Ma 6 PSET 2

Victoria Liu

October 27, 2020

Problem 1

We see that 2 is a Miller-Rabin witness for 1288119601. We factor $1288119601 - 1$ into $2^4 \cdot 80507475$. In other words, $s = 4$ and $d = 80507475$. We can write $80507475 = 2^{26} + 2^{23} + 2^{22} + 2^{19} + 2^{18} + 2^{14} + 2^{13} + 2^{12} + 2^9 + 2^6 + 2^4 + 2^1 + 2^0$, which will help with modular exponentiation since now we only have to exponentially modulate around $26 + 13$ times. We check our exponential modulation on Mathematica and see that:

$$2^{80507475} \equiv 95382061 \pmod{1288119601} \tag{1}$$

This means that we fail the first part of the Miller-Rabin primality test, where $a^d \equiv 1 \pmod{n}$ for a prime number n. So far, 2 is looking like a promising witness that 1288119601 is composite. In order to show that 1288119601 is composite, now we must fail the second part of the Miller-Rabin primarily test, which says that $\exists r$ where $0 \leq r < s$ such that $a^{2^r d} \equiv -1 \pmod{n}$. Since $s = 4$, we have $r = 0$, $r = 2$, and $r = 3$. Let's see the modular exponentiation when $r = 3$.

$$2^{161014950} \equiv 2066916 \pmod{1288119601} \tag{2}$$

This did not pass. What about for $r = 2$ and $r = 1$?

$$2^{322029900} \equiv 737154140 \pmod{1288119601} 2^{644059800} \equiv 745370093 \pmod{1288119601} \tag{3}$$

Clearly, for every $0 \leq r \leq 4$, $2^{2^r \cdot 80507475} \not\equiv -1 \pmod{1288119601}$. That's great. We have completely failed the Miller-Rabin primality test, with 2 as a witness.

Problem 2

2.a

Show that $n! \leq n^n$ for all natural number.

Proof. We do a proof by induction. I know that there is sometimes confusion over whether 0 is counted in the set of natural numbers, so I will just do two base cases of $n = 0$ and $n = 1$ to cover my "bases." For $n = 0$, $0! \leq 0^0$ because both sides are equal to 1. For $n = 1$, $1! \leq 1^1$ because both sides are again equal to 1. Thus the base case(s) hold.

Now, we assume that our statement is true for all numbers up to k, so $k! \leq k^k$. Then, we can multiply both sides by $k+1$ and manipulate both sides to show that the statement is also true for $k+1$:

$$(k+1) * k! \leq (k+1) * k^k \tag{4}$$

$$(k+1)! \leq (k+1) * (k+1)^k \tag{5}$$

$$(k+1)! \leq (k+1)^{k+1} \tag{6}$$

We know the second inequality is true because the function $y = x^a$ is strictly increasing when $a > 0$ and $x > 1$. By the third inequality, we have proved the statement for $k+1$, and our proof by induction is complete. QED

□

2.b

Show that $\left(1 + \frac{1}{k}\right)^k < \left(1 + \frac{1}{k+1}\right)^{k+1}$ for any natural number k.

Proof. We first note that this equality holds when $k = 1$. This is important because our proof won't rigorously cover the case of $k = 1$, but it's evident through substitution that the statement is true for $k = 1$.

We will do a direct proof by binomially expanding both sides of the inequality. Let's start with the left hand-side:

$$\left(1 + \frac{1}{k}\right)^k = \binom{k}{0} + \binom{k}{1} \cdot \frac{1}{k}^1 + \binom{k}{2} \cdot \frac{1}{k}^2 + \cdots + \binom{k}{k-1} \cdot \frac{1}{k}^{k-1} + \binom{k}{k} \cdot \frac{1}{k}^k \tag{7}$$

Let's write this more nicely with summation notation:

$$\left(1 + \frac{1}{k}\right)^k = \sum_{d=0}^{k} \binom{k}{d} \cdot \frac{1}{k}^d \tag{8}$$

Now, we can expand out each term of the summation in the following way:

$$\left(1+\frac{1}{k}\right)^k = \sum_{d=0}^{k} \frac{k!}{(k-d)!(d)!} \cdot \frac{1}{k^d} \tag{9}$$

$$\left(1+\frac{1}{k}\right)^k = \sum_{d=0}^{k} \frac{1}{d!} \cdot \frac{k}{k} \cdot \frac{k-1}{k} \cdots \frac{k-d+2}{k} \cdot \frac{k-d+1}{k} \tag{10}$$

$$\left(1+\frac{1}{k}\right)^k = \sum_{d=0}^{k} \frac{1}{d!} \cdot \left(1-\frac{0}{k}\right) \cdot \left(1-\frac{1}{k}\right) \cdots \left(1-\frac{d-2}{k}\right) \cdot \left(1-\frac{d-1}{k}\right) \tag{11}$$

This looks like we're getting somewhere. Let's do the same thing for the right hand side of the inequality:

$$\left(1+\frac{1}{k+1}\right)^{k+1} = \binom{k+1}{0} + \binom{k+1}{1} \cdot \frac{1}{k+1}^{1} + \cdots + \binom{k+1}{k} \cdot \frac{1}{k+1}^{k} + \binom{k+1}{k+1} \cdot \frac{1}{k+1}^{k+1} \tag{12}$$

$$\left(1+\frac{1}{k+1}\right)^{k+1} = \sum_{d=0}^{k+1} \binom{k+1}{d} \cdot \frac{1}{k+1}^{d} \tag{13}$$

$$\left(1+\frac{1}{k+1}\right)^{k+1} = \sum_{d=0}^{k+1} \frac{(k+1)!}{(k+1-d)!(d)!} \cdot \frac{1}{(k+1)^d} \tag{14}$$

$$\left(1+\frac{1}{k+1}\right)^{k+1} = \sum_{d=0}^{k+1} \frac{1}{d!} \cdot \frac{k+1}{k+1} \cdot \frac{k}{k+1} \cdots \frac{k-d+3}{k+1} \cdot \frac{k-d+2}{k+1} \tag{15}$$

$$\left(1+\frac{1}{k+1}\right)^{k+1} = \sum_{d=0}^{k+1} \frac{1}{d!} \cdot \left(1-\frac{0}{k+1}\right) \cdot \left(1-\frac{1}{k+1}\right) \cdots \left(1-\frac{d-2}{k+1}\right) \cdot \left(1-\frac{d-1}{k+1}\right) \tag{16}$$

$$\left(1+\frac{1}{k+1}\right)^{k+1} = \frac{1}{d!} \cdot \left(1-\frac{0}{k+1}\right) \cdots \left(1-\frac{k}{k+1}\right) + \sum_{d=0}^{k} \frac{1}{d!} \cdot \left(1-\frac{0}{k+1}\right) \cdot \left(1-\frac{1}{k+1}\right) \cdots \left(1-\frac{d-1}{k+1}\right) \tag{17}$$

The last two lines are related by taking out the $k+1^{st}$ term in the summation. In equation 17, we know that the $k+1^{st}$ term is positive because all the factors are greater than 0. Let's disregard this $k+1^{st}$ term for now, since we know that it will only help our proof and not hurt it. This will allow us to better compare equations 11 and 17. Now, we have k terms in each summation, and we see that each factor (as grouped in parentheses) of each addend in summation 11 has a one-to-one correlation with another factor (as grouped in parentheses) of each addend in summation 17. That was a mouthful, but basically the two equations are the exact same in terms of count and structure except for what is in the denominator; i.e. $\left(1-\frac{a}{k}\right)$ vs $\left(1-\frac{a}{k+1}\right)$ for $0 \leq a \leq d-1$. Since we have this one-to-one correspondence between the terms of the product, we can directly compare each term, and it is evident that $1 - \frac{a+1}{k}$ is greater than $1 - \frac{a}{k}$ for all $a < k$. This hand-wave-y proof suggests that:

$$\sum_{d=0}^{k} \frac{1}{d!} \cdot \left(1 - \frac{0}{k}\right) \cdot \left(1 - \frac{1}{k}\right) \cdots \left(1 - \frac{d-1}{k}\right) < \sum_{d=0}^{k} \frac{1}{d!} \cdot \left(1 - \frac{0}{k+1}\right) \cdot \left(1 - \frac{1}{k+1}\right) \cdots \left(1 - \frac{d-1}{k+1}\right) \tag{18}$$

I feel like the proof could end here, if we can accept inequality 18 as being logically true. Inequality 18 suggests that the RHS of 11 is less than the RHS of 17, and that $\left(1 + \frac{1}{k}\right)^k < \left(1 + \frac{1}{k+1}\right)^{k+1}$, thus completing our proof. So QED.

□

I'm not sure exactly how rigorous this proof has to be, so I will also include a section on proving 18: Let's try to prove 18 more rigorously. We follow the same line of logic as before, mainly that both the LHS and the RHS have a total of $k+1$ terms, and each subsequent term has an increasing number of factors of the form $1 - \frac{a}{k}$ or $1 - \frac{a}{k+1}$. We can ignore the $\frac{1}{d!}$ factor since they are the same between corresponding terms on the LHS and the RHS, and we can also ignore when $a = 0$ because that would just result in multiplying both sides by 1. Ignoring the two previous factors, each addend has an increasing number of factors, from 1 factor when $d = 1$ to $k-1$ factors when $d = k$. We will use induction on the number of factors, since we already know that the base case, where we have one factor, already holds for any $k \geq 2$. The base case is: $1 - \frac{a}{k} < 1 - \frac{a+1}{k}$ for all $0 < a < k$

Our general case is:

$$\prod_{a=1}^{n} \left(1 - \frac{a}{k}\right) < \prod_{a=1}^{n} \left(1 - \frac{a}{k+1}\right) \tag{19}$$

for $1 \leq n \leq k-1$.

We prove this with induction on n and let k be any number we'd like, subject to the constraint $2 \leq k$. Note that n is a proxy for the number of terms in 18. We've already shown the base case, so let's assume 19 holds true up to n = m. Then, we can write:

$$\prod_{a=1}^{m}\left(1-\frac{a}{k}\right) < \prod_{a=1}^{m}\left(1-\frac{a}{k+1}\right) \tag{20}$$

$$\left(1-\frac{m+1}{k}\right)\prod_{a=1}^{m}\left(1-\frac{a}{k}\right) < \left(1-\frac{m+1}{k}\right)\prod_{a=1}^{m}\left(1-\frac{a}{k+1}\right) \tag{21}$$

$$\left(1-\frac{m+1}{k}\right)\prod_{a=1}^{m}\left(1-\frac{a}{k}\right) < \left(1-\frac{m+2}{k+1}\right)\prod_{a=1}^{m}\left(1-\frac{a}{k+1}\right) \tag{22}$$

$$\prod_{a=1}^{m+1}\left(1-\frac{a}{k}\right) < \prod_{a=1}^{m+2}\left(1-\frac{a}{k+1}\right) \tag{23}$$

Thus, we have shown that inequality 19 is true by induction. By extension, inequality 19 mirrors inequality 18 and proves it rigorously. Now, we can say QED with less fear (refer to the previous explanation why 18 shows the inequality we are trying to prove in the problem).

2.c

Show that $n! > \frac{n^n}{e^n}$

Proof. We will prove this statement using induction. There is occasionally confusion about whether $0 \in \mathbb{N}$. Since this statement doesn't hold for $n = 0$, let's just say that $0 \notin \mathbb{N}$. So, our base case is $n = 1$, and the statement clearly holds because $1 > \frac{1}{e}$. Now, we assume that the statement is true up through $n = k$. Now let's manipulate our induction hypothesis:

$$k! > \frac{k^k}{e^k} \tag{24}$$

$$(k+1)\cdot k! > (k+1)\cdot\frac{k^k}{e^k} \tag{25}$$

$$(k+1)! > (k+1)\frac{k^k}{e^k}\cdot\frac{(k+1)^k}{(k+1)^k} \tag{26}$$

$$(k+1)! > \left(\frac{k}{k+1}\right)^k\cdot\frac{(k+1)^{k+1}}{e^k} \tag{27}$$

Before we go further, note that based on our definition of $e = \lim_{x\to\infty}\left(1+\frac{1}{x}\right)^x$ and our previous proof that $\left(1+\frac{1}{x}\right)^x < \left(1+\frac{1}{x+1}\right)^{x+1}$, we know that for any natural number x:

$$e \geq \left(1 + \frac{1}{x}\right)^{x} \tag{28}$$

$$e \geq \left(\frac{x+1}{x}\right)^{x} \tag{29}$$

Manipulating the equations, we get that

$$\frac{1}{e} \leq \left(\frac{x}{x+1}\right)^{x} \tag{30}$$

Great, let's substitute this back into inequality 27 to get:

$$(k+1)! > \frac{1}{e} \cdot \frac{(k+1)^{k+1}}{e^{k}} \tag{31}$$

$$(k+1)! > \frac{(k+1)^{k+1}}{e^{k+1}} \tag{32}$$

Ok, this is exactly what we wanted to show, that the statements holds true for $k+1$. By induction, we can now say that $n! > \frac{n^n}{e^n}$. QED

□

Problem 3

3.a

This is the same as $\frac{1}{\binom{47}{6}}$, which is:

$$\frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{47 \cdot 46 \cdot 45 \cdot 44 \cdot 43 \cdot 42} \tag{33}$$

Since we're in Jupyter Labs, let's just make our lives easier with the scipy function.

[1]:

```python
import scipy.special
#47 choose 6
combo_count = scipy.special.comb(47, 6)
print(combo_count, "combinations")
print(1 / combo_count, "chance")
```

```
10737573.0 combinations
9.313091515186905e-08 chance
```

We have a 1 in 10737573 chance of getting the right combination, or around $9.31 * 10^{-08}$ chance.

3.b

We calculate $\frac{1}{47\cdot46\cdot45\cdot44\cdot43\cdot42}$ to get: $\frac{1}{7731052560}$ chance (or around $1.29 * 10^{-10}$).

3.c

To find the total number of possible combinations, we multiply:

$$\binom{24}{3}\cdot\binom{23}{3} \tag{34}$$

We can get $\binom{24}{3}$ different ways of choosing 3 numbers from the first 24 numbers, and we can get $\binom{23}{3}$ different ways of choosing 3 numbers from the last 23 numbers. We multiply to get the total number of combinations. Then, we take the reciprocal, and we see we have a $\frac{1}{3584504}$ chance or $2.78 * 10^{-7}$ chance:

[2]:

```
combo_count = scipy.special.comb(24, 3) * scipy.special.comb(23, 3)
print(combo_count, "combinations")
print(1 / combo_count, "chance")
```

```
3584504.0 combinations
2.7897862577360775e-07 chance
```

3.d

Our chances of correctly guessing without any information is

$$\frac{1}{\binom{n}{6}} \tag{35}$$

Our chances of correctly guessing with the information is

$$\frac{1}{\binom{n/2}{3}\cdot\binom{n/2}{3}} \tag{36}$$

Our chances increase by this amount of times:

$$\frac{\frac{1}{\binom{n/2}{3}\cdot\binom{n/2}{3}} - \frac{1}{\binom{n}{6}}}{\frac{1}{\binom{n}{6}}} \tag{37}$$

Ok, now let's manipulate the expression to make it look nicer:

$$\frac{\binom{n}{6}}{\binom{n/2}{3} \cdot \binom{n/2}{3}} - 1 \tag{38}$$

$$\frac{\frac{n\cdot(n-1)\cdot(n-2)\cdot(n-3)\cdot(n-4)\cdot(n-5)}{6\cdot5\cdot4\cdot3\cdot2\cdot1}}{\frac{n\cdot(n-2)\cdot(n-4)\cdot n\cdot(n-2)\cdot(n-4)}{3!\cdot3!\cdot2^6}} - 1 \tag{39}$$

$$\frac{16}{5} \cdot \frac{(n-1)\cdot(n-3)\cdot(n-5)}{n\cdot(n-2)\cdot(n-4)} - 1 \tag{40}$$

Great, this is our final answer, in terms of how many times more likely our chances increased. To change to percentage, we would just multiply this by 100. It seems like a reasonably simple calculation, given any n. Let's see if our calculation matches up for a random case $n = 46$.

[3]:

```
#actual amount our chances increase by
prob_no_info = 1 / scipy.special.comb(46, 6)
prob_with_info = 1 / (scipy.special.comb(23, 3) * scipy.special.comb(23, 3))
print("Probability of winning without information:", prob_no_info)
print("Probability of winning with information:", prob_with_info)
print("Our chances improved by", (prob_with_info - prob_no_info) / prob_no_info,␣
 ↪"times")
```

```
Probability of winning without information: 1.0675982956433769e-07
Probability of winning with information: 3.188327151698374e-07
Our chances improved by 1.9864483342744215 times
```

What does our calculation say?

[4]:

```
chance_increase_by = (16 / 5) * (45 * 43 * 41) / 46 / 44 / 42 - 1
print ("Our chances should improve by", chance_increase_by, "times")
```

```
Our chances should improve by 1.9864483342744212 times
```

Problem 4

Let a be the number of vertices with degree 2 and b be the number of vertices with degree 5. We can write a systems of equations:

$$a + b = 6 \tag{41}$$

$$2a + 5b = 12 \cdot 2 \tag{42}$$

In the second equation, we double count the number of double-counted edges. This results in $a = 2$ and $b = 4$; 2 vertices of degree 2, and 4 vertices have degree 5. This can be easily achieved using parallel edges. There is no requirement that the graph must be simple, so this is fine. Fully connect four vertices and then add two sets of parallel edges such that each vertex has 4 edges. Then, add the two vertices of degree 2 in such a way that each vertex of degree 4 gains a single edge.

Problem 5

5.a

Proof. I'm pretty sure this statement only works for simple graphs, since it's very easy to create a non-simple graph that violates the statement. Therefore, let's only consider simple graphs. We will do a pigeonhole proof. Let's separate the problem into two scenarios: one where a graph of $n \geq 2$ vertices is completely connected, and one where the graph of $n \geq 2$ vertices is not completely connected.

In the first scenario where the graph is completely connected, individual vertices can have degrees 1 to $n-1$; none of the vertices can have degree 0 because the graph is fully connected, and none of the vertices can have degrees greater than $n-1$ because the graph is assumed to be simple. However, note that we have n vertices in total, and the pigeonhole principle suggests that at least two vertices will share the same degree.

In the second scenario where the graph is not completely connected, individual vertices can have degrees 0 to $n-2$. We cannot have a vertex of degree $n-1$ because that would imply that it is connected to all the other vertices and the graph is completely connected. Again, since we have more vertices (n) than the number of degrees, at least two vertices will share the same degree. □

5.b

Proof. We will do a proof by contradiction. Let's assume on the contrary that two maximum length paths in a connected graph do not intersect at any vertices. Let's call the first path *Path X* and the second path *Path Y*. Since the graph is connected, we will be able to find a *Path C* between *Path X* and *Path Y*. Say this connecting path connects vertex a of *Path X* to vertex b of *Path Y*; the connecting path may be a single edge or consist of multiple edges, but it is at least one edge long. Now, we see that vertex a divides *Path X* into two segments, and b divides *Path Y* into two segments as well. We examine the longer segments of *Path X* and *Path Y* (or, if the vertices divide *Path X* or *Path Y* into equal segments, we can choose either segment), and we can create a path with these two segments, connected by *Path C* at vertices a and b. This path is will be longer than either *Path X* or *Path Y* because it will be at least one edge longer, due to the connecting *Path C*. This is a contradiction toward our original premise that *Path X* and *Path Y* are the longest paths, and it shows that two maximum length paths in a connected graph must intersect.

□

5.c

Proof. For the sake of clarity, let's define all the terms. A tree is a non-cyclic subgraph of an undirected graph, a path graph is one that joins a sequence of distinct vertices. A leaf is a vertex that only has one edge. We will first show that a tree must have at least two leaves, and then we will show that a tree with two leaves is always a path graph. Then, putting these two pieces together, a non-path tree graph must have at least three leaves.

We show that a tree must have at least two leaves by examining the sum of the vertex degrees. Let V represent the set of all vertices in the tree, s represent the subset of leaves, n represent the total number of nodes (i.e. $|V| = n$), and $degree(v)$ represent the degree of vertex v. We note that the total number of edges is $n-1$ since there are no cycles, and the sum of the vertex degrees is $2(n-1)$ since each edge is counted twice. The sum of the vertex degrees can then be written as:

$$2n - 2 = \sum_{v \in V}^{n} degree(v) \tag{43}$$

$$2n - 2 = |s| + \sum_{v \in V \setminus s}^{n} degree(v) \tag{44}$$

We know that the internal vertices (i.e. non-leaves) must have have at least two edges, by definition (otherwise they would be leaves).

$$2n - 2 >= |s| + 2(n - |s|) \tag{45}$$

$$-2 >= 2n - |s| \tag{46}$$

$$2 <= |s| \tag{47}$$

Great, now we've shown that a tree must have at least two leaves. Now, let's show that tree with two leaves are always path graphs. We note that every tree must have a unique path between two vertices; if there was more than one path between two vertices, then we would have a cycle in the tree. Let's examine the path between two leaves of a two-leaf tree. Since the tree is fully connected, the only path from one leaf to the other traverses all the vertices, making the two-leaf tree a path graph. Thus, a non-path tree must have at least three vertices. It is easy to create such a tree; take a root node and have three children nodes that are all leaves.

□