MTH 233

Midterm (Solutions)

March 25, 2021

- You are allowed to use a basic four function calculator.
- Textbooks, additional notes, computer use besides zoom and gradescope, or communication with anyone else during the exam are not allowed.
- You must be in the zoom proctoring room with your camera on for the duration of the exam. Please stay on mute but have your volume on and chat open in case the proctor needs to reach you.
- You must write your exam on paper, not on a tablet or other device.

Before we begin, please copy the following honor pledge and sign your name. (The same honesty standards apply as detailed on the blackboard page. Cursive is not required).

I affirm that I will not give or receive any unauthorized help on this exam, and all work will be my own.

Submit your honesty pledge at the end of the exam as Question 8.

TO RECEIVE FULL CREDIT, JUSTIFY YOUR ANSWERS.

1. (14 points)

(a) Find the greatest common divisor $d = \gcd(665, 273)$.

(b) Find two integers x and y such that $665x + 273y = d$.

Using the extended Euclidean Algorithm, $d = 7$, and $665 \cdot (-16) + 273 \cdot 39 = 7$.

2. (16 points) Use the following numerical encoding for the letters A-Z:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(a) An affine cipher $\alpha x + \beta$ encodes the plaintext `bake` as `XOAY`. What are α and β?

(b) After encoding a message using the affine cipher from (a), you encode the resulting ciphertext a second time using the affine cipher $5x + 1$. This double encryption is equivalent to a single affine cipher $\gamma x + \delta$, with $0 \leq \gamma < 26$ and $0 \leq \delta < 26$. What are γ and δ?

(a) Since `a`$\mapsto$`O`, we have $0 \mapsto 14$, and thus $\beta = 14$. Since `b`$\mapsto$`X`, we have $1 \mapsto 23$, and so $\alpha + 14 = 23$ and $\alpha = 9$.

(b) This is just function composition:

$$\gamma x + \delta \equiv 5(9x + 14) + 1 \equiv 45x + 70 + 1 \equiv 19x + 19 \pmod{26}.$$

3. (18 points) Centuries from now, computers have invented their own language with only two characters, 0 and 1. In this language 0 occurs with frequency 10%, while 1 occurs with frequency 90%. You receive the ciphertext

1010100010

encrypted with a Vigenère cipher (mod 2 instead of mod 26) of key length 1, 2, or 3.

(a) What is the key length?

(b) What is the key?

(c) What is the plaintext?

(a) Line up the ciphertext with itself shifted i characters and count the matches:

- $i = 1$: 2 matches
- $i = 2$: 6 matches
- $i = 3$: 2 matches

Thus the key length is likely 2.

(b) The key consists of two shift ciphers. The first produces the plaintext (every other character) either 11101 or 00010 when the first character of the key is 0 or 1, and the second produces 00000 or 11111 when the second character of the key is 0 or 1. Based on the expected frequencies, the key is 01.

(c) Using this key, the decryption is 1111110111.

4. (12 points) Find all solutions to $x^2 \equiv 53 \pmod{91}$ with $0 \leq x < 91$.
Note: 91 is *not* prime.

$x^2 \equiv 53 \pmod{91}$ means $x^2 \equiv 53 \equiv 4 \pmod{7}$ and $x^2 \equiv 53 \equiv 1 \pmod{13}$. These each have solutions $x \equiv \pm 2 \pmod{7}$ and $x \equiv \pm 1 \pmod{13}$.

Combining these via the Chinese remainder theorem, we get $x \equiv 12, 40, 51, 79 \pmod{91}$.

5. (12 points) Compute $3^{2042} \pmod{41}$.

Since 41 is prime, $3^{40} \equiv 1 \pmod{41}$ by Fermat's little theorem. Thus,

$$3^{2042} \equiv 3^{40 \cdot 51 + 2} \equiv (3^{40})^{51} \cdot 3^2 \equiv 1 \cdot 3^2 \equiv 9 \pmod{41}.$$

6. (16 points) Suppose Bob's RSA public key modulus is $n = 33$.

(a) If Bob's public encryption exponent is $e = 3$, decrypt the ciphertext $c = 15$ sent to him.

(b) For what encryption exponent(s) e is Bob's decryption exponent d equal to e? You may ignore $e = 1$.

(a) $\phi(33) = (3-1) \cdot (11-1) = 20$, so we solve $d = e^{-1} \mod 20$ and find $d = 7$. Then

$$m \equiv c^d \equiv 15^7 \equiv 27 \pmod{33}.$$

(b) If $d = e$, then $e \equiv d \equiv e^{-1} \pmod{20}$, and so $e^2 \equiv 1 \pmod{20}$. This can be broken into $e^2 \equiv 1 \pmod{5}$ and $e^2 \equiv 1 \pmod{4}$, and the solutions are $e \equiv \pm 1 \pmod{5}$ and $e \equiv 1 \pmod{4}$. By the Chinese remainder theorem, the solutions are

$$e \equiv 1, 9, 11, 19 \mod 20.$$

7. (12 points) 137 is prime. You compute that $3^6 \equiv 44 \pmod{137}$ and $3^{10} \equiv 2 \pmod{137}$. Find an integer x with $0 \leq x < 137$ such that $3^x \equiv 11 \pmod{137}$.

Notice that $11 = 44 \cdot (2^{-2})$. Thus

$$11 \equiv 3^6 \cdot (3^{10})^{-2} \pmod{137}.$$

Since 137 is prime, we can take exponents mod 136, and so

$$3^6 \cdot (3^{10})^{-2} \equiv 3^{6-20} \equiv 3^{136+6-20} \equiv 3^{122} \pmod{137},$$

and $x = 122$ works.

8. (0 points) Upload your honesty statement as problem 8:

I affirm that I will not give or receive any unauthorized help on this exam, and all work will be my own.