HW 8 CMSC 452. Morally Due April 11
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.) (1) 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. DO NOT hand anything in for this problem. (2) Use GOOGLE to find thinks like $100 \pmod 7$. Just type in '100 mod 7' DO NOT hand anything in for this problem.

3. (20 points) Show that

   (a) There DOES NOT EXIST $c, d \in \mathsf{N}$ such that $351 = 17c + 23d$.

   (b) For every $n \geq 352$ there DOES EXIST $c, d \in \mathsf{N}$ such that $n = 17c + 23d$.

   SOLUTION TO PROBLEM THREE

   3.a) Assume, by way of contradiction:

$$351 = 17c + 23d$$

   Take this mod 23 to get

$$351 \equiv 17c \pmod{23}$$

   Using GOOGLE I found that

$$351 \equiv 6 \pmod{23}$$

   So we have

$$6 \equiv 17c \pmod{23}$$

   NOW I want the inverse of 17 mod 23. The website tells me its 19. Multiply both sides by 19

$$6 \times 19 \equiv 17 \times 19 \times c \pmod{23}$$

$$6 \times 19 \equiv c \pmod{23}$$

Using GOOGLE I found out that

$$6 \times 19 \equiv 22 \pmod{23}$$

So we have

$$c \equiv 22 \pmod{23}.$$

Therefore $c \geq 22$. Hence
$17c + 23d \geq 17 * 23 = 391 > 351$.
Therefore 351 cannot be written as a sum of 17's and 23's.

3.b) We prove this by induction on n.
Base Case: $352 = 17 \times 18 + 23 \times 2$
Ind. Hyp: Assume that $n \geq 352$ and that $(\exists c, d)[n = 17c + 23d]$.

$$n = 17c + 23d$$

I need some mult of 17 to be one more than a mult of 23.
I need some mult of 23 to be one more than a mult of 17.
So I wrote down mults of both:

Mults of 17:

17, 34, 51, 68, 85,

102, 119, 136, 153, 170,

187, 204, 221, 238, 255,

272, 289, 306, 323, 340.

Mult of 23:

23, 46, 69, 92, 115,

138, 161, 184, 207, 230,

253, 276, 299, 322, 345.

AH-HA: I spot $68, 69$ so $23 \times 3 - 17 \times 4 = 1$.

AH-HA: I spot $322, 323$ so $17 \times 19 - 23 \times 14 = 1$.

Case 1: $c \geq 4$. Then

$$n+1 = 17c+23d+1 = 17c+23d+23\times 3-17\times 4 = 17(c-4)+23(d+3).$$

Case 2: $d \geq 14$. Then

$$n+1 = 17c+23d+1 = 17c+23d+17\times 19-23\times 14 = 17(c+19)+23(d-14).$$

Case 3: $c \leq 3$ and $d \leq 13$. Then

$n = 17c + 23d \leq 17 \times 3 + 23 \times 13 = 51 + 299 = 350 < 352$. So this case cannot occur.

4. (20 points) Find a set of primes whose product is ≥ 352 and whose sum is as small as possible.

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 $2 + 3 + 5 + 7 + 11 = 28$.

Can we do better?

By trial and error I found that $2, 3, 5, 13$ works since $2 \times 3 \times 5 \times 13 = 390 > 352$.

$2 + 3 + 5 + 13 = 23$. So, can we do better than 23 states?

We show we cannot by looking at the largest prime in use. Note that we cannot use 23 so the largest prime to try is 19.

Case 1: If we use 19 then in order to do better than 23 states we can only use 4 more states. Hence we can only use a set of primes in $\{2, 3\}$ that sum to ≤ 4 whose product is $\ge \frac{352}{19} = 18.5\ldots$. It is easy to see that no such set exists. SO using 19 DOES NOT WORK.

Case 2: If we use 17 then in order to do better than 23 states we can only use 5 more states. Hence we can only use, in addition to 17, a set of primes in $\{2, 3, 5\}$ that sum to ≤ 5 whose product is $\ge \frac{352}{17} = 20.7\ldots$. It is easy to see that no such set exists. SO using 17 DOES NOT WORK.

Case 3: If we use 13 then in order to better than 23 states we can only use 9 more states. Hence we can only use, in addition to 13, a set of primes in $\{2, 3, 5, 7\}$ that sum to ≤ 9 whose product is $\ge 27.07\ldots$. It is easy to see that no such set exists. SO using 13 DOES NOT WORK.

Case 4: If we use 11 then in order to beat 23 we can only use 11 more states. Hence we can only use, in addition to 11, a set of primes in $\{2, 3, 5, 7\}$ that sum to ≤ 11 whose product is ≥ 32. It is easy to see that no such set exists. SO using 13 DOES NOT WORK.

Case 5: If the largest primes used is ≤ 7 then the product is $\le 2 * 3 * 5 * 7 = 210 < 352$.

5. (20 points) Use the answers Questions 4 and 5 to create a small NFA for $L = \{a^i : i \ne 351\}$. How many states does it have?

SOLUTION TO PROBLEM FIVE

Note that

$351 \equiv 1 \pmod 2$

$351 \equiv 0 \pmod 3$

$351 \equiv 1 \pmod 5$

$351 \equiv 0 \pmod{13}$

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

- An accept state that has two loops- one of size 17, one of size 23. Only the first state is an accept. This branch (1) will accept $\{a^i : i \geq 352\}$, (2) will not accept a^{351}, (3) we have not comment on what else it accepts. $17 + 23 = 40$ states.
- A loop of size 2 such that only $\{a^i : i \not\equiv 1 \pmod 2\}$ is accepted. 2 states.
- A loop of size 3 such that only $\{a^i : i \not\equiv 0 \pmod 3\}$ is accepted. 3 states.
- A loop of size 5 such that only $\{a^i : i \not\equiv 1 \pmod 5\}$ is accepted. 5 states.
- A loop of size 13 such that only $\{a^i : i \not\equiv 0 \pmod{13}\}$ is accepted. 13 states.

The total number of states is $40 + 2 + 3 + 5 + 13 + 1 = 64$. (The $+1$ is for the start state.)

The first branch accepts all $\{a^i : i \geq 352\}$.

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

$i \leq 351$

$i \equiv 1 \pmod 2$

$i \equiv 0 \pmod 3$

$i \equiv 1 \pmod 5$

$i \equiv 0 \pmod{13}$

We know that a^{351} satisfies the criteria. Since $351 < 2 \times 3 \times 5 \times 13$, it is the only such string.

6. (20 points) Let $L_n = \{a^i : i \neq n\}$

   (a) Create a small NFA for L_{352}. How many states does it have?

(b) For all x create a small NFA for L_{351+x}. How many states does it have (as a function on x). If you draw it you may use .... NOTE- your NFA probably won't work if x gets too big- thats okay- but figure out for which x it DOES work.

SOLUTION TO PROBLEM SIX

6.a) Since $(\forall n \geq 352)(\exists c, d)[n = 17c + 23d]$

$(\forall n \geq 353)(\exists c, d)[n = 17c + 23d + 1]$

Also note that

$352 \equiv 0 \pmod 2)$

$352 \equiv 1 \pmod 3)$

$352 \equiv 2 \pmod 5)$

$352 \equiv 1 \pmod{13}$.

The NFA has branches from the start state:

- ONE state (a reject one) and THEN an accept state that has two loops- one of size 17, one of size 23. Only the first state is an accept. This branch (1) will accept $\{a^i : i \geq 353\}$, (2) will not accept a^{351}, (3) we have not comment on what else it accepts. $1 + 17 + 23 = 41$ states.
- A loop of size 2 such that only $\{a^i : i \not\equiv 0 \pmod 2\}$ is accepted. 2 states.
- A loop of size 3 such that only $\{a^i : i \not\equiv 1 \pmod 3\}$ is accepted. 3 states.
- A loop of size 5 such that only $\{a^i : i \not\equiv 2 \pmod 5\}$ is accepted. 5 states.
- A loop of size 13 such that only $\{a^i : i \not\equiv 1 \pmod{13}\}$ is accepted. 13 states.

The total number of states is $41 + 2 + 3 + 5 + 13 + 1 = 65$. (The +1 is for the start state.)

6.b) Similar to 6.1 except that we have x states in branch 1 and need to use different things mod 2,3,5,13. The total number of states is $40 + x + 2 + 3 + 5 + 13 + 1 = 65 + x$. (The +1 is for the start state.)

We can use mods 2,3,5,13 so long as $352 + x \le 2 * 3 * 5 * 13 = 390$. So $x \le 38$.

7. (20 points) (Use L_n from the last problem.)

   (a) Find a number α such that $310 \le \alpha \le 350$ and α cannot be written as a sum of 17's and 23's. Try to make α as large as possible.

   (b) Create a small NFA for L_α. How many states does it have? (this will be an actual number, since α was.)

SOLUTION TO PROBLEM SEVEN

7.a) We want

$$17c + 23d = \alpha$$

to not have as solution. Take the equation mod 23

$$17c \equiv \alpha \pmod{23}$$

The inverse of 17 mod 23 is 19. Multiply both sides by 19.

$$c \equiv 19\alpha \pmod{23}$$

We want c to be LARGE, so large that $17c > \alpha$.

So we want $19\alpha \pmod{23}$ to be large.

Lets try to make it 22.

$$19\alpha \equiv 22 \pmod{23}$$

The inverse of 19 mod 22 is 17 (I used that website) Multiply both sides by 17

$$\alpha \equiv 22 * 17 \equiv -17 \equiv 6 \pmod{23}$$

SO we want $\alpha \equiv 6 \pmod{23}$.

Try $\alpha = 328$.

NOW lets just start over again:

$$17c + 23d = 328$$

Mod 23 this is

$$17c \equiv 6 \pmod{23}$$

Mult both sides by 19

$$c \equiv 19 * 6 \equiv 22 \pmod{23}$$

$$17c + 23d \geq 17 * 22 + 0 = 374 > 328$$

SO there is no solution to $17c + 23d = 328$

7.b) We build a small NFA for L_{328}.

We need what 328 is $\equiv$ mod 2,3,5,13.

$328 \equiv 0 \pmod{2}$

$328 \equiv 1 \pmod{3}$

$328 \equiv 3 \pmod{5}$

$328 \equiv 3 \pmod{13}$

The NFA has several branches:

- An accept state that has two loops- one of size 17, one of size 23. Only the first state is an accept. This branch (1) will accept $\{a^i : i \geq 353\}$, (2) will not accept a^{328}, (3) we have not comment on what else it accepts. $1 + 17 + 23 = 41$ states.
- A loop of size 2 such that only $\{a^i : i \not\equiv 0 \pmod{2}\}$ is accepted. 2 states.
- A loop of size 3 such that only $\{a^i : i \not\equiv 1 \pmod{3}\}$ is accepted. 3 states.

- A loop of size 5 such that only $\{a^i : i \not\equiv 3 \pmod 5\}$ is accepted. 5 states.
- A loop of size 13 such that only $\{a^i : i \not\equiv 3 \pmod{13}\}$ is accepted. 13 states.

The total number of states is $41 + 2 + 3 + 5 + 13 + 1 = 65$. (The $+1$ is for the start state.)