1. Circle true or false. Justify your answer. m and n are integers.

   (a) There exists an n such that for all m, $n + m \equiv 1 \pmod 3$.

   Solution: false. We argue by contradiction. Suppose such an n existed. When m equals $-n$, $n + m$ is zero modulo 3.

   (b) For all n there exists an m such that $n + m \equiv 1 \pmod 3$.

   Solution: true. Given any n, set $m = -n + 1$. Then $n + m \equiv 1 \pmod 3$.

2. Bob chooses $n = 77$ as the modulus and $e = 7$ as his RSA public key.

   (a) What is Bob's secret key d? Show how he calculated it.

   Solution: Bob sampled the modulus as the product of the primes $p = 11$ and $q = 7$. Then he chose his secret key to satisfy $ed \equiv 1 \pmod{(p-1)(q-1)}$, namely $7d \equiv 1 \pmod{60}$. To find d he calculates the multiplicative inverse of 7 modulo 60 via extended Euclid's algorithm:

$$\begin{aligned} E(60,7) &= E(7,4) & 60 &= 8 \cdot 7 + 4 \\ &= E(4,3) & 7 &= 4 + 3 \\ &= E(3,1) & 4 &= 3 + 1 \end{aligned}$$

   so that

$$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (60 - 8 \cdot 7) - 7 = -17 \cdot 7 + 2 \cdot 60$$

   and $d \equiv -17 \equiv 43 \pmod{60}$.

   (b) Alice wants to encrypt the message $m = 3$. What is the ciphertext that she sends to Bob?

   Solution: The ciphertext is $m^e \pmod n = 3^7 \pmod{77}$. Using fast modular exponentiation:

$$3^7 \equiv 3 \cdot 3^6 \equiv 3 \cdot 9^3 \equiv 3 \cdot 9 \cdot 9^2 \equiv 3 \cdot 9 \cdot 4 \equiv 108 \equiv 31 \pmod{77}.$$

3. A savings account offers 1% monthly interest and incurs a 10 dollar monthly fee after interest was applied.

   (a) Write a recurrence for the balance $f(n)$ after n months.

   Solution: $f(n) = 1.01 f(n-1) - 10$.

   (b) Your initial deposit is 2000 dollars. Solve the recurrence from part (a) to obtain a formula for $f(n)$.

   Solution: The initial condition is $f(0) = 2000$. Unwinding the recurrence gives

$$\begin{aligned} f(n) &= 1.01 f(n-1) - 10 \\ &= 1.01(1.01 f(n-2) - 10) - 10 = 1.01^2 f(n-2) - 1.01 \cdot 10 - 10 \\ &= 1.01^2(1.01 f(n-3) - 10) - 1.01 \cdot 10 - 10 = 1.01^3 f(n-3) + 1.01^2 \cdot 10 - 1.01 \cdot 10 - 10 \\ &\cdots \\ &= 1.01^n f(0) - 1.01^{n-1} \cdot 10 - \cdots - 1.01 \cdot 10 - 10. \end{aligned}$$

   Plugging in $f(0) = 2000$ and applying the geometric sum formula,

$$f(n) = 2000 \cdot 1.01^n - \frac{1.01^n - 1}{1.01 - 1} \cdot 10 = 1000 \cdot 1.01^n + 1000.$$

   Alternatively, we can homogenize the recurrence using the guess $f(n) = g(n) - c$. As long as $c = 1.01c + 10$, or $c = -1000$, $g(n)$ equals $1.01 g(n-1)$. Unwinding gives $g(n) = 1.01^n g(0) = 1.01^n \cdot 1000$ so $f(n) = g(n) - c = 1000 \cdot 1.01^n + 1000$.

4. Write an expression for the number of ways you can mark 11 cells in a grid with 15 rows and 10 columns

   (a) without restriction?

   Solution: The marked cells are in a bijection with the set A of all 11-element subsets of the set of 150 grid cells. There are $\binom{150}{11}$ possible subsets.

   (b) so that the marked cells span at least two columns?

   Solution: Let B the set of such markings. Then A is the disjoint union of B and the set of all markings that span exactly one column. There are 10 choices for the columns and $\binom{15}{11}$ choices for the ways to mark the column cells. By the product rule there are $10 \cdot \binom{15}{11}$ such markings. By the sum rule $|B| = \binom{150}{11} - 10 \cdot \binom{15}{11}$.

   (c) so that every column has at least one marked cell?

   Solution: In all such markings C, one column has two marked cells and all others have exactly one marked cell. Each such marking can be uniquely described by specifying the column with two marked cells, the set of two marked cells in that column, and a unique marked cell in all other columns. By the generalized product rule, $|C| = 10 \cdot \binom{15}{2} \cdot 15^9$.

5. The vertices of G_n are the numbers $1, 2, \ldots, n$. The edges are those pairs whose $\gcd(v, w)$ is 1. Circle true of false. Justify your answer.

   (a) For every even n, G_n has a perfect matching.

   Solution: true. The collection $\{1, 2\}, \{3, 4\}, \cdots, \{n-1, n\}$ is a perfect matching. Each of these pairs is an edge because $\gcd(k, k+1) = \gcd(k, 1) = \gcd(1, 0) = 1$. They form a matching because every vertex is touched exactly once.

   (b) For every n, G_n is connected.

   Solution: true. For every pair of vertices $\{u, v\}$ with $u < v$, the sequence $(u, u+1, \ldots, v)$ is a path from u to v. Each consecutive pair is of the form $\{k, k+1\}$. It is an edge by part (a).

   (c) For every n, G_n is bipartite.

   Solution: false. When $n \geq 3$ the graph contains the 3-cycle $(1, 2, 3)$. A graph with an odd-length cycle cannot be bipartite.

BONUS. Prove that the graph G_n in question 5 has $\Theta(n^2)$ edges.
(**Hint:** First prove that for every d, there are at most $\frac{1}{2}(n/d)^2$ unordered pairs of vertices whose GCD is d.)

Solution: G_n has at most $\binom{n}{2} \leq \frac{1}{2}n^2$ edges. It remains to show that it has at least cn^2 edges for some constant c when n is sufficiently large.

Let A_d be the set of all unordered pairs $\{u, v\}$ in $\{1, \ldots, n\}$ whose GCD is d. If $\{u, v\}$ is in A_d then d must divide both u and v. There can be at most n/d multiples of d as the quotient can never exceed this number. Therefore A_d has size at most $\binom{n/d}{2} \leq \frac{1}{2}(n/d)^2$.

As the union of $A_1, A_2, A_3, \ldots$ is the set of all $\binom{n}{2}$ unordered pairs $\{u, v\}$,

$$\binom{n}{2} = |A_1 \cup A_2 \cup A_3 \cup \cdots| \leq |A_1| + |A_2| + |A_3| + \cdots$$

from where

$$\begin{aligned} |A_1| &\geq \binom{n}{2} - \left(|A_2| + |A_3| + |A_4| + \cdots\right) \\ &\geq \binom{n}{2} - \left(\tfrac{1}{2}(n/2)^2 + \tfrac{1}{2}(n/3)^2 + \tfrac{1}{2}(n/4)^2 + \cdots\right) \\ &= \frac{n^2 - n}{2} - \frac{n^2}{2}\left(\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots\right) \end{aligned}$$

By the integral bound,

$$\frac{1}{3^2} + \frac{1}{4^2} + \cdots \leq \int_2^\infty \frac{1}{x^2} dx = -\frac{1}{x}\Big|_2^\infty = \frac{1}{2}$$

so

$$|A_1| \geq \frac{n^2 - n}{2} - \frac{n^2}{2}\left(\frac{1}{2^2} + \frac{1}{2}\right) = \frac{n^2}{8} - \frac{n}{8}$$

which is at least $n^2/16$ when $n \geq 3$.