Solving Modular Equations

Three types of equations

1. Equations in one variable

$$4x \equiv 2 \mod 5$$
$$7x \equiv 1 \mod 4$$
$$13x \equiv 12 \mod 71$$

2. Simultaneous equations

$$4x \equiv 2 \mod 5 \quad \text{and}$$
$$7x \equiv 1 \mod 4$$

Three types of equations

❸ Simultaneous equations in two variables

$$4x + y \equiv 2 \mod 5$$
$$3x + 2y \equiv 3 \mod 5$$

❹ Other equations★

$$x + \sqrt{x} \equiv 1 \mod 3$$
$$x^2 + y^2 \equiv -1 \mod 7$$

Equations in one variable

1 Equations in one variable

- For an equation $ax = b \mod n$ there is no solution unless $(a, n) \mid b$
- We can determine this via the euclidean gcd algorithm.
- If $(a, n) \mid b$ then the solution is unique mod $n/(a,b)$ and can be found by solving

$$ax - yn = b$$

as a linear diophantine equation.

Equations in one variable

❶ Example

- Solve $15x = 117 \mod 333$
- Via the euclidean gcd algorithm we have

$$(15,333) = (15,22 \times 15 + 3) = (15,3) = 3$$

- So since $3 \mid 117$, the solution is unique.

Equations in one variable

❶ Example

- We could divide now by 3.
- Via the euclidean gcd algorithm we have

$$5x \equiv 39 \mod 111$$

- This means we should solve

$$5x - 111y = 39$$

Equations in one variable

1 Example

- This means we should solve

$$5x - 111y = 39$$

- Use euclidean gcd to write

$$1 = 111 - 22 \times 5$$

- This gives the particular solution

$$x = -22 \times 39$$
$$y = -39$$

Equations in one variable

❶ Example

- The solution to the original equation was unique so

$$\begin{aligned} x &\equiv -22 \times 39 \mod 111 \\ &\equiv -39 - 21 \times 39 \\ &\equiv 72 - 7 \times 117 \\ &\equiv 72 - 7 \times 6 \\ &\equiv 30 \end{aligned}$$

Simultaneous equations

❷ Simultaneous equations

- To solve for $(m,n) = 1$

$$ax \equiv b \mod m$$
$$cx \equiv d \mod n$$

the solution is unique mod mn if each individual equation has a solution – meaning

$$(a,m) \mid b \quad \text{and} \quad (c,n) \mid d$$

Simultaneous equations

❷ Simultaneous equations

- Solve the equations individually, so that

$$x \equiv x_0 \bmod m \quad \text{and} \quad x \equiv x_1 \bmod n$$

- Then

$$x = x_0 + k_0 m \qquad x = x_1 + k_1 n$$

- Solve the diophantine equation

$$k_0 m - k_1 n = x_1 - x_0$$

Simultaneous equations

❷ Example

- Solve

$$3x \equiv 2 \bmod 7 \quad \text{and} \quad 3x \equiv 2 \bmod 8$$

- The individual solutions are

$$x = 3 + 7k_0 \qquad x = 6 + 8k_1$$

- Now we solve

$$7k_0 - 8k_1 = 3 \quad \text{so} \quad k_0 = 5, k_1 = 4$$

- Conclude $x = 38 \mod 56$

Simultaneous equations in two variables

❸ Simultaneous equations in two variables

- We want to solve

$$cx + ey \equiv a \bmod n \quad \text{and} \quad dx + fy \equiv b \bmod n$$

- The solution is unique if $(cf - de, n) = 1$ in which case it is sufficient to solve individually

$$(cf - de)x \equiv af - de \quad \text{and} \quad (cf - de)y = bc - ad$$

Simultaneous equations in two variables

❸ Example

- Solve

$$x + y \equiv 1 \bmod 19 \quad \text{and} \quad 7x + 17y \equiv 0 \bmod 19$$

- We have $(cf - de, n) = (10,19) = 1$ so solution is unique. Now we solve

$$10x \equiv 17 \quad \text{and} \quad 10y \equiv -7$$

and the solutions are

$$x = 15 \qquad y = 5$$

Other equations

4 Example

- Solve

$$x^2 \equiv -1 \mod 11$$

- We want x such that

$$x^2 \in \{10,21,32,43,54,65,76,87,98,109,120\}$$

not possible so no solution.