Study guide

- (§7) Understand the proof of the fundamental theorem of arithmetic (unique factorization into primes).
- (§8) Know the definition of $a \equiv b \mod m$.
- (§8) How do you solve *linear congurences* $ax \equiv b \mod m$?

1. (Textbook 8.1)
   Suppose that $a_1 \equiv b_1 (\mathrm{mod} m)$ and $a_2 \equiv b_2 (\mathrm{mod} m)$.
   (a) Verify that $a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod} m)$ and that $a_1 - a_2 \equiv b_1 - b_2 (\mathrm{mod} m)$.
   (b) Verify that $a_1 a_2 \equiv b_1 b_2 (\mathrm{mod} m)$.

2. For each number k between 0 and 8 (inclusive), either find two different prime numbers p such that $p \equiv k \pmod 9$, or prove that it is impossible to do so.

3. Solve each of the following linear congruences. Your answer should describe the set of all integer solutions, and can be stated in terms of congruences (e.g. like in class, when we saw that the solutions to $3x \equiv 5 \mod 8$ are given by $x \equiv 7 \mod 8$).
   (a) $7x \equiv 4 \pmod 5$
   (b) $x^2 \equiv 3 \pmod{13}$
   (c) $9x \equiv 6 \pmod{15}$

4. Two integers x and y are called *inverses* modulo 24 if $xy \equiv 1 \pmod{24}$.
   (a) Prove that if x has an inverse modulo 24, then this inverse is unique modulo 24 (that is, if y_1, y_2 are both inverses of x modulo 24, then $y_1 \equiv y_2 \pmod{24}$).
   (b) Which x between 0 and 23 inclusive have inverses modulo 24? For each such x, find an inverse y.

5. A notion closely related to the greatest common divisor $\gcd(a, b)$ is the least common multiple $\mathrm{lcm}(a, b)$, which is defined to be the smallest positive integer that is a multiple of both a and b. Throughout this problem, assume that a, b are positive integers (in particular, that neither is zero).
   (a) Prove that if $\gcd(a, b) = 1$, then $\mathrm{lcm}(a, b) = ab$.
   (b) Prove that for any positive integer k, $\mathrm{lcm}(ka, kb) = k \cdot \mathrm{lcm}(a, b)$.
   (c) Deduce from parts (a) and (b) that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$.