MATH 220.201 CLASS 6 SOLUTIONS

1. Let $n \in \mathbb{Z}$. Prove or disprove: n is odd if and only if $4n^3 - 2n + 1$ is odd.

   Solution: The statement is false, because the implication '$4n^3 - 2n + 1$ is odd implies n is odd' is false. Here is a counterexample: when $n = 2$, $4n^3 - 2n + 1 = 29$.[1]

Definition 0.1 (Divisibility)**.** *Let $a, b \in \mathbb{Z}$. a* **divides** *b (written $a|b$) if there is some $n \in \mathbb{Z}$ such that $b = an$. Here are some properties you can assume. They are a good warmup if you want practice with proofs.*

- $a|b \wedge b|c \implies a|c$
- $a|c \wedge b|d \implies ab|cd$
- $a|b \wedge a|c \implies a|(bx + cy)$
- $\forall a \in \mathbb{Z}, a|0$
- $\forall a \in \mathbb{Z}, 1|a$

2. Prove or find a counterexample: For all $a, b \in \mathbb{Z}$, if $3|ab$, then ($3|a$ or $3|b$).

   Proof. We prove the contrapositive, namely

$$\sim ((3|a) \vee (3|b)) \implies \sim (3|ab)$$

This is equivalent to prove that if $3 \nmid a$ *and* $3 \nmid b$, then $3 \nmid ab$. If $3 \nmid a$, then either $a \equiv 1 \pmod 3$ or $a \equiv 2 \pmod 3$. Similarly for b. So we divide it up into four cases.

Case 1: $a \equiv 1 \pmod 3, b \equiv 1 \pmod 3$. Then $a = 3x + 1$ and $b = 3y + 1$ for some $x, y \in \mathbb{Z}$. Then

$$ab = (3x + 1)(3y + 1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1$$

Thus, $ab \equiv 1 \pmod 3$ and so $3 \nmid ab$.

Case 2: $a \equiv 1 \pmod 3, b \equiv 2 \pmod 3$. Then $a = 3x + 1$ and $b = 3y + 2$ for some $x, y \in \mathbb{Z}$. Then

$$ab = (3x + 1)(3y + 2) = 9xy + 6x + 3y + 2 = 3(3xy + 2x + y) + 2$$

Thus, $ab \equiv 2 \pmod 3$ and so $3 \nmid ab$.

Case 3: $a \equiv 2 \pmod 3, b \equiv 1 \pmod 3$. This is similar to the last case.

Case 4: $a \equiv 2 \pmod 3, b \equiv 2 \pmod 3$. Then $a = 3x + 2$ and $b = 3y + 2$ for some $x, y \in \mathbb{Z}$. Then

$$ab = (3x + 2)(3y + 2) = 9xy + 6x + 6y + 4 = 3(3xy + 2x + 2y + 1) + 1$$

Thus, $ab \equiv 1 \pmod 3$ and so $3 \nmid ab$. □

[1] In fact, $4n^3 - 2n + 1$ is always odd when n is an integer.

3. Prove or find a counterexample: For all $a, b \in \mathbb{Z}$, if $4|ab$, then ($4|a$ or $4|b$).

   Solution: There is a counterexample, namely $a = 2$ and $b = 2$. Then $4|ab$, but $4 \nmid a$ and $4 \nmid b$.

Definition 0.2 (Congruence)**.** *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. a is* **congruent** *to b* **modulo** *n if n divides $a - b$. We write this as*

$$a \equiv b \pmod{n}$$

Here are some properties you can assume.

- $a \equiv b \pmod{n} \implies a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$
- $\exists r \in \{0, 1, 2, \ldots, n-1\}, a \equiv r \pmod{n}$

4. Prove or disprove: For all $n \in \mathbb{Z}$, $3|n$ or $n^2 \equiv 1 \pmod{3}$.

Proof. We consider three possible cases: $n \equiv 0, 1,$ or $2 \pmod{3}$.

Case 1: $n \equiv 0 \pmod{3}$. Then $3|n$.
Case 2: $n \equiv 1 \pmod{3}$. Then $n^2 \equiv 1 \pmod{3}$.
Case 3: $n \equiv 2 \pmod{3}$. Then $n^2 \equiv 4 \equiv 1 \pmod{3}$. □

5. Prove or disprove: For all $n \in \mathbb{Z}$,

$$((2 \nmid n) \wedge (3 \nmid n)) \implies \exists m \in \mathbb{Z}, mn \equiv 1 \pmod{6}$$

Proof. We consider six possible cases: $n \equiv 0, 1, 2, 3, 4,$ or $5 \pmod{6}$.
Case 1: $n \equiv 0 \pmod{6}$. Then $2|n$ and so the implication is vacuously true.
Case 2: $n \equiv 1 \pmod{6}$. Then let $m = 1$. We then have

$$mn = n \equiv 1 \pmod{6}$$

Case 3: $n \equiv 2 \pmod{6}$. Then $2|n$ and so the implication is vacuously true.
Case 4: $n \equiv 3 \pmod{6}$. Then $3|n$ and so the implication is vacuously true.
Case 5: $n \equiv 4 \pmod{6}$. Then $2|n$ and so the implication is vacuously true.
Case 6: $n \equiv 5 \pmod{6}$. Then let $m = -1$. We then have

$$mn = -n \equiv -5 \equiv 1 \pmod{6}$$

□

6. Prove or disprove: For all $n \in \mathbb{Z}$,

$$n^3 \not\equiv 1 \pmod{7} \implies (n^3 \equiv 1 \pmod{7}) \vee (n \equiv 0 \pmod{7})$$

Proof. We consider all seven possibilities for n modulo 7.
Case 1: $n \equiv 0 \pmod{7}$. Then the conclusion is true.
Case 2: $n \equiv 1 \pmod{7}$. Then $n^3 \equiv 1^3 \equiv 1 \pmod{7}$ and the conclusion is true.

Case 3: $n \equiv 2 \pmod 7$. Then $n^3 \equiv 2^3 \equiv 8 \equiv 7+1 \equiv 1 \pmod 7$ and the conclusion is true.

Case 4: $n \equiv 3 \pmod 7$. Then $n^3 \equiv 3^3 \equiv 27 \equiv 4 \cdot 7 - 1 \equiv -1 \pmod 7$ and the assumption is false.

Case 5: $n \equiv 4 \pmod 7$. Then $n^3 \equiv 4^3 \equiv 64 \equiv 9 \cdot 7 + 1 \equiv 1 \pmod 7$ and the conclusion is true.

Case 6: $n \equiv 5 \pmod 7$. Then $n^3 \equiv 5^3 \equiv 125 \equiv 18 \cdot 7 - 1 \equiv -1 \pmod 7$ and the assumption is false.

Case 7: $n \equiv 6 \pmod 7$. Then $n^3 \equiv 6^3 \equiv 216 \equiv 31 \cdot 7 - 1 \equiv -1 \pmod 7$ and the assumption is false. □

7. Prove: For all $n \in \mathbb{Z}$,

$$n \equiv 3 \pmod 4 \implies \sim (\exists a, b \in \mathbb{Z}, a^2 + b^2 = n)$$

Proof. We prove the contrapositive, namely we assume that $\exists a, b \in \mathbb{Z}, a^2 + b^2 = n$ and prove that $n \not\equiv 3 \pmod 4$. We consider four possible cases, based on the parity of a and b.

Case 1: a even, b even. Then $a^2 \equiv 0 \pmod 4$ and $b^2 \equiv 0 \pmod 4$. Then $n \equiv 0 + 0 \equiv 0 \pmod 4$.

Case 2: a even, b odd. Then $a^2 \equiv 0 \pmod 4$ and $b^2 \equiv 1 \pmod 4$. Then $n \equiv 0 + 1 \equiv 1 \pmod 4$.

Case 3: a odd, b even. This is similar to the previous case.

Case 4: a odd, b odd. Then $a^2 \equiv 1 \pmod 4$ and $b \equiv 1 \pmod 4$. Then $n \equiv 1 + 1 \equiv 2 \pmod 4$.

In all four cases, $n \not\equiv 3 \pmod 4$. Thus, this proves the conclusion. □

Definition 0.3 (Relatively prime)**.** *Let $a, b \in \mathbb{Z}$. a and b are* **relatively prime** *(written $\gcd(a, b) = 1$, or just $(a, b) = 1$) if*

$$\forall n \in \mathbb{N} \ s.t. \ n \geq 2, (n|a \implies n \nmid b)$$

8. Prove that 5 and 12 are relatively prime.

Proof. We want to show the statement

$$\forall n \in \mathbb{N} \text{ s.t. } n \geq 2, (n|5 \implies n \nmid 12)$$

Case 1: When $n \neq 5$, the implication is vacuously true, because $n \nmid 5$.

Case 2: When $n = 5$, the implication is true because $n \nmid 12$. □

9. Prove that if $a \equiv 7 \pmod{10}$, then a and 10 are relatively prime.

Proof. We will show the statement

$$\forall n \in \mathbb{N} \text{ s.t. } n \geq 2, (n|10 \implies n \nmid a)$$

If $n \neq 2, 5, 10$, then the implication is vacuously true. So assume we are in one of these three cases.

Case 1: $n = 2$. Since $a \equiv 7 \pmod{10}$, $a = 10x + 7$ for some $x \in \mathbb{Z}$. Then $a = 2(5x + 3) + 1$, and so a is odd. Therefore, $2 \nmid a$.

Case 2: $n = 5$. Since $a \equiv 7 \pmod{10}$, $a = 10x + 7$ for some $x \in \mathbb{Z}$. Then $a = 5(2x + 1) + 2$, and so $a \equiv 2 \pmod{5}$. Therefore, $5 \nmid a$.

Case 3: $n = 10$. Since $a \equiv 7 \pmod{10}$, $10 \nmid a$.

In all three cases, $n \nmid a$. This completes the proof. $\square$