The first exam will be on Monday, October 28, 2019. The syllabus will be Chapter 4 (Sections 4.1–4.3) and Chapter 5 (Sections 5.1–5.6) in Long.
Following are some of the concepts and results you should know:

- Know the definition and basic properties of *congruence modulo* m.
- Know what is meant by the *least residue modulo* m.
- Know how the integers are divided into *congruence classes modulo* m.
- Know the basic properties of the algebra of congruence modulo m, as expressed in Theorem 4.3, Corollaries 4.5, 4.5, and Theorem 4.6.
- Know the *cancellation law for congruence modulo* m: If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$.
- Know the theorem (Theorem 4.9) relating congruence modulo m, n and mn for relatively prime moduli m and n: If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ and $(m, n) = 1$, then $a \equiv b \pmod{mn}$.
- Know how to use congruence to establish some special divisibility criteria (Theorem 4.12).
- Know the definition of the *Euler ϕ-function* and *reduced residue system modulo* m.
- Know the key facts about $\phi(m)$:
  1. $\phi(1) = 1$
  2. $\phi(p^k) = p^k - p^{k-1}$ if p is prime and $k \geq 1$.
  3. $\phi(mn) = \phi(m)\phi(n)$ provided $(m, n) = 1$.
  4. If $n = \prod_{i-1}^{r} p_i^{k_i}$ with $k_i \geq 1$ and $p_1, p_2, \ldots, p_r$ distinct primes, then
  $$\phi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$
- If $S = \{a_1, a_2, \ldots, a_{\phi(m)}\}$ is a reduced residue system modulo m and $(k, m) = 1$, then $kS = \{ka_1, ka_2, \ldots, ka_{\phi(m)}\}$ is also a reduced residue system modulo m.
- Know *Fermat's Theorem*: If p is a prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.
- Know the extension of Fermat' theorem to arbitrary m (*the Euler-Fermat theorem*): If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.
- Know the criteria for solvability of linear congruences: The linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $d \mid b$, where $d = (a, m)$. If there are any solutions, then there are exactly d incongruent solutions modulo m.
- In addition to knowing the statement of the linear congruence theorem (Theorem 5.1), you should know how to use the Euclidean algorithm to find a single solution, and then all solutions: Write $d = ar + ms$ using the Euclidean algorithm. Since $d \mid b$ write $b = kd$ and multiply by k to get $b = kd = akr + mks$. Then $x_0 = kr$ is one solution. Then all of the incongruence solutions are:
$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}.$$

- Know how to use the solution of linear congruences to solve the linear diophantine equation $ax + by = r$: This equation is solvable in integers if and only if $d \mid r$, where $d = (a, b)$. If x_0, y_0 is any solution, then every solution is given by

$$x_k = x_0 + k\frac{b}{d}, \quad y_k = y_0 - k\frac{a}{d},$$

  where k is any integer.

- Know the *Chinese Remainder Theorem*: If m_1, m_2, ..., m_r are pairwise relatively prime positive integers (that is $(m_i, m_j) = 1$ for $i \neq j$), then the simultaneous system of congruences

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_r \pmod{m_r}, \end{aligned}$$

  is solvable and the solution is unique modulo $m = \prod_{i=1}^{r} m_i$.

  Know how to actually solve this system using the solution of linear congruences: Let $M_i = M/m_i$ and solve $M_i y \equiv 1 \pmod{m_i}$ for $y = b_i$, which is possible since $(m_i, M_i) = 1$. Then $x_0 = \sum_{i=1}^{r} c_i M - i b_i$ is a solution of the simultaneous congruence. All other solutions have the form $x = x_0 + kM$ for an integer k.

- Know how to translate the solution of a congruence modulo $m = \prod_{i=1}^{r} m_i$ with $(m_i, m_j) = 1$ for $k \neq j$ into a simultaneous system of congruences (Theorem 5.3), which can be handled by the Chinese Remainder Theorem: Any solution of $f(x) \equiv 0 \pmod{m}$ is a simultaneous solution of the system

$$\begin{aligned} f(x) &\equiv 0 \pmod{m_1} \\ f(x) &\equiv 0 \pmod{m_2} \\ &\vdots \\ f(x) &\equiv 0 \pmod{m_r}, \end{aligned}$$

  and conversely.

- Theorem 5.3 reduces the polynomial congruence $f(x) \equiv 0 \pmod{m}$ into a simultaneous system of congruences of the form $f(x) \equiv 0 \pmod{p^k}$ where p is a prime divisor of m. Know how to use linear congruences to find solutions of $f(x) \equiv 0 \pmod{p^k}$ from known solutions of $f(x) \equiv 0 \pmod{p^{k-1}}$ (Theorem 5.7):

  If p is a prime and $k \geq 2$ is an integer and x_{k-1} is a solution of the congruence $f(x) \equiv 0 \pmod{p^{k-1}}$, then x_k is a solution of $f(x) \equiv 0 \pmod{p^k}$ if and only if $x_k = x_{k-1} + y_0 p^{k-1}$ where y_0 is a solution of the linear congruence

$$\frac{f(x_{k-1})}{p^{k-1}} + y f'(x_{k-1}),$$

  where $f'(x)$ is the derivative of $f(x)$. (This is known as Hensel's lemma.)

- Know Lagrange's theorem: If p is a prime and $f(x) = \sum_{i=0}^{n} a_i x^i$ is an integer polynomial of degree n with $a_n \not\equiv 0 \pmod{p}$ then the polynomial congruence $f(s) \equiv 0 \pmod{p}$ has at most n incongruent solutions modulo p.
- Know examples where Lagrange's theorem fails if the modulus m is not prime.
- Know Wilson's theorem: If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.
- Know how to reduce a quadratic congruence $f(x) = ax^2 + bx + c \equiv 0 \pmod{p}$ where $p \nmid a$, via completion of the square to the congruence $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$. This then reduces to two problems: (1) Solve the quadratic $y^2 \equiv b^2 - 4ac \pmod{p}$, if possible, and (2) solve $2ax + b \equiv y \pmod{p}$. the second one will always be possible. The first may or may not be solvable.
- Know what is meant by *quadratic reside modulo p* and *quadratic nonresidue modulo p* for p a prime. Specifically, if n is an integer and $(n, p) = 1$ then n is a quadratic residue modulo p if $x^2 \equiv n \pmod{p}$ is solvable; otherwise n is a quadratic nonresidue modulo p.
- Know the definition of Legendre symbol (Definition 5.2): If p is an odd prime and $(n, p) = 1$ then the Legendre symbol $\left(\frac{n}{p}\right)$ is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } n \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

- Know the basic facts about Legenre symbols:
  1. $\left(\frac{n^2}{p}\right) = 1$.
  2. $\left(\frac{nn}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) = 1$.
  3. $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}$. (Euler's Criterion (Theorem 5.12))
  4. If $n \equiv m \pmod{p}$ then $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$.
- Know Gauss's lemma (Theorem 5.14): Let p be an odd prime and n an integer with $(n, p) = 1$. Let S be the set of least positive residues of the integers n, $2n$, ..., $\frac{1}{2}(p-1)n$. Let r be the number of elements of S that are greater than $p/2$. Then $\left(\frac{n}{p}\right) = (-1)^r$.
- Know Gauss's Quadratic Reciprocity Law (Theorem 5.15): If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

  An alternate statement is that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless p and q are both congruent to 3 modulo 4, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.
- Special cases:: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{for } p \equiv 1 \pmod{4} \\ -1 & \text{for } p \equiv 3 \pmod{4} \end{cases}$, $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{for } p \equiv \pm 1 \pmod{8} \\ -1 & \text{for } p \equiv \pm 3 \pmod{8} \end{cases}$.

Review Exercises

Be sure that you know how to do all assigned homework exercises. The following are a few supplemental exercises 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. Let $n = 13645x04142250$. Answer the following questions about n.

   (a) If $9 \mid n$ then what is x?

   ▶ **Solution.** The sum of the digits of n is $s = 1+3+6+4+5+x+0+4+1+4+2+2+5+0 = x + 37 \equiv 0 \pmod 9$ if $9 \mid n$. Thus, $x \equiv -37 \equiv -1 \pmod 9$. Since x is a digit of n, $x = 8$. ◀

   (b) If $n \equiv 5 \pmod{11}$ then what is x?

   ▶ **Solution.** If t is the alternating sum of the digits of n, then $t \equiv n \pmod{11}$. Thus, $t \equiv 5 \pmod{11}$ so

   $$t - 5 = 0 - 5 + 2 - 2 + 4 - 1 + 4 - 0 + x - 5 + 4 - 6 + 3 - 1 - 5 = x - 8 \equiv 0 \pmod{11},$$

   so $x = 8$. ◀

2. Decide whether the following linear Diophantine equations have any integer solutions. If so, give the general solution in integers, if not say why there are no solutions.

   (a) $33x + 21y = 20$.

   ▶ **Solution.** The greatest common divisor $(33,\ 21) = 3$ and $3 \nmid 20$ so there is no solution. ◀

   (b) $33x - 21y = 15$.

   ▶ **Solution.** The greatest common divisor $(33,\ -21) = 3$ and $3 \mid 15$ so there are solutions. Divide by 3 to get an equivalent equation $11x - 7y = 5$. By inspection, or use the Euclidean algorithm to get $11 \cdot 3 - 7 \cdot 4 = 5$, so one solution is $x = 3$, $y = 4$, and the general solution is $x_k = 3 + 7k$, $y_k = 4 + 11t$ for any integer k. ◀

3. What is the least residue of 554^{455} modulo 5?

   ▶ **Solution.** $554 \equiv -1 \pmod 5$ so $554^{455} \equiv (-1)^{455} \equiv -1 \equiv 4 \pmod 5$. ◀

4. Determine if each of the following statements is True or False.

   (a) $-63 \equiv 3 \pmod 3$ True

   (b) $\{15,\ 24,\ -3,\ -22,\ -1\}$ is a complete residue system modulo 5. False. $24 \equiv -11 \pmod 5$.

   (c) $\{1,\ 5,\ 7,\ 23\}$ is a reduced residue system modulo 12.True. $23 \equiv 11 \pmod{12}$.

(d) $15x \equiv 21 \pmod{35}$ has 5 solution modulo 35.False. $5 \nmid 21$ so there are no solutions.

(e) If $\{x_1, \ldots, x_k\}$ is a reduced residue system modulo m, then so is $\{-x_1, \ldots, -x_k\}$True. $(-1, m) = 1$

(f) Euler's theorem says that $a^{\phi(n)} \equiv 1 \pmod{n}$ for all positive integers a. False. Need the assumption $(a, m) = 1$.

(g) If $(n-1)! \equiv -1 \pmod{n}$, then n is prime. True. If $n = rs$ for $1 \leq r < n$ then $r \mid n$ and $r \mid (n-1)!$ so $r \mid -1$ which implies $r = 1$ and thus $s = n$. Hence n is prime.

(h) $\phi(55 \cdot 99) = \phi(55)\phi(99)$. False. $(55, 99) = 11 \neq 1$.

5. What is $\phi(350)$? $\phi(2400)$?

► **Solution.** $\phi(350) = \phi(2 \cdot 5^2 \cdot 7) = \phi(2) \cdot \phi(5^2) \cdot \phi(7) = (2-1)(5^2-5)(7-1) - 20 \cdot 6 = 120$.
$\phi(2400) = \phi(2^5 \cdot 3 \cdot 5^2) = (2^5 - 2^4)(3-1)(5^2-5) = 640$. ◄

6. Find three distinct positive integers n with $\phi(n) = 16$.

► **Solution.**

$$\begin{aligned}
16 = 2^4 = 2^5 - 2^4 &\implies n = 2^5 \\
16 = 17 - 1 &\implies n = 17 \text{ or } 2 \cdot 17 \\
16 = 2^2(5-1) &\implies n = 2^3 \cdot 5 \\
16 = 2(3-1)(5-1) &\implies n = 2^2 \cdot 3 \cdot 5 \\
16 = 2^3(3-1) &\implies n = 2^4 \cdot 3
\end{aligned}$$

Thus, integers with $\phi(n) = 16$ include $n = 17$, 32, 34, 40, 48, and 60. ◄

7. Determine if the following quadratic congruences are solvable? You may assume that 6869 is prime. Just determine if each is solvable; do not try to find a solution if it happens to be solvable.

(a) $x^2 \equiv -1 \pmod{6869}$

► **Solution.** $6869 = 4 \cdot 1717 + 1$ so $6869 \equiv 1 \pmod{4}$. Thus $\left(\frac{-1}{6869}\right) = 1$ and hence -1 is a quadratic residue modulo 6869. ◄

(b) $x^2 \equiv 2 \pmod{6869}$

► **Solution.** $6869 = 8 \cdot 858 + 5$ so $6869 \equiv 5 \pmod{8}$. Thus $\left(\frac{2}{6869}\right) = -1$ and hence 2 is a quadratic nonresidue modulo 6869. ◄

8. Use the Chinese Remainder Theorem to solve the following system of simultaneous congruences.

$$\begin{aligned}
x &\equiv 2 \pmod{5} \\
x &\equiv 4 \pmod{7} \\
x &\equiv 1 \pmod{8}
\end{aligned}$$

▶ **Solution.** $c_1 = 2$, $m_1 = 5$, $M_1 = 56$, $56x_1 \equiv 1 \pmod 5$ so $x_1 \equiv 1 \pmod 5$.
$c_2 = 4$, $m_2 = 7$, $M - 2 = 40$, $40x_2 \equiv 1 \pmod 7$ so $5x_2 \equiv 1 \pmod 7$ and $x_2 \equiv 3 \pmod 7$.
$c_3 = 1$, $m_3 = 8$, $M_3 = 35$, $35x_3 \equiv 1 \pmod 8$ so $3x_3 \equiv 1 \pmod 8$ and $x_3 \equiv 3 \pmod 8$.
$M = 5 \cdot 7 \cdot 8 = 280$. Thus,

$$\begin{aligned} x &\equiv c_1M_1x_1 + c_2M_2x_2 + c_3M_3x_3 \pmod M \\ &\equiv 2 \cdot 56 \cdot 1 + 4 \cdot 40 \cdot 3 + 1 \cdot 35 \cdot 3 \pmod{280} \\ &\equiv 697 \pmod{280} \\ &\equiv 137 \pmod{280}. \end{aligned}$$

Check: $5 \mid (137 - 2)$, $7 \mid (137 - 4)$, $8 \mid (137 - 1)$. ◀

9. For each of the following congruences, determine the number of incongruent solutions. It is not necessary to give the solutions, just the number.

   (a) $48x \equiv 128 \pmod{1000}$

   ▶ **Solution.** The greatest common divisor $(48, 1000) = 8$ and $8 \mid 128$ so the linear congruence is solvable and has 8 incongruent solution modulo 1000. ◀

   (b) $x^2 + x + 1 \equiv 0 \pmod{14}$

   ▶ **Solution.** There are no solutions. If there were a solution, then the same $x = a$ would also be a solution to $x^2 + x + 1 \equiv 0 \pmod 2$, but substituting 0 and 1 mod 2 into the polynomial gives 1 mod 2 so there is no solution mod 2 and hence none mod 14. ◀

   (c) $x^2 + x + 1 \equiv 0 \pmod{91}$

   ▶ **Solution.** Since $91 = 7 \cdot 13$, this congruence is equivalent to the system of simultaneous congruences

$$\begin{aligned} x^2 + x + 1 &\equiv 0 \pmod 7 \\ x^2 + x + 1 &\equiv 0 \pmod{13}. \end{aligned}$$

   Since $1 \equiv -6 \pmod 7$, the first congruence becomes $x^2 + x - 6 = (x + 3)(x - 2) \equiv 0 \pmod 7$ which has 2 incongruent solutions mod 7 (namely, 22, -3). Also, $1 \equiv -12 \pmod{13}$ so the second congruence becomes $x^2 + x - 12 = (x + 4)(x - 3) \equiv 0 \pmod{13}$, which has 2 incongruent solutions modulo 13, namely 3, -4. Hence, there are $4 = 2 \cdot 2$ solutions of the simultaneous system obtained by solving the 4 simultaneous congruences by the Chinese Remainder Theorem:

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod{13} \end{aligned} \qquad \begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv -4 \pmod{13} \end{aligned}$$

$$\begin{aligned} x &\equiv -3 \pmod 7 \\ x &\equiv 3 \pmod{13} \end{aligned} \qquad \begin{aligned} x &\equiv -3 \pmod 7 \\ x &\equiv 4 \pmod{13}. \end{aligned}$$

   (Solutions are 4, 9, 16, 81 modulo 91.) ◀

10. Find the least complete solution of each of the following quadratic congruences.

(a) $x^2 - 3x + 1001 \equiv 0 \pmod 3$

▶ **Solution.** Reduce the coefficients modulo 3 to get $x^2 - 1 \equiv 0 \pmod 3$ which has solutions $x \equiv \pm 1 \pmod 3$. ◀

(b) $x^2 - 3x + 1001 \equiv 0 \pmod 5$

▶ **Solution.** Reduce the coefficients modulo 5 to get $x^2 - 3x + 1 \equiv x^2 + 2x_1 \equiv (x+1)^2 \equiv 0 \pmod 5$. The unique solution is $x \equiv -1 \pmod 5$. ◀

(c) $x^2 - 3x + 1001 \equiv 0 \pmod{15}$

▶ **Solution.** This is equivalent to the simultaneous system of congruences

$$\begin{aligned} x^- 3x + 1001 &\equiv 0 \pmod 3 \\ x^- 3x + 1001 &\equiv 0 \pmod 5 \end{aligned}$$

From part (a) and (b), this becomes the simultaneous congruences

$$\begin{aligned} x &\equiv 1, \ -1 \pmod 3 \\ x &\equiv -1 \pmod 5 \end{aligned}$$

The solutions modulo 15 are 4 and 14. ◀

11. Find the least complete solution of the congruence $x^3 + x^2 + 1 \equiv 0 \pmod{27}$.

▶ **Solution.** Let $f(x) = x^3 + x^2 + 1$. Start with the congruence $f(x) \equiv 0 \pmod 3$. Using the following table we find that a complete solution is $x_1 = 1$:

x	0	1	2
$f(x)$	1	3	13

Note that $f'(x) = 3x^2 + 2x$. Look for solutions x_2 of $f(x) \equiv 0 \pmod 9$ of the form $x_2 = x_1 + 3y$ where y satisfies the linear congruence $\frac{f(x_1)}{3} + f'(x_1)y \equiv 0 \pmod 3$. For $x_1 = 1$ the linear congruence is $1 + 5y \equiv 0 \pmod 3$ and a complete solution is $y = 1$. Thus, $x_2 = 1 + 1 \cdot 3 = 4$.

Now find solutions of $f(x) \equiv 0 \pmod{27}$ of the form $x_3 = x_2 + 9y$ where y satisfies the linear congruence $\frac{f(x_2)}{9} + f'(x_2)y \equiv 0 \pmod 3$. For $x_2 = 4$, $f(x_2) = 64 + 16 + 1 = 81$ and $f'(x_2) = 3 \cdot 4^2 + 2 \cdot 4 = 56$. Thus the linear congruence is $9 + 56y \equiv 0 \pmod 3$ and a complete solution is $y = 0$. Thus, $x_3 = 4$ is a complete solution modulo 27 to the original congruence $f(x) \equiv 0 \pmod{24}$. ◀

12. Find the least complete solution of the congruence $3x^2 + 3x - 5 \equiv 0 \pmod{53}$.

▶ **Solution.** Note that the discriminant is $b^2 - 4ac = 9 - 4(3)(-5) = 69 \equiv 16 \pmod{53}$. Thus $y = \pm 4$ is a complete solution to $y^2 \equiv b^2 - 4ac \pmod{53}$. Now, we need to solve $2ax \equiv 2(3)x \equiv -3 \pm 4 \pmod{53}$ or $6x \equiv 1 \pmod{53}$ and $6x \equiv -7 \pmod{53}$. Since $9 \cdot 6 \equiv 1 \pmod{53}$, the solutions are obtained by multiplying by 9. Thus, the two solutions are 9 and $-63 \equiv 43 \pmod{53}$. ◀

13. Compute the following Legendre symbols.

(a) $\left(\frac{50}{71}\right)$ (b) $\left(\frac{32}{101}\right)$ (c) $\left(\frac{65}{67}\right)$ (d) $\left(\frac{162}{53}\right)$

▶ **Solution.** (a) $\left(\frac{50}{71}\right) = \left(\frac{2}{71}\right)\left(\frac{5^2}{71}\right) = \left(\frac{2}{71}\right) = 1$ since $71 \equiv -1 \pmod 8$.

(b) $\left(\frac{32}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{4^2}{101}\right) = \left(\frac{2}{101}\right) = -1$ since $101 \equiv 5 \pmod 8$.

(c) $\left(\frac{65}{67}\right) = \left(\frac{13}{67}\right)\left(\frac{5}{67}\right) = \left(\frac{67}{13}\right)\left(\frac{67}{5}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ since $13 \equiv 5 \pmod 8$.

(d) $\left(\frac{162}{53}\right) = \left(\frac{2}{53}\right)\left(\frac{9^2}{53}\right) = \left(\frac{2}{53}\right) = -1$ since $2 \equiv 5 \pmod 8$.

◀