

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, \dots, p_r distinct primes, then

$$\phi(n) = n \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

- If $S = \{a_1, a_2, \dots, a_{\phi(m)}\}$ is a reduced residue system modulo m and $(k, m) = 1$, then $kS = \{ka_1, ka_2, \dots, ka_{\phi(m)}\}$ 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's 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:

$$x_0, x_0 + \frac{m}{d}, \dots, x_0 + \frac{(d-1)m}{d}.$$

- 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, \dots, 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 residue 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 Legendre symbols:

1. $\left(\frac{n^2}{p}\right) = 1$.
2. $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) = 1$.
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 $n, 2n, \dots, \frac{1}{2}(p-1)n$. 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.

- Let $n = 13645x04142250$. Answer the following questions about n .
 - If $9 \mid n$ then what is x ?
 - If $n \equiv 5 \pmod{11}$ then what is x ?
- 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.
 - $33x + 21y = 20$.
 - $33x - 21y = 15$.
- What is the least residue of 554^{455} modulo 5?
- Determine if each of the following statements is True or False.
 - $-63 \equiv 3 \pmod{3}$
 - $\{15, 24, -3, -22, -1\}$ is a complete residue system modulo 5.
 - $\{1, 5, 7, 23\}$ is a reduced residue system modulo 12.
 - $15x \equiv 21 \pmod{35}$ has 5 solution modulo 35.
 - If $\{x_1, \dots, x_k\}$ is a reduced residue system modulo m , then so is $\{-x_1, \dots, -x_k\}$
 - Euler's theorem says that $a^{\phi(n)} \equiv 1 \pmod{n}$ for all positive integers a .
 - If $(n-1)! \equiv -1 \pmod{n}$, then n is prime.
 - $\phi(55 \cdot 99) = \phi(55)\phi(99)$.
- What is $\phi(350)$? $\phi(2400)$?
- Find three distinct positive integers n with $\phi(n) = 16$.
- 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.
 - $x^2 \equiv -1 \pmod{6869}$
 - $x^2 \equiv 2 \pmod{6869}$
- Use the Chinese Remainder Theorem to solve the following system of simultaneous congruences.

$$x \equiv 2 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

$$x \equiv 1 \pmod{8}$$

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

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

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

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

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

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

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

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

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

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) $\left(\frac{162}{53}\right)$