Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) says that given $a_1, \ldots, a_n \in \mathbb{Z}$, $m_1, \ldots, m_n \in \mathbb{Z}^+$, where the m_i are pairwise relatively prime, then the system of congruences:

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. We find this solution as follows. Let $M_k = \frac{m}{m_k}$. Then (since the m_i are pairwise relatively prime) there are inverses y_k such that $M_k y_k \equiv 1 \mod m_k$. Then $a_1 M_1 y_1 + \cdots + a_n M_n y_n \mod m$ is the solution.

1. Compute the solution to the following system of congruences:

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 5 \mod 7 \end{aligned}$$

2. Check that the following system of congruences has no solutions. (In general, there may or may not be solutions when the m_i are not pairwise relatively coprime.)

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 3 \mod 4 \\ x &\equiv 5 \mod 8 \end{aligned}$$

RSA cryptosystem

The RSA cryptosystem is designed to encode information using number theory. The algorithm is as follows.

1. Choose two prime numbers p and q, and an integer e such that $\gcd(e, (p-1)(q-1)) = 1$. (In general, larger p and q are more secure.)

2. Translate a given message into a sequence of integers by $A = 00, B = 01, \ldots, Z = 25$, and then group these integers into blocks of 4.

3. Encrypt each block M by replacing it with $M^e \mod n$.

4. To decrypt, compute an inverse d of $e \mod (p-1)(q-1)$. for each block C, compute $C^d \equiv M^{de} \equiv M \mod n$ to get back the original message.

(No exercises, but please feel free to ask questions about this.)

Induction

We use induction to prove an infinite family of statements. The outline for induction goes as follows: Let $P(n)$ be a statement about the integer n, and suppose we want to prove $P(n)$ for every integer n. Generally, we can do this in the following steps:

1. Prove $P(0)$ is true. (This is the base case.)
2. (This is the inductive hypothesis.)
   (a) For regular induction, assume $P(n)$ is true.
   (b) For strong induction, assume $P(0), P(1), \ldots, P(n)$ are true.
3. Prove that $P(n+1)$ is true, using the inductive hypothesis. This completes the proof.

You can apply induction in other cases. For example: prove $P(n)$ for all integers greater than $d \in \mathbb{Z}$. In this case, your base case is $P(d)$ instead of $P(0)$. For strong induction, you may need multiple base cases. Induction applies to other subset of $\mathbb{Z}$. For example, it is possible to prove something for all even numbers, or all multiples of 3, etc.

Exercises

1. Which numbers can be written as a sum $10a + 25b$ where $a, b \in \mathbb{Z}_{\geq 0}$?
2. Show that $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}(n(n+1)(2n+1))$.

Find the faults with the following proofs by induction:

1. Let $P(n)$ be the statement "$n = 0$".
   (a) Base case: $n = 0$. Then $P(0)$ is true.
   (b) Inductive hypothesis: $P(0), P(1), \ldots, P(n)$ are true.
   (c) Write $n + 1 = a + b$ where $0 \leq a, b < n + 1$. Then by our inductive hypothesis, $P(a)$ and $P(b)$ are true, so $a = b = 0$. Then $n + 1 = a + b = 0 + 0 = 0$.
   (d) Therefore any nonnegative integer is equal to 0.
2. We will prove that the sum of all positive integers is finite. Let $P(n)$ be the statement "the sum of the first n positive integers is finite."
   (a) Base case: $n = 1$. $P(1)$ is true.
   (b) Inductive hypothesis: $P(n)$ is true.
   (c) $1 + \cdots + (n+1) = (1 + \cdots + n) + (n+1)$. Using $P(n)$, the first sum $S = 1 + \cdots + n$ is finite. Therefore $S + (n + 1)$ is a sum of finite integers, therefore is finite.
   (d) Therefore the sum of all positive integers is finite.