7. Congruences (continued)

We continue with an application of congruences that we started last time. Recall that the following lemma was proved at the end of Lecture 6:

Lemma 6.6. *For any $x \in \mathbb{Z}$ we have $x^2 \equiv 0$ or 1 mod 4.*

We now use this lemma to prove the following interesting result.

Proposition 7.1. Let n be an integer of the form $4k + 3$ for some $k \in \mathbb{Z}$. Then n is not representable as a sum of two squares, that is, there are no $a, b \in \mathbb{Z}$ such that $n = a^2 + b^2$.

Proof. We argue by contradiction. Suppose $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. By Lemma 6.6 we have $a^2 \equiv 0$ or 1 mod 4 and $b^2 \equiv 0$ or 1 mod 4, whence by Theorem 6.3,

$$n = a^2 + b^2 \equiv \begin{cases} 0 + 0 = 0 & \text{or} \\ 0 + 1 = 1 & \text{or} \\ 1 + 1 = 2 & \end{cases} \quad \text{mod } 4.$$

On the other hand, by our original hypothesis $n \equiv 3 \mod 4$. This is a contradiction since $0, 1$ and 2 are not congruent to 3 mod 4 (and since congruence relation is transitive). □

Note that every odd integer is either of the form $4k+1$ or $4k+3$ for some k, and in view of the above proposition one may wonder if every positive integer of the form $4k + 1$ is representable as a sum of two squares. This is not true in general (for instance, 21 is not representable); however, quite surprisingly, it is true for primes:

Theorem 7.2 (Euler-Fermat). *Every prime of the form $4k + 1$ is representable as a sum of two squares.*

This result is beyond the scope of this course, but it is typically proved in number theory courses.

7.1. Solving systems of linear congruences.

We start with the following question:

Question. *Let $a, b, n, m \in \mathbb{Z}$ with $n, m \geq 2$. Does there exist $x \in \mathbb{Z}$ such that $x \equiv a \mod n$ and $x \equiv b \mod m$?*

The answer to this question in general is clearly negative. For instance, the system of congruences $x \equiv 1 \mod 4$ and $x \equiv 2 \mod 6$ has no solutions, as $x \equiv 1 \mod 4$ means that x has to be odd while $x \equiv 2 \mod 6$ forces x to be even.

However, the solution always exists if n and m are coprime. We start with an example and then formulate a general result.

Example 1. *Find the general solution to the following system of congruences:*

$$\begin{cases} x \equiv 2 \mod 15 \\ x \equiv 9 \mod 17 \end{cases}$$

We know that the general solution to the second congruence is $x = 9 + 17k$ for some $k \in \mathbb{Z}$. Thus, we can proceed by substituting $9 + 17k$ for x in the first congruence, solving the resulting congruence in k (using the method we discussed last time) and finally substituting the obtained formula for k in the equation $x = 9 + 17k$ to get the final answer in terms of x.

Setting $x = 9 + 17k$ in the first congruence, we get $9 + 17k \equiv 2 \mod 15$ which is equivalent to $17k \equiv -7 \mod 15$. We can solve this congruence using the method from last time (based on the Euclidean algorithm), but instead we will use an ad hoc method which is based on the following observation:

Observation. *Suppose we want to solve a congruence of the form $u \equiv w \mod n$ involving some unknown k. If we add a multiple of n to one of the sides keeping the other side unchanged, the new congruence will be equivalent to the original one (that is, the two congruences will have the same sets of solutions).*

Proof. WOLOG assume that we added a multiple of n to the left-hand side, and let $v \equiv w \mod n$ be the new congruence (note that both the original congruence $u \equiv w \mod n$ and the new one $v \equiv w \mod n$ may be true or false depending on the value of the unknown k; we have to show that they are both true or both false, no matter what k is). By construction, v is obtained from u by adding a multiple of n (that is, $v = u + nt$ for some $t \in \mathbb{Z}$), so the congruence $u \equiv v \mod n$ is always true. Since congruence relation is transitive, we conclude that $u \equiv w \mod n \iff v \equiv w \mod n$. □

We now implement this observation in our example:

$$\begin{array}{cl} 17k \equiv -7 \mod 15 & \\ \Updownarrow & \text{add } -15k \text{ to LHS} \\ 2k \equiv -7 \mod 15 & \\ \Updownarrow & \text{add 15 to RHS} \\ 2k \equiv 8 \mod 15 & \\ \Updownarrow & \text{cancellation law with } a = 2 \\ k \equiv 4 \mod 15 & \end{array}$$

The last congruence can be rewritten in the form $k = 4+15s$ for some $s \in \mathbb{Z}$. Plugging this in the formula $x = 9 + 17k$, we get the final answer in terms of x:

$x = 9+17(4+15s) = 77+15\cdot 17s$ for some $s \in \mathbb{Z}$. Note that this answer can also be expressed in the form of a congruence: x is a solution to the original system $\iff x \equiv 77 \mod 15\cdot 17$.

We now formulate the general theorem illustrated by the above example.

Theorem 7.3. *Let $a, b, n, m \in \mathbb{Z}$ where $n, m \geq 2$ and n and m are coprime. Then the system of congruences*

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$$

always has a solution, and if x_0 is a particular solution, then the general solution is $x = x_0 + mns$ for some $s \in \mathbb{Z}$ (equivalently, $x \equiv x_0 \mod mn$).

Proof. See the book or imitate the proof in Example 1. □

Now let us consider a similar example with 3 congruences:

Example 2. *Find the general solution to the following system of congruences:*

$$\begin{cases} x \equiv 2 \mod 15 \\ x \equiv 9 \mod 17 \\ x \equiv 13 \mod 19 \end{cases}$$

We will not solve this example explicitly, but rather indicate how to reduce it to the previous one. Indeed, by Example 1 the first two congruences are equivalent to a single congruence $x \equiv 77 \mod 17\cdot 15$, so our system is equivalent to the system of two congruences:

$$\begin{cases} x \equiv 77 \mod 17\cdot 15 \\ x \equiv 13 \mod 19 \end{cases}$$

Since the numbers $17\cdot 15$ and 19 are also coprime, this system can be solved as the one in Example 1.

7.2. Chinese Remainder Theorem.

Chinese Remainder Theorem. *Let $k, b_1, \ldots, b_k, n_1, \ldots, n_k$ be integers where $k \geq 1$, each $n_i \geq 2$ and $\{n_i\}$ are pairwise coprime (that is, n_i and n_j are coprime for any $i \neq j$). Then the system of congruences*

$$\begin{cases} x \equiv b_1 \mod n_1 \\ \ldots \\ x \equiv b_k \mod n_k \end{cases}$$

has a solution. Moreover, if x_0 is a particular solution, then the general solution is $x = x_0 + n_1 \ldots n_k s$ with $s \in \mathbb{Z}$ (equivalently $x \equiv x_0 \mod n_1 \ldots n_k$).

Sketch of the proof. The idea is to use the same trick as in Example 2. Indeed, by Theorem 7.3 the first two congruences in the above system can be replaced by a single congruence $x \equiv c_1 \mod n_1n_2$ (for some fixed c_1).

Thus, we replaced a system of k congruences by a system of $k-1$ congruences. In the same way we can replace a system of $k-1$ congruences by a system of $k-2$ congruences and keep going until we are left with 1 congruence (alternatively, we can argue by induction).

The only thing we have to make sure is that when we decrease the number of congruences in the system, the new system satisfies the hypotheses of the Chinese Remainder Theorem, that is, $n_1n_2, n_3, \ldots, n_k$ are still pairwise coprime. This is true by Lemma 7.4 below, which is left as an exercise. □

Lemma 7.4. *Let $m, k, l \in \mathbb{Z}$, and suppose that m and l are coprime and k and l are coprime. Then mk and l are coprime.*

We finish by outlining another proof of the Chinese Remainder Theorem illustrated using a specific example:

Example 3. *Let $a, b, c \in \mathbb{Z}$ be fixed. Find all $x \in \mathbb{Z}$ such that*

$$\begin{cases} x \equiv a \mod 5 \\ x \equiv b \mod 7 \\ x \equiv c \mod 11 \end{cases}$$

We claim that to solve the system (for arbitrary a, b and c) it suffices to find integers z_1, z_2, z_3 such that

$$\begin{cases} z_1 \equiv 1 \mod 5 & z_2 \equiv 0 \mod 5 & z_3 \equiv 0 \mod 5 \\ z_1 \equiv 0 \mod 7 & z_2 \equiv 1 \mod 7 & z_3 \equiv 0 \mod 7 \\ z_1 \equiv 0 \mod 11 & z_2 \equiv 0 \mod 11 & z_3 \equiv 1 \mod 11 \end{cases}$$

Indeed, let z_1, z_2 and z_3 be as above, and let $x_0 = az_1 + bz_2 + cz_3$. Then by Theorem 6.2 we have $az_1 \equiv a \mod 5$, $bz_2 \equiv b \cdot 0 = 0 \mod 5$ and $cz_3 \equiv c \cdot 0 = 0 \mod 5$, so by Theorem 6.3, $x_0 = az_1 + bz_2 + cz_3 \equiv a + 0 + 0 = a \mod 5$. Similarly $x_0 \equiv b \mod 7$ and $x_0 \equiv c \mod 11$. Thus, $az_1 + bz_2 + cz_3$ is a particular solution and the general solution (by the Chinese Remainder Theorem) is $x = az_1 + bz_2 + cz_3 + 5 \cdot 7 \cdot 11s$ with $s \in \mathbb{Z}$.

To find z_1, z_2 and z_3 as above note that the last two conditions on z_1 mean that z_1 is divisible by 7 and 11 $\iff$ $z_1 = 7 \cdot 11k_1 = 77k_1$ for some k_1, and the first condition on z_1 becomes $77k_1 \equiv 1 \mod 5$.

Similarly, we must have $z_2 = 55k_2$ and $z_3 = 35k_3$ for some $k_2, k_3 \in \mathbb{Z}$, with $55k_2 \equiv 1 \mod 7$ and $35k_3 \equiv 1 \mod 11$. Using ad hoc method, we find that $k_1 = 3$, $k_2 = -1$ and $k_3 = 6$ satisfy the required conditions. These give us $z_1 = 77 \cdot 3 = 231$, $z_2 = 55 \cdot (-1) = -55$ and $z_3 = 35 \cdot 6 = 210$.

Thus, the final answer is $x = 231a - 55b + 210c + 385s$ with $s \in \mathbb{Z}$.