Discussion 3A

CS 70, Summer 2024

1 Chinese Remainder Theorem

(a) $x = a + 3b + 4c$ solves the system.

(b) Let $a = (7 \cdot 11)j$ for some $j \in \mathbb{Z}$. We need $a \equiv 1 \pmod 3$, so

$$a \equiv (7 \cdot 11)j \equiv 2j \equiv 1 \pmod 3.$$

So j is an inverse of 2 modulo 3. We can use $j = 2^{-1} \bmod 3 = 2$. So $a = 77 \cdot 2 = 154$.

(c) Let $b = (3 \cdot 11)k$ for some $k \in \mathbb{Z}$. We need $b \equiv 1 \pmod 7$, so

$$b \equiv (3 \cdot 11)k \equiv 5k \equiv 1 \pmod 7.$$

So k is an inverse of 5 modulo 7. We can use $k = 5^{-1} \bmod 7 = 3$. So $b = 33 \cdot 3 = 99$.

(d) Let $c = (3 \cdot 7)\ell$ for some $\ell \in \mathbb{Z}$. We need $c \equiv 1 \pmod{11}$, so

$$c \equiv (3 \cdot 7)\ell \equiv 10\ell \pmod{11}.$$

So ℓ is an inverse of 10 modulo 11. We can use $\ell = 10^{-1} \bmod 11 = 10$. So $c = 21 \cdot 10 = 210$.

(e) Using parts **(a)** through **(d)**, our solution is

$$x = a + 3b + 4c = 154 + 3(99) + 4(210).$$

By Chinese remainder theorem, all solutions are congruent modulo $3 \cdot 7 \cdot 11 = 231$. So we can find the remainder of our answer modulo 231 to get the smallest positive integer solution.

$$x \equiv 154 + 3(99) + 4(210) \equiv 136 \pmod{231}.$$

The smallest positive integer solution is 136.

2 Fermat's Littler Theorem

(a) **Base case**. $n = 0$. Then $(a^n)^{-1} \equiv (a^0)^{-1} \equiv 1^{-1} \equiv 1 \equiv (a^{-1})^0 \pmod m$.

Induction case.

Induction hypothesis. Suppose that for some $n \in \mathbb{N}$ we have that $(a^n)^{-1} \equiv (a^{-1})^n \pmod m$.

Induction step. Consider $(a^{n+1})^{-1}$. Apply the definition of an inverse.

$$\begin{aligned}
(a^{n+1})^{-1}a^{n+1} &\equiv 1 && \pmod m \\
(a^{n+1})^{-1} \cdot a \cdot a^n &\equiv 1 && \pmod m \\
(a^{n+1})^{-1}a &\equiv (a^n)^{-1} && \pmod m \\
(a^{n+1})^{-1} &\equiv (a^n)^{-1}a^{-1} && \pmod m \\
(a^{n+1})^{-1} &\equiv (a^{-1})^n a^{-1} && \pmod m && \text{by the induction hypothesis} \\
(a^{n+1})^{-1} &\equiv (a^{-1})^{n+1} && \pmod m.
\end{aligned}$$

By the principle of mathematical induction, we have shown that for any $n \in \mathbb{N}$, $(a^n)^{-1} \equiv (a^{-1})^n \pmod m$.

(b) Each of the terms of the sequence must be in the set $\{1, \ldots, m-1\}$. There are m terms in the sequence and $m-1$ values each term in the sequence could take on. So some term in the sequence must repeat a value by the pigeonhole principle.

(c) Apply exponent rules and **(a)**.

$$\begin{aligned}
a^{j-i} &\equiv a^j a^{-i} && \pmod m \\
&\equiv a^j (a^i)^{-1} && \pmod m \\
&\equiv a^j (a^j)^{-1} && \pmod m && a^j \equiv a^i \pmod m \\
&\equiv 1.
\end{aligned}$$

(d) Therefore $a^{j-i} \cdot a^{-1} \equiv 1 \cdot a^{-1} \equiv a^{-1} \pmod{m}$, so $a^{j-i-1} \equiv a^{-1} \pmod{m}$.

3 Party Trick

(a) To find the last digit of a positive number, we can find its remainder when dividing by 10. So we use a modulus of 10.

(b) By exponent rules,

$$7^{482} \equiv 1^{482} \equiv 1 \pmod{2}.$$

(c) By exponent rules and Fermat's little theorem,

$$7^{482} \equiv 2^{482} \equiv (2^4)^{120} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod{5}.$$

(d) Consider the system of linear congruences

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 4 \pmod{5}. \end{aligned}$$

A solution is

$$x = 1 \cdot (5 \cdot (5^{-1} \bmod 2)) + 4 \cdot (2 \cdot (2^{-1} \bmod 5)) = 1 \cdot (5 \cdot 1) + 4 \cdot (2 \cdot 3) = 5 + 24 = 29.$$

Note that by parts **(b)** and **(c)**,

$$\begin{aligned} 7^{482} &\equiv 1 \pmod{2} \\ 7^{482} &\equiv 4 \pmod{5}, \end{aligned}$$

so 7^{482} is also a solution to the congruences. By the Chinese remainder theorem, all solutions are congruent modulo $2 \cdot 5 = 10$. Therefore

$$7^{482} \equiv 29 \equiv 9 \pmod{10}.$$

So the last digit of 7^{482} is 9.