MATH 470. Fall 2022.

Homework #4. Due: Sep 22, 11:10am. No late homework will be accepted.

Please write down your solutions clearly or type your solutions. It can be considered incorrect if it is hard to read. Collaboration is allowed, but everyone must write down and submit his/her solutions in his/her own words. Please submit your work to Gradescope.

All the questions mentioned below are in the Exercise part of the corresponding sections in the textbook.

- Required submission questions:
  - Section 2.2: 2.3(b)(c), 2.4(a)(c), 2.5

    (**Instruction:** For 2.4(a), find all possible values for $\log_2(23)$; for 2.4(c), just find one possible value for $\log_{627}(608)$.)

    (**Remark:** For 2.5, we say an integer k *modulo* $p-1$ *is even* if there exists an even integer k' such that $k \equiv k' \pmod{p-1}$. Note that when $p-1$ is even, all such k' are even. But for any odd integer n, every integer k modulo n is even, since $k \equiv k+n \pmod{n}$ and one of k and $k+n$ is even.)
  - Section 2.3: 2.6

    (**Instruction:** For the last part of this question "Can you figure out Alice's secret exponent?", just explain how you can find it without having to really find the value of the secret exponent, or explain why you cannot find it.)
  - Section 2.4: 2.8(a)(b)(c)
  - Section 2.6: 2.16
- Suggested practice:
  - Section 2.2: 2.3(a), 2.4(b)
  - Section 2.3: 2.7
  - Section 2.4: 2.9, 2.10
  - Read Section 2.5 in the textbook.