MAT 421 Number Theory
Takehome Exam 1

Note: Read the test instructions in my email carefully and thoroughly before you begin your exam. Failure to follow the instructions could result in point reductions or no point on individual problems.

1. Find $(165, 465)$ using the Euclidean algorithm. Then solve the equation
$$165x + 465y = (165, 465)$$
by going backward of the Euclidean algorithm from bottom to top.

Solution.

$$\begin{aligned} 465 &= 165 \cdot 2 + 135 \\ 165 &= 135 \cdot 1 + 30 \\ 135 &= 30 \cdot 4 + 15 \\ 30 &= 15 \cdot 2 + 0 \end{aligned}$$

Thus we have $(165, 465) = 15$. Now,

$$\begin{aligned} 15 &= 135 - 30 \cdot 4 \\ &= 135 - (165 - 135 \cdot 1)4 \\ &= 5 \cdot 135 - 4 \cdot 165 \\ &= 5(465 - 165 \cdot 2) - 4 \cdot 165 \\ &= 5 \cdot 465 - 14 \cdot 165 \end{aligned}$$

Since we have $165(-14) + 465(5) = 15$, $x = -14$ and $y = 5$ is a solution.

2. Prove: Given integers a, b, and c with a and b not both 0, there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $(a, b)|c$.

   Solution. Suppose that there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$. Since $(a, b)|a$ and $(a, b)|b$, $(a, b)|c$. Conversley, suppose that $(a, b)|c$. By Bezout's lemma, there exist $x', y' \in \mathbb{Z}$ such that $ax' + by' = (a, b)$. Since $(a, b)|c$, $c = (a, b)k$ for some $k \in \mathbb{Z}$. Let $x = x'k$ and $y = y'k$. Then we have $ax + by = c$.

3. Use the Euclidean algorithm to find one solution to $66x+51y = 300$.

   Solution. First, we find $(66, 51)$ using the Euclidean algorithm.

$$\begin{aligned} 66 &= 51 \cdot 1 + 15 \\ 51 &= 15 \cdot 3 + 6 \\ 15 &= 6 \cdot 2 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

   Thus, we have $(66, 51) = 3$. Next, we solve the equation $66x + 51y = 3$ by going backward of the above Euclidean algorithm from bottom to top.

$$\begin{aligned} 3 &= 15 - 6 \cdot 2 \\ &= 15 - (52 - 15 \cdot 3)2 \\ &= 15 \cdot 7 - 51 \cdot 2 \\ &= (66 - 51 \cdot 1)7 - 51 \cdot 2 \\ &= 66 \cdot 7 + 51(-9) \end{aligned}$$

   This means that $x' = 7$ and $y' = -9$ is a solution and hence, $x = 100x' = 700$ and $y = 100y' = -900$ is a solution of $66x + 51y = 300$.

4. Describe all solutions of $3x \equiv 4 \mod 7$.

   Solution. $(3, 7) = 1$ so there is a solution. First, we solve $3x + 7y = 1$. $3(-2) + 7 \cdot 1 = 1$, so $x_0 = -2 \cdot 4 = -8$ and $y_0 = 1 \cdot 4 = 4$ is a solution of $3x + 7y = 4$. Hence, all solutions are

$$\begin{aligned} x &= x_0 + \frac{b}{d}t = -8 + 7t \\ y &= y_0 - \frac{a}{d}t = 4 - 3t \end{aligned}$$

for all $t \in \mathbb{Z}$. That is, $x \equiv -8 \mod 7 \equiv 6 \mod 7$.

Solution 2. Since $(3,7) = 1$, there exists $3^{-1} \in \mathbb{Z}/7\mathbb{Z}$. In fact, $3 \cdot 5 = 15 \equiv 1 \mod 7$, so $5 = 3^{-1}$. Multiplying the equation by 5, we obtain

$$x \equiv 20 \mod 7 \equiv 6 \mod 7$$

or $x = 6 + 7n$ for all $n \in \mathbb{Z}$.

5. Find the smallest nonnegative solution of the system of congruences:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 4 \mod 11 \\ x &\equiv 5 \mod 16 \end{aligned}$$

Solution. $M = \prod_{i=1}^{4} m_i = 3 \cdot 5 \cdot 11 \cdot 16 = 2640$.

$$\begin{aligned} M_1 &= \frac{M}{m_1} = 5 \cdot 11 \cdot 16 = 880 \\ M_2 &= \frac{M}{m_2} = 3 \cdot 11 \cdot 16 = 528 \\ M_3 &= \frac{M}{m_3} = 3 \cdot 5 \cdot 16 = 240 \\ M_4 &= \frac{M}{m_4} = 3 \cdot 5 \cdot 11 = 165 \end{aligned}$$

Since $(M_1, m_1) = (880, 3) = 1$, $M_1 y + m_1 z = 528y + 5z = 1$ has a solution. Since $880 \cdot 1 + 3 \cdot (-27) = 1$, $N_1 = y = 1$. Likewise since $(M_2, m_2) = (528, 5) = 1$, $M_2 y + m_2 z = 528y + 5z = 1$ has a solution. By the Euclidean algorithm, we have

$$\begin{aligned} 528 &= 5 \cdot 105 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

Going backward of the above Euclidean algorithm from bottom to top, we obtain

$$
\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (5 - 3 \cdot 1) \cdot 1 \\
&= 3 \cdot 2 - 5 \\
&= (528 - 5 \cdot 105) \cdot 2 - 5 \\
&= 528 \cdot 2 - 5 \cdot 211
\end{aligned}
$$

This means that $N_2 = y = 2$. Similarly, we obtain $N_3 = 5$ and $N_4 = -3$. A solution of the system of the congruences is then given by

$$
\begin{aligned}
x &= \sum_{i=1}^{4} a_i M_i N_i \\
&= 2 \cdot 880 \cdot 1 + 3 \cdot 528 \cdot 2 + 4 \cdot 240 \cdot 5 + 5 \cdot 165 \cdot (-3) \\
&= 7253
\end{aligned}
$$

But this is not the smallest positive solution. $7253 \equiv 1973 \mod M = 2640$, so 1973 is the smallest positive solution.