Math 342 Tutorial

June 11, 2025

Question 1. Find all solutions to following systems of congruences in two ways: first, using the Chinese Remainder Theorem; and second, by iteratively solving and substituting linear congruences.

(a) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$.

(b) $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 6 \pmod 7$.

(a) We first employ CRT. We have $M = 2 \cdot 3 \cdot 5 = 30$, $M_1 = 15$, $M_2 = 10$, $M_3 = 6$. The inverses of M_1, M_2, M_3 modulo 2, 3, 5 are all 1. Then the unique solution modulo M is given by

$$(1)(15)(1) + (2)(10)(1) + (3)(6)(1) = 15 + 20 + 18 = 53 \equiv 23 \pmod{30}.$$

Now we use the second method. We are given $x = 1 + 2t$, so $1 + 2t \equiv 2 \pmod 3$. Solving, we obtain $t \equiv 2 \pmod 3$ so that $t = 2 + 3s$. Then $x = 1 + 2(2 + 3s) = 5 + 6s$. Then $5 + 6s \equiv 3 \pmod 5$. Solving again, we have $s \equiv 3 \pmod 5$ so that $s = 3 + 5r$. Then $x = 5 + 6(3 + 5r) = 23 + 30r \equiv 23 \pmod{30}$, and we're done.

(b) Note that we see at once by inspection that 6 is the required solution. However, we carry through the process using CRT. We have that $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, $M_3 = 42$, $M_4 = 30$. The inverses of M_3 and M_4 modulo 5, 7 are 3, 4, respectively. Then

$$x = (42)(3) + (6)(30)(4) = 846 \equiv 6 \pmod{210}.$$

We now use the second method. The first two congruences imply $x = 6t$. Then $6t \equiv 1 \pmod 5$, hence $t \equiv 1 \pmod 5$ and $t = 1 + 5s$. Then $x = 6(1 + 5s) = 6 + 30s$. Next, $6 + 30s \equiv 6 \pmod 7$. Solving, we have $s \equiv 0 \pmod 7$ and $s = 7r$. Then $x = 6 + 30(7r) = 6 + 210r \equiv 6 \pmod{210}$, and we're done.

Question 2. Give the following generalization of the Chinese Remainder Theorem. Let $m_1, \ldots, m_r$ be pairwise coprime integers. Then the system $a_1 x \equiv b_1 \pmod{m_1}, \ldots, a_r x \equiv b_r \pmod{m_r}$ has exactly one solution modulo $\frac{m_1}{(a_1, m_1)} \cdots \frac{m_r}{(a_r, m_r)}$ if and only if each $(a_i, m_i) \mid b_i$.

Note that $a_i x \equiv b_i \pmod{m_i}$ is soluble if and only if $(a_i, m_i) \mid b_i$. In this case, $a_i x \equiv b_i \pmod{m_i}$ is equivalent to $x \equiv b_i/(a_i, m_i) \pmod{m_i/(a_i, m_i)}$. The rest is simply the usual CTR since the $\{m_i/(a_i, m_i)\}$ are pairwise coprime.

Question 3. (a) Show that the system of congruences $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}$ has a solution if and only if $(m_i, m_j) \mid (a_i - a_j)$ for all $i < j$. Show that if a solution exists, then it is unique modulo $[m_1, \ldots, m_r]$. [Hint: succesively substitute linear equations.] (b) Solve the system $x \equiv 4 \pmod 6$, $x \equiv 13 \pmod{15}$. (c) Solve the system $x \equiv 5 \pmod 6$, $x \equiv 3 \pmod{10}$, $x \equiv 8 \pmod{15}$. (d) Does the system $x \equiv 1 \pmod 8$, $x \equiv 3 \pmod 9$, $x \equiv 2 \pmod{12}$ have any solutions?

(a) The proof is by induction on r. Consider the case $r = 2$, i.e., an arbitrary system of 2 linear congruences $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$. The first congruence implies $x = a_1 + m_1 k$ for some $k \in \mathbf{Z}$. Substituting, we have $a_1 + m_1 k \equiv a_2 \pmod{m_2}$, i.e., $m_1 k \equiv a_2 - a_1 \pmod{m_2}$. This has a solution in k if and only if $(m_1, m_2) \mid a_2 - a_1$. Assume k_0 is such a solution; then all incongruent solutions modulo m_2 are given by $k = k_0 + \frac{m_2}{(m_1, m_2)} t$. Then

$$x = a_1 + m_1 \left(k_0 + \frac{m_2}{(m_1, m_2)} t \right) = a_1 + k_0 m_1 + [m_1, m_2] t.$$

Therefore, the solution $x_0 = a_1 + k_0 m_1$ is unique modulo $[m_1, m_2]$. Since the system was arbitrary, we have shown the base case.

Next let $r > 2$ be arbitrary, and suppose the result holds for $r - 1$. If there is such a solution to the system $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, r$, then in particular there is a solution to the system $x \equiv a_i \pmod{m_i}$, $x \equiv a_r \pmod{m_r}$ for each $i = 1, \ldots, r-1$. From part (a), this implies that $(m_i, m_r) \mid a_r - a_i$, $i = 1, \ldots, r-1$. From the inductive hypothesis, we also have $(m_i, m_j) \mid a_j - a_i$ for $1 \leqq i < j < r$. We therefore have necessity for the given r.

Next, suppose $(m_i, m_j) \mid a_j - a_i$ for each $1 \leqq i < j \leqq r$. In particular, by the inductive hypothesis, there is a unique solution to the system $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, r-1$ modulo $M = [m_1, \ldots, m_{r-1}]$, say $A \pmod{M}$. We next consider the system $x \equiv A \pmod{M}$, $x \equiv a_r \pmod{m_r}$. From the base case, this admits a solution if and only if $(M, m_r) \mid A - a_r$. We are given that $(m_i, m_r) \mid a_i - a_r$ and $(m_i, m_r) \mid m_i \mid a_i - A$ for each $i = 1, \ldots, r-1$. Hence, $(m_i, m_r) \mid (a_i - a_r) - (a_i - A) = A - a_r$. Since this holds for each $i < r$, we have that $[(m_1, m_r), \ldots, (m_{r-1}, m_r)] \mid A - a_r$. But $[(m_1, m_r), \ldots, (m_{r-1}, m_r)] = ([m_1, \ldots, m_{r-1}], m_r) = (M, m_r)$. In other words, $(M, m_r) \mid A - a_r$, as required.

Because the system was arbitrary, the result holds for this r. By mathematical induction, the result holds for all $r \geqq 2$.

(b) Note $(6, 15) = 3 \mid 13 - 4 = 9$, so there is indeed a solution. From part (a), we desire a solution k to $15k \equiv 4 - 13 \equiv 3 \pmod{6}$. We may simply take $k = 1$. Then $x \equiv 13 + 15 \equiv 28 \pmod{30}$.

(c) One may check that the system is consistent, i.e., that $(m_i, m_j) \mid a_i - a_j$ for each $i < j$. We first find a solution to $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$. So, we seek a solution to $10k \equiv 5 - 3 \pmod{6}$ which is equivalent to $4k \equiv 2 \pmod{6}$. Taking $k = 2$, we see that $A = 3 + 2(10) = 23$ is to unique solution modulo $[6, 10] = 30$.

Now we seek a solution to $x \equiv 23 \pmod{30}$, $x \equiv 8 \pmod{15}$. But $23 \equiv 8 \pmod{15}$, so we're done.

(d) There is no solution because $(12, 8) = 4$ does not divide $2 - 1 = 1$.

Question 4. Show there are arbitrarily long strings of consecutive integers each divisible by a perfect square greater than 1. [Hint: Use CRT to show there is a simultaneous solution to the system $x \equiv 0 \pmod{4}$, $x \equiv -1 \pmod{9}$, $x \equiv -2 \pmod{25}$, $\ldots$, $x \equiv -k+1 \pmod{p_k^2}$ where p_k is the kth prime.]

Following the hint, we consider the system

$$x \equiv 0 \pmod{4},\ x \equiv -1 \pmod{9}, \ldots, x \equiv -k+1 \pmod{p_k^2}.$$

By CRT, there is a unique solution N modulo $4p_2^2 \cdots p_k^2$. Now the integers in the sequence N, $N+1, \ldots, N+k-1$ are each divisible by a square because $p_j^2 \mid N + j - 1$ as $N \equiv -j + 1 \pmod{p_j^2}$ as the solution to the CRT problem.

Question 5. Let $m = 2^{e_0} p_1^{e_1} \cdots p_k^{e_k}$. Show the congruence $x^2 \equiv 1 \pmod{m}$ has exactly r^{r+s} solutions where $s = a_0$ if $0 \leqq a_0 \leqq 2$, and $s = 4$ for $a_0 > 2$. [Hint: Use question 12 from the May 28th tutorial set.]

The congruence $x^2 \equiv 1 \pmod{m}$ is equivalent to the system $x^2 \equiv 1 \pmod{2^{e_0}}$, $x^2 \equiv 1 \pmod{p_i^{e_i}}$, $i = 1, \ldots, r$. Each of the odd prime congruences has two solutions given by $\pm 1 \pmod{p_i^{e_i}}$. For $a_0 = 0$, there is nothing to report. For $a_0 = 1$, there is one solution to $x^2 \equiv 1 \pmod{2}$. For $a_0 = 2$, there are two solutions given by $x = \pm 1 \pmod{4}$. For $a_0 > 2$, there are four solutions given by $x = \pm 1$ or $\pm\,(1 + 2^{k-1}) \pmod{2^k}$. In any event, there are 2^{s+r} solutions to $x^2 \equiv 1 \pmod{m}$.

Question 6. Find all solutions to the following congruences. (a) $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{121}$. (b) $x^2 + 4x + 2 \equiv 0 \pmod{343}$. (c) $13x^7 - 42x - 649 \equiv 0 \pmod{1323}$.

(a) Note that $121 = 11^2$, so we apply Hensel's Lemma. We first solve $f(x) = x^3 + 8x^2 - x - 1 \equiv 0 \pmod{11}$. Checking all possibilities, we find that $x = 4, 5$. Next, the derivative is $f'(x) = 3x^2 + 16x - 1$. Observe that 4 is not a root of the derivative modulo 11 but 5 is. We can lift 4 to a root r of $f(x) \pmod{121}$ as $r = 4 + 11t$ where

$$t \equiv -\overline{f'(4)} \left(\frac{f(4)}{11} \right) \equiv -\overline{111} \left(\frac{187}{11} \right) \equiv 5 \pmod{11}.$$

Therefore, $r = 59$. For the root 5, oberseve that $f(5) \not\equiv 0 \pmod{121}$, hence there are no liftings to roots of $f(x) \pmod{121}$. We have shown that the only root of $f(x) \pmod{121}$ is 59.

(b) We have $343 = 7^3$, so we apply Hensel's Lemma. Let $f(x) = x^2 + 4x + 2$. The solutions of $f(x) \equiv 0 \pmod 7$ are given by $x = 1, 2$. The derivative is $f'(x) = 2x + 4$. Note that neither $f(1)$ nor $f(2)$ is 0 modulo 49. We can therefore lift them to unique roots of $f(x)$ modulo 49. Using the lemma these are given by 8 and 37, respectively. Again, neither $f'(8)$ nor $f'(49)$ are zero modulo 7, hence they can be lifted uniquely. These lifts are given by 106 and 233, respectively.

(c) Note $1323 = 3^3 7^2$. Let $f(x) = 13x^7 - 42x - 649$. We handle the characteristic 3 first. The only solution to $f(x) \equiv 0 \pmod 3$ is $x = 1$. Observe that $f'(1) \not\equiv 0 \pmod 3$. Therefore, we may lift $x = 1$ to a unique root of $f(x)$ modulo 3^3. This root is given by 22.
Next, we handle the characteristic 7. Again, there is a unique root $f(x)$ modulo 7. It is given by $x = 2$. Now $f'(2) \equiv 0 \pmod 7$ and $f(2) \equiv 0 \pmod{49}$, hence it has 7 lifts given by $2 + 7t$ for $0 \leqq t < 7$, i.e., 2, 9, 16, 23, 30, 37, and 44.
Next, we need to pair each solution for 27 with each solution for 49. The system $x \equiv 22 \pmod{27}$, $x \equiv 2 \pmod{49}$ has solution $x \equiv 1129 \pmod{1323}$. The remaining systems have solutions 940, 751, 562, 373, 184, 1318.

Question 7. Suppose $(a, p) = 1$. Use Hensel's Lemma to find a recursive formula for the solutions of $ax \equiv 1 \pmod{p^k}$ for all positive integers k.

Since $(a, p) = 1$, a has an inverse b modulo p. Define $f(x) = ax - 1$. Then $f(b) = 0 \pmod p$ is the unique solution modulo p. But $f'(a) = a \not\equiv 0 \pmod p$, so we can lift it uniquely to larger characteristics. We have $r_k = r_{k-1} - f(r_{k-1})\overline{f'(b)} = r_{k-1} - (ar_{k-1} - 1)b = r_{k-1}(1 - ab) + b$.