FIRST MIDTERM EXAM: SOME PRACTICE PROBLEMS

Numerization key:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

1. Divide the given number b into the given number a, yielding a quotient and a remainder. That is, write
$$a = b \cdot q + r$$
where q and r are integers and $0 \leq r < b$.

   (a) $a = 465, b = 33$.

   (b) $a = 466{,}655, b = 3{,}233$.

   (c) $a = 3{,}333{,}333$, $b = 12$.

   (d) $a = 4{,}849, b = 12$.

   (e) $a = 4{,}848, b = 12$.

   (f) $a = 44$, $b = 44{,}332{,}211$.

   (g) $a = -47, b = 15$.

2. Let $k = 19$ and $m = 111 = 3 \cdot 37$.

   (a) Use RSA with this k and m to encode the message "C."

   (b) Check your work by decoding the coded message from part (a) of this problem, using the same k and m. Hint:
$$19 \cdot 19 - 72 \cdot 5 = 1.$$

3. Let $k = 31$ and $m = 221 = 13 \cdot 17$.

   (a) Use RSA with this k and m to encode the message "Y."

   (b) Check your work by decoding the coded message from part (a) of this problem, using the same k and m. Hint:
$$31 \cdot 31 - 192 \cdot 5 = 1.$$

4. Let $k = 43$ and $m = 1{,}517 = 37 \cdot 41$. (37 and 41 are both prime.)

   (a) Use RSA with this k and m to encode the message "AI."

   (b) Check your work by decoding the coded message from part (a) of this problem, using the same k and m. Hint:
   $$43 \cdot 67 - 1{,}440 \cdot 2 = 1.$$

5. Let $k = 49$ and $m = 1{,}271 = 31 \cdot 41$. (31 and 41 are both prime.)

   (a) Use RSA with this k and m to encode the message "AB."

   (b) Check your work by decoding the coded message from part (a) of this problem, using the same k and m. Hint:
   $$49 \cdot 49 - 1{,}200 \cdot 2 = 1.$$

6. A message is encoded using RSA, with $k = 83$ and $m = 323 = 17 \cdot 19$. Which of the following equations would be relevant to decoding? Circle the correct answer and explain.

   $83 \cdot 59 - 288 \cdot 17 = 1.$ $83 \cdot 144 - 323 \cdot 37 = 1.$ $288 \cdot 66 - 83 \cdot 229 = 1.$ $17 \cdot 9 - 19 \cdot 8 = 1.$

7. (a) Use the Euclidean Algorithm to find $\gcd(123, 321)$.

   (b) Find natural numbers x and y solving
   $$123x - 321y = \gcd(123, 321).$$

8. (a) Use the Euclidean Algorithm to find $\gcd(247, 156)$.

   (b) Find **integers** x and y solving
   $$247x - 156y = \gcd(247, 156).$$
   Here, x and y don't need to be positive.

   (c) Find **natural numbers** x and y solving
   $$247x - 156y = \gcd(247, 156).$$
   Hint: add 156 to the number x you found in part (b) of this problem. Then add the right thing to the number y you found in part (b) of this problem.

9. (a) Find natural numbers x and y such that
   $$45x - 56y = 1.$$

(b) Using the RSA decoding algorithm, with $k = 45$ and $m = 87$, decode the message "17," to obtain a one-letter message.

10. (a) Use the Euclidean Algorithm to find positive integers x and y such that

$$55x - 64y = 1.$$

(b) Using the numerization key above and the RSA decoding algorithm, with $k = 55$ and $m = 85$, decode the message "25," to obtain a one-letter message.

11. (a) Use the Euclidean algorithm to find gcd(31,$\varphi(55)$).

Answer: gcd(31,$\varphi(55)$) = _____.

(b) Use the Euclidean algorithm to find integers x and y with $31x - \varphi(55)y = 1$. Here, x and y do not need to be positive.

Answer: $x =$ _____, $y =$ _____

(c) Tweak your answer to the previous part of this problem, to find *positive* integers (that is, natural numbers) x and y with $31x - \varphi(55)y = 1$.

Answer: $x =$ _____, $y =$ _____

(d) Using $k = 31$ and $m = 55$, decode the message 12, and denumerize to obtain a single-letter message.

Answer: Message = _____

12. Find gcd(14,000, 7,700), by factoring both numbers into prime powers (do not use the Euclidean algorithm).

13. Find gcd(454,545,000, 9,990,000), by factoring both numbers into prime powers (do not use the Euclidean algorithm). Hints: $999 = 9 \cdot 111$; $111 = 3 \cdot 37$; $454{,}545 = 45 \cdot 10{,}101$; $45 = 9 \cdot 5$; $10{,}101 = 7 \cdot 13 \cdot 111$.

14. (15 points; 5 points each)

(a) Use the Euclidean algorithm to find gcd(63,111).

(b) Use the Euclidean algorithm to find integers x and y such that $63x - 111y =$ gcd(63,111).

(c) Find *positive* integers (that is, natural numbers) x and y such that $63x - 111y =$ gcd(63,111).

15. (15 points; 5 points each)

(a) Use the Euclidean algorithm to show that $\gcd(17,220) = 1$.

(b) Use the Euclidean algorithm to find natural numbers x and y with $17x - 220y = 1$.

(c) Use the RSA decoding algorithm with $k = 17$ and $m = 253 = 11 \cdot 23$ to decode the message 20. Express your answer as a single letter, using the numerization key above.