Math 135 Algebra
Midterm Solutions

Question 1. (a) [4 marks] Consider the following two statements:

$$\exists x\, \exists y (P(x) \implies Q(y)), \qquad \text{and} \qquad (\forall x\, P(x)) \implies (\exists y\, Q(y))$$

Give an example of a universe of discourse, and meaning for P and Q for which the **first** statement is **true**. Give an example where the **second** statement is **false**.

Solution: There are many possible correct answers to this question. Here's one:

For the positive integers, and $P(x) = Q(x) =$ "$x < 1$", the first statement is true.

For the positive integers, $P(x) =$ "$x \geq 1$", and $Q(y) =$ "$y < 1$", the second statement is false.

(b) [4 marks] Negate the two statements given in part (a) above, and simplify them so that no quantifier or compound statement is negated. Show the steps in the simplification.

Solution: $\neg(\exists x\, \exists y\, (P(x) \implies Q(y)))$ is equivalent to

$$\begin{aligned} &\forall x\, \forall y\, \neg(P(x) \implies Q(y)) \\ &\forall x\, \forall y\, (P(x)) \ \wedge\ \neg Q(y)). \end{aligned}$$

$\neg((\forall x\, P(x)) \implies (\exists y\, Q(y)))$ is equivalent to

$$\begin{aligned} &(\forall x\, P(x)) \ \wedge\ \neg(\exists y\, Q(y)) \\ &(\forall x\, P(x)) \ \wedge\ (\forall y\, \neg Q(y)). \end{aligned}$$

(c) [4 marks] Are the two statements given in part (a) above equivalent? Justify your answer appropriately.

Solution: The two statements are equivalent.

There are several ways of proving this. The easiest is to prove that the negations of the two statements we obtained in part (b) above are equivalent. We prove this below.

Let S_1 be the negation of the first statement, S_2 that of the second. Suppose S_1 is true. Then, for every pair of elements x, y in the universe, $P(x)$ is true and $Q(y)$ is false. This means that $\forall x\, P(x)$ is true, and $\forall y\, (\neg Q(y))$ is also true. This implies that S_2 is true.

Conversely, suppose that S_2 is true. Then, the two statements $\forall x\, P(x)$ and $\forall y\, (\neg Q(y))$ are both true. Thus, for every pair x, y in the universe, $P(x) \ \wedge\ \neg Q(y)$ is true. In other words, S_1 is true.

Question 2. (a) [4 marks] Factorize the two integers 11571 and 9338 into a product of primes, and compute their greatest common divisor. Explain the method you used to factorize the numbers, and show your steps.

Solution: We repeatedly use Theorem 2.55, which states that any composite number $x > 1$ has a prime factor $\leq \sqrt{x}$. We try out division by successive primes $\leq \sqrt{x}$ until we find a divisor, or run out of primes.

Dividing by small primes first, we find that $11571 = 3 \cdot 3857 = 3 \cdot 7 \cdot 551$. Now, $\sqrt{551} = 23.47\ldots$. Dividing 551 by all primes up to 23, we find that $551 = 19 \cdot 29$.

Similarly, $9338 = 2 \cdot 4669 = 2 \cdot 7 \cdot 667$. Now, $\sqrt{667} = 25.82\ldots$. Dividing by primes up to 23 again, we have $667 = 23 \cdot 29$.

So

$$\begin{aligned} 11571 &= 3 \cdot 7 \cdot 19 \cdot 29 \\ 9338 &= 2 \cdot 7 \cdot 23 \cdot 29. \end{aligned}$$

Therefore, by Theorem 2.57, the GCD is $7 \cdot 29 = 203$.

(b) [6 marks] Find all integers x, y such that $\gcd(11571, 9338) = 11571x + 9338y$.

Solution: We have to find the complete integer solution to the equation

$$11571x + 9338y = 203.$$

Dividing throughout by the GCD 203, we get

$$57x + 46y = 1.$$

Following the Extended Euclidean Algorithm, we get

i	s_i	t_i	r_i	q_i
0	1	0	57	
1	0	1	46	1
2	1	-1	11	4
3	-4	5	2	5
4	21	-26	1	2
5	-46	57	0	

Check: $21 \cdot 57 = 1197$, $-26 \cdot 46 = -1196$, and their sum is 1.

A particular solution to the equation is $x_1 = 21, y_1 = -26$. The complete integer solution is therefore $x = 21 + 46n$, $y = -26 - 57n$ for all $n \in \mathbb{Z}$.

Question 3. (a) [6 marks] Prove that $\gcd(a, c) = \gcd(b, c) = 1$ if and only if $\gcd(ab, c) = 1$.

Solution: This problem was assigned in two homeworks. See the solutions for HW3, HW4.

(b) [6 marks] The nickel slot of a pay phone will not accept coins. Can a call costing 95 cents be paid for exactly using only dimes and quarters? If so, in how many ways can it be done?

Solution: We have to solve the Diophantine equation $10x + 25y = 95$ for $x, y \geq 0$, where x represents the number of dimes and y the number of quarters required.

We can run through the obvious values of x from 0 to 9, and see if some $y \geq 0$ satisfies the equation. That would also be a valid solution.

The systematic way of doing this would be the following.

The $\gcd(10, 25) = 5$ and $5|95$, so there is a solution to the equation. Dividing by 5 we obtain the equivalent equation $2x + 5y = 19$. By inspection $2(-2) + 5(1) = 1$. Multiplying by 19 gives $2(-38) + 5(19) = 19$.

Therefore, a particular solution is $x = -38$ and $y = 19$. This tells us that the general solution is

$$\left.\begin{array}{l} x = -38 + 5n \\ y = 19 - 2n \end{array}\right\} \text{ for all } n \in \mathbb{Z}.$$

Since we want a non-negative solution (to pay 95 cents exactly), $x = -38 + 5n \geq 0$ or $n \geq \frac{38}{5}$, or $n \geq 8$ as n is an integer. Similarly, $y = 19 - 2n \geq 0$ which yields $n \leq \frac{19}{2}$ or $n \leq 9$. Therefore, n can take on two values 8 or 9. So the call can be paid in two ways using only dimes and quarters:

$$\begin{array}{lllllllll} \text{for } n & = & 8, & x & = & 2 & \text{and} & y & = & 3 \\ \text{for } n & = & 9, & x & = & 7 & \text{and} & y & = & 1. \end{array}$$

Hence use 2 dimes and 3 quarters, or 7 dimes and 1 quarter.

Question 4. [12 marks] Let $a, b, c \in \mathbb{Z}$. State whether the following statements are true or false, and give a short justification.

(i) If $c = ax + by$ for some $x, y \in \mathbb{Z}$, then $c = \gcd(a, b)$.

Solution: False. Consider $c = 2, a = 3, b = 5, x = -1, y = 1$. GCD of $5, 3$ is 1, not 2.

(ii) Any common divisor of $a, b \in \mathbb{Z}$ divides $\gcd(a, b)$.

Solution: True. There are integers $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$. Any common divisor of a, b also divides the RHS, so also the LHS.

(iii) If $c|(ab)$, then $c|a$ or $c|b$.

Solution: False. Consider $c = 4, a = b = 2$.

(iv) $\gcd(ab, c) = \gcd(a, c) \cdot \gcd(b, c)$ if a and b are prime numbers.

Solution: False. Consider $a = b = c = 2$. $\gcd(ab, c) = 2 \neq 4 = \gcd(a, c) \cdot \gcd(b, c)$.

(v) If a, b are distinct primes, then $ax + by = c$ has an integer solution x, y for every c.

Solution: True. The equation has an integer solution iff $\gcd(a, b)|c$. In this case, $\gcd(a, b) = 1$.

(vi) If $a \equiv b \pmod{c}$ for some $c > 0$, then b is the remainder when a is divided by c.

Solution: False. For example, $1 \equiv 1 \pmod{1}$.

Question 5. (a) [4 marks] Prove that for all $a, b \in \mathbb{Z}$, $\quad \gcd(a, a + b) = \gcd(a, b)$.

Solutions: Let $d = \gcd(a, a + b)$ and $d' = \gcd(a, b)$.

If $a = b = 0$, then $d = d' = 0$. If not both a, b are zero, then $d, d' > 0$.

Since $d|a$, and $d|(a + b)$, $d|(a + b) - a = b$. Therefore, d is a common divisor of a, b, and $d \leq d'$.

Moreover, $d'|a$, $d'|b$, so $d'|(a + b)$. So d' is a common divisor of $a, a + b$, and therefore $d' \leq d$.

Together, $d = d'$.

(b) [4 marks] Recall from the lectures that the Fibonacci sequence is defined as

$$\begin{aligned} f_0 = 0, \quad \text{and} \quad f_1 &= 1 \\ f_n \quad = \quad f_{n-1} + f_{n-2}, &\quad \text{for all } n \geq 2. \end{aligned}$$

Prove that for all $n \geq 0$, $\quad \gcd(f_n, f_{n+1}) = 1$.

Solutions: We will prove this by induction over n.

For the base case $n = 0$, note that $\gcd(0, 1) = 1$.

Assume for some $k \geq 0$, that $\gcd(f_k, f_{k+1}) = 1$.

Then, $\gcd(f_{k+1}, f_{k+2}) = \gcd(f_{k+1}, f_{k+1} + f_k)$ by definition of the Fibonacci sequence. From part (a) above, this GCD is equal to $\gcd(f_{k+1}, f_k)$. By the induction hypothesis, this GCD is 1, so

$$\gcd(f_{k+1}, f_{k+2}) = 1$$

as well. This completes the inductive step, and the proof.

Question 6. (a) [6 marks] Let $n \geq 1$ be an integer. Recall from the lectures that the n-th harmonic number H_n is defined as

$$H_n \quad = \quad 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n-1} + \frac{1}{n}.$$

Using mathematical induction, prove that $H_{2^m} \leq 1 + m$ for all $m \geq 0$. (In H_{2^m}, the subscript 2^m is 2 raised to the power m.)

Solution: For the base case, $m = 0$, we see that $H_{2^m} = H_1 = 1 \leq 1 + 0$ which is true.

For the induction step, assume that $H_{2^k} \leq 1 + k$, for some $k \geq 0$. We will prove that $H_{2^{k+1}} \leq 1 + (k + 1)$.

Now,

$$\begin{aligned} H_{2^{k+1}} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k} + \frac{1}{2^k + 1} + \cdots + \frac{1}{2^{k+1}} \\ &= H_{2^k} + \frac{1}{2^k + 1} + \cdots + \frac{1}{2^{k+1}} \\ &\leq H_{2^k} + 2^k \cdot \frac{1}{2^k} \quad = \quad H_{2^k} + 1, \end{aligned}$$

since each of the last 2^k terms is at most $1/2^k$. Moreover, from the induction hypothesis, $H_{2^k} \leq 1+k$. Combining these, we get $H_{2^{k+1}} \leq (1 + k) + 1$.

(b) [4 marks] Define the notation $a \equiv b \pmod{m}$.

Solution: Let $a, b, m \in \mathbb{Z}$, and $m > 0$. Then, a is congruent to b modulo m ($a \equiv b \pmod{m}$) iff $m|(a - b)$.

Question 7. (a) [4 marks] For each of the 16 integers $x \in X = \{0, 1, 2, 3, \ldots, 15\}$, find the smallest **positive** integer y such that $x^2 \equiv y \pmod{16}$.

Solution: Note that $a^2 \equiv (-a)^2 \equiv (16-a)^2 \pmod{16}$. Therefore, we need only find the numbers y for x up to 8. Dividing the squares by 16 we get the remainder, which is the smallest positive integer congruent to the square unless it is 0. If the remainder is 0, the smallest positive number congruent to the square would be 16 itself.

x	0	1	2	3	4	5	6	7	8
x^2	16	1	4	9	16	9	4	1	16

(b) [4 marks] Using the properties of congruences, find the smallest **positive** integer congruent to 10^{45} modulo 7. Show the steps in your calculations.

Solution:

$$\begin{aligned} 10^{45} &\equiv 3^{45} \\ &\equiv (3^3)^{15} = 27^{15} \\ &\equiv (-1)^{15} = -1 \\ &\equiv 6 \pmod 7. \end{aligned}$$

No number less than 6 is congruent to it modulo 7, so 6 is our solution.