Note 3.6 is a summary section for Chapter 3 and would probably be good review.

3.5: #2, 11, 22

5.4: #2, 5, 7

3.5 (The Division Algorithm & Congruence)

* **2.** **(a)** Use cases based on congruence modulo 3 and properties of congruence to prove that for each integer n, $n^3 \equiv n \pmod 3$.

for any integer n, $n \pmod 3$ exists in $\in \{0,1,2\}$.

We know $n \equiv n \pmod 3$, it follows $n^3 \equiv n^3 \pmod 3$

We must show $n \pmod 3 \equiv n^3 \pmod 3$.

<u>CASE 1|</u> let $n \pmod 3 = 0$. Thus $3 | n$ & there exists some integer m such that $3m = n$. $n^3 = 27m^3$ Thus $3 | n^3$. As $3 | n^3$, $n^3 \pmod 3 = 0$. It follows $n \pmod 3 = n^3 \pmod 3$ as $0 = 0$.

<u>CASE 2|</u> let $n \pmod 3 = 1$ Thus $3 | (n-1)$ & there exists some int. m such that $3m = n-1$, so $n = 3m+1$ & $n^3 = 27m^3 + 18m^2 + 6m + 1$ we can write n^3 as $3(9m^3 + 6m^2 + 2m) + 1$, & as m is an int., there exists an int $\dot{m} = 9m^3 + 6m^2 + 2m$, Thus $n^3 = 3\dot{m} + 1$

It follows $(n^3 - 1) = 3\dot{m}$ thus $3 | (n^3 - 1)$. This shows $n^3 \pmod 3 = 1$

As $1 = 1$, $n \pmod 3 = n^3 \pmod 3$

CASE 3

Case 3) Similarly, let $n \pmod 3 = 2$, thus $3 \mid (n-2)$

$\exists m \mid 3m = (n-2)$ so $n = 3m+2$, now $n^3 = 27m^3 + 45m^2 + 36m + 8$

which can be written as $3(9m^3 + 15m^2 + 12m + 2) + 2$. As $m \in \mathbb{Z}$,

$\exists \dot{m} \in \mathbb{Z} \mid \dot{m} = 9m^3 + 15m^2 + 12m + 2$. Now $n^3 = 3\dot{m} + 2$ & $(n^3 - 2) = 3\dot{m}$

Thus $3 \mid (n^3 - 2)$ & $n^3 \pmod 3 = 2$, As this is the last case which shows $n \pmod 3 = n^3 \pmod 3$, as $2 = 2$,

Our proof is complete ☺

(b) Explain why the result in Part (a) proves that for each integer n, 3 divides $(n^3 - n)$. Compare this to the proof of the same result in Proposition 3.27.

We know $n^3 \equiv n \pmod 3$ & $n \equiv n \pmod 3$ & $-n \equiv -n \pmod 3$

by Theorem 3.28, $(n^3 - n) \equiv (n - n) \pmod 3 \equiv 0 \pmod 3$. This states $3 \mid (n^3 - n)$ perfectly with no remainder.

The proof for part (a) is very similar to the proof of prop. 3.27 as both instances consider the set $E: \{0, 1, 2\}$

This set is both the possible remainders for any number divided by 3, and the possible results for any number mod 3.

In fact, these are stating the same thing and thus logically equivallent.

the quotient, q, used in prop. 3.27's proof is represented by m in case 1, & $\dot{m}$ in case 2 & 3 above.

11. **(a)** Use the result in Proposition 3.33 to help prove that the integer $m = 5,344,580,232,468,953,153$ is not a perfect square. Recall that an integer n is a perfect square provided that there exists an integer k such that $n = k^2$. **Hint**: Use a proof by contradiction.

Proposition 3.33 states that if $a \not\equiv 0 \pmod 5$, then $a^2 \equiv 1 \pmod 5$, or $a^2 \equiv 4 \pmod 5$. It follows that if $a \equiv 0 \pmod 5$, then $a^2 \equiv 0 \pmod 5$

For any $k \in \mathbb{Z}$, we know $a = 5k$, $a^2 = 25k^2 = 5(5k^2)$, thus as $5k^2 \in \mathbb{Z}$, $5 \mid a^2$.

What we can see is that for any int. a^2, 1 of 3 CASES IS TRUE.

① $a^2 \equiv 0 \pmod 5$ ② $a^2 \equiv 1 \pmod 5$ or ③ $a^2 \equiv 4 \pmod 5$

We can notice that any multiple of 5 ends in a 0, or 5.

From this for any perfect square, a^2, to exist, it must hold that the last digit is of the following: $\{0,1,4,5,6,9\}$ as $2 \pmod 5 \equiv 2$, $3 \pmod 5 \equiv 3$, $2 \pmod 5 \equiv 7$, & $3 \pmod 5 \equiv 8$; which do not suffice the given conditions for a perfect square.

Formalizing the work above; $\maltese$ if the last digit of some int m is within the set $\lambda = \{0,1,4,5,6,9)$, then m is a perfect square of the form $m = a^2$ with a also some int. $\maltese$

A proof by contradiction follows: As the last digit, 3, of the number $5,344,580,232,468,953,153 = m$, is not included in λ, m is not of the form $m = a^2$, thus m is not a perfect square. ∎

(b) Is the integer $n = 782,456,231,189,002,288,438$ a perfect square? Justify your conclusion.

Following proof in a) ; As the last digit, 8, of $n = 782,456,231,189,002,288,438$, is not in the set $\lambda = \{0,1,4,5,6,9\}$, n is not of the form $n = a^2$ & thus n is not a perfect square. ∎

12. **(a)** Use the result in Proposition 3.33 to help prove that for each integer a, if 5 divides a^2, then 5 divides a.

From prop. 3.33 ; If $a \not\equiv 0 \pmod 5$, then $a^2 \equiv 1 \pmod 5$, or $a^2 \equiv 4 \pmod 5$. This states $(5 \nmid a) \to (5 \mid a^2-1) \vee (5 \mid a^2-4)$. We also Know that $(5 \mid a) \to (5 \mid a^2)$. The contrapositive of these statements are as follows. $(5 \nmid a^2) \to (5 \nmid a)$, and $(5 \nmid a^2-1) \wedge (5 \nmid a^2-4) \to (5 \mid a)$. We will take the hypothesis as true. Thus we have $(5 \mid a^2)$. From here we Know both that $(5 \nmid a^2-1) \wedge (5 \nmid a^2-4)$ as neither 1 or 4 are multiples of 5. Thus we Know that $(5 \mid a)$ and have proven that $(5 \mid a^2) \to (5 \mid a)$ ∎

It follows from this and the prior proof that we now Know $(5 \mid a) \leftrightarrow (5 \mid a^2)$

(b) Prove that the real number $\sqrt{5}$ is an irrational number.

A rational number can be represented by 2 ints., say m & n, such that $n \neq 0$, then $\frac{m}{n}$ is rational. irrationals cannot be represented by this combination of integers.

Assuming $\sqrt{5}$ is Rational, let $\sqrt{5} = \frac{m}{n}$, thus $5 = \frac{m^2}{n^2}$.

We can now see $n^2 = \frac{m^2}{5}$, & $n = \frac{m}{\sqrt{5}}$.

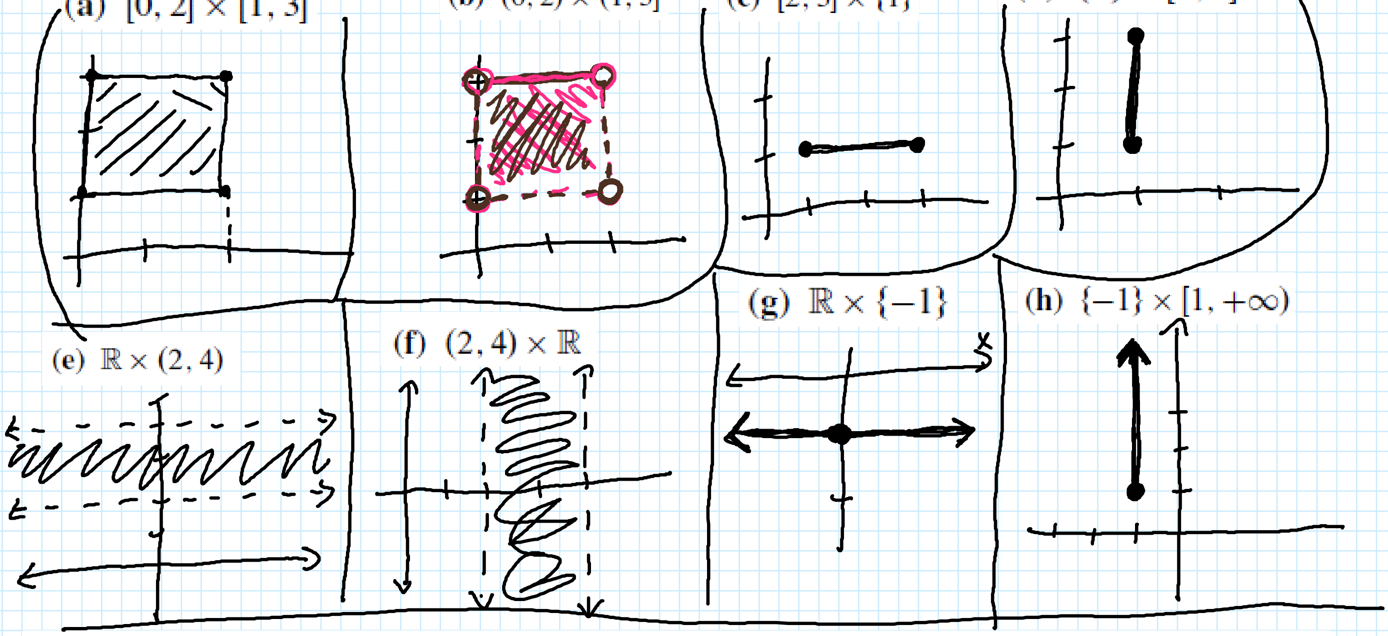
Because m is an int, n cannot be an int. Let alone because $\sqrt{5}$ is real, and not an int., n cannot even be a Rational number. This leads to a contradiction, thus $\sqrt{5}$ cannot be rational by definition. ∎

5.4 (Cartesian Products)

2. Sketch a graph of each of the following Cartesian products in the Cartesian plane.

(a) $[0, 2] \times [1, 3]$ (b) $(0, 2) \times (1, 3]$ (c) $[2, 3] \times \{1\}$ (d) $\{1\} \times [2, 3]$

(e) $\mathbb{R} \times (2, 4)$ (f) $(2, 4) \times \mathbb{R}$ (g) $\mathbb{R} \times \{-1\}$ (h) $\{-1\} \times [1, +\infty)$



5. Prove Theorem 5.25, Part (5): $A \times (B - C) = (A \times B) - (A \times C)$.

Let $(\alpha, \gamma) \in [A \times (B - C)]$. thus $\alpha \in A$ & $\gamma \in (B - C)$. Thus $\gamma \in B$ & $\gamma \notin C$ We can now see that $(\alpha, \gamma) \in (A \times B)$ as $\alpha \in A$ & $\gamma \in B$. Additionaly $(\alpha, \gamma) \notin (A \times C)$ as $\gamma \notin C$. It follows that for any (α, γ) in $[A \times (B - C)]$, (α, γ) will be in $(A \times B)$ & not in $(A \times C)$. It is now easy to see that $[A \times (B - C)] \cap (A \times C) = \emptyset$ as no element in $[A \times (B - C)]$ is in $(A \times C)$.

given an element β is included in both B & C, (α, β) will not be in $[A \times (B - C)]$ as it is not in $(B - C)$. we must show that $(\alpha, \beta) \notin [(A \times B) - (A \times C)]$.

$(\alpha, \beta) \in (A \times B)$ as $\alpha \in A$ & $\beta \in B$.

Also $(\alpha, \beta) \in (A \times C)$ as $\alpha \in A$ & $\beta \in C$. It is now self evident that $(\alpha, \beta) \notin [(A \times B) - (A \times C)]$ as $(\alpha, \beta) \in (A \times C)$

we have thus proved that any element in, or not in $[A \times (B - C)]$ will be similarly in, or not in $[(A \times B) - (A \times C)]$

Going the other direction, let $(\alpha,\gamma)\in[(A\times B)-(A\times C)]$

$\therefore$ $(\alpha,\gamma)\in(A\times B)$ & $(\alpha,\gamma)\notin(A\times C)$. it follows as

$\gamma\in B$ & $\gamma\notin C$, thus $\gamma\in(B-C)$ & $(\alpha,\gamma)\in[A\times(B-C)]$ ■

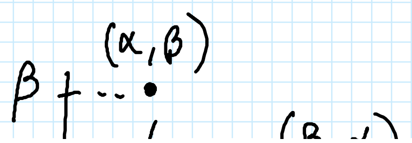
7. Let $A = \{1\}$, $B = \{2\}$, and $C = \{3\}$.

(a) Explain why $A \times B \neq B \times A$.

The Cartesian Product consists of "ordered" pairs, thus the order in which element appear within a pair matter.

It cannot be assumed that $A\times B = B\times A$ for this reason. if $A=B$ we could use this. looking at elements $\alpha\in A$ & $\beta\in B$, $A\times B$ is thus (α,β), while $B\times A$ is (β,α). thes pairs have different order...

A graphical representation is easy to see.

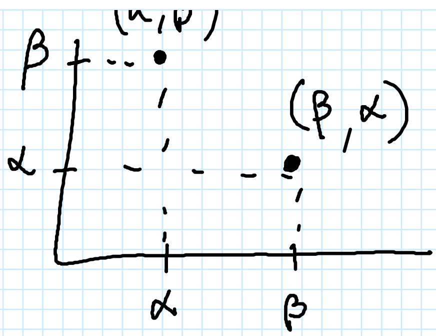


(b) Explain why $(A \times B) \times C \neq A \times (B \times C)$.

lets populate A,B,C, all with 1 element. Let $x\in A$, $y\in B$, & $z\in C$.

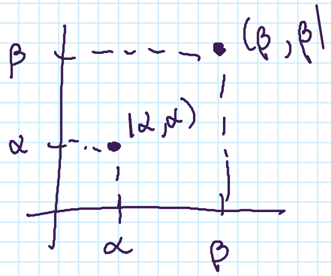
Now $(A\times B)$ is $\{(x,y)\}$ so $(A\times B)\times C$ is $\{((x,y),z)\}$. on the other hand, $(B\times C)$ is $\{(y,z)\}$ thus $A\times(B\times C) = \{(x,(y,z))\}$. A simple way to explain this discrepency is through events. in $(A\times B)\times C$, the first event happened @ (x,y), & the second @ z. In the case for $A\times(B\times C)$, the first event happens at x, and the second at (y,z). From this description, not a single event happened at the same place.

Graphically



In the Rare Case For

$A \times A$ or $B \times B$



Graphically