Theory of Numbers homework 5
Linear congruences, Chinese remainder theorem
Due October 15th, 2018

Exercise 1. Solve the following linear congruences:

1. \(6x \equiv 15 \pmod{21}\).

   Solution. We have \(\gcd(6, 21) = 3\), which divides 15, so we have 3 solutions. We see that a particular solution is given by \(x_0 = 6\). By the theorem in the lecture notes, the other solutions are given by \(6 + \frac{21}{3} = 13\) and \(6 + 2 \times \frac{21}{3} = 20\).

2. \(34x \equiv 60 \pmod{98}\).

   Solution. First of all, \(\gcd(34, 98) = 2\), so there are two solutions. To find a particular solution, divide everything by 2 to get \(17x \equiv 30 \pmod{49}\).

   Now, write the Euclidean algorithm for 49 and 17:
   \[
   49 = 17 \times 2 + 15 \\
   17 = 15 \times 1 + 2 \\
   15 = 2 \times 7 + 1
   \]

   so that the extended Euclidean algorithm will give:
   \[
   1 = 15 - 2 \times 7 = 15 - (17 - 15 \times 1) \times 7 = 15 \times 8 - 17 \times 7
   \]
   \[
   = (49 - 17 \times 2) \times 8 - 17 \times 7 = 49 \times 8 - 17 \times 23.
   \]

   Thus, we have \(17 \times (-23) \equiv 1 \pmod{49}\). Multiplying by 30, we see that

   \[-23 \times 30 = -23 \times 3 \times 10 = -69 \times 10 \equiv -20 \times 10 \equiv 45 \pmod{49}.\]

   Therefore, 45 is a particular solution. By the formula from the theorem, the other solution is given by \(45 + 49 = 94\).

Exercise 2. Solve the following system of simultaneous congruences:

\[
\begin{align*}
  x &\equiv 5 \pmod{6} \\
  x &\equiv 4 \pmod{11} \\
  x &\equiv 3 \pmod{17}
\end{align*}
\]

Solution. We proceed as in the proof of the Chinese Remainder Theorem. We have \(N_1 = 11 \times 17\), \(N_2 = 6 \times 17\) and \(N_3 = 6 \times 11\). We have \(N_1 \equiv 1 \pmod{6}\), so that an inverse \(x_1\) of \(N_1\) modulo 6 is given by \(x_1 = 1\). We have \(N_2 \equiv 3 \pmod{11}\), so an inverse \(x_2\) of \(N_2\) modulo 11 is given by \(x_2 = 4\). We have \(N_3 \equiv -2 \pmod{17}\), so an inverse \(x_3\) of \(N_3\) modulo 17 is given by \(x_3 = 8\). Put

\[
x = (\underbrace{11 \times 17}_{\text{mod 6}} \times \text{5}) + (\underbrace{6 \times 17}_{\text{mod 11}} \times \underbrace{4}_{\text{inverse of 3}} \times 4) + (\underbrace{6 \times 11}_{\text{mod 17}} \times \underbrace{-2}_{\text{inverse of -2}} \times 8 \times 3).
\]

By construction, this is the (unique) solution modulo \(6 \times 11 \times 17 = 1122\). In particular, \(x \equiv 785 \pmod{1122}\).
Exercise 3. Solve the linear congruence $17x \equiv 3 \pmod{210}$ by reducing it to a system of simpler linear congruences.

Solution. We can solve the system of congruences:

$$
\begin{align*}
17x &\equiv 3 \pmod{2} \\
17x &\equiv 3 \pmod{3} \\
17x &\equiv 3 \pmod{5} \\
17x &\equiv 3 \pmod{7}.
\end{align*}
$$

Some quick calculations show that this is equivalent to the system:

$$
\begin{align*}
x &\equiv 1 \pmod{2} \\
2x &\equiv 0 \pmod{3} \\
2x &\equiv 3 \pmod{5} \\
3x &\equiv 3 \pmod{7}.
\end{align*}
$$

Finally, inverting the coefficients of $x$ in each equation:

$$
\begin{align*}
x &\equiv 1 \pmod{2} \\
x &\equiv 0 \pmod{3} \\
x &\equiv 4 \pmod{5} \\
x &\equiv 1 \pmod{7}.
\end{align*}
$$

Apply the proof of the Chinese Remainder Theorem as in Exercise 2 to obtain

$$x = 729 \equiv 99 \pmod{210}.$$ 

A computation shows that $17 \times 99 = 1683 \equiv 3 \pmod{210}$.

Exercise 4. A basket contains a certain number of apples. If I take them out 5 at a time, 3 apples remain. If I take them out 6 at a time, 1 apple remains. What is the smallest number of apples that this basket may contain?

Solution. This corresponds to the simultaneous congruences

$$x \equiv 3 \pmod{5} \quad \text{and} \quad x \equiv 1 \pmod{6}.$$ 

We can use the usual method to solve them, or find a solution by inspection. Indeed, the first congruence means that the final digit of a solution should be 3 or 8. The second congruence implies that any solution is odd, so the final digit must be 3. We then find that 13 is a solution.

Since it is unique modulo $5 \times 6 = 30$, it is the smallest positive solution.

Exercise 5. Find three consecutive positive integers which are not square-free. Recall that $n$ is said to be square-free if it is not divisible by $m^2$ for any $m > 1$.

Solution. To find such integers, we are going to find an integer $a$ such that $2^2|a - 1$, $3^2|a$ and $5^2|a + 1$. This translates into the system of congruences

$$
\begin{align*}
a &\equiv 1 \pmod{4} \\
a &\equiv 0 \pmod{9} \\
a &\equiv -1 \pmod{25}
\end{align*}
$$

which we can solve because 4, 9, 25 are pairwise relatively prime. We put $N_1 = 9 \times 25 = 225$, $N_2 = 4 \times 25 = 100$, and $N_3 = 4 \times 9 = 36$. Now, first of all, we solve $N_1x \equiv 1 \pmod{4}$, which may be simplified into $x \equiv 1 \pmod{4}$, so that $x_1 = 1$ is a solution. Now, we solve $N_3x \equiv 1$
(mod 25), which simplifies to $11x \equiv 1 \pmod{25}$. We find by inspection that $x = -9$ is a solution.

Now, put $a = N_1x_1 - N_3x_3 = 225 + 36 \times 9 = 549$ (note that we do not need to solve $N_2x \equiv 1 \pmod{9}$ because the solution of this would appear with a coefficient zero anyway in the final solution). Thus, we have our sequence of three non-squarefree integers: 548, 549, 550. We may check that it is indeed so: 548 is divisible by $2^2$, 549 = $9 \times 61$ is divisible by $3^2$, and 550 = $25 \times 22$ is divisible by $5^2$.

**Exercise 6.** 1. Let $m, n > 1$ be integers. Prove that the congruences

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}$$

admit a simultaneous solution if and only if $\gcd(m, n)$ divides $a - b$.

**Solution.** Assume these congruences have a simultaneous solution $x$. Then there exist integers $k$ and $l$ such that

$$x = a + mk = b + nl.$$

Thus, we have

$$a - b = nl - mk.$$

The $\gcd$ of $m$ and $n$ divides the right-hand side, so it has to divide the left-hand side.

Conversely, assume $\gcd(m, n)$ divides $a - b$. Then, by corollary 2.3.7 in the lecture notes, there exist integers $u$ and $v$ such that

$$a - b = um + vn.$$

This means that the integers $a - um$ and $b + vn$ are equal: their common value $x$ is a solution to our system of congruences.

2. If a solution to the above system exists, check that it is unique modulo $\text{lcm}(m, n)$.

**Solution.** Let $x$ and $y$ be two solutions of the system. It suffices to show that they are congruent modulo $\text{lcm}(m, n)$. First of all, since they are both congruent to $a$ modulo $m$, we have $x \equiv y \pmod{m}$, so $m$ divides $x - y$. In the same manner, $n$ divides $x - y$. Thus, $x - y$ is a common multiple of $m$ and $n$, so it is divisible by $\text{lcm}(m, n)$.

**Remark** Recall that when proving proposition 2.4.2 in the notes, we showed in particular that all common multiples of $a$ and $b$ were divisible by $\text{lcm}(a, b)$. Indeed, we showed that $\frac{ab}{\gcd(a, b)}$ was a common multiple of $a$ and $b$, and that any other common multiple was divisible by $\frac{ab}{\gcd(a, b)}$. From this we deduced that $\frac{ab}{\gcd(a, b)}$ was in fact the least common multiple, and it follows from what we just said that $\text{lcm}(a, b)$ divides all other common multiples of $a$ and $b$.

3. Do the congruences

$$x \equiv 17 \pmod{45} \quad \text{and} \quad x \equiv 3 \pmod{20}$$

admit a simultaneous solution?

**Solution.** No, because $\gcd(45, 20) = 5$ does not divide $17 - 3 = 14$. 