MATH 2001-001: Intro to Discrete Math

September 22, 2025

First In-class Midterm Exam

SOLUTIONS

1. (21 points; 7 points each) Let $a = 747474$ and $b = 4814810$.

(a) Write a as a product of powers of distinct primes. Hint 37 is prime. Also

$$747474 = 74 \cdot 10101, \qquad 10101 = 3 \cdot 7 \cdot 13 \cdot 37.$$

$$747474 = 74 \cdot 10101 = 2 \cdot 37 \cdot 3 \cdot 7 \cdot 13 \cdot 37 = 2 \cdot 3 \cdot 7 \cdot 13 \cdot 37^2.$$

(b) Write b as a product of powers of distinct primes. Hints:

$$4814810 = 13 \cdot 37 \cdot 1001 \cdot 10, \qquad 1001 = 7 \cdot 11 \cdot 13.$$

$$4814810 = 13 \cdot 37 \cdot 1001 \cdot 10 = 13 \cdot 37 \cdot 7 \cdot 11 \cdot 13 \cdot 2 \cdot 5 = 2 \cdot 5 \cdot 7 \cdot 11 \cdot 13^2 \cdot 37.$$

(c) Find $\gcd(a, b)$, using the above factorizations of a and b. (Do not use the Euclidean algorithm.)

$$\gcd(a, b) = \gcd(2 \cdot 3 \cdot 7 \cdot 13 \cdot 37^2,\ 2 \cdot 5 \cdot 7 \cdot 11 \cdot 13^2 \cdot 37) = 2 \cdot 7 \cdot 13 \cdot 37 = 6734.$$

2. (24 points; 8 points each)

(a) Use the Euclidean algorithm to find $\gcd(24, 57)$.

Answer: $\gcd(24, 57) =$ __3__.

(b) Use the Euclidean algorithm to find (not necessarily positive) integers x and y such that

$$24x - 57y = \gcd(24, 57).$$

Answer: $x =$ __-7__, $y =$ __-3__.

(c) Use your answer to the previous part of this problem to find *positive* integers (that is, natural numbers) x and y such that

$$24x - 57y = \gcd(24, 57).$$

Answer: $x =$ __50__, $y =$ __21__.

3. Let $k = 13$ and $m = 85 = 5 \cdot 17$.

(a) (4 points) Find $\varphi(m)$.

Answer: $\varphi(m) =$ __64__.

(b) (4 points) Fill in the blank (you should be able to figure this out with some simple algebra):

$$13 \cdot \underline{\ 5\ } - 64 \cdot 1 = 1.$$

(c) (10 points) Fill in the blanks (there are 10 of them) to decode the message 37, to obtain a one-letter message.

Step 1:

$$5 = \underline{\ 4\ } + \underline{\ 1\ }.$$

Step 2:

$$37^1 \equiv \underline{\ 37\ } \pmod{85}$$

$$37^2 \equiv 1369 \equiv 85 \cdot 16 + 9 \equiv \underline{\ 9\ } \pmod{85}$$

$$37^4 \equiv (37^2)^2 \equiv 9^2 \equiv \underline{\ 81\ } \pmod{85}$$

Step 3:

$$37^5 \equiv 37^{4+1} \equiv 37^4 \cdot 37^1$$

$$\equiv \underline{\ 81\ } \cdot 37$$

$$\equiv 2997 \equiv 85 \cdot \underline{\ 35\ } + \underline{\ 22\ } \equiv \underline{\ 22\ } \pmod{85}.$$

So the one-letter message is __L__.

4. Let $k = 7$ and $m = 119 = 7 \cdot 17$.

(a) (4 points) Compute $\varphi(m)$.

Answer: $\varphi(m) = \underline{\quad 96 \quad}$.

(b) (4 points) Explain why k and $\varphi(m)$ are coprime. You don't have to use the Euclidean algorithm here. Hint: $96 = 2^5 \cdot 3$. 7 has no prime factors in common with $2^5 \cdot 3$.

(c) (4 points) Numerize the message the message "I," using the key on your fact sheet.

Answer: I$\to$ $\underline{\quad 19 \quad}$.

(d) (4 points) Let n be the numerization of "I" that you found in the previous part of this problem. Explain why n and m are coprime. Again, you don't have to use the Euclidean algorithm; just look at prime factors. 19 has no prime factors in common with $7 \cdot 17$.

(e) (8 points) Encode the message "I" using RSA, with $k = 11$ and $m = 119 = 7 \cdot 17$ as above. Please show all of your work. For example, if you were to arrive a number like 527, don't just write $527 \equiv 51 \pmod{119}$; write $527 \equiv 119 \cdot 4 + 51 \equiv 51 \pmod{119}$.

Step 1:

$$11 = 8 + 2 + 1.$$

Step 2:

$$\begin{aligned}
19^1 &\equiv 19 \pmod{119} \\
19^2 &\equiv 361 \equiv 119 \cdot 3 + 4 \equiv 4 \pmod{119} \\
19^4 &\equiv (19^2)^2 \equiv 4^2 \equiv 16 \pmod{119} \\
19^8 &\equiv (19^4)^2 \equiv 16^2 \equiv 256 \equiv 119 \cdot 2 + 18 \equiv 18 \pmod{119}
\end{aligned}$$

Step 3:

$$\begin{aligned}
19^{11} \equiv 19^{8+2+1} &\equiv 19^8 \equiv 19^2 \cdot 19^1 \\
&\equiv 18 \cdot 4 \cdot 19 \\
&\equiv 72 \cdot 19 \equiv 1368 \\
&\equiv 119 \cdot 11 + 59 \equiv 59 \pmod{119}.
\end{aligned}$$

5. (10 points; 2 points for each blank) Fill in the blanks (there are 5 of them) to complete the following proof:

Proposition. Let $a, b, c, d, m \in \mathbb{Z}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Hint: $ac - bd = c(a - b) + b(c - d)$.

Proof. Assume $a, b, c, d, m \in \mathbb{Z}$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$. Since $a \equiv b \pmod{m}$, we know that $m|(a - b)$, so $a - b = \underline{\quad m \quad} \cdot q$ for some integer q. Moreover, since $c \equiv d \pmod{m}$, we know that $m|(\underline{\quad c - d \quad})$, so $c - d = m \cdot s$ for some integer s.

But then, by the hint,

$$ac - bd = c(a - b) + b(c - d) = c \cdot (m \cdot q) + b \cdot (m \cdot \underline{\quad s \quad})$$
$$= m \cdot (c \cdot q + \underline{\quad b \quad} \cdot s).$$

Since c, q, b, and s are integers, so is $c \cdot q + b \cdot s$. So we have shown that $ac - bd$ equals m times an integer. This tells us that $m|(\underline{\quad ac - bd \quad})$, which tells us that $ac \equiv bd \pmod{m}$. So our proposition is proved. □

(end of exam)