Math 135, Fall 2019, Sample Answers to Homeworks 5 and 6

Homework 5:

Theorem 1. Let a, b, and c be integers, where a and b are not both zero, and c is not zero. Then $\gcd(ac, bc) = c \cdot \gcd(a, b)$.

Proof: [Note: As stated, this theorem is not true! If $c < 0$ it is not possible for $\gcd(ac, bc) = c \cdot \gcd(a, b)$ because a greatest common divisor is always positive. I will give a proof that assumes that $c > 0$.]

Let $d = gcd(a, b)$ and $e = gcd(ac, bc)$. Since $d \mid a$ and $d \mid b$, it follows easily that $dc \mid ac$ and $dc \mid bc$. So, dc is a common divisor of ac and bc. Since e is the greatest common divisor, we must have $dc \leq e$.

We know d can be written as $d = ak + b\ell$ for some integers k and ℓ, and multiplying both sided by c gives $dc = ack + bc\ell$. We also know that e is the **smallest** positive integer that can be written in the form $aci + bcj$ for integers i and j. Since dc can be written in that form, we must have $dc \geq e$.

Since $dc \leq e$ and $dc \geq e$, it follows that $e = dc$, as we wanted to show.

Theorem 2. Let $a, b, c \in \mathbb{N}$, If a does not divide bc, then a does not divide b.

Proof: We prove the contrapositive: If $a \mid b$ then $a \mid bc$. This is a theorem that we have previously proved. [In fact, $a \mid b$ means $b = ka$ for some integer k. Then $bc = bka = a(bk)$, which means that $a \mid bc$.]

Theorem 3. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Proof: Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Since $a \equiv b \pmod{n}$, $n \mid (a - b)$, and $(a - b) = kn$ for some integer k. Since $c \equiv d \pmod{n}$, $n \mid (c - d)$, and $(c - d) = \ell n$ for some integer ℓ. So, $ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b) = a\ell n + dkn = n(a\ell + dk)$. We see that $n \mid (ac - bd)$, and therefore $ac \equiv bd \pmod{n}$.

Theorem 4. Let r and s be rational numbers. The $r + s$ is rational.

Proof: Suppose that r and s are rational. Since r is rational, we can write $r = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$. Since s is rational, we can write $s = \frac{c}{d}$, where $c, d \in \mathbb{Z}$ and $d \neq 0$. Then, $r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{cb}{bd} = \frac{ad+cb}{bd}$. Since $ad + cb$ and bd are integers and $bd \neq 0$, we see that $r + s$ is rational.

Theorem 5. For any real number x, one of the numbers x and $x - \pi$ is irrational.

Proof: Suppose, for the sake of contradiction, that both x and $x - \pi$ are rational. Since the negative of a rational number is rational, $\pi - x$ is also rational. By the previous theorem, $x + (\pi - x)$ is rational, because it is the sum of two rational numbers. But $x + (\pi - x)$ is π, which we know to be irrational. This contradiction proves that at least one of x and $\pi - x$ must be irrational.

Homework 6:

1. Prove: If a and b are integers, then $(a + b)^3 \equiv a^3 + b^3 \pmod{3}$.

Proof: Note that $(a + b)^3 - (a^3 + b^3) = a^3 + 3a^2b + 3ab^2 + b^3 - a^3 - b^3 = 3(a^2b + ab^2)$. So $3 \mid \big((a + b)^3 - (a^3 + b^3)\big)$, which means by definition that $(a + b)^3 \equiv a^3 + b^3 \pmod{3}$.

2. Prove using the contrapositive method: If the product of two integers is odd, then both of the numbers are odd.

Proof: We prove the contrapositive: If it is not the case that both integers are odd, then the product of the two numbers is not odd.

Let a and b be two integers that are not both odd. Then at least one of the integers is even. Say, without loss of generality, that a is even. Then $a = 2k$ for some integer k, and $ab = 2kb$. This shows that ab is even. That is, ab is not odd.

3. Prove using proof by contradiction: If a is a rational number and b is an irrational number, then $a+b$ is an irrational number.

Proof: Assume, for the sake of contradiction, that $a+b$ is rational. Since a is rational, $-a$ is also rational [since $-\frac{p}{q} = \frac{-p}{q}$]. We have previously proved that the sum of two rational numbers is rational. So $(a+b)+(-a)$ is rational. But $(a+b)+(-a) = b$, and b is irrational, not rational. This contradiction shows that $a+b$ cannot be rational.

4. Prove using the contrapositive method: If n is an integer and $n \equiv 2 \pmod 3$, then n is not a square. (Saying that n is not a square means that there is no integer a such that $n = a^2$.)

Proof: We prove the contrapositive: If n is a square, then $n \not\equiv 2 \pmod 3$. Let n be an integer that is a square, and let $a \in \mathbb{Z}$ such that $n = a^2$. We need to show that $a^2 \not\equiv 2 \pmod 3$. Since every integer is congruent to exactly one of 0, 1, or 2 (mod 3), we can show that for any integer a, either $a^2 \equiv 0 \pmod 3$ or $a^2 \equiv 1 \pmod 3$. We use a proof by cases. Using the Division Algorithm, we can write $a = 3q + r$ where q and r are integers and r is 0, 1, or 2.

In the case $a = 3q + 0$, we have that $a^2 = (3q)^2 = 3 \cdot 3q^2$. This means $3 \mid a^2$, and $a^2 \equiv 0 \pmod 3$.

In the case $a = 3q + 1$, we have that $a^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3 \cdot (3q^2 + 2q) + 1$. This means $3 \mid (a^2 - 1)$, and $a^2 \equiv 1 \pmod 3$.

In the case $a = 3q + 2$, we have that $a^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 3 \cdot (3q^2 + 4q + 1) + 1$. This means $3 \mid (a^2 - 1)$, and $a^2 \equiv 1 \pmod 3$.

So, in any case, one of $a^2 \equiv 0 \pmod 3$ or $a^2 \equiv 1 \pmod 3$ is true, as we wanted to show.

5. Prove using proof by contradiction: No rational number is a solution of the equation $x^3 + x + 1 = 0$. (Outline of proof: Suppose $x = \frac{p}{q}$ is a solution, where p and q are not both even. Substitute $\frac{p}{q}$ into the equation, and multiply by q^3 to clear the denominator. Now show that the left side of the equation is odd, which means that it cannot be zero. To show the left side is odd, use a proof by cases.)

Proof: Suppose, for the sake of contradiction, that there is a rational number $x = \frac{p}{q}$ such that $x^3 + x + 1 = 0$. We can assume that the fraction is in lowest terms so that, in particular, p and q are not both even. We have $\left(\frac{p}{q}\right)^3 + \left(\frac{p}{q}\right) + 1 = 0$. Multiplying this equation by q^3 to clear the denominators gives us $p^3 + pq^2 + q^3 = 0$. We show that the left-hand side of this equation is an odd number, and so cannot be equal to zero. This contradiction will complete the proof.

To show $p^3 + pq^2 + q^3$ is odd, we use a proof by cases. Since we know that p and q are not both even, the cases are: both p and q are odd, p is odd and q is even, or p is even and q is odd.

In the case where p and q are both odd, then, because the product of odd numbers is odd, we know that p^3, pq^2, and q^3 are all odd. Since the sum of odd numbers is odd, it follows that $p^3 + pq^2 + q^3$ is odd.

In the case where p is odd and q is even, we have that p^3 is odd and $pq^2 + q^3 = q(pq + q^2)$ is even. Since the sum of an odd number and an even number is odd, $p^3 + pq^2 + q^3$ is odd.

Finally, in the case where p is even and q is odd, we have that q^3 is odd and $p^3 + pq^2 = p(p^2 + q^2)$ is even. Since the sum of an odd number and an even number is odd, $p^3 + pq^2 + q^3$ is odd.