MATH 113: DISCRETE STRUCTURES
SUNZI'S THEOREM

The Chinese mathematician Sunzi Suanjing considered the following problem in the 3-rd century C.E. A general arrays his soldiers on the parade grounds. He first organizes them into columns of 3, but there are only 2 soldiers in the final column. He then organizes them into columns of 5, but there are only 3 soldiers in the final column. Finally, he organizes them into columns of 7, and again there are only 2 soldiers in the final column. How many soldiers does the general command?

Using the language of congruences, we can phrase the general's observations as

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

What (if any) integers x simultaneously satisfy these congruences?

Let us begin by solving the first two congruences, $x \equiv 2 \pmod 3 \equiv 3 \pmod 5$. By guess-and-check, we quickly see that $x = 8$ is a solution. In fact, if $x \equiv 8 \pmod{15}$, we solve both congruences. Indeed, such x are equal to $15k + 8$ for some $k \in \mathbb{Z}$, and $15 \equiv 0$ modulo both 3 and 5.

We now need to solve the congruences $x \equiv 8 \pmod{15} \equiv 2 \pmod 7$. A little thought reveals that $x = 23$ works, and the same logic as before shows that $x \equiv 23 \pmod{105}$ gives all solutions (because $105 = 15 \cdot 7$).

This brief exploration indicates the following theorem and its proof.

Theorem 1 (Sunzi's Theorem [née Chinese Remainder Theorem]). *Suppose $N = n_1 n_2 \cdots n_k$ and that the n_i are pairwise relatively prime integers (so $\gcd(n_i, n_j) = 1$ for $i \neq j$). Then for any integers $a_1, \dots, a_k$ the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has precisely one solution $x = x_0$ with $0 \leq x_0 < N$ and all solutions are of the form $x \equiv x_0 \pmod N$.

Proof. We proceed by induction on k. If $k = 1$, then we may take x to be the remainder of a_1 divided by n_1 and clearly all solutions are of the form $x + n_1 r = x + Nr$, $r \in \mathbb{Z}$.

Fix $s \geq 1$ and suppose that all such systems with $k = s$ terms have solutions as described. Now consider a system of $s + 1$ congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_s \pmod{n_s} \\ x &\equiv a_{s+1} \pmod{n_{s+1}}. \end{aligned}$$

where the n_i are pairwise relatively prime. Let us first endeavor to solve the first two congruences. Since n_1 and n_2 are relatively prime, there are integers m_1 and m_2 such that $1 = m_1 n_1 + m_2 n_2$.

Construct the number $a_{1,2} = a_2 m_1 n_1 + a_1 m_2 n_2$. Since $m_1 n_1 = 1 - m_2 n_2$, we have $a_{1,2} = a_2(1 - m_2 n_2) + a_1 m_2 n_2 = a_2 + n_2(a_1 m_2 - a_2 m_2)$. Reducing mod n_2, we get $a_{1,2} \equiv a_2 \pmod{n_2}$. If we begin with the substitution $m_2 n_2 = 1 - m_1 n_1$, we similarly get $a_{1,2} \equiv a_1 \pmod{n_1}$. Thus $a_{1,2}$ is a simultaneous solution of the first two congruences. We get all such solutions by considering $x \equiv a_{1,2} \pmod{n_1 n_2}$. (The diligent reader should check this.) Thus we can solve the original $s+1$ congruences by solving the system

$$\begin{aligned} x &\equiv a_{1,2} \pmod{n_1 n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \\ x &\equiv a_{s+1} \pmod{n_{s+1}} \end{aligned}$$

with only s congruences. Note that all the moduli are relatively prime, so we may invoke the inductive hypothesis, and we are done. $\square$

This method of proof is constructive, in that it provides us with a method via which we can solve our system of congruences. By repeated application of the extended Euclidean algorithm, we can eliminate congruences one at a time until we get to a final congruence $x \equiv a_{1,2,\ldots,k} \pmod{N}$, where $a_{1,2,\ldots,k}$ is our solution.

In practice, this is not the fastest way to find a solution. (It requires $k-1$ applications of the extended Euclidean algorithm.) Instead, suppose that n_k is the largest of the moduli. There are $N/n_k = n_1 n_2 \cdots n_{k-1}$ numbers x such that $0 \leq x < N$ and $x \equiv a_k \pmod{n_k}$. If N/n_k is relatively small, we (or a computer) can simply check if each of these numbers satisfies all k congruences.

As an example, consider the system of congruences $x \equiv 0 \pmod{2} \equiv 1 \pmod{3} \equiv 2 \pmod{5} \equiv 3 \pmod{7}$. The solutions to $x \equiv 3 \pmod{7}$ with $0 \leq x < 2 \cdot 3 \cdot 5 \cdot 7 = 210$ are $x = 3, 10, 17, \ldots, 206$. Eliminating odd x we are left with $x = 10, 24, 38, 52, 66, 80, 94, 108, 122, 136, 150, 164, 178, 192, 206$ as possible solutions. It is easy to see that only $x = 52, 122, 192$ are congruent to $2 \pmod{5}$, and then that only $x = 52$ is $1 \pmod{3}$. We conclude that the only solutions to this system of congruences are integers $x \equiv 52 \pmod{210}$.

There is a direct way to construct solutions as well. Let $N_i = N/n_i$ for $i = 1, \ldots, k$. Observe that N_i and n_i are relatively prime, so we can find M_i and m_i such that

$$1 = M_i N_i + m_i n_i.$$

The reader may check that

$$x = \sum_{i=1}^{k} a_i M_i N_i$$

is a solution to the system of congruences, and thus all solutions are of the form

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{N}.$$

This recipe gives us a function

$$\begin{aligned} f : \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} &\longrightarrow \mathbb{Z}/N\mathbb{Z} \\ (a_1, a_2, \ldots, a_k) &\longmapsto \sum_{i=1}^{k} a_i M_i N_i \end{aligned}$$

(We have engaged in the standard subterfuge of conflating integers and their congruence classes.) There is another natural function $g : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ sending x to the k-tuple consisting of the reductions of x modulo each n_i. The interested reader may check that these functions are inverse to each other, and thus these sets are in bijection. In fact, these assignment also respect addition and thus are *isomorphisms of abelian groups*, a topic one can explore more fully in Math 332!

Problem 1. Find all solutions to the system of congruences

$$\begin{aligned} x &\equiv 2 \pmod{11} \\ x &\equiv 3 \pmod{12} \\ x &\equiv 4 \pmod{13}. \end{aligned}$$

Problem 2. Does Sunzi's theorem still hold if we drop the requirement that the n_i are relatively prime? Prove your assertion or provide a counterexample.