1. Miscellaneous proofs

Proposition 1. $\sqrt{3}$ *is irrational.*

Proof. Suppose $\sqrt{3}$ is rational. Then there exists 2 integers x and y such that $\sqrt{3} = \frac{x}{y}$. Suppose also that there are no common denominators between x and y. Then $3 = \frac{x^2}{y^2}$, $y^2 = 3x^2$ and $x^2 = 3y^2$. Thus both x and y are divisible by 3. Since we already stipulated that there are no common denominators between x and y, this results in a contradiction. Thus $\sqrt{3}$ is irrational. □

Proposition 2. *Let $a \in \mathbb{Z}$. Prove that if a is odd, then $a+1$ is even.*

Proof. By definition, if a is *odd*, then there is an integer x such that $a = 2x+1$. Thus $a+1 = (2x+1)+1 = 2x+2 = 2(x+1)$. By definition, if a is *even*, then there is an integer y such that $a = 2y$. Therefore, a + 1 is even. □

Proposition 3. *If 7 does not divide ab, then 7 divides neither a nor b.*

Contrapositive Proof.

Proof. Let $a, b \in \mathbb{Z}$. Suppose that 7 divides a or 7 divides b.

Case 1. Without loss of generality, suppose 7 divides a but 7 does not divide b. By definition $a = 7x$ for some $x \in \mathbb{Z}$ and $b \neq 7y$ for some $y \in \mathbb{Z}$. Hence $ab = 7(xb)$. Therefore 7 divides ab.

Case 2. Suppose 7 divides a and 7 divides b. By definition $a = 7m$ and $b = 7n$ for some $m, n \in \mathbb{Z}$. Then $ab = 7(7mn)$. Therefore 7 divides ab. □

Proposition 4. *Let $a, b \in Z$. Prove that if 7 does not divide ab, then 7 divides neither a nor b.*

Proof. (Contrapositive) Suppose 7 divides a or 7 divides b and $a, b \in Z$. By definition, $7m = a$ and $7n = b$ for some $m, n \in Z$. Thus, if 7 divides a, then $ab = 7(mb)$. Next, if 7 divides b, then $ab = 7(na)$. In either situation, ab is a multiple of seven. Therefore, it follows that 7 divides ab. Since the contrapositive is true, it follows that the original statement is true. □

Proposition 5. *Let $x \in \mathbb{R}$. If $x^2 + 5x < 0$, then $x < 0$.*

Contrapositive: Let $x \in \mathbb{R}$. If $x \geq 0$, then $x^2 + 5x \geq 0$.

Proof. Let x be a real number greater than or equal to 0.

Case 1: $x > 0$. By definition of positive numbers, since $x > 0$, $5x > 0$. By definition of squares, x^2 is greater than 0. Since two positive numbers added together equal a third positive number, $x^2 + 5x$ is greater than 0.

Case 2: $x = 0$. Since a number times 0 is 0, $5x = 5(0) = 0$. Similarly, $0^2 = 0$. Thus, $x^2 + 5x = 0 + 0 = 0$.

Therefore, for all real numbers $x \geq 0$, $x^2 + 5x \geq 0$.

Therefore, by contrapositive, if $x^2 + 5x < 0$, then $x < 0$. □

Proposition 6. *Let $x \in \mathbb{Z}$. If x is odd, then $8 \mid (x^2 - 1)$.*

Proof. Let $x \in \mathbb{Z}$ and odd. By definition, $\exists a \in \mathbb{Z}$ such that $x = 2a+1$. Hence, $x^2 = 4a(a+1)+1$ and $8 \mid (x^2-1) = 8 \mid 4a(a+1)$. We know that $a(a+1)$ is always even (because any number multiplied by an even produces an even), so $\exists b$ such that $a(a+1) = 2b$. Thus $8 \mid 4a(a+1) = 8 \mid 8b$. Since 8 divides 8, we know that $8 \mid (x^2 - 1)$. □

Proposition 7. *Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|(b+c)$, then $a|c$*

Proof. Suppose $a|b$ and $a|(b+c)$ for some integers a, b, c. By definition, there exists $x, y \in \mathbb{Z}$ such that $ax = b$ and $ay = b+c$. Then $ay - ax = a(y-x) = b + c - b = c$. Therefore, since $(y - x)$ is an integer, $a|c$. □

Proposition 8. *Suppose $x \in \mathbb{Z}$. Then x is even if and only if $3x+5$ is odd.*

Proof. Proving this directly we suppose x is even. By definition there is an integer a such that $x = 2a$. Thus $3x + 5 = 3(2a) + 5 = 6a + 5 = 2(3a + 2) + 1 = 2(c) + 1$. Where $c = 3a + 2$ for some integer c. Hence $3x + 5$ is odd by definition.

Conversely, if $3x + 5$ is odd, then x is even. Proving this using a contrapositive proof. Suppose x is not even, so then x is odd. By definition there is an integer b such that $x = 2b+1$. Thus $3x+5 = 3(2b+1)+5 = 6b+3+5 = 6b+8 = 2(3b+4) = 2(d)$. Where $d = 3b + 4$ for some integer d. Hence $3x + 5$ is even by definition.

In either case $7 \nmid ab$. □

2. Problem 9 of worksheet 3

Proposition 9. *For any $a, b \in \mathbb{Z}$, it follows that $(a+b)^3 \equiv a^3 + b^3 (mod 3)$.*

Proof. Suppose $a, b \in \mathbb{Z}$. Thus, there is an integer x such that $x = a^2b + ab^2$. Hence $3x = 3a^2b + 3ab^2 = (a+b)^3 - a^3 - b^3$. It follows that $3|(a+b)^3 - a^3 - b^3$. Therefore, $(a+b)^3 \equiv a^3 + b^3 (mod 3)$. □

Proof. Suppose $a, b \in \mathbb{Z}$. Then $(a+b)^3 \equiv a^3 + 3a^2b + 3ab^2 + b^3$. Hence $(a+b)^3 - (a^3+b^3) = 3a^2b + 3ab^2 = 3(a^2b + ab^2)$. We see that $a^2b + ab^2$ is an integer. Thus by definition $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. □

Proof. Let $a, b, \in \mathbb{Z}$. Then $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. Hence $(a+b)^3 - (a^3+b^3) = a^3 + 3a^2b + 3ab^2 + b^3 - a^3 - b^3$. This is equivalent to $3a^2b + 3ab^2 = 3(a^2b + ab^2)$. We see that $a^2b + ab^2$ is an integer, thus by the definition of divisibility which states that for any integer x, y, we say that x divides y if there is an integer c such that $y = xc$, $3 \mid [(a+b)^3 - (a^3+b^3)]$. Therefore, by the definition of congruence, $(a+b^3) \equiv a^3 + b^3 (mod 3)$. □

Proof. Suppose a and b are integers. As a and b are integers, $(a+b)^3$ and $a^3 + b^3$ are themselves integers. As the two of them are integers, their difference is an integer. In addition, $(a+b)^3 - (a^3+b^3) = 3(a^2b + ab^2)$. This fits Definition 2 as $(a^2b + ab^2)$ is an integer, so $n = 3(a^2b + ab^2)$ for some integer x. It follows then that $3m = 3(a^2b + ab^2)$ for some integer m. Thus $3m = 3(a^2b + 2ab^2) = a^3 + 3a^2b + 3ab^2 + b^3 - (a^3+b^3)$. Hence $3m = (a+b)^3 - (a^3+b^3)$. Therefore, $3|(a+b)^3 - (a^3+b^3)$, and finally $(a+b)^3 \equiv a^3 + b^3 (\mod 3)$. □

Proof. Suppose $a, b \in \mathbb{Z}$. Now, $(a+b)^3 - (a^3+b^3) = a^3 + 3a^2b + 3ba^2 + b^3 - (a^3+b^3) = a^3 + b^3 + 3(a^2b + ab^2) - (a^3+b^3) = a^3 + b^3 - a^3 - b^3 + 3(a^2b + ab^2) = 3(a^2b + ab^2)$ where $(a^2b + ab^2)$ is an integer under integer operation rules. By Definition 1, $3 \mid 3(a^2b + ab^2)$. Therefore, $3 \mid (a+b)^3 - (a^3+b^3)$ also. This fits the definition of congruence (Definition 2).

Thus, for any $a, b \in \mathbb{Z}$, it follows that $(a+b)^3 \equiv a^3 + b^3\ (mod\ 3)$. □

Proof. Let $a, b \in \mathbb{Z}$. Now examine the equation $(a+b)^3$. This equation can be expanded $(a+b)^3 = a^3 + 3ab^2 + 3a^2b + b^3$. Now, if we subtract $a^3 + b^3$ from both sides we are left with $(a+b)^3 - (a^3+b^3) = a^3 + 3ab^2 + 3a^2b + b^3 - (a^3+b^3) = 3(ab^2 + a^2b)$. We have been shown that $(a+b)^3 - (a^3+b^3) = 3(ab^2 + a^2b)$ so, by definition, $3 \mid (a+b)^3 - (a^3+b^3)$. Therefore, by definition, $(a+b)^3 \equiv (a^3+b^3) \pmod 3$. □