Intro Number Theory and Proofs

Alex Shaffer

Basic Sets Recap

- Natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \ldots\}$
  - Has something called the “Well ordering principle” which states that every nonempty subset of the natural numbers has a least element.
    - For example, $\{1, 2, 3\}$ is a subset of the natural numbers and has the least element 1.
- Integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- The integers are closed under addition, subtraction, and multiplication.

Intro to Proof Writing

- A proof is way of showing some mathematical statement is true.
- It uses fundamental principles (axioms or postulates) to show that it is true.
- Usually proof show us that a “theorem” is true.
  - A theorem is a mathematical statement that usually takes the form “if <condition>, then <result>”

Proof Example

- Theorem: The quadratic formula. As an if-then statement, this reads, If f is a quadratic function of the form $f(x) = ax^2 + bx + c$, then its roots are $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
  - Proof: A root of f is the x such that $f(x) = 0$.
  - Start with $ax^2 + bx + c = 0$.
  - Divide both sides by a to get $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$
  - Subtract $\frac{c}{a}$ from both sides to get $x^2 + \frac{b}{a}x = -\frac{c}{a}$
  - Add $\left(\frac{b}{2a}\right)^2$ to both sides to get $x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{\mathrm{c}}{\mathrm{a}}$

Proof continued

- Complete the square to get $\left(x+\frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{\mathrm{c}}{\mathrm{a}}$
- Take the square root of both sides accounting for positive and negative values: $x+\frac{b}{2a} = \pm\left(\left(\frac{b}{2a}\right)^2 - \frac{c}{a}\right)^{\frac{1}{2}}$
- Subtract $\frac{b}{2a}$ from both sides to get $x = -\frac{b}{2a} \pm \left(\left(\frac{b}{2a}\right)^2 - \frac{c}{a}\right)^{\frac{1}{2}}$
- You can always multiply by 1, and $1 = \frac{2a}{2a}$ so we multiply the second term in the right had side by that.
- $x = -\frac{b}{2a} \pm \frac{\left((2a)^2\left(\frac{b}{2a}\right)^2 - \frac{(2a)^2 c}{a}\right)^{\frac{1}{2}}}{2a} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$

Divisibility

- We are going to restrict our discussion of division to exclusively integer division.
- If a divides b then then there is no remainder left over.
  - It also means that there exists some integer k such that $ak = b$.
- If a divides b, then we write that as $a|b$. If a doesn’t divide b then we write $a \nmid b$.

Modular Congruences

- We are going to define modular congruences as follows.
  - If $a \equiv b \ (mod\ n)$ then a and b have the same remainder when divided by n.
  - If $a \equiv b \ (mod\ n)$ then that means $n|(a - b)$.
    - This is more useful for writing proofs about modular congruences.

Reflexive Property

- Theorem: If a and n are integers with $n > 0$. Then $a \equiv a \ (mod\ n)$
- Proof:
  - By the definition of modular congruence, we need to show that $n|(a\ -a)$.
  - However, $(a\ -a) = 0$ so we need only show $n|0$.
  - $n|0$ means that there must exist some integer k such that $kn = 0$. We know that if $k = 0$ this must be true, so $n|k$.
  - Therefore, $a \equiv a\ (mod\ n)$

Symmetry Property

- Theorem: If a, b, and n are integers with $n > 0$, and $a \equiv b \ (mod\ n)$, then $b \equiv a \ (mod\ n)$.
- Proof
  - $a \equiv b \ (mod\ n)$ implies that $n|(a - b)$.
  - In turn, this implies that there exists some integer k such that $kn = a - b$
  - Multiplying by (-1) give us $-kn = -(a - b) = (b - a)$
  - Since $-k$ is still an integer, $n|(b - a)$
  - By the definition of modular congruence, then $b \equiv a(mod\ n)$