MATH 3094 - PRACTICE MIDTERM 1

YOUR NAME: ÁLVARO LOZANO-ROBLEDO

P1	P2	P3	P4	P5	Extra	Total

Show all your work. Explain all your answers. Do not use calculator programs.

Problem 1. (20 points) For each problem below, **explain** your steps to find the answer.

(1) (5 points) *Practice the fast powering algorithm, e.g.,* find an integer between 0 and 10 that is congruent to 5^{321} mod 11.

By Fermat's little theorem $5^{10} \equiv 1 \bmod 11$ (b/c 11 ∤ 5).

Thus $5^{321} \equiv 5^{32 \cdot 10} \cdot 5 \equiv (5^{10})^{32} \cdot 5 \equiv 1^{32} \cdot 5 \equiv \boxed{5 \bmod 11}$

(2) (5 points) *Practice solving Bezout's identity, e.g.,* find integers x and y such that $7x + 47y = 1$ using Euclid's algorithm.

We use Euclid's:

$47 = 7 \cdot 6 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + \boxed{1}$

$1 = 5 - 2 \cdot 2$

$= 5 - (7-5) \cdot 2$

$= 3 \cdot 5 - 2 \cdot 7$

$= (47 - 7 \cdot 6) \cdot 3 - 2 \cdot 7$

$= 3 \cdot 47 - 20 \cdot 7$

so

$\boxed{1 = (-20) \cdot 7 + 3 \cdot 47}$

$\boxed{x = -20 \quad y = 3}$

(3) (5 points) *Practice finding multiplicative inverses, e.g.,* find the multiplicative inverse of 7 mod 47.

Since $1 = (-20) \cdot 7 + 3 \cdot 47$ if we reduce modulo 47:

$1 \equiv (-20) \cdot 7 \bmod 47 \Rightarrow 7 \cdot 27 \equiv 1 \bmod 47$

$\Rightarrow \boxed{7^{-1} \equiv 27 \bmod 47}$

(4) (5 points) *Practice finding negative powers of integers in modular arithmetic, e.g.,* find an integer between 0 and 10 that is congruent to 7^{-3} mod 11.

$7^3 \equiv 7^2 \cdot 7 \equiv 49 \cdot 7 \equiv 5 \cdot 7 \equiv 35 \equiv 2 \bmod 11$

$7^{-3} \equiv (7^3)^{-1} \equiv 2^{-1} \equiv \boxed{6 \bmod 11}$

Problem 2. (20 points)

(1) *Practice encrypting and decrypting using Caesar/shift ciphers, e.g.,* let A through Z be encoded by 0 through 25 mod 26 (so that $A \equiv 0$, $B \equiv 1$, ..., $Z \equiv 25 \bmod 26$) and encrypt "MATH" using the shift cipher $e_3(\ell) \equiv \ell + 3 \bmod 26$.

e ↓

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
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

MATH $\xmapsto{e}$ PDWK

(2) *Practice encrypting and decrypting using Caesar/shift ciphers, e.g.,* the word "SOJZKXS" was encrypted using a shift cipher, and you know that O corresponds to I. Decrypt the message.

e ↓

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
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F

SOJZKXS $\xmapsto{d}$ MIDTERM

(3) *Practice working with affine ciphers, e.g.,* let $e(m) \equiv 3 \cdot m + 3 \bmod 26$. Can this function be used as an affine cipher to encrypt the alphabet? If so, what is the decryption function $d(c)$? Yes b/c 3 is invertible mod 26.

If $C \equiv 3m + 3 \bmod 26$ then $m \equiv 3^{-1} \cdot (C - 3)$
$\equiv 9 \cdot (C + 23) \bmod 26$

is an inverse function, i.e.,

$d(c) \equiv 9 \cdot (C + 23) \bmod 26$ is a decryption functions.

(4) *Practice working with affine ciphers, e.g.,* let $e(m) \equiv 4 \cdot m + 4 \bmod 26$. Can this function be used as an affine cipher to encrypt the alphabet? If so, what is the decryption function $d(c)$?

No this cannot be a cipher b/c the inverse/decrypt function would be

$d(c) \equiv 4^{-1}(C - 4) \bmod 26$

but 4 is NOT invertible mod 26 ($\gcd(4, 26) = 2 \neq 1$).

Problem 3. (20 points)

(1) *Practice working with primitive roots, e.g.,* find **all** the primitive roots modulo 11.

2 is a p.r. :

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	5	10	9	7	3	6	1

then the p.r's are 2^m w/ $\gcd(m, 10) = 1$ so

$$2, 2^3, 2^7, 2^9 \equiv \boxed{2, 8, 7, 6 \bmod 11}$$

(2) *Practice solving the DLP, e.g.,* find x such that $2^x \equiv 5 \bmod 11$.

Using the table above :

$$2^4 \equiv 5 \bmod 11 \quad \text{so} \quad \boxed{x = 4}$$

(3) *Practice finding multiplicative orders, e.g.,* what is the multiplicative order of 2 mod 11? How about 4 mod 11?

$\boxed{\text{ord}_{11}(2) = 10}$ by the table above.

$\boxed{\text{ord}_{11}(4) = \text{ord}_{11}(2^2) = 5}$

bc $(2^2)^5 \equiv 2^{10} \equiv 1$ and $2^1 \not\equiv 1$.

(4) *Practice setting up a Diffie-Hellman key exchange, e.g.,* Alice and Bob want to communicate securely and first they will use Diffie-Hellman (DH) key exchange, using $p = 11$ and $g = 4$. Alice picks $a = 3$ and Bob picks $b = 2$ for their secret keys. What is the secret key K mod 11 that the DH algorithm produces?

$$A \equiv 4^3 \equiv 4^2 \cdot 4 \equiv 20 \equiv 9 \bmod 11$$

$$\Rightarrow K \equiv A^b \equiv 9^2 \equiv 81 \equiv \boxed{4 \bmod 11}$$

(Similarly $K \equiv B^a \bmod 11$)

$\equiv 4$.

Problem 4. (20 points) *Practice setting up and working with an Elgamal crypto system, e.g.,* set up an Elgamal system with $p = 13$, $g = 4$, and Alice's choice $a = 3$.

(1) First compute $A \equiv g^a \bmod p$.

$A \equiv 4^3 \equiv 4^2 \cdot 4 \equiv 3 \cdot 4 \equiv 12 \bmod 13$

(2) Then, encrypt the messages $m_1 = 7$ and $m_2 = 8$ using the Elgamal system you just set up.

Pick $k=2$

$m=7$ $\quad (c_1, c_2) \equiv (g^k, mA^k)$

$\equiv (4^2, 7 \cdot 12^2)$ $\quad 12 \equiv -1 \Rightarrow 12^2 \equiv (-1)^2 \equiv 1$

$\equiv (3, 7 \cdot 1) \equiv (3,7) \bmod 13$

$m=8$ $\quad (c_1, c_2) \equiv (g^k, mA^k)$

$\equiv (4^2, 8 \cdot 12^2)$

$\equiv (3, 8) \equiv (3.8) \bmod 13$

Problem 5. (20 points) *Practice using Shank's baby-step giant-step algorithm, e.g.,* use Shank's baby-step giant-step algorithm to find x such that

$$2^x \equiv 3 \bmod 19.$$

(1) Find the order of 2 mod 19.

The order divides $18 = 19 - 1 \Rightarrow$ order is $1, 2, 3, 6, 9,$ or 18

$2^2 \equiv 4, 2^3 \equiv 8, 2^6 \equiv 7, 2^9 \equiv 18 \Rightarrow$ order is 18

(2) Compute $n = 1 + \lfloor \sqrt{18} \rfloor$.

$n = 1 + \lfloor \sqrt{18} \rfloor = 5$

(3) Compute List 1: $1, g, g^2, \ldots, g^n \bmod 19$.

$1, 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16, 2^5 \equiv 13$

$\{1, 2, 4, 8, 16, 13\}$

(4) Compute $u \equiv g^{-n} \bmod 19$.

$u \equiv g^{-n} \equiv 2^{-5} \equiv (2^5)^{-1} \equiv 3 \bmod 19$

(5) Compute List 2: $h, h \cdot u, h \cdot u^2, \ldots, h \cdot u^n \bmod 19$.

$h = 3, \quad 3, \; 3 \cdot 3, \; 3 \cdot 3^2, \; 3 \cdot 3^3, \; 3 \cdot 3^4, \; 3 \cdot 3^5$

$\equiv 3, 9, 8, 5, 15, 7$

(6) Use the information above to finish the baby-step giant-step algorithm and find x such that $2^x \equiv 3 \bmod 19$.

8 is repeated in both lists!

$g^3 \equiv h \cdot (g^{-n})^2$

$\Rightarrow x = i + jn = 3 + 2 \cdot 5 = 13$

$x = 13$ so $2^{13} \equiv 3 \bmod 19$