MAT 512 Exam 1 Solutions

1. Use the Euclidean algorithm to compute the greatest common divisor of 576 and 258. Then find two integers s and t with the property that $(576, 258) = 576s + 258t$. Write your solution in such a way that one can easily follow all the steps in the calculation.

Solution: The Euclidean algorithm is repeated division with remainder:

$$\begin{aligned} 576 &= 2 \cdot 258 + 60 \\ 258 &= 4 \cdot 60 + 18 \\ 60 &= 3 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 \end{aligned}$$

Since the greatest common divisor remains the same in each step, we get

$$(576, 258) = (258, 60) = (60, 18) = (18, 6) = 6.$$

We can use the above equations in reverse to write the greatest common divisor as a linear combination of 576 and 258:

$$\begin{aligned} 6 &= 60 - 3 \cdot 18 \\ &= 60 - 3 \cdot (258 - 4 \cdot 60) = 13 \cdot 60 - 3 \cdot 258 \\ &= 13 \cdot (576 - 2 \cdot 258) - 3 \cdot 258 = 13 \cdot 576 - 29 \cdot 258 \end{aligned}$$

So we can take $s = 13$ and $t = -29$.

2. Suppose we want to find an integer x that solves the congruence $ax \equiv b \mod m$. Here a and b are two integers, and $m \geq 2$ is the modulus of the congruence. Explain why b must be divisible by (a, m) in order for the congruence to have a solution.

Solution: Suppose that we have an integer x that solves the congruence. This means that $ax - b$ is divisible by m, and so we have $ax - b = ym$ for some integer y. We can rearrange the terms to get $b = ax - ym$. Now the greatest common divisor (a, m) divides both a and m, and because $b = ax - ym$, it also divides b. So if the congruence has a solution, then b must be a multiple of (a, m).

3. Continuing from the previous question, suppose now that b is indeed divisible by (a, m). Prove that, in that case, the congruence always has an integer solution x. Write your answer clearly and in complete sentences.

Solution: We know from Bézout's theorem that (a, m) can be written as a linear combination of a and m. This means that there are two integers s and t such that $(a, m) = as + tm$. By hypothesis, b is divisible by (a, m), and so we have $b = n(a, m)$ for some integer n. Putting both things together, we get

$$b = n(a, m) = n(as + tm) = ans + tnm.$$

Modulo m, this becomes the congruence

$$b \equiv ans \mod m,$$

and so $x = ns$ is an integer solution.

4. We know that every positive integer has a unique prime factorization. Write down a precise mathematical statement of this fact. Explain clearly what it means to say that the prime factorization is "unique".

Solution: Every integer $a \geq 2$ can be uniquely written as a product $a = p_1 p_2 \cdots p_n$, where $p_1, \ldots, p_n$ are prime numbers and $p_1 \leq p_2 \leq \cdots \leq p_n$. Uniqueness means that there is only one way of writing a as a product of prime numbers, as long as we put the prime numbers in the factorization in increasing order.

Another way to say that the prime factorization is unique is the following. Suppose that we have two prime factorizations $a = p_1 \cdots p_n$ and $a = q_1 \cdots q_k$, where $p_1 \leq \cdots \leq p_n$ and $q_1 \leq \cdots \leq q_k$. Then the number of factors is the same ($n = k$) and all the prime numbers in the two factorizations are the same ($p_i = q_i$ for $i = 1, \ldots, n$).