Lecture 11

Welcome to the last week in number theory. This week we will use the Chinese Remainder theorem to solve a practical problem, namely finding exact solutions to systems of equations with rational coefficients.

First I'd like to say a few words about simplifying the computations in the Chinese Remainder Theorem. Last week you used the fact that the Euclidean Algorithm constructs a c_i so that $c_iM_i \equiv 1 \mod m_i$, and hence $a_iM_i \equiv 0 \mod m_j$ for $j \neq i$. This is great for proofs but not so great for computation. Remember that you are working mod m_i. So you can first take $M_i \mod m_i$ and possibly guess the c_i and check it. For example, solve
$x \equiv 4 \mod 5$
$x \equiv 6 \mod 8$
$x \equiv 5 \mod 9$.
Then $M_1 = 72,\ M_2 = 45,\ M_3 = 40$. So we need to find c_i such that $72c_1 \equiv 1 \mod 5$. But $72 \equiv 2 \mod 5$ and $2 \times 3 \equiv 1 \mod 5$, so we can take $c_1 = 3$. Similarly, $45 \equiv 5 \mod 8$ and $5^2 \equiv 1 \mod 8$, so we can take $c_2 = 5$. Lastly, $40 \equiv 4 \mod 9$ and $28 \equiv 1 \mod 9$ so we can take $c_3 = 7$ or even easier $c_3 = -2$. Now we put them together and $4(3)(72) + 6(5)(45) + 5(-2)(40) = 864 + 1350 - 400 = 1814 \equiv 14 \mod 360$. A quick check shows that 14 is indeed a correct answer. You will get plenty of practice in the exercises and problems. If you run into trouble, please email me.