MT231 - Finite Maths

Homework #2

Angel Cervera Roldan
21319203

Problem 1

Prove Euclid's lemma

Euclid's lemma states that if a prime p divides ab, then it must divide a, b or both.
We can prove this by contradiction by writing a and b as their prime factors. $a = p_{a_1}p_{a_2}...$ and $b = p_{b_1}p_{b_2}....$
Because $p|ab$, $p|(p_{a_1}p_{a_2}...)(p_{b_1}p_{b_2}...)$
If we assume that $p \nmid a$ and $p \nmid b$, then that means that $p \nmid (p_{a_1}p_{a_2}...)$ and $p \nmid (p_{b_1}p_{b_2}...)$.
Therefore $p \neq p_{a_i}$ for any i and $p \neq p_{b_i}$ for any i.
But p divides $(p_{a_1}p_{a_2}...)(p_{b_1}p_{b_2}...)$, this means that $(p_{a_1}p_{a_2}...)(p_{b_1}p_{b_2}...) = np$ for some natural number n. Because p isn't a part of a's or b's prime decomposition, then it means that there are a two numbers, neither of which are p, which when multiplied together give you p. This is a contradiction, since there are no two numbers (neither of which are 1 or p) that when multiplied give you p.
Therefore, if $p|ab$, then either a or b or both contain p in their prime decomposition, which means that p divides a or b or both.

Problem 2

Problem 3

Use Euclid's algorithm to find the greatest common factor of the two given integers a and b. Furthermore, express $gcd(a, b)$ as a linear combination of a and b for the following

1. a = 1841, b = -392
2. a = 23427, b = 26049
3. a = -1931, b = 4722

1) a = 1841, b = -392

Note: $gcd(a, b) = gcd(b, a) = gcd(|a|, |b|)$ (Remark 4.01)

i	q_i	r_i	x_i	y_i
-1		1841	1	0
0	4	392	0	1
1	1	273	1	-4
2	2	119	-1	5
3	3	35	3	-14
4	2	14	-10	47
5	2	7	23	-108
6		0		

Therefore, $gcd(1841, 392) = 7$, and $(1841)(23) + (392)(-108) = 7$

Problem 4

Determine all positive integer solutions for the following linear equations

1. 172x + 20y = 1000
2. 123x + 360y = 91
3. 158x - 57y = 7

1) 172x + 20y = 1000

First we check if any solutions exist. To do this we find the $gcd(172, 20)$, using the same algorithm as in last part, we get $gcd(123, 360) = 4$.
$1000 = 4 \cdot (250)$, therefore the exist solutions.

$$1000 = 172x + 20y$$
$$250 = 43x + 5y$$

Because 250 is divisible by 5, $43x + 5y$ must be divisible by 5, therefore $5y$ is divisible by 5, which is true for ant integer, and $43x$ is divisible by 5. Because 5 is prime, we have, by euclid's lemma that 43 divides 5 or that x divides 5. We know that 43 does not divide 5, therefore x must divide 5. We can now rewrite x as $5n$, $n \in \mathbb{N}$.

$$250 = 43x + 5y$$
$$250 = 43(5n) + 5y$$
$$50 = 43n + y$$
$$y = 50 - 43n$$

Now that we have both x and y in terms of n, we can re write the original equation as:

$$1000 = 172(5n) + 20(50 - 43n)$$

Because we are only interested in positive integer solutions, $50 - 43n > 0$ $\frac{50}{43} > n$. Because we are interested in positive integers, $5n > 0$, therefore $n > 0$
From the above two inequalities, we get that n must be 1, therefore there exists only one solution where x and y are positive integers (non-zero):

$$1000 = 172(5) + 20(7)$$

Problem 4 continued on next page. . .

2) $123x + 360y = 91$

First we check if any solutions exist. To do this we find the $gcd(123, 360)$, using the same algorithm as in last part, we get $gcd(123, 360) = 3$.
However, 91 is not a multiple of 3, meaning that there exist no integer values for x, y such that the equation holds.

Problem 5

A farmer bought 100 livestock for a total cost of 4000 Euro. Calves cost 120 Euro each, Lambs 50 each and Piglets 25 Euro each. If the farmer obtained an even number of animals of each type, how many did he buy?

From the information above, we can form two equations:

$$\begin{aligned} 4000 &= 120x + 50y + 25z \\ 100 &= x + y + z \end{aligned}$$

Where $x, y, z \in \mathbb{N}_0$. x being the number of calves purchased, y being the number of lambs purchased, and z being the number of piglets purchased. We aso know that x, y, z are all even numbers.
First we must verify if the above equations can be satisfied with integer solutions.
The first equation above has solutions since the gcd of 120, 50, and 25 is just 5, and $5|4000$ The second one also has solutions since the gcd of 1, 1, and 1, is just one, and $1|100$

$$n \coloneqq 2y + z$$

We can now rewrite the first equation above:

$$\begin{aligned} 4000 &= 120x + 25(2y + z) \\ 4000 &= 120x + 25n \\ 800 &= 24x + 5n \end{aligned}$$

Because 800 is divisible by 5, $24x + 5n$ must be divisible by 5. Therefore $5|24x \implies 5|x$. Let $x = 5p$

$$\begin{aligned} 800 &= 24(5p) + 5n \\ 160 &= 24p + n \\ n &= 160 - 24p \end{aligned}$$

Now we have $\forall p \in \mathbb{N},\ 4000 = 120(5p) + 25(160 - 24p)$
Now we need to put $25(160 - 24p)$ back into the form $50y + 25z$, to do this, we will use the following two equations:

$$\begin{aligned} 100 &= x + y + z \\ &= 5p + y + z \\ 2y + z &= 160 - 24p \end{aligned}$$

$$\begin{aligned}
100 &= 5p + y + z \\
\Rightarrow y &= 100 - 5p - z \\
2y + z &= 160 - 24p \\
2(100 - 5p - z) + z &= 160 - 24p \\
200 - 10p - z &= 160 - 24p \\
-z - -40 - 14p \\
z &= 40 + 14p
\end{aligned}$$

Now that we know z in terms of p, we know that:

$$\begin{aligned}
y &= 100 - 5p - z \\
&= 100 - 5p - 40 - 14p \\
&= 60 - 19p
\end{aligned}$$

Now we have x, y, z in terms of p:

$$\begin{aligned}
x &= 5p \\
y &= 60 - 19p \\
z &= 40 + 14p
\end{aligned}$$

Therefore:

$$\forall p \in \mathbb{N}_0 : \ 4000 = 120(5p) + 50(60 - 19p) + 25(40 + 14p)$$

Note that because the farmer only bought pair numbers of animals, $2|5p$, and $p|60 - 19p$, therefore $2|p$. $40 + 14p$ will always be even.
Also, he cant buy a negative number of animals, so $60 - 19p \geq 0$, which holds for any $p \leq 3$.
Because $p|2$, then $p \in \{0, 2\}$
So the answer is:
- He bought 10 calves, 22 lambs, and 68 piglets.
- He bought 0 calves, 60 lambs, and 40 piglets.

Problem 6

1

> Alcuin of York (775 ad): A hundred bushels of grain are distributed among 100 persons in such a way that each man receives 3 bushels, each woman 2 bushels, and each child 1 2 a bushel. How many men, women and children are there?

Let m be the number of men, w be the number of women, and c the number of children. From the above information, we can form two equations

$$\begin{aligned} 100 &= m + w + c \\ 100 &= 3m + 2w + \frac{1}{2}c \end{aligned}$$

We can rewrite the first of the two equations above to get c in terms of m and w.

$$\begin{aligned} 100 &= m + w + c \\ c &= 100 - m - w \end{aligned}$$

$$\begin{aligned} 100 &= 3m + 2w + \frac{1}{2}(100 - m - w) \\ 200 &= 6m + 4w + 100 - m - w \\ 100 &= 5m + 3w \end{aligned}$$

Because 100 is divisible by 5, then $5m + 3w$ must be divisible by 5. This implies that $5m$ is divisible by 5, this is true for any m. It also implies that $3w$ is divisible by 5, because 5 and 3 are both primes, w must be divisible by 5. Let $5p = w$

$$\begin{aligned} 100 &= 5m + 3(5p) \\ 20 &= m + 3p \\ m &= 20 - 3p \end{aligned}$$

Now we have both m and n in terms of p, we can also find c in terms of p by subbing the values of m and n as follows

$$
\begin{aligned}
c &= 100 - m - w \\
c &= 100 - (20 - 3p) - (5p) \\
c &= 100 - 20 + 3p - 5p \\
c &= 80 - 2p
\end{aligned}
$$

We can prove that the two initial equations hold for any value of p

$$
\begin{aligned}
100 &= m + w + c \\
100 &= (20 - 3p) + (5p) + (80 - 2p) \\
100 &= 20 - 3p + 5p + 80 - 2p \\
100 &= 100
\end{aligned}
$$

$$
\begin{aligned}
100 &= 3m + 2w + \frac{1}{2}c \\
100 &= 3(20 - 3p) + 2(5p) + \frac{1}{2}(80 - 2p) \\
100 &= 60 - 9p + 10p + 40 - p \\
100 &= 100
\end{aligned}
$$

However we cannot have a negative amount of people, therefore, $20 - 3p > 0$, $p \leq 6$
Now we can get the all the solutions:

$$
\begin{aligned}
100 &= 3(20 - 3p) + 2(5p) + \frac{1}{2}(80 - 2p) \\
100 &= 3(17) + 2(5) + \frac{1}{2}(78) \\
100 &= 3(14) + 2(10) + \frac{1}{2}(76) \\
100 &= 3(11) + 2(15) + \frac{1}{2}(74) \\
100 &= 3(8) + 2(20) + \frac{1}{2}(72) \\
100 &= 3(5) + 2(25) + \frac{1}{2}(70) \\
100 &= 3(2) + 2(30) + \frac{1}{2}(68)
\end{aligned}
$$

So one answer to the question would be 8 men, 20 women, and 72 children.

Problem 7

Find an example for integers a, b, c and an integer $n \geq 1$ such that $ac \equiv bc \pmod{n}$, but $a \not\equiv b \pmod{n}$

$$(3)6 \equiv (4)6 \pmod{2}$$
$$3 \not\equiv 4 \pmod{2}$$

$$a = 3$$
$$b = 4$$
$$c = 6$$
$$n = 2$$

Problem 8

Let $a, b, c, d \in \mathbb{Z}$ with $n \geq 0$. Suppose $a \equiv b \pmod{n}$, and $c \equiv d \bmod n$.

1

$$ac \equiv bd \bmod n$$

a divided by n, and b divided by n both have the same remainder, call that remainder r.
c divided by n, and d divided by n both have the same remainder, call that remainder s.
This means that a can be written as $a = nk_a + r$ for some $k_a \in \mathbb{N}_0$, and b can be written as $b = nk_b + r$ for some $k_b \in \mathbb{N}$, also similarly, $c = nk_c + s$, and $d = nk_d + s$, where $k_c, k_d \in \mathbb{N}$

$$\begin{aligned} ac &= (nk_a + r)(nk_c + s) = n(nk_ak_c + k_as + k_cr) + sr \\ &= nk_{ac} + sr \\ bd &= (nk_b + r)(nk_d + s) = n(nk_bk_b + k_bs + k_dr) + sr \\ &= nk_{bd} + sr \end{aligned}$$

Where $k_{ac} = nk_ak_c + k_as + k_cr$, and $k_{bd} = nk_bk_b + k_bs + k_dr$.
We know, from lemma 6.3 that $a \equiv b \pmod{n}$ if and only if $n|(a - b)$

$$ac - bd = nk_{ac} + sr - nk_{bd} - sr = n(k_{ac} + k_{bd})$$

Therefore, $n|(ac - bd)$, so $ac \equiv bd \pmod{n}$

2

$$a^k \equiv b^k \bmod n,\ k \in \mathbb{N}$$

From the previous part, we know that if $a \equiv b \bmod n$, and $c \equiv d \bmod n$, then $ac \equiv bd \bmod n$.
Using this fact, we can prove this question using induction.
$a^0 = b^0 = 1$ therefore, $a^0 \equiv b^0 \bmod n$ holds. We can also see that it holds for $k = 1$, as $a^1 \equiv b^1 \bmod n$ hold (per question description).
Now we assume that it hold for some k, and show that if thats the case, then it should hold for $k + 1$.

$$\begin{aligned} a^{k+1} &\equiv b^{k+1} \pmod{n} \\ a^k \cdot a &\equiv b^k \cdot b \pmod{n} \end{aligned}$$

By assumption, we know that $a^k \equiv b^k \pmod{n}$ holds, we also know that $a \equiv b \pmod{n}$ holds.

Problem 8 continued on next page. . .

From the rule proved in part one this question, that indicates that $a^k \cdot a \equiv b^k \cdot b \pmod{n}$ also holds.
This means that $a^{k+1} \equiv b^{k+1} \pmod{n}$ holds.
Therefore, for any integer k greater or equal to 0, $a^k \equiv b^k \bmod n$