Mark Mark RSA-2048

Judge View | Tree View | List of Debates | Hide notes | Side: None | Phase: **Make Argument** Remaining: **10:00**

At root

0 Q (H): is RSA-2048 a prime number?

H: No

D: Yes

Notes:

uhhh this is going to be difficult because I don't actually know anything about primality tests, or like... the reason why I think RSA-2048 is composite is because it says so on wikipedia, but I'm pretending it's some other large composite number handed to the debaters. The debaters know it's composite because they understand primality tests, so I'm going to just pretend that I also understand primality tests.

ok so the problem is something like D wants to talk about factors, H wants to talk about primality tests, they're both maximially uncertain over eachothers arguments and they both only want to talk about their arguments. Anytime the top level question is on H, then D says something like "this can't be true because p is prime. p is prime because it has no factors!"

Anytime the top level question is on D, H says something like "there must be a factor because p is composite. p is composite because it doesn't pass this primality test!"

then the debate oscillates back and forth and back and forth, with no one really able to establish anything? Then the debate is just a draw, and in some framework the person who paid most recently loses. In others, it's the person who paid the most number of times.

D can use some cleverness with how they split up the intervals + recursion time thinking to create a bunch of depth 1 subthings that will give them epsilon score every time? the amount of extra score D can eek out during recursion time thinking is proportional to the ratio of recursion time to answering time and the speed at which D can think. I think if you make the recursion cost epsilon and you penalize by log loss, that sort of creates a threshold, e.g. if H thinks 0.01 and D thinks 0, then D doesn't even want to recurse because the recursion costs more than potential gain in score.

Q: If a number satisfies PROPERTY is it prime?

H: Yes

D: Maybe

3 Payment: H ○ D ○ None ◉ Recurse

Notes: PROPERTY is something like "passes AKS primality test" or something

---

Q: Is the smallest number that isn't 1 that divides RSA-2048 from [3, sqrt(RSA-2048)/2]?

H: Maybe

D: No

1 Payment: H ○ D ○ None ◉ Recurse

Notes: take floors/ceilings as appropriate

Q: does RSA-2048 satisfy PROPERTY?

H: No

D: Maybe

4 Payment: H ○ D ○ None ◉ Recurse

Notes:

Q: Is the smallest number that isn't 1 that divides RSA-2048 from [3, sqrt(RSA-2048)/2]?

H: Maybe

D: No

2 Payment: H ○ D ○ None ◉ Recurse

Notes: take floors/ceilings as appropriate