The third exam will be on Monday, November 25, 2019. The syllabus will be Sections 2.6, 5.7, 6.3, 7.1, and 8.1 – 8.4 in Long.
Following are some of the concepts and results you should know. The material covered was cumulative and some basic results from previous sections is also summarized, since it is commonly needed for the current material.

- Know the definition of *Pythagorean triple* and *primitive Pythagorean triple*: Three positive x, y, z form a Pythagorean triple if $x^2 + y^2 = z^2$. Thus, a triple x, y, z is a Pythagorean triple if and only if there is a right triangle with sides x, y, and hypotenuse z. The Pythagorean triple is primitive provided $(x, y, z) = 1$.

- Know the description of primitive Pythagorean triples given in Theorem 2.26: The positive integers x, y, z with x even form a primitive Pythagorean triple if and only if there are positive integers $s < t$, with $(s, t) = 1$, with one of s and t even and the other odd, such that $x = 2st$, $y = t^2 - s^2$, and $t^2 + s^2$.

- 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.

- 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 the definition of *order of a modulo n*, denoted $k = \operatorname{ord}_n a$. If $n > 1$ and $(a, n) = 1$, then the order of a modulo n is the smallest positive integer k with $a^k \equiv 1 \pmod{n}$.

- Know the basic properties of order:

  1. If $\operatorname{ord}_n a = k$, then $a^h \equiv 1 \pmod{n}$ if and only if $k \mid h$. In particular, from Euler's theorem, it follows that $k \mid \phi(n)$.

2. If $\operatorname{ord}_n a = k$, then $a^r \equiv a^s \pmod{n}$ if and only if $r \equiv s \pmod{k}$. Thus, if $\operatorname{ord}_n a = k$, then a, a^2,..., a^k are incongruence modulo n.
3. Know the relationship between $\operatorname{ord}_n a^h$ and $\operatorname{ord}_n a$: If $\operatorname{ord}_n a = k$ and $h > 0$, then

$$\operatorname{ord}_n a^h = \frac{k}{(h,\, k)}.$$

In particular, $\operatorname{ord}_n a^h = k = \operatorname{ord}_n a$ if and only if $(h,\, k) = 1$.

- Know what it means for a to be a *primitive root modulo* n: If $(a,\, n) = 1$ and $\operatorname{ord}_n(a) = \phi(n)$, then a is a primitive root modulo n.
- Theorem: If $(a,\, n) = 1$ and a is a primitive root modulo n, then the powers a, a^2, ... , $a^{\phi(n)}$ are a reduced residue system modulo n.

  Corollary: If there is a primitive root modulo n, then there are exactly $\phi(\phi(n))$ primitive roots modulo n.
- Know Gauss's lemma: If $n \geq 1$ then $n = \sum_{d|n} \phi(d)$ where the sum is over all positive divisors of n.
- Know Theorem 5.24: If p is a prime number then there is at least one integer a such that a is a primitive root modulo p.

  Corollary: There are exactly $\phi(p-1)$ primitive roots modulo p for each prime p.
- Know the definition of index modulo p: If p is an odd prime and q is a primitive root modulo p, then r *is the index of* n *to the base* q *modulo* p, denoted $r = \operatorname{ind}_q n \pmod{p}$ if and only if $n \equiv q^r \pmod{p}$ and $0 \leq r < p-1$. In other words, $\operatorname{ind}_q n \pmod{p}$ is the exponent r such that $q^r \equiv n \pmod{p}$.
- Know the arithmetic rules for index summarized in Theorem 5.25 and know how to use them, in conjunction with index tables, to solve power congruence equations.
- Know Theorem 5.26: If p is an odd prime, $(n,\, p) = 1$ and q is a primitive root modulo p. Then for $m > 1$, the congruence $x^m \equiv n \pmod{p}$ is solvalbe if and only if $d \mid \operatorname{ind}_q n$, where $d = (m,\, p-1)$. If the congruence is solvable, then there are precisely d incongruent solutions modulo p.
- Know the RSA public key encryption system. The pubic part is the modulus $n = pq$ where p and q are primes, and the enciphering exponent e, chosen so that $(e,\, \phi(n)) = 1$. The secret deciphering exponent d is obtained by solving for $de \equiv 1 \pmod{\phi(n)}$. Enciphering is done by the rule $M^e \equiv r \pmod{n}$ while deciphering of the received message r is done by $r^d \equiv M \pmod{n}$. You will not be expected to do large power calculations on an exam.
- Know the formula for writing the product of sums of two squares as a sum of two squares: If $m = a^2 + b^2$ and $n = c^2 + d^2$ then

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

- Know the characterization of which primes can be written as a sum of two squares: An odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod{4}$.

- There is actually a stronger statement about uniqueness: A prime p of the form $4k+1$ can be represented uniquely (except for order and $\pm$) as a sum of two squares.
- Know the general criterion for representing a positive integer n as a sum of two squares: A positive integer n can be represented as the sum of two squares if and only if each prime factor of n of the form $4k+3$ occurs to an even power in the prime factorization of n.
- Know what it means for a number theoretic function to be *multiplicative*: f is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$.
- Main theorem on multiplicative functions: Assume that f is a multiplicative function and define F by
$$F(n) = \sum_{d|n} f(d).$$
Then F is also multiplicative.
- Know how to calculate the values of multiplicative functions from the prime factorization of n.
- Know how to calculate the values of concrete multiplicative functions, such as $\tau(n)$, $\sigma_s(n) = \sum_{d|} d^s$, and $\phi(n)$.
- Know the basic properties of the Möbius function $\mu(n)$: $\mu(n)$ is defined by the rule
$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \text{ where } p_i \text{ are distinct primes.} \end{cases}$$
- The function μ is a multiplicative function.
- Know the Möbius inversion formula: Let F and f be two number-theoretic functions related by the formula
$$F(n) = \sum_{d|n} f(d).$$
Then
$$f(n) \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$
- Theorem: $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$

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. Find all right-angled triangles with relatively prime integer sides and:

   (a) base 44

   ▶ **Solution.** Need a Pythagorean triple with $x = 44$. Then $x = 2st = 44$ so $st = 22$ and there are 2 cases.
   Case 1: $s = 1$, $t = 22$. Then $y = t^2 - s^2 = 22^2 - 1^2 = 484 - 1 = 483$, and $z = t^2 + s^2 = 22^2 + 1^2 = 485$.
   Case 2: $s = 2$, $t = 11$. Then $y = t^2 - s^2 = 11^2 = 2^2 = 117$, and $z = t^2 + s^2 = 11^+2^2 = 125$.
   Thus, the possible triangles have (base, height, hypotenuse) = (44, 483, 485) or (44, 117, 125). ◀

   (b) base 33

   ▶ **Solution.** In this case, we need $y = t^2 - s^2 = 33$. Thus, $t^2 - s^2 = (t+s)(t-s) = 33$. Again, there are 2 cases.
   Case 1: $t+s = 33$, $t-s = 1$ which gives $s = 16$, $t = 17$ and then $x = 2st = 2 \cdot 17 \cdot 16 = 544$ and $z = t^2 + s^2 = 17^2 + 16^2 = 545$.
   Case 2: $t + s = 11$, $t - s = 3$ which gives $s = 4$, $t = 7$ and then $x = 2 \cdot 4 \cdot 7 = 56$ and $7^2 + 4^2 = 65$.
   Thus, the possible sides of triangles are (544, 33, 545) and (56, 33, 65). ◀

   (c) hypotenuse 65

   ▶ **Solution.** In this case $t^2 + s^2 = 65$. Since either s or t is less that $\sqrt{65/2} < 6$ check to see which of $65 - s^2$ is a perfect square, for $s = 1, 2, 3, 4, 5$. $65 - 1^2 = 8^2$ and $65 - 4^2 = 7^2$ are the only possibilities. Again, there are 2 cases.
   Case 1. $t = 8$, $s = 1$ so that $x = 2 \cdot 8 \cdot 1 = 16$ and $y = t^2 - s^2 = 8^2 - 1^2 = 63$.
   Case 2. $t = 7$, $s = 4$ so that $x = 2 \cdot 7 \cdot 4 = 56$ and $y = 7^2 - 4^2 = 33$
   Thus, the triangles have sides (56, 33, 65) and (16, 63, 65). ◀

2. Verify that the right-angled triangles with sides the Pythagorean triples x, y, z generated by the pairs $(s, t) = (133, 88)$ and $(s, t) = (152, 35)$ have the same area. What is the common area?

   ▶ **Solution.** $(s, t) = (133, 88)$ gives $x = 2 \cdot 133 \cdot 88 = 23,408$ and $y = s^2 - t^2 = 9,945$. The area of the triangle with this base and height is $\frac{1}{2}xy = \frac{1}{2} \cdot 23408 \cdot 9945 = 116,396,280$.
   $(s, t) = (152, 35)$ gives $x = 2 \cdot 152 \cdot 35 = 10,640$ and $y = s^2 - t^2 = 21,879$. The area of the triangle with this base and height is $\frac{1}{2}xy = \frac{1}{2} \cdot 10640 \cdot 21879 = 116,396,280$.
   Thus, both triangles have the same area. ◀

3. (a) Suppose that $(a, m) = 1$. Define $\operatorname{ord}_m a$, the order of a modulo m.

▶ **Solution.** $\operatorname{ord}_m a$ is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. ◀

(b) If $\operatorname{ord}_m a = 10$, then what is $\operatorname{ord}_m a^6$?

▶ **Solution.** $\operatorname{ord}_m a^6 = \frac{10}{(6,10)} = \frac{10}{2} = 5$. ◀

(c) Suppose that $(a, 17) = 1$. What does Fermat's Little Theorem tell you about $\operatorname{ord}_{17} a$?

▶ **Solution.** Fermat's theorem says that $a^{16} \equiv 1 \pmod{17}$ which implies that $\operatorname{ord}_{17} a \mid 16$ so that $\operatorname{ord}_{17} a = 1, 2, 4, 8$ or 16. ◀

(d) Find $\operatorname{ord}_{17} 8$.

▶ **Solution.** $8^1 \equiv 8 \pmod{17}$, $8^2 \equiv 64 \equiv 13 \pmod{17}$, $8^4 \equiv 13^2 \equiv 168 \equiv -1 \pmod{17}$, $8^8 \equiv (-1)^2 \equiv 1 \pmod{17}$ Thus $\operatorname{ord}_{17} 8 = 8$. ◀

4. (a) Evaluate $\operatorname{ord}_{19} 2$. Is 2 a primitive root modulo 19?

▶ **Solution.** Since $\phi(19) = 18$ it follows that $\operatorname{ord}_{19} a = 1, 2, 3, 6, 9$ or 18. Calculate (modulo 19): $2^1 = equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^6 \equiv 8^2 \equiv 7$, $2^9 \equiv 2^6 \cdot 2^3 = equiv 7 \cdot 8 \equiv -1$. Then $2^{18} \equiv 1 \pmod{19}$ and $\operatorname{ord}_{19} 2 = 18$. Hence 2 is a primitive root modulo 19. ◀

(b) If $\operatorname{ord}_m b = 42$, then $\operatorname{ord}_m b^{30}$ is what?

▶ **Solution.** $(b^{30})^k \equiv 1 \pmod{m} \iff 42 \mid 30k \iff 7 \mid 5k \iff 7 \mid k$. Therefore, $\operatorname{ord}_m b^{30} = 7$. ◀

5. (a) Give a reduced residue system modulo 20.

▶ **Solution.** The least reduced residue system modulo 20 is $R = \{1, 3, 7, 9, 11, 13, 17, 19\}$, and an equivalent reduced residue system modulo 20 is $S = set \pm 1, \pm 3, \pm 7, \pm 9$. ◀

(b) Show that every a in a reduced residue system modulo 20 satisfies $a^4 \equiv 1 \pmod{20}$.

▶ **Solution.** $(\pm 1)^4 \equiv 1$, $(\pm 3)^4 \equiv 81 \equiv 1$, $(\pm 7)^2 \equiv 9$, so $(\pm 7)^4 \equiv 1$. $(\pm 9)^2 \equiv 1$ so $(\pm 9)^4 \equiv 1$. Hence, $a^4 \equiv 1$ for all $a \in S$. ◀

(c) Is there a primitive root modulo 20? If so, find one. If not, explain why?

▶ **Solution.** From part (b), there is no element with order greater than 4, and $\phi(20) = 8$ so there is no primitive root modulo 20. ◀

Here is a table of the indices to base 2 modulo 13. (Note that 2 is a primitive root modulo 13.) It can be used to solve the next three problems.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6

6. If possible, solve each of the congruences:

   (a) $x^{20} \equiv 5 \pmod{13}$

   ▶ **Solution.** Applying the index to base 2 to the equation gives $20 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 5 \equiv 9 \pmod{12}$. This linear congruence can be solved for $\operatorname{ind}_2 x$ if and only if $(20, 12) \mid 9$. But $(20, 12) = 4 \nmid 9$ so the linear congruence is not solvable and hence the original congruence is not solvable. ◀

   (b) $x^{15} \equiv 5 \pmod{13}$

   ▶ **Solution.** In this case the linear congruence to be solved is $15 \operatorname{ind}_2 x \equiv 9 \pmod{12}$ and in this case, the linear congruence has a solution since $(15, 12) = 3 \mid 9$, and thus there are $(15, 12) = 3$ solutions to the linear congruence, and hence to the original congruence. To solve $15 \operatorname{ind}_2 x \equiv 9 \pmod{12}$ note that it can be rewritten as $3 \operatorname{ind}_2 x \equiv 9 \pmod{12}$ since $15 \equiv 3 \pmod{12}$. Thus, one solution is 3 and the remaining solutions modulo 12 are $3 + \frac{12}{3} = 3 + 4 = 7$ and $3 + 2\frac{12}{3} = 3 + 2 \cdot 4 = 11$. Thus, $\operatorname{ind}_2 x = 3$, 7, or 11, which, from the index table, gives the values of $x \equiv 8$, 11, or 7 modulo 13. ◀

7. Solve the congruence $8x^5 \equiv 3 \pmod{13}$.

   ▶ **Solution.** Applying ind_2 to the congruences gives the linear congruence

   $$\operatorname{ind}_2 8 + 5 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 3 \pmod{12}.$$

   Using the index table, this becomes the linear congruence $3 + 5 \operatorname{ind}_2 x \equiv 4 \pmod{12}$ or $5 \operatorname{ind}_2 x \equiv 1 \pmod{12}$. Since $(5, 12) = 1$ this congruence has a unique solution, which is $\operatorname{ind}_2 x \equiv 5 \pmod{12}$. Thus, the unique solution of the original congruence is $x \equiv 6 \pmod{13}$. ◀

8. Solve the congruence $11^{3x} \equiv 5 \pmod{13}$.

   ▶ **Solution.** Applying ind_2 to the congruence give the linear congruence

   $$3x \operatorname{ind}_2 11 \equiv \operatorname{ind}_2 5 \pmod{12}.$$

   Using the index table, this becomes the linear congruence (since $\operatorname{ind}_2 11 = 7$) $21x \equiv 9 \pmod{12}$. Since $(21, 12) = 3$ and $3 \mid 9$ this congruence is solvable and has 3 incongruent solutions modulo 12. Reducing the coefficients modulo 12 gives the linear congruence $9x \equiv 9 \pmod{12}$ which has the obvious solution $x \equiv 1$ and the remaining solutions are $x \equiv 1 + 4 \equiv 5$ and $x \equiv 1 + 2 \cdot 4 \equiv 9$. Thus, the solutions of the original congruence are $x \equiv 1, 5, 9 \pmod{12}$. ◀

9. You have decided to do RSA cryptography with modulus $n = 421 \cdot 401$ and enciphering exponent $e = 247$. Give (but do not solve) a congruence that you would use to find the deciphering exponent d.

   ▶ **Solution.** The congruence that needs to be solved is $de \equiv 1 \pmod{\phi(n)}$, which becomes $247d \equiv 1 \pmod{420 \cdot 400}$ or $247d \equiv 1 \pmod{168,000}$. ◀

10. Express $41 \cdot 53$ as a sum of two squares.

▶ **Solution.** $41 \cdot 53 = (5^2 + 4^2)(7^2 + 2^2) = (5 \cdot 7 + 4 \cdot 2)^2 + (5 \cdot 2 - 4 \cdot 7)^2 = 43^2 + 18^2$. There is more than one answer. Interchanging the 4 and 5 gives $41 \cdot 53 = 38^2 + 27^2$. ◀

11. Determine if each of the following numbers is representable as the sum of two squares.

(a) 157 (b) 341 (c) 873

▶ **Solution.** 157 is prime and $157 \equiv 1 \pmod 4$ so it is a sum of two squares.
$341 = 11 \cdot 31$ and $11 \equiv 3$ so 341 is not a sum of two squares.
$873 = 3^2 \cdot 97$ and $97 \equiv 1 \pmod 4$ so 873 is a sum of two squares. ◀

12. Let p, q, and r be distinct primes such that $p \equiv 1 \pmod 4$ and $q \equiv 3 \equiv r \pmod 4$. Determine if each of the following numbers is expressible as the sum of two squares.

(a) $2^3 p^3 q^4 r^5$

▶ **Solution.** This cannot be written as a sum of two squares since $r \equiv 3 \pmod 4$ and r appears to an odd power in the prime facttorization. ◀

(b) $2p^5 q^4 r^6$

▶ **Solution.** This can be written as a sum of two squares since all prime factors congruent to 3 modulo 4 (namely q and r) appear to even powers in the prime factorization. ◀

13. Define $G(n) = \sum_{d|n} \mu(d)\sigma(d)$ where μ is the Möbius function and σ is the sum of divisors function. Assuming μ and σ are multiplicative functions, explain why G is a multiplicative function.

▶ **Solution.** $g(n) = \mu)n)\sigma(n)$ is multiplicative since each of $\mu(n)$ and $\sigma(n)$ is multiplicative. Then $G(n) = \sum_{d|n} g(d)$ is the divisor sum function of the multiplicative function g, and hence is also multiplicative. ◀

(a) If p is a prime, then compute $G(p^k)$.

▶ **Solution.** The divisors of p^k are p^r for $0 \le r \le k$. Then,

$$\begin{aligned} G(p^k) = \sum_{d|p^k} \mu(d)\sigma(d) &= \mu(a)\sigma(1) + \mu(p)\sigma(p) + \cdots + \mu(p^k)\sigma(p^k) \\ &= 1 \cdot 1 + (-1)(1+p) + 0 \cdot \sigma(p^2) + \cdots + 0 \cdot \sigma(p^k) \\ &= -p. \end{aligned}$$

◀

(b) Evaluate $G(350)$.

▶ **Solution.** $G(350) = G(2 \cdot 5^2 \cdot 7) = G(2)G(5^2)G(7) = (-2)(-5)(-7) = -70.$ ◀

14. Suppose that $f(n)$ is the multiplicative function satisfying

$$n^2 = \sum_{d|n} f(d).$$

(a) From the Möbius inversion formula $f(n) = \sum_{d|n}$ _____.

▶ **Solution.** In this case, $F(n) = n^2$ so the Möbius inversion formula gives

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^2.$$

◀

(b) If p is a prime, then $f(p^k) =$ _____.

▶ **Solution.** The divisors of p^k are p^r for $0 \le r \le k$. Then,

$$\begin{aligned} f(p^k) = \sum_{d|p^k} \mu(d) \left(\frac{n}{d}\right)^2 &= \mu(a) \left(\frac{p^k}{1}\right)^2 + \mu(p) \left(\frac{p^k}{p}\right)^2 + \cdots + \mu(p^k) \left(\frac{p^k}{p^k}\right)^2 \\ &= 1 \cdot (p^k)^2 + (-1)(p^{k-1})^2 + 0 + \cdots + 0 \\ &= p^{2k} - p^{2k-2}. \end{aligned}$$

◀

(c) Evaluate $f(350)$.

▶ **Solution.** f is multiplicative, so

$$f(350) = f(2)f(5^2)f(7) = (2^2 - 1)(5^4 - 5^2)(7^2 - 1) = 86,400.$$

◀