MATH 420 Exam 1 practice.
This is a bit long, but it will prepare you well, and let you know what to expect.

Short answer

1. Divisibility and gcd’s.

(a) Define: a divides b.
   For \( a, b \in \mathbb{Z} \), \( a \mid b \) if there exists \( d \in \mathbb{Z} \) such that \( b = ad \).
   That is the functional definition (useful) - conceptual: a divides b if b is a multiple of a.

(b) Explain why, if \( a, b \geq 0 \) and \( a \mid b \) and \( b \mid a \), then \( a = b \). What can you say if we remove the restriction that \( a \) and \( b \) can be positive or negative?
   If \( a \mid b \) and \( b \mid a \), then there exist \( h, k \in \mathbb{Z} \) such that \( b = ah \) and \( a = bk \). By substitution we see that \( b = bkh \) and, thus by cancellation, \( 1 = hk \), since \( a \) and \( b \) are positive, \( h \) and \( k \) must be positive, and thus \( h = k = 1 \), so \( a = b \).

(c) State the division algorithm.
   Given \( a, b \in \mathbb{Z} \), \( b > 0 \), there exist unique \( q, r \in \mathbb{Z} \) such that \( a = bq + r \), where \( 0 \leq r < b \).

(d) What is the remainder when -17 is divided by 4?
   \[ -17 = 4(-5) + 3 \]
   So the remainder is \( r = 3 \).

(e) Define: \( d \) is the greatest common divisor of \( a \) and \( b \).
   \( d \) is the greatest common divisor of \( a \) and \( b \) if
   i. \( d \) is a common divisor of \( a \) and \( b \),
   ii. if \( c \) is any common divisor of \( a \) and \( b \), then \( d \mid c \).

(f) Use the Euclidean algorithm to find \( \gcd(150, 84) \), and then express the gcd as a linear combination of 150 and 84. Do NOT use matrix method for this problem (you can use it later if you need to solve such a problem.)
   You should have obtained a gcd of 6 after 4 steps (5 if you count the step where you get 0 as the remainder.)

   After working it backwards, you should get \( \gcd(150, 84) = 6 = 84 \times 9 - 150 \times 5 \).

(g) Define: for \( a, b \in \mathbb{Z} \), \( a \) and \( b \) are relatively prime.
   \( a \) and \( b \) are relatively prime if \( \gcd(a, b) = 1 \).

2. Subsets of integers.

(a) for \( a \in \mathbb{Z} \), define \( a\mathbb{Z} \).
   \( a\mathbb{Z} = \{ax : x \in \mathbb{Z}\} \) (the set of all multiples of \( a \).

(b) Prove: \( a\mathbb{Z} \subseteq b\mathbb{Z} \) if and only if \( a \mid b \).
   This isn’t true. try examples, such as \( a = 2 \), \( b = 6 \)
   What is true?
   \( b\mathbb{Z} \subseteq a\mathbb{Z} \) if and only if \( a \mid b \).
   Proof: Two directions here:
   i. \( \Rightarrow \) If \( b\mathbb{Z} \subseteq a\mathbb{Z} \), then \( b \in a\mathbb{Z} \), so there exists \( t \in \mathbb{Z} \) such that \( b = at \), and thus \( a \mid b \).
   ii. \( \Leftarrow \) If \( a \mid b \), then \( b = as \) for some \( s \in \mathbb{Z} \), thus for any \( x \in b\mathbb{Z} \), \( x = bq \), for some \( q \in \mathbb{Z} \), and by substitution, \( x = aq \in a\mathbb{Z} \).

3. Prove or disprove: \( a\mathbb{Z} \cup b\mathbb{Z} \subseteq \text{lcm}[a, b] \).
   This isn’t true, try some examples. Can you prove that \( \text{lcm}[a, b]\mathbb{Z} \subseteq a\mathbb{Z} \cup b\mathbb{Z} \).

4. Define: \( a \in \mathbb{Z} \) is prime; \( b \in \mathbb{Z} \) is composite.
   \( a \) is prime if it’s only divisors are \( \pm 1 \) and \( \pm a \). A number is composite if it is not prime. Alternatively, \( a \) is composite if it has a divisor other than \( \pm 1 \) and \( \pm a \).
5. Explain why \( a \in \mathbb{Z} \) \( a > 0 \) is prime if and only if \( a \) does not have any divisors \( d \), where \( 0 < d \leq \sqrt{a} \). 

(\( \Rightarrow \)) If \( a \) is prime then it’s only only positive divisors are 1 and \( a \), and these are not in the specified range.

(\( \Leftarrow \)) Do by contradiction, suppose that \( a \) has positive divisors, but none less than \( \sqrt{a} \), then \( a = bc \), where, \( b, c > \sqrt{a} \), and thus \( a = bc > \sqrt{a} \cdot \sqrt{a} = a \), which is a contradiction, and the result follows.

6. Define: \( a \) is congruent to \( b \) modulo \( n \). Then give an equivalent characterization and prove that it is equivalent.

\( a \) and \( b \) are congruent modulo \( n \) if \( a \) and \( b \) have the same divisor when divided by \( n \).

Equivalently, \( n | (b - a) \). See book for proof.

7. Find 6 different integers that are congruent to 4 modulo 17.

Any integer \( c = 17k + 4 \), \( k \in \mathbb{Z} \) will do. So I’ll go with -13, 21, 38, 55, 72, 89.

8. Suppose that \( p_1, p_2, p_3, p_4 \) are distinct primes, and \( a = p_1^3p_2^2p_3 \) and \( b = p_4^2p_3^1p_4^2 \). What are the factorizations of the lcm and gcd of \( a \) and \( b \)?

\( \text{lcm is } p_1^3p_2^2p_3^2 \),

\( \text{gcd is } p_1^1p_3^1p_4^1 \).

Longer answer.

9. Prove: If \( I \) is a subset of integers that is closed under addition and subtraction, then \( I \) is either \( \{0\} \) or \( I = a\mathbb{Z} \) for some \( a \in \mathbb{Z}^+ \).

This is in the book.

10. If we divide \( a \) by \( b \), yielding \( ax + r = b \), then prove \( \text{gcd}(a, b) = \text{gcd}(b, r) \). \([\text{Hint: recall if all common divisors of } a \text{ and } b \text{ divide } r, \text{ then } \text{gcd}(a, b) \text{ divides both } b \text{ and } r. \text{ Thus it divides } \text{gcd}(b, r)].\) Rewrite the equality and similarly prove \( \text{gcd}(b, r) \) divides \( \text{gcd}(a, b) \), and draw your conclusion.

Note \( ax - b = -r \), so if \( d \) divides \( a \) and \( b \), then \( d \) divides \( r \). Thus the gcd of \( a \) and \( b \) divides \( r \). Now clearly, the gcd also divides \( b \), so \( \text{gcd}(a, b) = \text{gcd}(b, r) \).

A similar argument shows that the reverse divides is true too. Then answer follows by 1b above.

11. Prove: if \( (a, b) = 1 \) and \( (a, c) = 1 \), then \( (a, bc) = 1 \).

You know this - if not, it’s in the book.

12. Prove: if \( p \) is prime, and \( p | ab \), then \( p | a \) or \( p | b \). SAME

13. Linear congruences

(a) State a necessary and sufficient condition for \( ax \equiv b \pmod{n} \) to have a solution. [“‘Necessary and sufficient’” is another way of saying “‘if and only if’”]

\( ax \equiv b \pmod{n} \) if and only if \( \text{gcd}(a, n) = b \)

Solve the ones below by checking first if there is a solution. If so, change to a linear combo and use Euclidean algorithm.

(b) Solve: \( 6x \equiv 5 \pmod{8} \)

No solution - 2 doesn’t divide 5.

Next two are similar to example in class.

(c) Solve: \( 7x \equiv 1 \pmod{16} \) (not by inspection)

(d) Find a solution to \( 7x \equiv 3 \pmod{16} \)

14. Prove: if \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( a - c \equiv b - d \pmod{n} \).

See book and notes. END NOTE: MAKE SURE you look at the problems I suggested during review.)

DON’T FORGET EASY INDUCTION PROBLEM EXPECTED?