Chinese Remainder Theorem

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

$$x \equiv 1 \mod 3$$
$$x \equiv 3 \mod 5$$
$$x \equiv 5 \mod 7$$

Solution: Compute $m = 3 * 5 * 7 = 105$. Compute $M_1 = 35, M_2 = 21, M_3 = 15$. Compute inverses:

$$M_1 y_1 \equiv 35 y_1 \equiv 1 \pmod 3 \implies y_1 \equiv 2 \mod 3$$
$$M_2 y_2 \equiv 21 y_2 \equiv 1 \pmod 5 \implies y_2 \equiv 1 \mod 5$$
$$M_3 y_3 \equiv 15 y_3 \equiv 1 \pmod 7 \implies y_3 \equiv 1 \mod 7$$

Then plug this in: $x \equiv 1 * 35 * 2 + 3 * 21 * 1 + 5 * 15 * 1 \equiv 208 \equiv 103 \mod 105$.

(Alternatively, you could have noticed that $1 \equiv -2 \mod 3, 3 \equiv -2 \mod 5$, and $5 \equiv -2 \mod 7$ to find $x \equiv -2 \mod 105$.

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.)

$$x \equiv 1 \mod 2$$
$$x \equiv 3 \mod 4$$
$$x \equiv 5 \mod 8$$

It is enough to check all cases for $x \mod 8$.

If $x \not\equiv 5 \mod 8$, then the last congruence is violated. If $x \equiv 5 \mod 8$, then we will have $x \equiv 1 \mod 2$ (can you see why?). However, we will not have $x \equiv 3 \mod 4$. For example, $5 \equiv 1 \mod 4$, not 3.

The problem here is that $x \equiv 5 \mod 8$, gives a congruence for all divisors of 8, because if $8 \mid x - 5$, then since $2, 4 \mid 8$, then we also have $2, 4 \mid x - 5$.

Induction

Exercises

1. Which numbers can be written as a sum $10a + 25b$ where $a, b \in \mathbb{Z}_{\geq 0}$?

   Solutions: We can write 0, 10, and all numbers of the form $20 + 5k$ for $k \in \mathbb{Z}_{\geq 0}$.

   $0 = 10 * 0 + 25 * 0$. $10 = 10 * 1 + 25 * 0$. We prove the last part by strong induction:

   Let $P(n)$ be the statement $20 + 5k$ can be written as $10a + 25b$ for $a, b \in \mathbb{Z}_{\geq 0}$.

   Our base cases are $P(0) : 20 + 5(0) = 20 = 10 * 2 + 25 * 0$ and $P(1) : 20 + 5(1) = 25 = 10 * 0 + 25 * 1$.

   For the inductive hypothesis, assume $P(0), P(1), \ldots, P(n)$ are true. Then we will use them to prove that $P(n + 1)$ is true.

   $20 + 5(n + 1) = 20 + 5n + 5$. We consider two cases: if $n > 1$, then we have that $20 + 5n + 5 - 10 = 20 + 5(n - 1) = 10a + 25b$ because of $P(n - 1)$. Adding 10 to this gives $10(a + 1) + 25b = 20 + 5(n + 1)$. Thus $P(n + 1)$ is true.

   In the other case, if $n \geq 1$, then $n = 0$ or $n = 1$, and these are our base cases.

2. Show that $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}(n(n + 1)(2n + 1))$.

   Solution: Let $P(n)$ be the statement $\sum_{i=1}^{n} i^2 = \frac{1}{6}(n(n + 1)(2n + 1))$.

   Our base case is $P(1) : 1^2 = \frac{1}{6}(1(2)(3)) = 1$.

   For the inductive hypothesis, assume $P(n)$. Then we will use this to prove $P(n + 1)$.

   $1^2 + \cdots + n^2 + (n + 1)^2 = \frac{1}{6}(n(n + 1)(2n + 1)) + (n + 1)^2$ using $P(n)$. Then just solve:

$$
\begin{aligned}
\frac{1}{6}(n(n+1)(2n+1)) + (n+1)^2 &= (n+1)(\frac{1}{6}(n(2n+1)) + (n+1)) \\
&= (n+1)\left(\frac{n(2n+1) + 6n + 6}{6}\right) \\
&= (n+1)\frac{2n^2 + 7n + 6}{6} \\
&= \frac{n+1}{6}(2n+3)(n+2) \\
&= \frac{1}{6}(n+1)((n+1)+1)(2(n+1)+1)
\end{aligned}
$$

   and this proves $P(n + 1)$.

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.

   The problem here occurs for $n = 0$. When we want to show $P(1)$, we need to write $0 + 1 = 1 = a + b$ where $0 \leq a, b < 1$. This forces $a = b = 0 \implies a + b = 0 \neq 1$, so the proof by induction fails.

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.

   The problem is that the sum of all positive integers is not of the form "sum of the first n positive integers" for any n. It is important to distinguish what we've shown here. We shown $P(n)$ for all natural numbers n, but what we want is $P(\mathbb{Z}^+)$, but $\mathbb{Z}^+$ is not a positive integer.