CSE 311: Foundations of Computing I

Section 5: Number Theory Solutions

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

Translate this formal proof to English.

Solution:

Suppose $a \mid b$, $b \mid a$, and $a \neq 0$. By the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ja, a = kb$ for some integers j, k. Combining these equations, we see that $a = k(ja) = (kj)a$. Since $a \neq 0$, we can divide both sides by a to see that $kj = 1$.

By the properties of integer multiplication, $kj = 1$ is only possible if $j = k = 1$ or $j = k = -1$. If the first holds, then we have $a = kb = b$. If the second holds, then we have $a = kb = -b$. Hence, in either case, we have $a = b$ or $a = -b$.

(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.

Solution:

1.	$(((n \mid m) \wedge (n > 1)) \wedge (m > 1)) \wedge (a \equiv b \pmod{m})$	Given
2.	$((n \mid m) \wedge (n > 1)) \wedge (m > 1)$	Elim $\wedge$: 1
3.	$(n \mid m) \wedge (n > 1)$	Elim $\wedge$: 2
4.	$n \mid m$	Elim $\wedge$: 3
5.	$n > 1$	Elim $\wedge$: 3
6.	$m > 1$	Elim $\wedge$: 2
7.	$a \equiv b \pmod{m}$	Elim $\wedge$: 1
8.	$\exists k\,(kn = m)$	Def of "$\mid$": 4
9.	$kn = m$	Elim $\exists$: 8, special k
10.	$m \mid a - b$	Def of $\equiv$: 7
11.	$\exists k\,(km = a - b)$	Def of "$\mid$": 10
12.	$jm = a - b$	Elim $\exists$: 11, special j
13.	$a - b = mj = (kn)j = (kj)n$	Algebra: 12, 9
14.	$\exists k\,(kn = a - b)$	Intro $\exists$: 13
15.	$n \mid a - b$	Def of "$\mid$": 14
16.	$a \equiv b \pmod{n}$	Def of $\equiv$: 15

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. □

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

Solution:

Neither proof 1 or proof 2 is helpful in trying to write a formal proof. Here is a translation of Proof 3:

1.	Square(n^2+1)	Given
2.	$\exists k\,(n^2+1=k^2)$	Def of Square: 1
3.	$n^2+1=k^2$	Elim ∃: 2, special k
4.1.	Odd(n)	Assumption
4.2.	$\exists j\,(n=2j+1)$	Def of Odd: 4.1
4.3.	$n=2j+1$	Elim ∃: 4.2
4.4.	$n^2+1=(2j+1)^2+1=4(j^2+j)+2$	Algebra: 4.3
4.5.	$(n^2+1) \bmod 4 = 2$	Def of $\bmod$: 4.4
4.6.	$(n^2+1) \bmod 2 = 0$	Def of $\bmod$: 4.4
4.7.1.	Even(k)	Assumption
4.7.2.	$\exists \ell\,(k=2\ell)$	Def of Even: 4.7.1
4.7.3.	$k=2\ell$	Elim ℓ: 4.7.2
4.7.4.	$k^2=(2\ell)^2=4\ell^2+0$	Algebra: 4.7.3
4.7.5.	$k^2 \bmod 4 = 0$	Def of $\bmod$: 4.7.4
4.7.6.	$(n^2+1) \bmod 4 = 0$	Substitute: 3, 4.7.5
4.7.6.	F	Negation: 4.7.6, 4.5
4.7.	Even$(k) \to$ F	Direct Proof
4.8.1.	¬Even(k)	Assumption
4.8.2.	Odd(k) ∨ Even(k)	Prop of Integers
4.8.3.	Odd(k)	Elim ∨: 4.8.1, 4.8.2
4.8.4.	$\exists \ell\,(k=2\ell+1)$	Def of Odd: 4.8.3
4.8.5.	$k=2\ell+1$	Elim ℓ: 4.8.4
4.8.6.	$k^2=2(2\ell^2+2\ell)+1$	Algebra: 4.8.5
4.8.7.	$k^2 \bmod 2 = 1$	Def of $\bmod$: 4.8.6
4.8.8.	$(n^2+1) \bmod 2 = 1$	Substitute: 3, 4.8.6
4.8.9.	F	Negation: 4.8.8, 4.5
4.8.	¬Even$(k) \to$ F	Direct Proof
4.9.	F	Proof by Cases: 4.4, 4.5
4.	Odd$(n) \to$ F	Direct Proof
5.	¬Odd(n) ∨ F	Law of Implication: 4
6.	¬Odd(n)	Identity: 5
7.	Odd(n) ∨ Even(n)	Prop of Integers
8.	Even(n)	Elim ∨: 6, 7

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

Solution:

The write hand side is of the form $4q + r$ with $0 \leq r < 4$, we get immediately that this value mod 4 is equal to 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?

Solution:

I think this would make it easier to read. In general, for English proofs, telling the reader where you are going beforehand is helpful.

3. Divisors and Primes

Write an English proof of the following claim about a positive integer n: if the sum of the divisors of n is $n+1$, then n is prime.

Hint: note that $n \mid n$ is always true.

Solution:

Let the distinct divisors of n be $d_1, d_2, \ldots, d_k$, each of which is positive. Writing $n = 1 \cdot n$, we see that $1 \mid n$ and $n \mid n$, by the definition of "|", so these two numbers are in the list. Moving them around in the list, we can take $d_1 = n$ and $d_2 = 1$.

By assumption, we have $n + 1 = d_1 + d_2 + \cdots + d_k$. Substituting the values of d_1 and d_2 from above, we have

$$n + 1 = n + 1 + d_3 + d_4 + \cdots + d_k.$$

Subtracting $n + 1$ from both sides, we see that

$$0 = d_3 + d_4 + \cdots + d_k.$$

Since each divisor in the list is positive, this is only possible if the right hand side is an empty list. That is, we must have $k = 2$, meaning the list of divisors is just 1 and n. By definition, this says that n is prime.

(This is an example of a proof that would be difficult to formalize. In particular, the formal system does not give us a way to name to all the divisors of n as we did above. It is possible to write a formal proof of this, but it would be much more complicated than the English proof.)

4. 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.

Solution:

As we saw in lecture, if $a \equiv b \pmod m$, then $a + c \equiv b + c \pmod m$ and $ac \equiv bc \pmod m$. More generally, we can replace a with b in any expression involving only addition (or subtraction) and multiplication, and the result will still be congruent modulo m. We will use that fact to complete this proof.

Suppose that $n \equiv 0$ (mod 9). Write n in terms of its decimal digits as $n = x_0 + 10x_1 + 10^2 x_2 + \cdots + 10^m x_m$. The latter is an expression using only addition and multiplication, so we can replace all occurrences of 10 with any value congruent to it and the result will be congruent to n. Since $10 = 1 \cdot 9 + 1$, we see that $10 \equiv 1 \pmod 9$, so we can substitute 1 for 10 if we work mod 9.

Carrying out that calculation gives us:

$0 \equiv n \pmod 9$	Given
$\equiv x_0 + 10x_1 + 10^2x_2 + \cdots + 10^m x_m \pmod 9$	Definition of x_i's
$\equiv x_0 + 1x_1 + 1^2x_2 + \cdots + 1^m x_m \pmod 9$	Substitute 1 for 10
$\equiv x_0 + 1x_1 + 1^2x_2 + \cdots + 1^m x_m \pmod 9$	$1^k = 1$ for all $k \geq 1$
$\equiv x_0 + x_1 + x_2 + \cdots + x_m \pmod 9$	1 is the multiplicative identity

The final line is the sum of the digits of n, taken modulo 9. Since it is congruent to 0 modulo 9, this says that the sum is a multiple of 9.