Homework 3: Mod, GCD, Euclid, Inverse

Instructions:

- We expect that you will study with friends and often work out problem solutions together, but *you must write up your own solutions, in your own words.* **Cheating will not be tolerated**.
- *To get full credit*, **show INTERMEDIATE steps** leading to your answers, throughout.

Problem 1 Linear Ciphers

You have received an email from a senior who took this class as a first-year, subject line "Discrete Structures." On opening the email, you find the following message, encrypted with a cipher:

XHQKFBX GEX HFGE

i. You notice that X is the most common single letter, and that the two letter combination GE appears twice. Use the Internet to figure out what the single most common letter in English is, and what the most common two letter combination ("digraph") is. What common word is the middle word most likely to be?

ii. Let say your guess about the middle word is correct, how can you tell this is not a Caesar cipher?
Caesar cipher uses a seceret constant b to encode every letter by shifting with b mod 26: $x \to x + b \mod 26$. Assume the numerical encoding below, where 'a'=0, 'b'=1, and so forth:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

iii. Since it isn't a Caesar cipher, your next guess is a linear cipher $x \to ax + b \mod 26$ using two constants a and b. Write down equations of the form $ax + b = c \pmod{26}$ for the ciphertext letters G and E, substituting your guesses about the plaintext letters for x and the ciphertext letters for c.

iv. Subtract your equation for the ciphertext 'E' from the equation for the ciphertext 'G' to cancel the b's. You should now have the equation:

$$12a = 2 \pmod{26}$$

Show that this is the case. (If you messed up somewhere, continue assuming you got this result.)

v. You also know that a must be relatively prime with 26 for a linear cipher to work on the normal English alphabet. How many such numbers are there, including 1? And, how do we know a is not 1?

vi. Since the space of possible values for a is small, you decide to try brute force, seeing whether any of the possible values for a fits the equation you produced two steps ago. Determine what a is in this way.

vii. Use the extended form of Euclid's algorithm to solve for the multiplicative inverse of a (mod 26).

viii. Subtract b from each letter (mod 26) and apply the multiplicative inverse of a to each. What does the message say? (You may write a program to do this part if you wish, if you submit the code.)

Problem 2 Wilson's Theorem

Prove that integer $p > 1$ is prime if and only if $(p-1)! = -1(\mod p)$
Hint: Every not zero $a \in \mathbb{Z}_p$ has an inverse a^{-1}, due from the theorem in class. Think of these as two categories: the ones being their own inverse $a = a^{-1}$, and the other ones not being such $a \neq a^{-1}$. Precisely which a-s are in the first category?

Problem 3 Bezout Coefficients coverage

part A. Prove that running all possible linear combinations of a and b gives exactly all multiples of the $\gcd(a,b)$. That is proove that the following two sets are equal

$$\{xa + yb | x, y \in Z\} = \{kd | k \in Z\}$$

part B. In the special case when a, b are coprime ($d = \gcd(a, b) = 1$) we are interested in solving the Diophantine equation $xa + yb = c$ for variables x, y. Prove that the solutions set for this equation is exactly

$$\{(x, y)|xa + yb = c\} = \{\big(x = bk + c(a^{-1} \mod b), y = \frac{c - xa}{b}\big)|k \in Z\}$$

Problem 4 Perfect Numbers

A number is "perfect" if it is exaclty the sum of its divisors (except itself). For example 6 = 1+2+3; or 28=1+2+4+7+14.

i. Prove by contradiction that $2^k - 1$ is prime $\Rightarrow k$ is prime

ii. Prove that
$2^k - 1$ is prime $\Rightarrow 2^{k-1}(2^k - 1)$ is perfect
Hint: Recap geometric formula $(x-1)(1+x+x^2+...x^{k-1}) = x^k - 1$. Enumerate the divisors and sum them up.

iii. Prove that
$2^{k-1}(2^k - 1)$ is perfect $\Rightarrow 2^k - 1$ is prime

Problem 5 The only Perfect Numbers

For any integer $n > 1$ we define $\sigma(n)$ = sum of divisors including n. For example $\sigma(6) = 1 + 2 + 3 + 6 = 12$ and $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$. Its easy to see that n being perfect means $\sigma(n) = 2n$

i. ★ Prove that $\sigma()$ is multiplicative for coprimes, that is $\gcd(a, b) = 1 \Rightarrow \sigma(ab) = \sigma(a)\sigma(b)$

ii. ★★ (optional, no credit). Prove that any n even and perfect must be of the form
$n = 2^{k-1}(2^k - 1)$ for some integer k.