HW01 Solution

Prob 3: Elts of $\{0, 1, \ldots, 20\}$ with mult invs mod 21

Prob 3: Elts of $\{0, 1, \ldots, 20\}$ with mult invs mod 21

SOLUTION: Only elts rel prime to 21 have mult invs.

n	$n^{-1} \pmod{21}$
1	1 obvious
2	11 easy to guess
4	16 Since $4 \times 5 \equiv 20 \equiv -1$ we know $-5 \equiv 16$ works
5	17 Since $5 \times 4 \equiv 20 \equiv -1$ we know thta $-4 \equiv 17$ works
8	8 Looked at numbers $\equiv 1 \pmod{21}$: 22, 43, 64 OH!
10	19 Since $10 \times 2 \equiv 20 \equiv -1$ we know that $-2 \equiv 19$ works
11	2 OH, already know $2 \times 11 \equiv 1$
13	13We did last. 13 was never an inverse, so now it is
16	4 OH, already know $4 \times 16 \equiv 1$
17	5 OH, already know $5 \times 17 \equiv 1$
19	10 OH, already know $10 \times 19 \equiv 1$
20	20OH, $20 \equiv -1$ so $20 \times 20 \equiv 1$

Prob 4a: Pattern of $10^i \pmod{14}$

Prob 4a: Pattern of $10^i \pmod{14}$

$$10^0 \equiv 1 \pmod{14}$$
$$10^1 \equiv -4 \equiv 10 \pmod{14}$$
$$10^2 \equiv 2 \pmod{14}$$
$$10^3 \equiv 6 \pmod{14}$$
$$10^4 \equiv 4 \pmod{14}$$
$$10^5 \equiv 12 \pmod{14}$$
$$10^6 \equiv 8 \pmod{14}$$
$$10^7 \equiv -4 \equiv 10 \pmod{14}$$

Pattern on next slide

Prob 4a: Pattern of 10^i (mod 14) (cont)

Prob 4a: Pattern of 10^i (mod 14) (cont)

$$10^n \equiv \begin{cases} 1 & \text{if } n = 0 \\ 10 & \text{if } n \geq 1 \land n \bmod 6 = 1 \\ 2 & \text{if } n \geq 1 \land n \bmod 6 = 2 \\ 6 & \text{if } n \geq 1 \land n \bmod 6 = 3 \\ 4 & \text{if } n \geq 1 \land n \bmod 6 = 4 \\ 12 & \text{if } n \geq 1 \land n \bmod 6 = 5 \\ 8 & \text{if } n \geq 1 \land n \bmod 6 = 0 \end{cases}$$

Prob 4b: "Trick" for Mod 14

We can get the trick by replacing 10^i with the pattern that we found from the previous problem

Prob 4b: "Trick" for Mod 14

We can get the trick by replacing 10^i with the pattern that we found from the previous problem

The number $a_n a_{n-1} a_{n-2} \cdots a_0$ is $\equiv$ to the following $\pmod{14}$.

$$\begin{array}{lllllll} a_0 & +a_1(10) & +a_2(2) & +a_3(6) & +a_4(4) & +a_5(12) & +a_6(8) \\ & +a_7(10) & +a_8(2) & +a_9(6) & +a_{10}(4) & +a_{11}(12) & +a_{12}(8) \\ & +a_{13}(10) & +a_{14}(2) & +a_{15}(6) & +a_{16}(4) & +a_{17}(12) & +a_{18}(8) \\ & +\vdots & +\vdots & +\vdots & +\vdots & +\vdots & +\vdots \end{array}$$

Prob 4c: The DFA for Mod 14. Intuition

We need to keep track of the following:

Prob 4c: The DFA for Mod 14. Intuition

We need to keep track of the following:

1. Whether the digit is (1) the 0th digit or not

Prob 4c: The DFA for Mod 14. Intuition

We need to keep track of the following:

1. Whether the digit is (1) the 0th digit or not
2. If not then
   is it the 0th digit mod 6 (so 6th or 12th or . . .) OR
   is it the 1th digit mod 6 (so 1st or 7th or 13th or . . .) OR
   ⋮
   is it the 5th digit mod 6 (so 5th of 11th or . . .) OR

Prob 4c: The DFA for Mod 14. Intuition

We need to keep track of the following:

1. Whether the digit is (1) the 0th digit or not
2. If not then
   is it the 0th digit mod 6 (so 6th or 12th or . . .) OR
   is it the 1th digit mod 6 (so 1st or 7th or 13th or . . .) OR
   $\vdots$
   is it the 5th digit mod 6 (so 5th of 11th or . . .) OR
3. The weighted sum mod 14:

$$\begin{array}{lllllll} a_0 & +a_1(10) & +a_2(2) & +a_3(6) & +a_4(4) & +a_5(12) & +a_6(8 \\ & +a_7(10) & +a_8(2) & +a_9(6) & +a_{10}(4) & +a_{11}(12) & +a_{12}(8 \\ & +a_{13}(10) & +a_{14}(2) & +a_{15}(6) & +a_{16}(4) & +a_{17}(12) & +a_{18}(8 \\ & +\vdots & +\vdots & +\vdots & +\vdots & +\vdots & +\vdots \end{array}$$

Prob 4c: The DFA for Mod 14. Formal Set Up

Prob 4c: The DFA for Mod 14. Formal Set Up

1. States are $\{s\} \cup \{0, 1, \cdots, 5\} \times \{0, 1, \ldots, 13\}$.

Prob 4c: The DFA for Mod 14. Formal Set Up

1. States are $\{s\} \cup \{0, 1, \cdots, 5\} \times \{0, 1, \ldots, 13\}$.
2. s is start state.

Prob 4c: The DFA for Mod 14. Formal Set Up

1. States are $\{s\} \cup \{0, 1, \cdots, 5\} \times \{0, 1, \ldots, 13\}$.
2. s is start state.
3. First coordinate is position mod 6 (except 0th place).

Prob 4c: The DFA for Mod 14. Formal Set Up

1. States are $\{s\} \cup \{0, 1, \cdots, 5\} \times \{0, 1, \ldots, 13\}$.
2. s is start state.
3. First coordinate is position mod 6 (except 0th place).
4. Second is the running weighted sum mod 14.

Prob 4c: The DFA for Mod 14. Formal Set Up

1. States are $\{s\} \cup \{0, 1, \cdots, 5\} \times \{0, 1, \ldots, 13\}$.
2. s is start state.
3. First coordinate is position mod 6 (except 0th place).
4. Second is the running weighted sum mod 14.
5. The final states are $(i, 5)$ and $(j, 7)$ for all $i, j \in \{0, 1, \cdots, 5\}$.

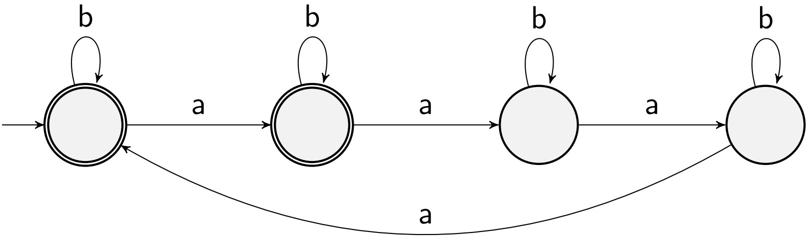
Prob 4c: The DFA for Mod 14. Transition Table

Prob 4c: The DFA for Mod 14. Transition Table

The transition table is below. In the table $0 \le x \le 13$.

State	Symbol	Next State
s	σ	$(1, \sigma)$
$(0, x)$	σ	$(1, x + 8\sigma \pmod{14})$
$(1, x)$	σ	$(1, x + 10\sigma \pmod{14})$
$(2, x)$	σ	$(3, x + 2\sigma \pmod{14})$
$(3, x)$	σ	$(4, x + 6\sigma \pmod{14})$
$(4, x)$	σ	$(5, x + 4\sigma \pmod{14})$
$(5, x)$	σ	$(0, x + 12\sigma \pmod{14})$

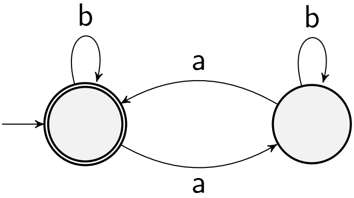
Prob 5: DFA for $\{w \mid \#_a(w) \equiv 0, 1 \pmod 4\}$



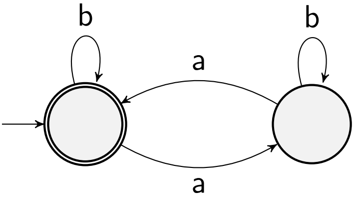
This has 4 states.

Prob 5: DFA for $\{w \mid \#_a(w) \equiv 0, 2 \pmod 4\}$

Prob 5: DFA for $\{w \mid \#_a(w) \equiv 0, 2 \pmod{4}\}$



Prob 5: DFA for $\{w \mid \#_a(w) \equiv 0, 2 \pmod 4\}$



This DFA has 2 states.