Quick Review

- Exponents behave nicely in modular arithmetic (e.g. a^x is bounded, periodic).
  - ↳ Can be computed by iteratively squaring
- We can use inverses to solve linear congruences
  - ↳ Can be computed using EGCD
- We can use CRT to solve systems of congruences
  - ↳ Knowledge of x mod a bunch of small, coprime numbers gives us knowledge of x mod their product.
  - ↳ Some nice parallels w/ projections in linear algebra

Modular Practice

3A #1

Solve the following for x and/or y:

(a) $9x + 5 \equiv 7 \pmod{11}$

(b) Show that $3x + 15 \equiv 4 \pmod{21}$ does not have a solution.

(c) $3x + 2y \equiv 0 \pmod 7$
$2x + y \equiv 4 \pmod 7$

(d) $13^{2019} \equiv x \pmod{12}$

(e) $7^{21} \equiv x \pmod{11}$

When / Why Can We Use CRT?

3A #2

Let $a_1, \ldots, a_n, m_1, \ldots, m_n$ be integers such that $m_i > 1$ $\forall i$ and $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. (In other words, the m_i are pairwise relatively prime). Let $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ and consider the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

(a) Show that x is unique modulo m.

(b) Suppose the m_i's were not pairwise relatively prime. Is it guaranteed that a solution exists?

(c) Assume the m_i's were not pairwise relatively prime and a solution exists. Is that solution guaranteed to be unique mod m?

Mechanical CRT

3A # 3

In this problem, we will solve

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 4 \pmod 7$$

(a) Find $(5 \cdot 7)^{-1} \bmod 3$.

(b) What is the smallest $a > 0$ such that $5 \mid a$, $7 \mid a$, and $a \equiv 2 \pmod 3$?

(c) Find $(3 \cdot 7)^{-1} \bmod 5$.

(d) What is the smallest $b > 0$ such that $3 \mid b$, $7 \mid b$, and $b \equiv 3 \pmod 5$?

(e) Find ~~the~~ $(3 \cdot 5)^{-1} \bmod 7$.

(f) What is the smallest $c > 0$ such that $3 \mid c$, $5 \mid c$, and $c \equiv 4 \pmod 7$?

(g) Solve the system using what you've calculated.