Math 580/780I Notes 8

The Chinese Remainder Theorem:

- **Theorem 14.** *Let $m_1, \dots, m_k$ be pairwise relatively prime positive integers. Let $b_1, \dots, b_k$ be arbitrary integers. Then the system*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $m_1 \cdots m_k$.

- **Proof (Constructive):** Let $M = m_1 \cdots m_k$. For $j \in \{1, 2, \dots, k\}$, define $M_j = M/m_j$. If i and j are in $\{1, 2, \dots, k\}$ with $i \neq j$, then $(m_i, m_j) = 1$. It follows that for each $j \in \{1, 2, \dots, k\}$, $(M_j, m_j) = 1$ so that there is an $M_j' \in \mathbb{Z}$ such that

$$M_j M_j' \equiv 1 \pmod{m_j}.$$

We set $x = \sum_{j=1}^{k} b_j M_j M_j'$. Then

$$x \equiv b_j M_j M_j' \equiv b_j \pmod{m_j} \qquad \text{for } j \in \{1, 2, \dots, k\}.$$

This proves the existence of a solution to the system of congruences in the statement of the theorem.

For uniqueness, suppose that y also satisfies $y \equiv b_j \pmod{m_j}$ for each $j \in \{1, 2, \dots, k\}$. Then $y - x \equiv 0 \pmod{m_j}$ for each such j, and we deduce that each m_j divides $y - x$. As the m_j are relatively prime, we obtain $M | (y - x)$. In other words, $y \equiv x \pmod{m_1 \cdots m_k}$.

- **Examples.**

(1) Solve $17x \equiv 3 \pmod{210}$ by using the Chinese Remainder Theorem. Use that $210 = 2 \times 3 \times 5 \times 7$ and observe that solving $17x \equiv 3 \pmod{210}$ is equivalent to solving the system $x \equiv 1 \pmod{2}$, $x \equiv 0 \pmod{3}$, $x \equiv -1 \pmod{5}$, and $x \equiv 1 \pmod{7}$. The latter is equivalent to $x \equiv 1 \pmod{14}$ and $x \equiv 9 \pmod{15}$. Therefore,

$$x \equiv 1 \times 15 \times 1 + 9 \times 14 \times (-1) \equiv -111 \equiv 99 \pmod{210}.$$

(2) Solve each system of congruences below. In other words, determine those integers x that satisfy all of the congruences in each of the systems. (These are to be done in class. Note that one system does not have any solutions.)

System 1	System 2	System 3
$x \equiv 1 \pmod{21}$	$x \equiv 5 \pmod{9}$	$x \equiv 5 \pmod{12}$
$x \equiv 3 \pmod{10}$	$x \equiv 4 \pmod{28}$	$x \equiv 3 \pmod{10}$
	$x \equiv 4 \pmod{21}$	$x \equiv 11 \pmod{21}$

(3) Prove that there exists a positive integer k for which $2^n k + 1$ is composite for all positive integers n. (It is known that $k = 78557$ has this property and it is an open problem to determine

whether or not 78557 is the smallest such k.) We use the Fermat numbers $F_n = 2^{2^n}+1$. Recall that F_n is prime for $0 \le n \le 4$ and F_5 is composite with 641 a “proper” divisor. Explain the following implications:

$$\begin{array}{llllll}
n \equiv 1 \pmod{2} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{3} & \text{provided} & k \equiv 1 \pmod{3}, \\
n \equiv 2 \pmod{4} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{5} & \text{provided} & k \equiv 1 \pmod{5}, \\
n \equiv 4 \pmod{8} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{17} & \text{provided} & k \equiv 1 \pmod{17}, \\
n \equiv 8 \pmod{16} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{257} & \text{provided} & k \equiv 1 \pmod{257}, \\
n \equiv 16 \pmod{32} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{65537} & \text{provided} & k \equiv 1 \pmod{65537}, \\
n \equiv 32 \pmod{64} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{641} & \text{provided} & k \equiv 1 \pmod{641}, \\
n \equiv 0 \pmod{64} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{F_5/641} & \text{provided} & k \equiv -1 \pmod{F_5/641}.
\end{array}$$

By the Chinese Remainder Theorem, there are infinitely many positive integers k satisfying the conditions on k on the right above (note that the last modulus is relatively prime to the others). Also, every integer n can be seen to satisfy at least one of the congruences involving n on the left. It follows that there are infinitely many positive integers k such that for every positive integer n, the number $2^n k + 1$ is divisible by one of 3, 5, 17, 257, 65537, 641, and $F_5/641$. If k is sufficiently large with this property, then it will suffice for a value of k for this example

- **Comments:** If every integer satisfies at least one of a set of congruences $x \equiv a_j \pmod{m_j}$, for $j = 1, \dots, k$, then the congruences are said to form a covering of the integers. It is unkown whether or not there is a covering consisting of distinct odd moduli > 1. Also, it is not known whether or not there is a constant $C > 0$ such that every covering using distinct moduli contains a modulus $< C$.

Homework:

(1) Determine the integers that satisfy the indicated congruence.

(a) $17x \equiv 11 \pmod{180}$

(b) $17x \equiv 10 \pmod{180}$

(2) Solve the system of congruences below. In other words, determine those integers x that satisfy all of the congruences.

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{11} \end{aligned}$$

(3) Solve the system of congruences below.

$$\begin{aligned} x &\equiv 1 \pmod{6} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{8} \end{aligned}$$

(4) Find the smallest positive integer $n > 2$ such that 2 divides n, 3 divides $n+1$, 4 divides $n+2$, 5 divides $n+3$, and 6 divides $n+4$. Prove your answer is the least such n.

(5) A *squarefree number* is a positive integer n which is not divisible by a square > 1. For example, 1, 2, 3, 5, and 6 are squarefree but 4, 8, 9, and 12 are not. Let k be an arbitrary positive integer. Prove that there is a positive integer m such that $m+1, m+2, \ldots, m+k$ are each NOT squarefree. (Use that there are infinitely many primes.)

(6) Calculate the remainder when the number $123456789101112\ldots20092010$ is divided by 180.

Challenge Problem 1:

Calculate the remainder when the number $123456789101112\ldots19781979$ is divided by 1980.

Challenge Problem 2:

If a and b are integers, then the point (a, b) is called a *lattice point*. A *visible* lattice point is one for which $\gcd(a, b) = 1$ (it is visible from the origin). Prove that there are circles (or squares) in the plane which are arbitrarily large and have the property that each lattice point in the circles (or squares) is not visible. (Use that there are infinitely many primes.)