The second exam will be on Thursday, March 29. The syllabus will consist of Chapter NT from the text, together with the two number theory supplements passed out in class (Divisibility and Congruences). For reference, I will refer to these as Supplement D and Supplement C. You should be able to do all of the assigned problems, both suggested and those that were turned in.
Following are some of the concepts and results that were covered in class and that you should know:

- Know the definition of a *divides* b for integers a and b (notation: $a|b$). This is also referred to as b is *divisible* by a. (Definition 1.1, Supp. D).
- Know the *Division Algorithm*. (Theorem 1.2, Supp. D).
- Know the definition of the *greatest common divisor* of the integers a and b (notation: (a, b) or $\gcd(a, b)$).
- Know the *Euclidean Algorithm* (Theorem 1.11, Supp. D and Example 12, Section NT-2, Page 70) and how to use it to compute the greatest common divisor of integers a and b.
- Know how to use the Euclidean algorithm to write the greatest common divisor g of two integers a and b in the form $g = ax + by$, for some integers x and y. (See Page 8, Supp. D.)
- Know the definition of *relatively prime integers*.
- Be sure to know Theorem 1.10 (Page 7, Supp. D) which relates the relative primeness of two integers to a divisibility conclusion: *If* $c|ab$ *and* $\gcd(b, c) = 1$*, then* $c|a$.
- Know the definition of *least common multiple* of integers a and b (notation: $[a, b]$ or $\text{lcm}(a, b)$).
- Know the relationship between the greatest common divisor, least common multiple, and the product of integers a and b: $ab = (a, b)[a, b]$.
- Know the definition of *prime* number.
- Know the definition of *composite* number.
- Know Euclid's Lemma (Theorem 1.15 Page 14, Supp. D): If p is a prime, a and b are integers, and $p|ab$, then $p|a$ or $p|b$.
- Know the Fundamental Theorem of Arithmetic (Theorem 1.16, Page 14, Supp. D, and Theorem 1, Page 55 of Section NT-1.), and how to use it to compute the greatest common divisor and least common multiple of two integers a and b (Theorem 6, Page 69, Section NT-2, and Pages 15-16 of Supp. D).
- Know Euclid's argument to show that there are infinitely many prime integers. (Theorem 1.17, Page 16 of Supp. D, and Theorem 2, Page 56 of Section NT-1.)
- Know what it means for an integer a to be *congruent modulo* n to another integer b (notation $a \equiv b \mod n$).
- Know the definition of *congruence class or residue class of* a *modulo* n (notation $[a]_n = n\mathbb{Z} + j = \{nk + j : k \in \mathbb{Z}$ and j is the remainder when a is divided by $n\}$). Sup. C, Page 53 or Section NT-1, Page 58.

- Know the number system $\mathbb{Z}_n$ of congruence classes modulo n, and how to do arithmetic in $\mathbb{Z}_n$:

$$\begin{aligned} [a]_n + [b]_n &= [a+b]_n \\ [a]_n[b]_n &= [ab]_n \end{aligned}$$

  See Supp. C, Page 53 or Theorem 4, Section NT-1, Page 59.

- Know what it means to solve a *linear congruence*

$$ax \equiv b \mod n.$$

  In particular, know that the solutions form congruence classes modulo n, so that they can be identified with elements of $\mathbb{Z}_n$. See Theorem 8.1, Supp. C.

- Know the criterion for solvability of a linear congruence, namely Theorem 8.1, Supp. C, and know how to find all of the solutions to a linear congruence using the algorithm on Page 56 Supp. C, based on the Euclidean algorithm to find the greatest common divisor of a and n.

- The congruence class $[a]_n$ *is invertible* in $\mathbb{Z}_n$, or a is invertible modulo n if the congruence equation $ax \equiv 1 \pmod{n}$ is solvable. A solution of this congruence is denoted $x = [a]_n^{-1}$

- Know the criterion of invertibility of $[a]_n$: An element $[a]_n \in \mathbb{Z}_n$ is invertible (or a has a multiplicative inverse modulo n) if and only if $(a,\, n) = 1$, that is, if and only if a and n are relatively prime. Moreover, if r and s are integers such that $ar + ns = 1$, then $[a]_n^{-1} = [r]_n$. See the note following Theorem 8.1, Supp. C.

- Know how to use the Euclidean algorithm to compute $[a]_n^{-1}$, when the inverse exists.

- Know Fermat's theorem: if p is prime and p does not divide a then $a^{p-1} \equiv 1 \mod p$. (Theorem 9.1, Page 61 of Supp. C).

- The Euler phi-function is defined by

$$\varphi(n) = \#\left\{a : 1 \le a \le n \text{ and } \gcd(a,\, n) = 1\right\},$$

  where $\#S$ denotes the number of elements in the set S. Thus $\varphi(n)$ is the *number of integers between* 1 *and* n *that are relatively prime to* n.

- Know how to use Theorem 11.1 (Supp. C, Page 72) to compute $\varphi(n)$ from the prime factorization of n: If $n = p_1^{k_1} \cdots p_r^{k_r}$, then

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_1^{k_r} - p_1^{k_r-1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

- Know Euler's Theorem: If $n \ge 2$ and a is relatively prime to n, then

$$a^{\varphi(n)} \equiv 1 \mod n.$$

- Know how to use Euler's Theorem to compute powers a^k modulo n, as we did in class and on Exercise Set 5.

- Know the Chinese Remainder Theorem (Theorem 11.2, Page 74 of Supp. C), and how to solve simultaneous congruences.

Review Exercises

Be sure that you know how to do all assigned homework exercises. The following are supplementary exercises, in many but not all cases, similar to those already assigned as homework. These exercises are listed randomly. That is, there is no attempt to give the exercises in the order of presentation of material in the text.

1. The following are **True/False** questions. Decide if each statement is True or False. You should be able to explain your reasoning.

   (a) If a, b, and c are nonzero integers such that $c|a$ and $c|b$, then $\gcd(a, b) \leq c$.

   (b) $\gcd(a, 1) = 1$ for any integer a.

   (c) The integers 77 and 105 are relatively prime.

   (d) If a, b, and c are integers such that $a|bc$, then $a|b$ or $a|c$.

   (e) If a, b, and c are integers such that $a|b$ and $c|b$, then $ac|b$.

   (f) If $\gcd(a, b) = \text{lcm}(a, b)$, then $a = b$.

   (g) If $a|c$ and $b|c$, then $\text{lcm}(a, b) \leq c$.

   (h) If a and b are relatively prime natural numbers, then $\text{lcm}(a, b) = ab$.

   (i) If $(a, b) = 1$ and $(c, d) = 1$, then $(ac, bd) = 1$.

   (j) If there exist integers r and s such that $ra + sb = d$, then $d = (a, b)$.

   (k) Every natural number $n \geq 2$ cam be written $n = p_1 p_2 \cdots p_r$ as the product of distinct prime numbers $p_1, p_2, \ldots, p_r$.

   (l) For all $n \in \mathbb{N}$, $n > 1$, there exists a prime p such that $p|n$.

   (m) There exists a prime p such that $p|n$ for all $n \in \mathbb{N}$, $n > 1$.
   (The position of the universal quantifier makes a lot of difference!)

   (n) $5x \equiv 3 \pmod{10}$ has no solution.

   (o) $49x \equiv 1 \pmod{81}$ has no solution.

   (p) $84^{10} \equiv 1 \pmod{11}$.

2. Find the remainder when b is divided by a if:

   (a) $a = 6$, $b = 25$

   (b) $a = -6$, $b = -25$

3. This problem involves arithmetic modulo 16. All answers should only involve expressions of the form $[a]_{16}$, with a an integer and $0 \leq a < 16$.

   (a) Compute $[4]_{16} + [15]_{16}$.

   (b) Compute $[4]_{16}[15]_{16}$.

   (c) Compute $[15]_{16}^{-1}$.

   (d) List the invertible elements of $\mathbb{Z}_{16}$.

4. Express 24 and 102 a products of primes and use this information to calculate (12, 102) and [12, 102].

5. Find the prime factorization of each of the following natural numbers.
   (a) 856 (b) 2323
   (c) 6647 (d) $(2^8 - 1)^{20}$

6. Determine all $x \in \mathbb{Z}$ that solve the linear congruence
$$6x \equiv 9 \mod 15.$$

7. (a) Find the greatest common divisor $d = (803, 154)$ of 803 and 154, using the Euclidean Algorithm.
   (b) Write $d = (803, 154)$ in the form $d = s \cdot 803 + t \cdot 154$.
   (c) Find the least common multiple [803, 154].

8. Compute $3^{80} \pmod 7$.

9. Find all integers such that $5x \equiv 1 \pmod{100}$. Briefly explain your answer.

10. Solve the system of congruences:
$$\begin{aligned} x &\equiv 5 \pmod{25} \\ x &\equiv 23 \pmod{32}. \end{aligned}$$

11. Find the smallest positive integer that gives a remainder of 5 when divided by 341 and a remainder of 11 when divided by 189.

12. Give an example of integers a, b, m, n such that the system of congruences
$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$
has no solution.