135 Discrete Structures Spring 2024

WRITTEN HOMEWORK ASSIGNMENT No. 8

Due Friday 04/12/2024 11:59 pm

Please adhere to the following rules:

- This assignment should be submitted via Canvas. Late assignments will not be accepted.
- You should attempt to solve the problems on your own. You are permitted to study with friends but you can have only high-level discussions about the problems. *You must write up your own solutions, in your own words.*
- Using large language models such as ChatGPT to find solutions, copying solutions from the Internet or asking students not enrolled in the class (or the class staff) is strictly prohibited.
- Please explain your answers. There will be penalties for unexplained solutions when the answers are not obvious.
- All submissions should be neat, preferably submitted either as Word or PDF files. We reserve the right to reject handwritten submissions if they are unacceptably messy or too difficult to read.
- I encourage you to learn how to typeset documents with LATEX . You can download Texmaker at http://www.xm1math.net/texmaker/. It is available for most platforms. Another option is to use online service https://www.overleaf.com/. There is a wealth of information online on how to format documents with LATEX and you can always post a question on Moodle's Technical Forum. Most scholarly articles in Mathematics and Computer Science, and even many books, are typeset with this tool. There is, however, an initial learning curve one needs to climb before getting comfortable with LATEX – hence this great tool is not required for this course.

1. Suppose that p and $p+2$ are both prime numbers and $p \neq 3$. Show that there exists an integer $k \in \mathbb{Z}^+$ such that

$$p = 6k - 1 \text{ and } p + 2 = 6k + 1$$

2. (a) Using extended Euclidean algorithm find the multiplicative inverse of 20 mod 1343.

   (b) Solve the following linear congruence

$$20x = 7 \pmod{1343}$$

3. (a) Calculate the value $\phi(100)$ where ϕ is Euler's Totient function.
   (b) Using Euler's theorem find the last two digits of the number

$$17^{800,000,000,000,000,000,000,000,000,000,000,001}$$

   (the exponent has 36 digits).

4. Just before he passed away a wealthy businessman met individually with each of his four sons to give them an encoded combination to a vault where he held his fortune. The businessman gave very little explanation as to how the encoding worked. The first son was given a small scrap of paper with the mysterious text "$x \equiv 8 \bmod 11$" written on it. The son was told not to reveal it to anyone he did not trust. Similarly, the other three sons received scraps of paper with "$x \equiv 5 \bmod 17$", "$x \equiv 16 \bmod 29$" , and "$x \equiv 24 \bmod 31$". After many unsuccessful attempts to open the safe individually, the sons met and shared the information given to them by their father. One of them, a computer scientist, realized how to find the combination and opened the safe. Explain how he did it and what was the combination x assuming that it had at most 5 digits.

5. Let a, b, c be integers $a \neq 0 \neq b$. Using Bezout's theorem prove that if $gcd(a, b) = 1$, $a|c$, and $b|c$, then $ab|c$.

6. Show by providing a counterexample that the theorem in problem 5 is not true when $g(a, b) > 1$.