UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations
Lecture 2.04 – Solving linear modular congruences

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Linear congruences

Definition. A linear congruence is an expression of the form $ax \equiv c \pmod{m}$ for given integers a, c, and m. Note that this expression only makes sense if the unknown x is also an integer.

A linear congruence can have no solutions or infinitely many solutions, which can be expressed together as values in certain moduli. We shall investigate this in more detail on the next slides.

Notice that the linear equation $ax + my = c$, when considered modulo m, becomes the linear congruence

$$\begin{aligned} ax + my &\equiv c \pmod{m}, \\ ax + 0y &\equiv c \pmod{m}, \\ ax &\equiv c \pmod{m}. \end{aligned}$$

In fact, the solutions to $ax \equiv c \pmod{m}$ are precisely the integer x-values that solve $ax + my = c$ for integers x and y. So what we have learned about solving integer linear equations will also have applications when solving linear congruences.

Linear congruences – Checking all multiples

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{7}$.
Solution. Checking the multiples of 6 while working modulo 7, we have:

x	0	1	2	3	4	5	6
$6x$	0	6	5	4	3	2	1

So the only solution is $x \equiv 3 \pmod{7}$.

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{8}$.
Solution. Checking the multiples of 6 while working modulo 8, we have:

x	0	1	2	3	4	5	6	7
$6x$	0	6	4	2	0	6	4	2

So the only solutions are $x \equiv 2 \pmod{8}$ and $x \equiv 6 \pmod{8}$.
Equivalently, the only solution is $x \equiv 2 \pmod{4}$.

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{9}$.
Solution. Checking the multiples of 6 while working modulo 9, we have:

x	0	1	2	3	4	5	6	7	8
$6x$	0	6	3	0	6	3	0	6	3

So there are no solutions to $6x \equiv 4 \pmod{9}$.

Linear congruences – Using rules of modular arithmetic

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod 7$.
Solution. We have

$$\begin{aligned} 6x &\equiv 4 \pmod 7, \\ -x &\equiv 4 \pmod 7, \\ x &\equiv -4 \pmod 7, \\ x &\equiv 3 \pmod 7. \end{aligned}$$

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod 8$.
Solution. We have

$$\begin{aligned} 6x &\equiv 4 \pmod 8, && \\ 3x &\equiv 2 \pmod 4 && (\text{since } 2 \mid 8), \\ 3x &\equiv 6 \pmod 4, && \\ x &\equiv 2 \pmod 4 && (\text{since } \gcd(3,4) = 1). \end{aligned}$$

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod 9$.
Solution. We must have $6x = 4 + 9k$ for some integer k. But this means $4 = 6x - 9k = 3(2x - 3k)$ where $2x - 3k \in \mathbb{Z}$, which cannot ever be true since $3 \nmid 4$. So there are no solutions.

Solving linear congruences

To solve the general linear congruence $ax \equiv c \pmod{m}$, first consider simplifying the problem using the standard rules of modular arithmetic.

If the coefficient and/or modulus are too large for this to be practical, we can always follow the below method, inspired by the method of finding integer solutions to $ax + my = c$:

- Find $d = \gcd(a, m)$. If $d \nmid c$, there is no solution.
- If $d \mid c$, then solutions exist, and there are exactly d solutions in the original modulus m. To find these solutions:
  - Find integers x' and y' satisfying $ax' + my' = d$ by applying the Euclidean algorithm to a and m and working backwards.
  - The general solution is then $x \equiv \frac{c}{d}x' \pmod{\frac{m}{d}}$.
  - If $d > 1$ and we wish to find all d solutions in the original modulus m, take the solution $\frac{c}{d}x'$ and repeatedly add $\frac{m}{d}$ to it until there are d different solutions. That is,

$$x \equiv \frac{c}{d}x' + \frac{m}{d}k \pmod{m}$$

for each $k \in \{0, 1, 2, \ldots, d-1\}$.

Solving linear congruences – Example 1

Example. Solve $29x \equiv 11 \pmod{101}$.

Solution. First apply the Euclidean algorithm to the coefficient 29 and the modulus 101. We have

$$\begin{aligned} 101 &= 3 \times 29 + 14, \\ 29 &= 2 \times 14 + 1, \\ 14 &= 14 \times 1 + 0. \end{aligned}$$

So $\gcd(29, 101) = 1$. Since $1 \mid 11$, there are solutions to the congruence, and there should be exactly 1 solution modulo 101.

Working backwards, we find

$$\begin{aligned} 1 &= 29 - 2 \times 14 \\ &= 29 - 2(101 - 3 \times 29) \\ &= 7 \times 29 - 2 \times 101. \end{aligned}$$

So an integer solution to $29x' + 101y' = 1$ is $x' = 7$ and $y' = -2$.

Since the right-hand side of the congruence is 11, we need to multiply this answer for x' by $\frac{11}{1} = 11$ (and the modulus remains as $\frac{101}{1} = 101$).

So the general solution is $x \equiv 11 \times 7 \equiv 77 \pmod{101}$.

Solving linear congruences – Example 2

Example. Solve $119x \equiv 27 \pmod{252}$.

Solution. First apply the Euclidean algorithm to the coefficient 119 and the modulus 252. We have

$$\begin{aligned} 252 &= 2 \times 119 + 14, \\ 119 &= 8 \times 14 + 7, \\ 14 &= 2 \times 7 + 0. \end{aligned}$$

So $\gcd(119, 252) = 7$. Since $7 \nmid 27$, there cannot be any solutions to this congruence.

To justify this conclusion, notice that we are trying to solve the equation $119x = 27 + 252k$ for some integer k. But this can be rearranged to give $27 = 119x - 252k = 7(17x - 36k)$ where $17x - 36k \in \mathbb{Z}$, which cannot be true since $7 \nmid 27$. So there are no solutions.

Solving linear congruences – Example 3

Example. Solve $130x \equiv 125 \pmod{245}$.

Solution. First apply the Euclidean algorithm to the coefficient 130 and the modulus 245. We have

$$\begin{aligned} 245 &= 1 \times 130 + 115, \\ 130 &= 1 \times 115 + 15, \\ 115 &= 7 \times 15 + 10, \\ 15 &= 1 \times 10 + 5, \\ 10 &= 2 \times 5 + 0. \end{aligned}$$

So $\gcd(130, 245) = 5$. Since $5 \mid 125$, there are solutions to the congruence, and there should be exactly 5 solutions modulo 245.

Working backwards, we eventually find $5 = 17 \times 130 - 9 \times 245$. So an integer solution to $130x' + 245y' = 5$ is $x' = 17$ and $y' = -9$.

Since the right-hand side of the congruence is 125, we need to multiply this answer for x' by $\frac{125}{5} = 25$ and reduce the answer modulo $\frac{245}{5} = 49$.

So the general solution is $x \equiv 17 \times 25 \equiv 33 \pmod{49}$, or in the original modulus, by adding 49 repeatedly to our answer, we have $x \equiv 33, 82, 131, 180, \text{or } 229 \pmod{245}$.

Solving linear congruences – Example 3

Example. Solve $130x \equiv 125 \pmod{245}$.

Alternative approach. Observing that $\gcd(130, 245) = 5$ and that $5 \mid 125$, we first divide everything through by 5 to get the equivalent congruence $26x \equiv 25 \pmod{49}$. Applying the Euclidean algorithm to 26 and 49 gives:

$$\begin{aligned} 49 &= 1 \times 26 + 23, \\ 26 &= 1 \times 23 + 3, \\ 23 &= 7 \times 3 + 2, \\ 3 &= 1 \times 2 + 1, \\ 2 &= 2 \times 1 + 0. \end{aligned}$$

Working backwards, we eventually find $1 = 17 \times 26 - 9 \times 49$.

Multiplying this equation through by 25 gives the equation $25 = 425 \times 26 - 225 \times 49$. Considering this equation modulo 49 shows that $25 \equiv 425 \times 26 \equiv 33 \times 26 \pmod{49}$.

So the general solution is $x \equiv 33 \pmod{49}$, or in the original modulus, we have $x \equiv 33, 82, 131, 180, \text{or } 229 \pmod{245}$.

Solving linear congruences – Example 3

Example. Solve $130x \equiv 125 \pmod{245}$.

Alternative solution. We have

$$\begin{aligned}
130x &\equiv 125 \pmod{245}, \\
26x &\equiv 25 \pmod{49} && \text{(since } 5 \mid 245\text{)}, \\
75x &\equiv 25 \pmod{49}, \\
3x &\equiv 1 \pmod{49} && \text{(since } \gcd(25, 49) = 1\text{)}, \\
3x &\equiv -48 \pmod{49}, \\
x &\equiv -16 \pmod{49} && \text{(since } \gcd(3, 49) = 1\text{)}, \\
x &\equiv 33 \pmod{49}.
\end{aligned}$$

So the general solution is $x \equiv 33 \pmod{49}$, or in the original modulus, we have $x \equiv 33, 82, 131, 180, \text{or } 229 \pmod{245}$.

Note that this method is much more efficient, but is reliant on finding useful substitutions and is not guaranteed to work efficiently in general.

Multiplicative inverses

Definition. The (multiplicative) inverse of an integer x modulo m (if it exists) is the integer y for which $0 \leq y < m$ and $xy \equiv 1 \pmod{m}$.

Notation. If it exists, we write the inverse of x modulo m as $x^{-1} \bmod m$.

For example, the multiplicative inverse of 3 modulo 7 is 5, since $3 \times 5 = 15 \equiv 1 \pmod{7}$. So $3^{-1} \equiv 5 \pmod{7}$. Similarly, we can find:

x	0	1	2	3	4	5	6
$x^{-1} \bmod 7$	none	1	4	5	2	3	6

Example. Find the multiplicative inverse of 26 modulo 49.

Solution. We want to solve $26x \equiv 1 \pmod{49}$. From the previous example, we saw via the (reversed) Euclidean algorithm that $1 = 17 \times 26 - 9 \times 49$, so $26 \times 17 \equiv 1 \pmod{49}$, meaning that $26^{-1} \equiv 17 \pmod{49}$.

When given the general linear congruence $ax \equiv c \pmod{m}$, if the multiplicative inverse of a exists, we can multiply both sides of the congruence by this value a^{-1}, giving $x \equiv a^{-1}c \pmod{m}$.

If the multiplicative inverse of a does not exist, either there is no solution to the congruence, or $\gcd(a, m) \mid c$, in which case dividing the whole congruence through by $\gcd(a, m)$ will produce a new congruence that we can solve by repeating the above approach.