MAT 421 Number Theory
Takehome Final Exam

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 $(217, 341)$ using the Euclidean algorithm. Then solve the equation
$$217x + 341y = (217, 341)$$
by going backward of the Euclidean algorithm from bottom to top.

   Solution. Using the Euclidean algorithm, we have
$$\begin{aligned} 341 &= 217 \cdot 1 + 124 \\ 217 &= 124 \cdot 1 + 93 \\ 124 &= 93 \cdot 1 + 31 \\ 93 &= 31 \cdot 3 + 0 \end{aligned}$$
   Thus, we find $(217, 341) = 31$. Now,
$$\begin{aligned} 31 &= 124 - 93 \cdot 1 \\ &= 124 - (217 - 124) \\ &= 2 \cdot 124 - 217 \\ &= 2(341 - 217) - 217 \\ &= 2 \cdot 341 - 3 \cdot 217 \end{aligned}$$
   Since $217(-3) + 341(2) = 31$, $x = -3$ and $y = 2$ is a solution.

2. Find all solutions of $6x + 8y = 120$ with x and y positive.

Solution. $8 = 6\cdot 1+2$, so $(6,8) = 2$. Since $6(-1)+8(1) = 2$, $x' = -1$ and $y' = 1$ is a soluiton to $6x+8y = 2$ and so $x_0 = -60$ and $y_0 = 60$ is a solution to $6x + 8y = 120$. Hence, all other solutions are given by $x = -60 + 4t$ and $y = 60 - 3t$, $-\infty < t < \infty$. Imposing the conditions $x > 0$ and $y > 0$ results in $16 \leq t \leq 19$.

3. Find the smallest nonnegative solution of the system of congruences

$$\begin{aligned} 19x &\equiv 103 \mod 900 \\ 10x &\equiv 511 \mod 841 \end{aligned}$$

Solution. $(19,900) = 1$, so there exists $19^{-1} \in \mathbb{Z}/900\mathbb{Z}$ and $19^{-1} \equiv 379 \mod 900$. Since $(10,841) = 1$, there exists $10^{-1} \in \mathbb{Z}/841\mathbb{Z}$ and $10^{-1} \equiv 757 \mod 841$. Thus, each congruence equation can be solved for x as:

$$\begin{aligned} x &\equiv 379 \cdot 103 \mod 900 \\ &\equiv 337 \mod 900 \\ x &\equiv 757 \cdot 511 \mod 841 \\ &\equiv 808 \mod 841 \end{aligned}$$

We solve this system of congruence equations using Chinese remainder theorem.

$$\begin{aligned} M_1 &= \frac{M}{m_1} = 841 \\ M_2 &= \frac{M}{m_2} = 900 \end{aligned}$$

Using the Euclidean algorithm, we find a solution to $841y + 900z = 1$:

$$y = N_1 = 61,\ z = N_2 = -57$$

Now,

$$\begin{aligned} x &= a_1 M_1 N_1 + a_2 M_2 N_2 \\ &= -24161963 \\ &\equiv 58837 \mod M = 900 \cdot 841 = 756900 \end{aligned}$$

4. Use the repeated squaring method to find $38^{75} \mod 103$.

   Solution.

$$\begin{aligned} 57 &= (1001011)_2 \\ &= 1\cdot 2^6 + 0\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 \\ &= 64 + 8 + 2 + 1 \end{aligned}$$

k	$38^k \mod 103$
1	38
2	$38^2 = 1441 \equiv 2 \mod 103$
4	$2^2 = 4$
8	$4^2 = 16$
16	$16^2 = 256 \equiv 50 \mod 103$
32	$50^2 = 2500 \equiv 28 \mod 103$
64	$28^2 = 784 \equiv 63 \mod 103$

   Hence,

$$\begin{aligned} 38^{75} &= 38^{64+8+2+1} \\ &= 38^{64}\cdot 38^8 \cdot 38^2 \cdot 38 \\ &\equiv 63\cdot 16\cdot 2\cdot 38 \mod 103 \\ &\equiv 79 \mod 103 \end{aligned}$$

5. Use the Lucas-Lehmer test to determine if $M_{13} = 2^{13} - 1$ is a prime.

   Solution.

$$\begin{aligned} S_4 &= 194^2 - 2 \equiv 4870 \mod 2^{13} - 1 = 8191 \\ S_5 &= 4870^2 - 2 \equiv 3953 \mod 8191 \\ S_6 &= 3953^2 - 2 \equiv 5970 \mod 8191 \\ S_7 &= 5970^2 - 2 \equiv 1857 \mod 8191 \\ S_8 &= 1857^2 - 2 \equiv 36 \mod 8191 \\ S_9 &= 36^2 - 2 = 1294 \\ S_{10} &= 1294^2 - 2 \equiv 3470 \mod 8191 \\ S_{11} &= 3470^2 - 2 \equiv 128 \mod 8191 \\ S_{12} &= 128^2 - 2 \equiv 0 \mod 8191 \end{aligned}$$

   Therefore, by Lucas-Lehmer test, $M_{13} = 2^{13} - 1$ is a prime.