Section 05: Solutions

1. Modular Arithmetic I

Let the domain of discourse be integers. Consider the following claim:

$$\forall a \forall b((a \mid b \wedge b \mid a) \rightarrow (a = b \vee a = -b))$$

.

For this question, you may use the following fact:
Fact 1: $\forall a \forall b(ab = 1 \rightarrow a = 1 \vee a = -1)$

(a) Translate the claim into English. **Solution:**

For any integers a and b, if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

(b) Write a formal proof that the claim holds. **Solution:**

1.1. Let a and b be arbitrary

1.2.1.	$a \mid b \wedge b \mid a$	[Assumption]
1.2.2.	$a \mid b$	[Elim $\wedge$: 1.2.1]
1.2.3.	$b \mid a$	[Elim $\wedge$: 1.2.1]
1.2.4.	$a \neq 0 \wedge \exists k(b = ka)$	[Def Of Divides: 1.2.2]
1.2.5.	$b \neq 0 \wedge \exists j(a = jb)$	[Def Of Divides: 1.2.3]
1.2.6.	$\exists k(b = ka)$	[Elim $\wedge$: 1.2.4]
1.2.7.	$b = ka$	[Elim $\exists$: 1.2.6]
1.2.8.	$\exists j(a = jb)$	[Elim $\wedge$: 1.2.5]
1.2.9.	$a = jb$	[Elim $\exists$: 1.2.8]
1.2.10.	$a = j(ka)$	[Substitution: 1.2.7, 1.2.9]
1.2.11.	$1 = jk$	[Algebra: 1.2.10, since $a \neq 0$ from 1.2.4]
1.2.12.	$\forall a \forall b(ab = 1 \rightarrow a = 1 \vee a = -1)$	[Given: Fact 1]
1.2.13.	$\forall b(jb = 1 \rightarrow j = 1 \vee j = -1)$	[Elim $\forall$: 1.2.12]
1.2.14.	$jk = 1 \rightarrow j = 1 \vee j = -1)$	[Elim $\forall$: 1.2.13]
1.2.15.	$j = 1 \vee j = -1$	[Modus Ponens: 1.2.11, 1.2.14]
1.2.16.	$a = b \vee a = -b$	[Substitution: 1.2.14, 1.2.9]

1.2. $(a \mid b \wedge b \mid a) \rightarrow (a = b \vee a = -b)$ [Direct Proof]

1. $\forall a \forall b((a \mid b \wedge b \mid a) \rightarrow (a = b \vee a = -b))$ [Intro $\forall$]

(c) Translate your proof to English. **Solution:**

Let a and b be arbitrary integers.

Suppose that $a \mid b$ and $b \mid a$. By the definition of divides, we have $a \neq 0$, $b \neq 0$, $b = ka$ and $a = jb$ for some integers k, j. Substituting the equation for b into the equation for a, we see that $a = j(ka)$. Then, dividing both sides by a, we get $1 = jk$. Since j and k are integers, this equation only holds if $j = 1$ or $j = -1$. Substituting the possible values of j back into the equation for b, it follows that $a = b$ or $a = -b$.

Since a and b were arbitrary, we have proven the claim.

2. Modular Arithmetic II

Let the domain of discourse be positive integers, and let n and m not be equal to 1. Consider the following claim:

$$\forall n\ \forall m\ \forall a\ \forall b\ ((n \mid m \wedge a \equiv_m b) \rightarrow a(\equiv_n b))$$

.

(a) Translate the claim into English. **Solution:**

For any positive integers n, m, a, and b where $\neg(n = 1)$ and $\neg(m = 1)$, if $n \mid m$ and $a \equiv_m b$ then $a \equiv_n b$.

(b) Write a formal proof that the claim holds. **Solution:**

1. $\neg(n = 1)$ [Given]
2. $\neg(m = 1)$ [Given]
    - 3.1. Let n, m, a and b be arbitrary
        - 3.2.1. $n \mid m \wedge a \equiv_m b$ [Assumption]
        - 3.2.2. $n \mid m$ [Elim $\wedge$: 3.2.1]
        - 3.2.3. $\exists k(m = kn)$ [Def Of Divides: 3.2.2]
        - 3.2.4. $m = kn$ [Elim $\exists$: 3.2.3]
        - 3.2.5. $a \equiv_m b$ [Elim $\wedge$: 3.2.1]
        - 3.2.6. $m|a - b$ [Def Of Congruent: 3.2.5]
        - 3.2.7. $\exists j(a - b = mj)$ [Def Of Divides: 3.2.6]
        - 3.2.8. $a - b = mj$ [Elim $\exists$: 3.2.7]
        - 3.2.9. $a - b = (kn)j$ [Substitution: 3.2.4, 3.2.8]
        - 3.2.10. $a - b = n(kj)$ [Algebra: 3.2.9]
        - 3.2.11. $\exists r(a - b = rn)$ [Intro $\exists$: 3.2.10]
        - 3.2.12. $n \mid a - b$ [Def of Divides: 3.2.11]
        - 3.2.13. $a \equiv_n b$ [Def of Congruent: 3.2.12]
    - 3.2. $(n \mid m \wedge a \equiv_m b) \rightarrow (a \equiv_n b)$ [Direct Proof]
3. $\forall n \forall m \forall a \forall b((n \mid m \wedge a \equiv_m b) \rightarrow (a \equiv_n b))$ [Intro $\forall$]

(c) Translate your proof to English. **Solution:**

Let n, m, a and b be arbitrary positive integers.

Suppose $n \mid m$ with $n \neq 1$ and $m \neq 1$, and $a \equiv_m b$. By definition of divides, we have $m = kn$ for some $k \in \mathbb{Z}$. By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Substituting the equation for m into the equation for $a - b$, we see that $a - b = (knj) = n(kj)$. By definition of divides, $n \mid a - b$ holds. By definition of congruence, we have $a \equiv_n b$, as required.

Since n, m, a and b were arbitrary, we have proven the desired result.

3. Euclid's Lemma[1]

Let the domain of discourse be integers. Consider the following claim:

$$\forall p \forall a \forall b\, ((Prime(p) \land p \mid ab) \to (p \mid a \lor p \mid b))$$

Recall the definition of prime given in lecture:

$$Prime(p) := \neg(p = 1) \land \forall x\, ((x \mid p) \to (x = 1 \lor x = p))$$

For this question, you can use the following facts:
Fact 1: If an integer p divides ab and $\gcd(p, a) = 1$, then p divides b.
Fact 2: GCD(a,b) | a and GCD(a,b) | b.

(a) Translate the claim into English. **Solution:**

For any integers a, b and p, if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$ holds.

(b) Write a formal proof that the claim holds. **Solution:**

1.1. Let p, a and b be arbitrary
- 1.2.1. $Prime(p) \land p \mid ab$ [Assumption]
- 1.2.2. $Prime(p)$ [Elim ∧: 1.2.1]
- 1.2.3. $p \mid ab$ [Elim ∧: 1.2.1]
- 1.2.4. $gcd(p, a) = 1 \lor gcd(p, a) \neq 1$ [Tautology]
  - 1.2.5.1. $gcd(p, a) = 1$ [Assumption]
  - 1.2.5.2. $p \mid b$ [Fact 1: 1.2.3, 1.2.5.1]
  - 1.2.5.1. $p \mid a \lor p \mid b$ [Intro ∨: 1.2.5.2]
- 1.2.5. $gcd(p, a) = 1 \to p \mid a \lor p \mid b$ [Direct Proof]
  - 1.2.6.1. $gcd(p, a) \neq 1$ [Assumption]
  - 1.2.6.2. $\neg(p = 1) \land \forall x\, ((x \mid p) \to (x = 1 \lor x = p))$ [Def Of Prime: 1.2.2]
  - 1.2.6.3. $\forall x\, ((x \mid p) \to (x = 1 \lor x = p))$ [Elim ∧: 1.2.6.2]
  - 1.2.6.4. $((gcd(p, a) \mid p) \to (gcd(p, a) = 1 \lor gcd(p, a) = p))$ [Elim ∀: 1.2.6.3]
  - 1.2.6.5. $gcd(p, a) \mid p$ [Fact 2]
  - 1.2.6.6. $gcd(p, a) = 1 \lor gcd(p, a) = p))$ [Modus Ponens: 1.2.6.5, 1.2.6.4]
  - 1.2.6.7. $gcd(p, a) = p$ [Elim ∨: 1.2.6.1, 1.2.6.6]
  - 1.2.6.8. $p \mid a$ [Fact 2]
  - 1.2.6.9. $p \mid a \lor p \mid b$ [Intro ∨: 1.2.6.8]
- 1.2.6. $gcd(p, a) \neq 1 \to p \mid a \lor p \mid b$ [Direct Proof]
- 1.2.7. $p \mid a \lor p \mid b$ [Cases: 1.2.4, 1.2.5, 1.2.6]

1.2. $(Prime(p) \land p \mid ab) \to (p \mid a \lor p \mid b)$ [Direct Proof]

1. $\forall p \forall a \forall b((Prime(p) \land p \mid ab) \to (p \mid a \lor p \mid b))$ [Intro ∀]

(c) Translate your proof to English. **Solution:**

[1] This proof isn't much longer than what you've seen before, but it can be a little easier to get stuck — use these as a chance to practice how to get unstuck if you do!

Let p, a and b be arbitrary integers.

Suppose that $p \mid ab$ for prime number p.

There are two cases, either $\gcd(p, a) = 1$ or $\gcd(p, a) \neq 1$.

Case 1: $\gcd(p, a) = 1$
In this case, $p \mid b$ by Fact 1 above.

Case 2: $\gcd(p, a) \neq 1$
In this case, p and a share a common positive factor greater than 1. But since p is prime, its only positive factors are 1 and p, meaning $\gcd(p, a) = p$. This says p is a factor of a, that is, $p \mid a$.

In both cases, we have shown that $p \mid a$ or $p \mid b$.

Since p, a and b were arbitrary, we have proven the claim.

4. 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, 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.)

5. Have we derived yet?

Each of the following proofs has some mistake in its reasoning - identify that mistake.

(a) *Proof.* If it is sunny, then it is not raining. It is not sunny. Therefore it is raining. $\square$

Solution:

Let p be the proposition that it is sunny and r be the proposition that it is not raining. We know $p \to \neg r$ and $\neg p$. Using this, the proof shows the inverse $\neg p \to r$. However, the inverse is not equivalent to the implication, so we cannot infer the inverse from the given statement.

(b) Prove that if $x + y$ is odd, either x or y is odd but not both.

Proof. Suppose without loss of generality that x is odd and y is even.

Then, $\exists k\ x = 2k+1$ and $\exists m\ y = 2m$. Adding these together, we can see that $x + y = 2k + 1 + 2m = 2k + 2m + 1 = 2(k + m) + 1$. Since k and m are integers, we know that $k + m$ is also an integer. So, we can say that $x + y$ is odd. Hence, we have shown what is required. □

Solution:

Looking at this logically, let's let p be the proposition that $x + y$ is odd and r be the proposition that either x or y is odd but not both. This proof shows $r \to p$ instead of $p \to r$.

This proof is incorrect because we have assumed the conclusion. Remember, the converse is not equivalent to the implication.

(c) Prove that $2 = 1$. :)

Proof. Let a, b be two equal, non-zero integers. Then,

$$\begin{aligned}
a &= b \\
a^2 &= ab && [\textsc{Multiply both sides by a}] \\
a^2 - b^2 &= ab - b^2 && [\textsc{Subtract } b^2 \textsc{ from both sides}] \\
(a-b)(a+b) &= b(a-b) && [\textsc{Factor both sides}] \\
a + b &= b && [\textsc{Divide both sides by } a - b] \\
b + b &= b && [\textsc{Since } a = b] \\
2b &= b && [\textsc{Simplify}] \\
2 &= 1 && [\textsc{Divide both sides by b}]
\end{aligned}$$

□

Solution:

In line 5, we divided by $a - b$. Since $a = b$, $b - a = 0$. Therefore, this was dividing by 0. Dividing by 0 is an undefined operation (!) so this was an invalid step in the proof.

(d) Prove that $\sqrt{3} + \sqrt{7} < \sqrt{20}$

Proof.

$$\begin{aligned}
&\sqrt{3} + \sqrt{7} < \sqrt{20} \\
&(\sqrt{3} + \sqrt{7})^2 < 20 \\
&3 + 2\sqrt{21} + 7 < 20 \\
&19.165 < 20
\end{aligned}$$

It is true that $19.165 < 20$, hence, we have shown that $\sqrt{3} + \sqrt{7} < \sqrt{20}$ □

Solution:

Like part (b), here too, we have assumed the conclusion was true. In this case, instead of showing that this statement is true, we have shown this statement $\to T$. Remember, this does not necessarily mean that p is true! If you think back to the truth table for the implication $p \to q$, the implication becomes a vacuous truth if q is true: we know nothing about the truth value of p.

6. GCD

(a) Calculate gcd(100, 50).

Solution:

50

(b) Calculate gcd(17, 31).

Solution:

1

(c) Find the multiplicative inverse of 6 (mod 7).

Solution:

6

(d) Does 49 have an multiplicative inverse (mod 7)?

Solution:

It does not. Intuitively, this is because 49x for any x is going to be 0 mod 7, which means it can never be 1.

7. Extended Euclidean Algorithm

(a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv_{33} 1$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

Solution:

First, we find the gcd:

$$\begin{aligned}
\gcd(33,7) &= \gcd(7,5) & 33 &= \boxed{7} \bullet 4 + 5 && (1)\\
&= \gcd(5,2) & 7 &= \boxed{5} \bullet 1 + 2 && (2)\\
&= \gcd(2,1) & 5 &= \boxed{2} \bullet 2 + 1 && (3)\\
&= \gcd(1,0) & 2 &= 1 \bullet 2 + 0 && (4)\\
&= 1 & & && (5)
\end{aligned}$$

Next, we re-arrange equations (1) - (3) by solving for the remainder:

$$\begin{aligned}
1 &= 5 - \boxed{2} \bullet 2 && (6)\\
2 &= 7 - \boxed{5} \bullet 1 && (7)\\
5 &= 33 - \boxed{7} \bullet 4 && (8)\\
& && (9)
\end{aligned}$$

Now, we backward substitute into the boxed numbers using the equations:

$$\begin{aligned} 1 &= 5 - \boxed{2} \bullet 2 \\ &= 5 - (7 - \boxed{5} \bullet 1) \bullet 2 \\ &= 3 \bullet \boxed{5} - 7 \bullet 2 \\ &= 3 \bullet (33 - \boxed{7} \bullet 4) - 7 \bullet 2 \\ &= 33 \bullet 3 + 7 \bullet -14 \end{aligned}$$

So, $1 = 33 \bullet 3 + \boxed{7} \bullet -14$. Thus, $33 - 14 = 19$ is the multiplicative inverse of 7 mod 33.

(b) Now, solve $7z \equiv_{33} 2$ for all of its integer solutions z.

Solution:

If $7y \equiv_{33} 1$, then

$$2 \cdot 7y \equiv_{33} 2$$

So, $z \equiv_{33} 2 \times 19 \equiv_{33} 5$. This means that the set of solutions is $\{5 + 33k \mid k \in \mathbb{Z}\}$.

(c) Prove that the solutions to the equation from (b) are the same as the equation $5z + 1 \equiv_{33} 3 - 2z$, with an English proof. **Solution:**

Let z be arbitrary.

Suppose that z satisfies $7z \equiv_{33} 2$. Adding $-2z + 1$ to both sides gives us $5z + 1 \equiv_{33} 3 - 2z$ and shows that z also satisfies that equation.

Suppose that z satisfies $5z + 1 \equiv_{33} 3 - 2z$. Adding $2z - 1$ to both sides gives us $7z \equiv_{33} 2$ and shows that z also satisfies that equation.

Together, this shows that z satisfies $7 \equiv_{33} 2$ iff it satisfies $5z + 1 \equiv_{33} 3 - 2z$.

Since z was arbitrary, we have proven this is true for all integers.

(d) Show that the equation $22x \equiv_{33} 15$ has no solutions, with an English proof. **Solution:**

Suppose that x is any solution to the equation $22x \equiv_{33} 15$. By definition, we know $15 = 22x + 33k$ for some $k \in \mathbb{Z}$. This can be rewritten as $15 = 11(2x + 3k)$. The right-hand side is a multiple of 11, while the left-hand side is not. Therefore, the two sides cannot be equal for any value of x. This is a contradiction to the earlier assumption that the two sides are equal.

8. Efficient Modular Exponentiation

(a) Compute $2^{71} \mod 25$ using the efficient modular exponentiation algorithm. **Solution:**

$$
\begin{aligned}
2^1 &\equiv_{25} 2 \\
2^2 &\equiv_{25} 4 \\
2^4 &\equiv_{25} 16 \\
2^8 &\equiv_{25} 16^2 \equiv_{25} 6 \\
2^{16} &\equiv_{25} 6^2 \equiv_{25} 11 \\
2^{32} &\equiv_{25} 11^2 \equiv_{25} 21 \\
2^{64} &\equiv_{25} 21^2 \equiv_{25} 16
\end{aligned}
$$

Therefore, since $71 = 64 + 4 + 2 + 1$, we see that

$$
\begin{aligned}
2^{71} &\equiv_{25} 2^{64} \times 2^4 \times 2^2 \times 2^1 \\
&\equiv_{25} 16 \times 16 \times 4 \times 2 \\
&= 16 \times 16 \times 8 \equiv_{25} 16 \times 16 \times 8 \\
&= 16 \times 128 \equiv_{25} 16 \times 3 \\
&= 48 \equiv_{25} 23
\end{aligned}
$$

(b) How many multiplications does the algorithm use for this computation?

Solution:

6 to compute the exponents + 3 for the final result = 9.