CECS 229: HW 5 (Solving Congruences, Chinese Remainder Theorem, Fermat’s Little Theorem, Affine Cipher)

Spring 2021

Remember, we will not be collecting or grading homework. The homework is optional but highly recommended. Quiz questions will be similar to the homework questions but not identical. Solutions to these problems are posted on BeachBoard.

1. Do the following questions:
   a. Use Euclidean algorithm to compute G= gcd(34, 89)
   b. Find integers a and b such that G $= 34a + 89b$
   c. Use your answer to (b) to find an integer $0 \leq c < 89$ such that $34c \equiv 7(mod\ 89)$

2. Do the following questions:
   a. Use Euclidean algorithm to compute G= gcd(35, 153)
   b. Find integers a and b such that G $= 35a + 153b$
   c. Use your answer to (b) to find an integer $0 \leq c < 153$ such that $35c \equiv 2(mod\ 153)$

3. If solvable, find all possible values of x for each congruence:
   a. $54x - 12 \equiv 30x + 12\ (mod\ 7)$
   b. $11x + 13 \equiv 7\ (mod\ 16)$
   c. $19x - 10 \equiv -9x + 91\ (mod\ 20)$

4. If possible, find all integers x such that it satisfies…

$$x \equiv 1\ (mod\ 3)$$
$$x \equiv 4\ (mod\ 5)$$

   Try both back substitution and Chinese Remainder Theorem

5. If possible, find all integers x such that it satisfies…

$$x \equiv 1\ (mod\ 3)$$
$$x \equiv 4\ (mod\ 7)$$
$$x \equiv 2\ (mod\ 8)$$

   Try both back substitution and Chinese Remainder Theorem

6. User Fermat’s Little Theorem to compute
   a. $3^{402}\ mod\ 5$
   b. $3^{402}\ mod\ 7$
   c. $3^{402}\ mod\ 11$

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
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

7. We mentioned that the parameter, a, for the affine cipher should be relatively prime to 26 if you want a functional encryption/decryption system. See what happens if your affine cipher uses the parameters $a = 13, b = 5$ and you try to encrypt “ABCD”.

8. Using an affine cipher with parameters $a = 9, b = 19$, decrypt “Tld”