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) $a = 465, b = 33$. $465 = 33 \cdot 14 + 3$.

(b) $a = 466{,}655, b = 3{,}233$. $466{,}655 = 3{,}233 \cdot 144 + 1{,}103$.

(c) $a = 3{,}333{,}333$, $b = 12$. $3{,}333{,}333 = 277{,}777 \cdot 12 + 9$.

(d) $a = 4{,}849, b = 12$. $4{,}849 = 404 \cdot 12 + 1$.

(e) $a = 4{,}848, b = 12$. $4{,}848 = 404 \cdot 12 + 0$.

(f) $a = 44$, $b = 44{,}332{,}211$. $44 = 44{,}332{,}211 \cdot 0 + 44$.

(g) $a = -47, b = 15$. $-47 = 15 \cdot (-4) + 13$.

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

(a) Use RSA with this k and m to encode the message "C." $13^{19} \equiv 61 \pmod{111}$.

(b) Check your work by decoding the coded message from part (a) of this problem, using the same k and m. Hint:

$$19 \cdot 19 - 72 \cdot 5 = 1.$$

$61^{19} \equiv 13 \pmod{111}$.

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

(a) Use RSA with this k and m to encode the message "Y." $35^{31} \equiv 35 \pmod{221}$.

(b) Check your work by decoding the coded message from part (a) of this problem, using the same k and m. Hint:

$$31 \cdot 31 - 192 \cdot 5 = 1.$$

$35^{31} \equiv 35 \pmod{221}$.

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."

   $1{,}119^{43} \equiv 867 \pmod{1{,}517}$.

   (b) Check your work by decoding the coded message from part (a) of this problem, using the same k and m. Hint:

   $$43 \cdot 67 - 1{,}440 \cdot 2 = 1.$$

   $867^{67} \equiv 1{,}119 \pmod{1{,}517}$.

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."

   $1{,}112^{49} \equiv 705 \pmod{1{,}271}$.

   (b) Check your work by decoding the coded message from part (a) of this problem, using the same k and m. Hint:

   $$49 \cdot 49 - 1{,}200 \cdot 2 = 1.$$

   $705^{49} \equiv 1{,}112 \pmod{1{,}271}$.

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.

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

   We want natural numbers x and y such that

   $$kx - \varphi(m)y = 83x - 288y = \gcd(k, \varphi(m)) = \gcd(83, 288) = 1.$$

   The first equation gives us that.

7. (a) Use the Euclidean Algorithm to find $\gcd(123, 321)$. $=3$.

(b) Find natural numbers x and y solving

$$123x - 321y = \gcd(123, 321).$$

$$123 \cdot 47 - 321 \cdot 18 = 3.$$

8. (a) Use the Euclidean Algorithm to find $\gcd(247, 156)$. $=13$.

(b) Find **integers** x and y solving

$$247x - 156y = \gcd(247, 156).$$

Here, x and y don't need to be positive.

$$247(-5) - 156(-8) = 13.$$

(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.
Add 156 to -5 to get 151. Then add 247 to -8 to get 239. Check that

$$247 \cdot 151 - 156 \cdot 239 = 13.$$

9. (a) Find natural numbers x and y such that

$$45x - 56y = 1.$$

$$45 \cdot 5 - 56 \cdot 4 = 1.$$

(b) Using the RSA decoding algorithm, with $k = 45$ and $m = 87$, decode the message "17," to obtain a one-letter message. $17^5 \equiv 17 \pmod{87} \to$ G.

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

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

$$55 \cdot 7 - 64 \cdot 6 = 1.$$

(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. $25^7 \equiv 15 \pmod{85} \to$ E.

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

Answer: gcd(31,$\varphi(55)$) = 1.

(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: $x =$ -9, $y =$ -7

(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: $x =$ 31, $y =$ 24

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

Answer: Message = M.

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

$$\begin{aligned} \gcd(14{,}000, 7{,}700) &= \gcd(14 \cdot 1000, 77 \cdot 100) = \gcd(2 \cdot 7 \cdot 2^3 \cdot 5^2, 7 \cdot 11 \cdot 2^2 \cdot 5^2) \\ &= \gcd(2^4 \cdot 5^2 \cdot 7, 2^2 \cdot 5^2 \cdot 7 \cdot 11) = 2^2 \cdot 5^2 \cdot 7 = 700. \end{aligned}$$

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

$$\begin{aligned}\gcd(454{,}545{,}000, 9{,}990{,}000) &= \gcd(454{,}545 \cdot 1{,}000, 999 \cdot 10{,}000) \\ &= \gcd(45 \cdot 10{,}101 \cdot 2^3 \cdot 5^3, 9 \cdot 111 \cdot 2^4 \cdot 5^4) \\ &= \gcd(3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 3 \cdot 37 \cdot 2^3 \cdot 5^3, 3^2 \cdot 3 \cdot 37 \cdot 2^4 \cdot 5^4) \\ &= \gcd(2^3 \cdot 3^3 \cdot 5^4 \cdot 7 \cdot 13 \cdot 37, 2^4 \cdot 3^3 \cdot 5^4 \cdot 37) \\ &= 2^3 \cdot 3^3 \cdot 5^4 \cdot 37 = 4{,}995{,}000.\end{aligned}$$

14. (15 points; 5 points each)

(a) Use the Euclidean algorithm to find gcd(63,111). =3.

(b) Use the Euclidean algorithm to find integers x and y such that $63x - 111y = \gcd(63{,}111)$. $63 \cdot (-7) - 111 \cdot (-4) = 3$.

(c) Find *positive* integers (that is, natural numbers) x and y such that $63x - 111y = \gcd(63{,}111)$.
$63 \cdot 104 - 111 \cdot 59 = 3$.

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 $17x - 220y = 1$.
$17 \cdot 13 - 220 \cdot 1 = 1$.

(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. $20^{13} \equiv 14 \pmod{253} \to$ D.