MA 630 - Homework 6 (Module 3 - Section 2)

Solutions must be typeset in LaTeX and submitted to Canvas as a .pdf file. When applicable, write in complete sentences. Use only results which have been discussed in our class.

1. Use the Chinese remainder theorem to solve the system of linear congruences

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}.$$

Express your answer as a congruence class.

Solution: In the expression

$$x_0 = a_1 y_1 N_1 + a_2 y_2 N_2 + a_3 y_3 N_3$$

we have

$$\begin{aligned} a_1 &= 2 \\ a_2 &= 3 \\ a_3 &= 4. \end{aligned}$$

Next we compute y_1 as the multiplicative inverse of $5 \cdot 7 = 35 \mod 3$, which is the same as $2 \mod 3$. Normally we would use the Extended Euclidean Algorithm to find y_1 but here it is immediately obvious that this is 2. This is because $2 \cdot 2 = 4 \equiv 1 \mod 3$.

Next to find y_2 we find the multiplicative inverse of $3 \cdot 7 = 21 \mod 5$. This time it's even more trivial since already $21 \equiv 1 \mod 5$, so already we have $y_2 = 1$. Next we find y_3 as the inverse of $15 \mod 7$. Again since this is the same as $1 \mod 7$ then $y_3 = 1$.

Next we find that

$$\begin{aligned} N_1 &= 5 \cdot 7 = 35 \\ N_2 &= 3 \cdot 7 = 21 \\ N_3 &= 3 \cdot 5 = 15. \end{aligned}$$

We are now able to compute

$$\begin{aligned} x_0 &= 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 4 \cdot 1 \cdot 15 \\ &= 263. \end{aligned}$$

The solution is then the congruence class of $[263] \bmod N = 105$.

2. (a) Suppose $x, y, z \in \mathbb{Z}$, and that x and y are relatively prime. Prove that if x divides z and y divides z, then xy divides z.
Proof: Since $gcd(x, y) = 1$ then there exist integers m, n such that

$$mx + ny = 1.$$

We let $z = ax$ and $z = by$. Then we have

$$\begin{aligned} zmx + zny &= z \\ bymx + axny &= z \\ xy(bm + an) &= z \end{aligned}$$

Since $bm + an \in \mathbb{Z}$ we have that $xy|z$. □

(b) Let $m, n \in \mathbb{N}$, and suppose that m and n are relatively prime. Prove that if $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{mn}$.
Proof: By definition we have that m and n each divide $a - b$. From the above theorem, since $gcd(m, n) = 1$, we have that $mn|a-b$. By definition then $a \equiv b \pmod{mn}$. □

3. Let $n \in \mathbb{N}$, and let $a, b, c, d \in \mathbb{Z}$. Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

   Proof: We have that $a - b = nk_1$ for some integer, k_1. Likewise for some integer k_2 we have $c - d = nk_2$. Therefore

$$\begin{aligned} ac &= (nk_1 + b)(nk_2 + d) \\ &= n^2 k_1 k_2 + nk_1 d + nk_2 b + bd. \end{aligned}$$

   From this we can infer that $ac - bd = n(nk_1k_2 + k_1d + k_2b)$. Therefore $ac - bd | n$ and so $ac \equiv bd \pmod{n}$. □

4. Let $a, m \in \mathbb{Z}$.

   (a) Prove that $a^2 \equiv 0 \pmod{4}$ or $a^2 \equiv 1 \pmod{4}$.

   Proof: The proof is by cases: Either a is even or a is odd.

   Case 1: If a is even and $a = 2k$ then $(2k)^2 = 4k^2$ and hence $a^2 - 0 | 4$. This means that $a^2 \equiv 0 \pmod{4}$.

   Case 2: If a is odd and $a = 2k + 1$ then $(2k + 1)^2 = 4k^2 + 4k + 1$ and hence $a^2 - 1 = 4(k^2 + k)$. This means that $a^2 \equiv 1 \pmod{4}$.

   Since in either case, we have either $a^2 \equiv 0 \pmod{4}$ or $a^2 \equiv 1 \pmod{4}$, then this holds for all integers a.

   (b) Prove that if $m \equiv 3 \pmod{4}$, then m is not equal to the sum of two squares of integers.

   Proof: We prove the converse, so suppose that a, b are integers such that $m = a^2 + b^2$. From the above we know that each are equivalent to 0 or 1 mod 4. We can express this by saying that there are numbers x, y such that each are either 0 or 1, and $a^2 - x = 4k_1$ and $b^2 - y = 4k_2$, for some integers k_1, k_2.

   Now $a^2 + b^2 = 4(k_1 + k_2) + x + y$ and $x + y < 3$. Hence $m \not\equiv 3 \pmod{4}$.

5. Let n be an odd integer. Prove that $n^2 \equiv 1 \pmod{8}$. *Hint: First, use the division algorithm to prove that n can be written in the form $8k + 1$, $8k + 3$, $8k + 5$, or $8k + 7$ for some $k \in \mathbb{Z}$.*

   Proof: By the division algorithm we have that n can be written as $8k + r$ for some integer k and integer $0 \leq r < 8$. We also know that r cannot be even,

for if $r = 2m$ then $n = 8k + 2m = 2(4k + m)$. This would contradict the assumption that n is odd. Hence n can be written as $8k + r$ where r is an odd number $1 \leq r \leq 7$.

Now we consider the square of n in each of these four cases.

Case 1: If $n = 8k + 1$ then

$$\begin{aligned} n^2 - 1 &= 64k^2 + 16k + 1 - 1 \\ &= 8(8k^2 + 2k) \end{aligned}$$

and so $n^2 \equiv 1 \pmod 8$.

Case 2: If $n = 8k + 3$ then

$$\begin{aligned} n^2 - 1 &= 64k^2 + 48k + 9 - 1 \\ &= 8(8k^2 + 6k + 1) \end{aligned}$$

and so $n^2 \equiv 1 \pmod 8$.

Case 3: If $n = 8k + 5$ then

$$\begin{aligned} n^2 - 1 &= 64k^2 + 80k + 25 - 1 \\ &= 8(8k^2 + 10k + 3) \end{aligned}$$

and so $n^2 \equiv 1 \pmod 8$.

Case 4: If $n = 8k + 7$ then

$$\begin{aligned} n^2 - 1 &= 64k^2 + 112k + 49 - 1 \\ &= 8(8k^2 + 14k + 6) \end{aligned}$$

and so $n^2 \equiv 1 \pmod 8$.