CSE 311: Foundations of Computing I

Section 5: Number Theory

1. Modular Arithmetic

(a) Consider the following claim in the domain of integers: if $a \mid b$, $b \mid a$, and $a \neq 0$, then $a = b$ or $a = -b$.

Here is a formal proof of the claim:

1.	$((a \mid b) \land (b \mid a)) \land (a \neq 0)$	Given
2.	$(a \mid b) \land (b \mid a)$	Elim $\land$: 1
3.	$a \mid b$	Elim $\land$: 2
4.	$\exists k\,(ka = b)$	Def of "$\mid$": 3
5.	$ja = b$	Elim $\exists$: 4, special j
6.	$b \mid a$	Elim $\land$: 2
7.	$\exists k\,(kb = a)$	Def of "$\mid$": 6
8.	$kb = a$	Elim $\exists$: 7, special k
9.	$a = kb = k(ja) = (kj) \cdot a$	Algebra: 8, 5
10.	$a \neq 0$	Elim $\land$: 1
11.	$kj = 1$	Algebra (division): 9, 10
12.	$(j = 1 \land k = 1) \lor (j = -1 \land k = -1)$	Prop of integer mult: 11
	13.1. $j = 1 \land k = 1$ — Assumption	
	13.2. $k = 1$ — Elim $\land$: 13.1	
	13.3. $a = kb = b$ — Algebra: 8, 13.2	
	13.4. $a = b \lor a = -b$ — Intro $\lor$: 13.3	
13.	$(j = 1 \land k = 1) \to (a = b \lor a = -b)$	Direct Proof
	14.1. $\neg(j = 1 \land k = 1)$ — Assumption	
	14.2. $j = -1 \land k = -1$ — Elim $\lor$: 12, 14.1	
	14.3. $k = -1$ — Elim $\land$: 14.2	
	14.4. $a = kb = -b$ — Algebra: 8, 14.3	
	14.5. $a = b \lor a = -b$ — Intro $\lor$: 14.4	
14.	$\neg(j = 1 \land k = 1) \to (a = b \lor a = -b)$	Direct Proof
15.	$a = b \lor a = -b$	Proof by Cases: 13, 14

Translate this formal proof to English.

(b) Consider the following claim in the domain of integers: if $n \mid m$, with $n, m > 1$, and $a \equiv b \pmod{m}$, then we must have $a \equiv b \pmod{n}$.

Here is an English proof of that claim...

Proof: Suppose $n \mid m$, with $n, m > 1$, and $a \equiv b \pmod{m}$. By definition of divides, the first part says $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, the second part says $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we have $a - b = mj = (kn)j = (kj)n$. The latter says that $a \equiv b \pmod{n}$, by the definition of congruence. $\square$

Translate this English proof into a formal proof.

2. Perfect Squares

Let n be a positive integer. Consider the following claim: if n^2+1 is a square, then n is even.

Here are a few different proofs of the claim...

Proof 1: There are no positive numbers n such that n^2+1 is a square, so the implication is true because it's premise is false. $\square$

Proof 2: The claim supposes that n^2+1 is a square, but n^2 is also a square by definition, so the premise asks us to suppose that we have two squares (n^2 and n^2+1) that differ by 1. However, if we take a list of all positive integers $1, 2, 3, 4, \ldots$ and square them all, we get $1, 4, 9, 16, \ldots$, and we can see that the gap between adjacent numbers is increasing, so the smallest gap is between the first two numbers, and it is just 3. Hence, the premise cannot be true. This means that the claim, however, is true, since its premise is false. $\square$

Proof 3: Suppose that n^2+1 is a square. Then, by definition, we have $n^2+1=k^2$ for some $k \in \mathbb{Z}$. Now, to establish a contradiction, suppose that n is odd. Then, $n=2j+1$ for some $j \in \mathbb{Z}$, and we have

$$n^2+1=(2j+1)^2+1=4j^2+4j+1+1=4(j^2+j)+2.$$

This shows that $(n^2+1) \bmod 4 = 2$, by definition, and similarly $(n^2+1) \bmod 2 = 0$.

Now, if k is even, then we have $k^2=(2\ell)^2=4\ell^2$ for some $\ell \in \mathbb{Z}$. This means $k^2 \bmod 4 = 0$, contradicting that $k^2 \bmod 4 = (n^2+1) \bmod 4 = 2$. On the other hand, if k is odd, then we have $k^2=(2\ell+1)^2=4\ell^2+4\ell+1=2(2\ell^2+2\ell)+1$ for some $\ell \in \mathbb{Z}$. But this says that $k^2 \bmod 2 = 1$, contradicting that $k^2 \bmod 2 = (n^2+1) \bmod 2 = 0$. In either case, we have a contradiction. $\square$

(a) Which of these English proofs would you prefer to translate to a formal proof? Do so.

(b) Why is it helpful, in Proof 3, to write rewrite $4j^2+4j+1+1$ as $4(j^2+j)+2$?

(c) Would it be helpful to note, at the beginning of the second paragraph of Proof 3, that we are going to complete the proof (finding a contradiction) by cases?

3. Casting Out Nines

Let $n \in \mathbb{N}$. Write an English proof that, if $n \equiv 0 \pmod 9$, then the sum of the digits of n is a multiple of 9.

You may also use without proof the fact that we can substitute a congruent value into another congruence and the results is still true. E.g, if we have $a \equiv 7 \pmod m$ and also $a+b \equiv 3(b-a) \pmod m$, then we can substitute for a in the second congruence to get $7+b \equiv 3(b-7) \pmod m$.

Hint: apply the fact that every integer has a decimal expansion.