MATH 350 Assignment 7 Solutions

Dylan Scofield

Fall 2024

5.24

Proof. Suppose $a \equiv b \mod n$ and $c \equiv d \mod n$. It will be shown that $ac \equiv bd \mod n$.
By definition of congruence modulo n, we see $n \mid (a-b)$ and $n \mid (c-d)$.
Applying definition of divides yields $nj = (a-b)$ and $nk = (c-d)$ for some $j,k \in \mathbb{Z}$.
Notice that this implies that $a = nj + b$ and $c = nk + d$. Observe

$$\begin{aligned} ac &= (nj+b)(nk+d) \\ &= n^2jk + bnk + dnj + bd \\ &= n(njk + bk + dj) + bd. \end{aligned}$$

Subtracting both sides by bd gives us

$$ac - bd = n(njk + bk + dj).$$

Note that $njk + bk + dj = x$ is an integer, and we see that $ac - bd = nx$.
Thus $n \mid ac - bd$ by definition of divisibility.
By definition of congruence modulo n we conclude that $ac \equiv bd \mod n$ as desired. □

6.5

Proof. We will prove that $\sqrt{3}$ is irrational. We will proceed via contradiction[1], and assume that $\sqrt{3}$ is rational. Thus by definition of rational,$\exists a, b \in \mathbb{Z}$ such that $\sqrt{3} = \frac{a}{b}$. We can assume that $\frac{a}{b}$ is in lowest terms. Specifically, a and b have no common factors. We then see that

$$\begin{aligned} \sqrt{3}b &= a \\ 3b^2 &= a^2. \end{aligned}$$

Thus $3 \mid a^2$ by definition of divisibility. With this let us show that $3 \mid a$.
Let us prove the contrapositive. Thus let us suppose $3 \nmid a$.
By the division algorithm this means that either $a = 3x+1$ or $a = 3y+2$ for some integers $x, y \in \mathbb{Z}$.
Case 1: $a = 3x + 1$.
Thus $a^2 = (3x+1)^2 = 9x^2 + 6x + 1 = 3(3x^2 + 2x) + 1$. Let $p = 3x^2 + 2x$. Thus $a^2 = 3p + 1$.
From this we see that $3 \nmid a^2$ as it has a remainder of one.
Case 2: $a = 3y + 2$.
So $a^2 = (3y+2)^2 = 9y^2 + 12y + 4 = 9y^2 + 12y + 3 + 1 = 3(3y^2 + 4y + 1) + 1$. Let $q = 3y^2 + 4y + 1$. Thus $a^2 = 3q + 1$. We conclude that $3 \nmid a^2$ as again it has a remainder of 1.
Therefore $3 \mid a$. By definition of divides, $\exists k \in \mathbb{Z}$ such that $3k = a$. Thus,

$$\begin{aligned} 3b^2 &= a^2 \\ 3b^2 &= (3k)^2 \\ 3b^2 &= 9k^2 \\ b^2 &= 3k^2. \end{aligned}$$

Again we apply the definition of divisibility to see that $3 \mid b^2$. This implies that $3 \mid b$. This is a contradiction as $3 \mid a$, and we assumed that a and b had no common factors.

□

[1] It is good practice to tell the reader how you are approaching the proof by describing the strategy you are going to use.

6.9

Proof. Suppose $a, b \in \mathbb{R}$, a is rational, and that ab is irrational. We wish to show b is irrational.
By way of contradiction, suppose b is rational.
Thus by definition of rational, $a = \frac{x}{y}$ and $b = \frac{n}{m}$ for some $x, y, n, m \in \mathbb{Z}$.
So

$$\begin{aligned} ab &= \frac{x}{y} \cdot \frac{n}{m} \\ &= \frac{xn}{ym}. \end{aligned}$$

Notice that xn and ym are both integers. Thus ab is rational by definition.
This contradicts the assumption that ab is irrational. Therefore, b is irrational. □

7.15

Proof. Suppose $a, b \in \mathbb{Z}$. It will be proven that $a + b$ is even if and only if a and b have the same parity.
($\Rightarrow$)Suppose that $a + b$ is even. We will show a and b have the same parity.
We will proceed by contradiction and suppose that a and b have different parity. Without loss of generality, say a is even and b is odd.
By definition of even and odd respectfully, $\exists j, k \in \mathbb{Z}$ such that $a = 2k$ and $b = 2j + 1$.
Consider

$$\begin{aligned} a + b &= 2k + 2j + 1 \\ &= 2(k + j) + 1. \end{aligned}$$

Let $\ell = (k + j)$. Then $a + b = 2\ell + 1$ and thus is odd by definition. This is a contradiction of the fact that we assumed it was even. Therefore, a and b have the same parity.
($\Leftarrow$)Suppose a and b have the same parity. It will be shown that $a + b$ is even.
Let us analyze this with cases.
Case 1: a and b are both even.
Then $a = 2x$ and $b = 2y$ for some $x, y \in \mathbb{Z}$ by definition of even.
Then $a + b = 2x + 2y = 2(x + y)$. Since $x + y$ is an integer, this implies $a + b$ is even by definition.
Case 2: a and b are both odd.
Thus by definition of odd there exists $p, q \in \mathbb{Z}$ such that $a = 2q + 1$ and $b = 2p + 1$.
Then, $a + b = (2q + 1) + (2p + 1) = 2p + 2q + 2 = 2(p + q + 1)$. Since $p + q + 1$ is an integer, $a + b$ is again even by definition.
Therefore $a + b$ is even. □

7.17

Proof. Let us see that there is a prime number between 90 and 100.
Consider[2] 97.
We only need to check prime integers in the set $\{2, 3, 4, 5, 6, 7, 8, 9\}$. We only need to check up to $\sqrt{97}$.
Since 97 is odd, 2 cannot divide it and thus 4,6,8 cannot either.
The digits of 97 sum to 16. This is not divisible by 3, so neither is 97. This also rules out 9.
Since 97 does not end in 0 or 5, it is not divisible by 5. (Think about mod 5)
This leaves 7, notice that $98 = 2 \cdot 7^2$ and thus is divisible by 7. Observe

$$\begin{aligned} 98 &\equiv 0 \mod 7 \\ 98 - 1 &\equiv 0 - 1 \mod 7 \\ 97 &\equiv 6 \mod 6. \end{aligned}$$

Thus 97 is not divisible by 7.[3]
Thus 97 is prime as it has no factors that are not 1 and 97. □

[2] An example if sufficient to show existence, but we should justify why this number is prime since it isn't immediately obvious. For example, 91 looks prime but is the product of 13 and 7. Plus this gives me a reason to show you some cool divisibility tricks.

[3] There is a cool trick for figuring out if a number is divisible by 7, but it is a little convuluted for this. Email me if you are interested.