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.

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

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{9}$.
Solution.

Linear congruences – Using rules of modular arithmetic

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

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

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{9}$.
Solution.

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.

Solving linear congruences – Example 2

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

Solution.

Solving linear congruences – Example 3

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

Solution.

Solving linear congruences – Example 3

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

Alternative approach.

Solving linear congruences – Example 3

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

Alternative solution.

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
$x^{-1} \bmod 7$							

Example. Find the multiplicative inverse of 26 modulo 49.

Solution.

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.