiv a \pmod{m}$
 - (b) Symmetric: If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.
 - (c) Transitive: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
53. (Problem 4.2) Prove and extend *or* disprove and salvage (with another if and only if statement): Let a, b and m be integers with $m > 1$. Then $a \equiv b \pmod{m}$ if and only if the remainder when a is divided by m equals the remainder when b is divided by m .
54. (Problem 4.4) Prove and extend *or* disprove and salvage: Let a, b, c, c' be integers with $m > 1$. Suppose that $c \equiv c' \pmod{m}$. If $a \equiv b \pmod{m}$, then $(a + c) \equiv (a + c') \pmod{m}$ and $ac \equiv bc' \pmod{m}$.
55. Prove and extend *or* disprove and salvage (with another if and only if statement): Let a, b, c and m be integers with $m > 1$. Then $ac \equiv bc \pmod{m}$ if and only if $a \equiv b \pmod{m}$.
56. (Problem 4.8) Prove and extend *or* disprove and salvage: Suppose that a and m are relatively prime integers with $m > 1$. Then the integers $a, 2a, 3a, \dots, (m - 1)a$ are distinct modulo m .
57. (Problem 4.10) Prove Fermat's Little Theorem: Let p be a prime and a be an integer relatively prime to p . Then $a^{p-1} \equiv 1 \pmod{p}$.
58. (Problem 4.11) Prove and extend *or* disprove and salvage: Let a and m be two integers with $m > 1$. Then $a^m \equiv a \pmod{m}$.
59. (Problem 4.12) Prove: Let n be any integer. Then 15 divides $11n^8 + 4n^4$.