Spring 2021, Math 522: Problem Set 5
Due: Thursday, March 4th, 2021
The Chinese Remainder Theorem

(D1) *Solving modular systems.*

(a) Determine which elements of $\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$, and $\mathbb{Z}_{12}$ have a multiplicative inverse. For each, find their inverse.

(b) Compare the full solution set of $7x \equiv 7 \bmod 14$ to the full solution set of $x \equiv 1 \bmod 14$. What lessons/cautions can we learn from this?

(c) Find a complete set of solutions to each of the following systems.

(i) $9x \equiv 5 \bmod 11$

(ii) $9x + 7 \equiv 2 \bmod 12$

(iii) $9x + 7 \equiv 1 \bmod 12$

(iv) $2x \equiv 6 \bmod 12, \qquad 3x \equiv 6 \bmod 12$

(v) $3x \equiv 15 \bmod 30, \qquad 5x \equiv 15 \bmod 30$

(vi) $x \equiv 8 \bmod 10, \qquad x \equiv 1 \bmod 12$

(vii) $x \equiv 8 \bmod 10, \qquad x \equiv 4 \bmod 12$

(D2) *The Chinese Remainder Theorem.* The goal for this problem is to prove the following.

Theorem (Chinese Remainder Theorem)**.** *Suppose $n_1, \ldots, n_k$ are pairwise coprime, and* $\gcd(a_i, n_i) = 1$ *for each i. There is a unique simlutaneous solution to the system*

$$a_1x \equiv b_1 \bmod n_1, \qquad a_2x \equiv b_2 \bmod n_2, \qquad \ldots, \qquad a_kx \equiv b_k \bmod n_k$$

modulo $N = n_1n_2 \cdots n_k$.

(a) Determine which of the following systems can be solved **using the Chinese Remainder Theorem**. For those that can, find all solutions.

(i) $x \equiv 5 \bmod 7, \qquad x \equiv 3 \bmod 11$

(ii) $2x \equiv 3 \bmod 7, \qquad 4x \equiv 1 \bmod 11$

(iii) $2x \equiv 3 \bmod 7, \qquad 4x \equiv 1 \bmod 11, \qquad 4x \equiv 4 \bmod 8$

(iv) $2x \equiv 3 \bmod 7, \qquad 4x \equiv 1 \bmod 10, \qquad 4x \equiv 4 \bmod 8$

(b) Prove the Chinese Remainder Theorem when $k = 1$.

(c) Locate a **single** modular equation with identical solution set to the system

$$x \equiv b_1 \bmod n_1 \qquad \text{and} \qquad x \equiv b_2 \bmod n_2.$$

Prove that your equation has the same solution set.

(d) Using the previous 2 parts as the bulk of your argument, give an inductive proof of the Chinese Remainder Theorem in the special case $a_1 = \cdots = a_k = 1$.

(e) Using the previous part, prove the Chinese Remainder Theorem in full.

(f) Describe a procedure for solving the system in the Chinese Remainder Theorem.

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, n, p \in \mathbb{Z}$ are arbitrary with $p > 1$ prime and $n \geq 2$.

(H1) Find all $x, y \in \mathbb{Z}_7$ that are solutions to both of the equations

$$x + [2]_7 y = [4]_7 \qquad \text{and} \qquad [4]_7 x + [3]_7 y = [4]_7.$$

(H2) Find a complete set of incongruent solutions modulo 770 to the system of equations

$$\begin{aligned} 2x &\equiv 3 \bmod 5 \\ 2x &\equiv 3 \bmod 7 \\ 2x &\equiv 3 \bmod 11. \end{aligned}$$

(H3) (a) Locate 3 consecutive integers a, b, c such that a is divisible by the square of a prime, b is divisible by the cube of a prime, and c is divisible by the 4th power of a prime.

(b) Is part (a) possible if at least 2 of the 3 primes are equal?

(H4) Prove that for each n, there exists a sequence of n consecutive integers each of which is divisible by a perfect square other than 1.

(H5) Determine whether each of the following is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) If $\gcd(n_1, n_2) = 2$ and $\gcd(a_1, n_1) = \gcd(a_2, n_2) = 1$, then the system

$$\begin{aligned} a_1 x &\equiv b_1 \bmod n_1 \\ a_2 x &\equiv b_2 \bmod n_2 \end{aligned}$$

has a common solution.

(b) If $n \geq 3$ and $a \not\equiv 0 \bmod n$, then there exists $x \in \mathbb{Z}$ such that $ax \not\equiv b \bmod n$.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Suppose $n_1 \mid n_2$. Develop a criterion (in terms of $a_1, a_2, b_1, b_2, n_1, n_2$) for when the system

$$\begin{aligned} a_1 x &\equiv b_1 \bmod n_1 \\ a_2 x &\equiv b_2 \bmod n_2 \end{aligned}$$

has a common solution.