HW7 available, take home quiz due next Wed 5/21

Professor Shadow
Belching Beaver Tasting Room
Saturday 5/17
12-4pm
4223 30th St (North Park)
Office Hours TBD next week, and Notes

- Sunday (5/18) Homework HW7 due Sunday by 11:59pm
- Wednesday (5/21) Take home quiz due
- Week 8 On official travel 5/22-5/27, guest lecturer Friday 5/23

Other Notes
- Help me pick office hours for next week, I am free Monday, Tuesday after 5:30pm and Wednesday from 2-3 and after 8pm.
- Please have a fun and also be safe today at the festival.
- Applications for tutors now available for CSE 20 Summer Session I
  [https://academicaffairs.ucsd.edu/Modules/ASES/Apply.aspx?cid=875](https://academicaffairs.ucsd.edu/Modules/ASES/Apply.aspx?cid=875)
Office Hours Week 8 poll results:

- Wednesday 5/21 (5:30-7) and Friday 5/23 (11-12) will have to be canceled for week 8 (:.
- We will have social office hours on Wednesday 2-3pm at The Loft and at least one of...

Vote for the time / venue you are most interested in

A. Monday 6-8 with Amer in the CSE basement, maybe somewhere afters.
B. Monday 7-10pm Brabant (South Park)
C. Tuesday 7-9pm (with Kacy and Tracy), CSE basement
D. Wednesday 8-9pm at Pines (Muir College)
E. Wednesday 8-10pm at Homeplate
Office Hours for Week 8

- Wednesday 5/21 (5:30-7) and Friday 5/23 (11-12) will have to be canceled for week 8 :(  

Office Hours for Week 8

- Monday (5/19) 6-8pm with Amer in the CSE basement, maybe somewhere afters.
- Wednesday (5/21) 2-3pm at The Loft (with tutors, some TAs)
- Wednesday (5/21) 8-10pm at Homeplate (with tutors)
  - Make sure you hand in your quiz to me by 10pm at Homeplate, or turn it in during Wednesday’s class.
Topics for Next week

- Recursion
  - Induction
  - Fibonacci numbers
  - The mating habits of *Oryctolagus cuniculus* (European rabbits).
  - Addition chains
  - Matrix multiplication
  - Matrix determinants

- Complexity
  - Asymptotics
  - Big *O* notation $O(n^2)$
  - *Little o* notation (important to say this with an English accent)
  - Big Omega $\Omega(n^2)$
  - Big Theta $\Theta(n^2)$

- Complexity Zoo
  - $NP$ – complete
  - $NP$ – hard
  - $co$ – $NP$
  - $P$
  - $RP$
Without factoring P or Q, perform probabilistic tests to help decide if they are composites or probable primes. You may use http://www.akalin.cx/intro-primality-testing or write code to calculate the following:

\[ P = 294571791067375389885907239089503408618560001 \]

1. Take the numerical part of your PID (a12345678 becomes \( a = 12345678 \)).
2. Calculate \( t = a^{P-1} \pmod{P} \).
3. Question 2 was one randomized Fermat Primality test on \( P \). What can you conclude from your result?

\[ Q = 108628836495712919311107552952534229085134089 \]

4. Calculate \( r = a^{Q-1} \pmod{Q} \). (use \( a \) as in part 1)
5. Question 4 was one randomized Fermat Primality test on \( Q \). What can you conclude from your result?