HW 8 CMSC 452. Morally Due April 3
SOLUTIONS

1. (5 points) What is your name? Write it clearly. Staple the HW.

2. (0 points, but you may want to use this on some of the problems.)

   (a) Look at `https://planetcalc.com/3311/` which is a website that has a calculator that computes mod inverses; calculate a few things to get a sense of what it can do.

   (b) Use Google to find things like $100 \pmod 7$. Just type in '100 mod 7'

3. (25 points) Show that:

   (a) There DOES NOT EXIST $c, d \in \mathsf{N}$ such that $719 = 19c + 41d$. (HINT: Assume $719 = 19c+41c$. Them mod the equation mod 41. Then multiply both sides by 13. Why 13? Because $19 \times 13 \equiv 1 \pmod{41}$. Use this!)

   (b) For every $n \geq 720$ there DOES EXIST $c, d \in \mathsf{N}$ such that $n = 19c + 41d$. (HINT: Factor the following numbers: 246, 247, 532, 533)

   SOLUTION TO PROBLEM THREE

   3.a) Assume, by way of contradiction:

$$719 = 19c + 41d$$

   Take this mod 41 to get

$$719 \equiv 19c \pmod{41}$$

   Using GOOGLE, I found that

$$719 \equiv 22 \pmod{41}$$

   So we have

$$22 \equiv 19c \pmod{41}$$

NOW, I want the inverse of 19 mod 41. The website tells me it's 13. Multiply both sides by 13.

$$22 \times 13 \equiv 19 \times 13 \times c \pmod{41}$$

$$22 \times 13 \equiv c \pmod{23}$$

Using GOOGLE, I found out that

$$22 \times 13 \equiv 40 \pmod{41}$$

So we have

$$c \equiv 40 \pmod{41}.$$

Therefore $c \geq 40$. Hence

$19c + 41d \geq 19 * 40 = 760 > 719$.

Therefore 719 cannot be written as a sum of 19's and 41's.

3.b) We prove this by induction on n.

Base Case: $720 = 19 \times 12 + 41 \times 12$

Ind. Hyp: Assume that $n \geq 721$ and that $(\exists c, d)[n = 19c + 41d]$.

$$n = 19c + 41d$$

I need some multiple of 19 to be one more than a multiple of 41.

I need some multiple of 41 to be one more than a multiple of 19.

Multiples of 19:

19, 38, 57, 76, 95,

114, 133, 152, 171, 190,

209, 228, 247*, 266, 285,

304, 323, 342, 361, 380,

399, 418, 437, 456, 475, 494,

513, 532**, 551, 570,

Mult of 41:

41, 82, 123, 164, 205,

246*, 287, 328, 369, 410,

451, 492, 533**, 574,

We note that

$247 = 13 \times 19$, $246 = 6 \times 41$. NOTE: if want to use this then you need to subtract 6 41's and add 13 19's. So you need to have 6 41's to subtract.

$532 = 28 \times 19$, $533 = 13 \times 41$ NOTE: if want to use this then you need to subtract 28 19's and add 13 19's. So you need to have 28 19's to subtract.

Case 1: $c \geq 28$. Then

$$n = 19c + 41d$$

$$n + 13 \times 41 - 28 \times 19 = 19(c - 28) + 41(d + 13)$$

$$n + 1 = 19(c - 28) + 41(d + 13)$$

Case 2: $d \geq 6$. Then

$$n = 19c + 41d$$

$$n + 13 \times 19 - 6 \times 41 = 19(c + 13) + 41(d - 6)$$

$$n + 1 = 19(c + 13) + 41(d - 6)$$

Case 3: $c \leq 27$ and $d \leq 5$. Then

$n = 19c + 41d \leq 19 \times 27 + 41 \times 5718 < 721$. So this case cannot occur.

4. (25 points) Find a set of primes whose product is ≥ 720 and whose sum is ≤ 30.

SOLUTION TO PROBLEM FOUR

We first try the first few primes until the product is big enough

$2 \times 3 \times 5 \times 7 = 210$. Too small

$2 \times 3 \times 5 \times 7 \times 11 = 2310$. Big enough.

The sum is $2 + 3 + 5 + 7 + 11 = 28$.

By trial and error we can show that

$2 \times 5 \times 7 \times 11 = 770$. Big enough.

The sum is $2 + 5 + 7 + 11 = 25$.

We show we cannot do any better. We do this by cases based on the largest

Case 1: Largest prime used is ≥ 29. Then sum is ≥ 25.

Case 2: Largest prime used is 23. To do better than 25 the remaming primes have to sum to ≤ 2 and have product $\geq \frac{720}{23} \sim 31$ The only sets of primes are $\{2\}$.

In all future cases we will not consider sets with sum ≤ 2 since we will need even bigger products then 31.

Case 3: Largest prime used is 19. To do better than 25 the remaining primes have to sum to ≤ 5 and have product $\geq \frac{720}{19} \sim 37$. The only possible sets of primes with sum ≤ 5 are

$\{3\}$, $\{5\}$, $\{2, 3\}$ which has product $6 < 37$.

In all future cases we will not consider sets with sum ≤ 5 since we will need even bigger products then 37.

Case 4: Largest prime used is 17. To do better than 25 the remaining primes have to sum to ≤ 7 and product $\ge \frac{720}{17} \sim 42$. The only possible sets of primes with sum ≤ 7 are

$\{7\}$, $\{2,5\}$.

All of the products are < 42.

In all future cases we will not consider sets with sum ≤ 7 since we will need even bigger products then 42.

Case 5: Largest prime used is 13. To do better than 25 the remaining primes have to sum to ≤ 11 and product $\ge \frac{720}{13} \sim 55$. The only possible sets of primes with sum ≤ 11 are

$\{11\}$, $\{2,7\}$, $\{3,5\}$, $\{3,7\}$, $\{2,3,5\}$.

All of the products are < 55.

Case 6: Largest prime used is 11. To do better than 25 the remaining primes have to sum to ≤ 13 and product $\ge \frac{720}{11} \sim 65$. The only possible sets of primes with sum ≤ 13 are

$\{3\}$, $\{2,11\}$, $\{2,3,7\}$.

All of the products are < 65.

Case 7: Largest prime used is 7. The you cannot get the product large enough since $2 \times 3 \times 5 \times 7 = 210 < 720$.

$\{13\}$, $\{2,11\}$, $\{2,3,7\}$.

5. (25 points) Use the answers Questions 4 and 5 to create a small NFA for $L = \{a^i : i \ne 719\}$. How many states does it have?

   SOLUTION TO PROBLEM FIVE

   Note that

   $719 \equiv 1 \pmod 2$

   $719 \equiv 4 \pmod 5$

   $719 \equiv 5 \pmod 7$

   $719 \equiv 4 \pmod{11}$

   Let M be the NFA that has an e transition to each of the following:

- An accept state that has one loop of size 41 and a shortcut chord so that the loop can also (nondet) come back to the start state after 19. Only the first state is an accept. This branch (1) will accept $\{a^i : i \geq 720\}$, (2) will not accept a^{719}, (3) we have not comment on what else it accepts, (4) M has 41 states (not including the start state).
- A loop of size 2 such that only $\{a^i : i \not\equiv 1 \pmod 2\}$ is accepted. 2 states.
- A loop of size 5 such that only $\{a^i : i \not\equiv 4 \pmod 5\}$ is accepted. 5 states.
- A loop of size 7 such that only $\{a^i : i \not\equiv 5 \pmod 7\}$ is accepted. 7 states.
- A loop of size 13 such that only $\{a^i : i \not\equiv 4 \pmod{11}\}$ is accepted. 11 states.

The total number of states is $41 + 2 + 5 + 7 + 11 + 1 = 67$. (The $+1$ is for the start state.)

The first branch accepts all $\{a^i : i \geq 720\}$.

The only string rejected by all the branches is a^i such that

$i \leq 719$

$i \equiv 1 \pmod 2$

$i \equiv 4 \pmod 5$

$i \equiv 5 \pmod 7$

$i \equiv 11 \pmod{11}$

We know that a^{351} satisfies the criteria. Since $719 < 2 \times 5 \times 7 \times 11$, it is the only such string.

6. (25 points) (HINT: Use the results from prior problems for this problem. Do not start from scratch.) Let $L_n = \{a^i : i \neq n\}$

   (a) Create a small NFA for L_{720}. How many states does it have?

   (b) For $2 \leq x \leq 10$ create a small NFA for L_{719+x}. How many states does it have (as a function on x). If you draw it you may use ...

(c) (Think about, no points) For large x the technique you used in the last part would not work. Why is that and when does it happen?

SOLUTION TO PROBLEM SIX

We just sketch it: Take the same NFA for L_{719} and

1) ADD x states before going into the loop, so that rather than accept all $\{a^y : y \geq 720\}$ you accept all $\{a^y : y \geq 720 + x\}$. This only adds x states.

2) Adjust the mods appropriately. This adds NO states as it just changes which states are final and non-final.

Recall that the product of the mods was 760. If $719 + x > 760$ then the technique breaks down- thought not seriously, you would add another prime loop. However, better off finding a slightly bigger big loop.