pset 4

Jaden Lee*

2/12/26

https://yale.instructure.com/courses/113840/assignments/558952

1 Problem 1

Problem 1 (6 points): Prove that for any three digit positive integer, if the sum of the digits is a multiple of 3, then the number is a multiple of 3. (Hint: if the hundreds digit of n is a and the tens digit is b and the ones digit is c, what is n equal to in terms of a, b, and c?)

*made in Overleaf

1.1 solution

1	Suppose c is a three-digit positive integer with digits x, y, z	supposition
2	$c = 100 \cdot x + 10 \cdot y + z$	representation of 3-digit number
3	Suppose $3 \mid (x + y + z)$	supposition (given hypothesis)
4	$100 \equiv 1 \pmod{3}$	computation: $100 = 3(33) + 1$
5	$10 \equiv 1 \pmod{3}$	computation: $10 = 3(3) + 1$
6	$c = 100x + 10y + z \equiv 1 \cdot x + 1 \cdot y + z \pmod{3}$	modular arithmetic (lines 4, 5)
7	$c \equiv x + y + z \pmod{3}$	algebra (line 6)
8	Since $3 \mid (x + y + z)$, we have $x + y + z \equiv 0 \pmod{3}$	definition of divisibility
9	$c \equiv 0 \pmod{3}$	substitution (lines 7, 8)
10	$\therefore 3 \mid c$	definition of congruence

2 problem 2

(6 points): Use the modular arithmetic corollary of the Quotient/Remainder Theorem to prove that for all integers $n, n^8 \equiv 0 \pmod{5}$ or $n^8 \equiv 1 \pmod{5}$

2.1 solution

By the Modular Arithmetic Corollary of the Quotient/Remainder Theorem, every integer n satisfies exactly one of: $n \equiv 0, 1, 2, 3, 4 \pmod{5}$. We examine each case:

1	**Case 1:** $n \equiv 0 \pmod{5}$	supposition
2	$n^8 \equiv 0^8 \equiv 0 \pmod{5}$	exponentiation

3	**Case 2:** $n \equiv 1 \pmod 5$	supposition
4	$n^8 \equiv 1^8 \equiv 1 \pmod 5$	exponentiation
5	**Case 3:** $n \equiv 2 \pmod 5$	supposition
6	$n^2 \equiv 2^2 \equiv 4 \equiv -1 \pmod 5$	computation
7	$n^4 \equiv (n^2)^2 \equiv (-1)^2 \equiv 1 \pmod 5$	exponentiation (line 6)
8	$n^8 \equiv (n^4)^2 \equiv 1^2 \equiv 1 \pmod 5$	exponentiation (line 7)
9	**Case 4:** $n \equiv 3 \pmod 5$	supposition
10	$n^2 \equiv 3^2 \equiv 9 \equiv 4 \equiv -1 \pmod 5$	computation
11	$n^4 \equiv (-1)^2 \equiv 1 \pmod 5$	exponentiation (line 10)
12	$n^8 \equiv 1^2 \equiv 1 \pmod 5$	exponentiation (line 11)
13	**Case 5:** $n \equiv 4 \pmod 5$	supposition
14	$n \equiv -1 \pmod 5$	since $4 \equiv -1 \pmod 5$
15	$n^8 \equiv (-1)^8 \equiv 1 \pmod 5$	exponentiation
16	$\therefore \forall n \in \mathbb{Z} : n^8 \equiv 0 \pmod 5 \vee n^8 \equiv 1 \pmod 5$	exhaustive cases (lines 1-15)

3 problem 3

(8 points): Prove that, for any integers n, a, b, c, d with $n \geq 2$ and $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$

3.1 solution

1	Suppose $n \geq 2$ and $a, b, c, d \in \mathbb{Z}$	supposition
2	Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$	supposition (given)
3	$n \mid (a - b)$ and $n \mid (c - d)$	definition of congruence
4	$\exists k, m \in \mathbb{Z}$ s.t. $a - b = nk$ and $c - d = nm$	definition of divisibility
5	$a = b + nk$ and $c = d + nm$	algebra (line 4)
6	$ac = (b + nk)(d + nm)$	substitution (line 5)
7	$ac = bd + bnm + dnk + n^2km$	algebra (expansion)
8	$ac = bd + n(bm + dk + nkm)$	algebra (factoring)
9	$ac - bd = n(bm + dk + nkm)$	algebra (line 8)
10	Since $bm + dk + nkm \in \mathbb{Z}$, we have $n \mid (ac - bd)$	definition of divisibility
11	$\therefore ac \equiv bd \pmod{n}$	definition of congruence

4 problem 4

(8 points): Complete the proof that the Euclidean algorithm is correct by showing that for all integers a, b, r if $b \neq 0$ and $a = b \cdot q + r$ for some integer q, then $\gcd(b, r) \leq \gcd(a, b)$.

4.1 solution

1	Suppose $a, b, r, q \in \mathbb{Z}$ with $b \neq 0$	supposition
2	Suppose $a = bq + r$	supposition (given)
3	Let $d = \gcd(b, r)$	definition
4	$d \mid b$ and $d \mid r$	definition of gcd (line 3)
5	Since $d \mid b$, we have $d \mid (bq)$	divisibility property
6	Since $d \mid r$ and $d \mid (bq)$, we have $d \mid (bq + r)$	divisibility of sums
7	$d \mid a$	substitution (lines 2, 6)
8	Therefore d is a common divisor of a and b	lines 4, 7
9	Since $\gcd(a, b)$ is the *greatest* common divisor, $d \leq \gcd(a, b)$	definition of gcd
10	$\therefore \gcd(b, r) \leq \gcd(a, b)$	substitution (lines 3, 9)