The first exam will be on Wednesday, September 25, 2019. The syllabus will be Chapter 1 (Sections 1.1–1.7); Chapter 2 (Sections 2.1–2.5); and Chapter 3 (Sections 3.2 and 3.4) in Long.
Following are some of the concepts and results you should know:

- Know the *Induction Principle* and how to use it to do proofs by induction.
- Know the *Strong Induction Principle* and how to use it to do proofs by induction.
- Know the *Well-ordering principle:* Any set of positive integers which has at least one element contains a smallest element.
- Know the *Division Algorithm:* For any integers n and m with $m > 0$, there are *unique* integers q and r with $n = mq + r$ and $0 \leq r < m$.
- Know the definition of a *divides* b for integers a and b (notation: $a \mid b$): a divides b if $b = ac$ for some integer c.

  Some properties of a divides b:

  1. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.
  2. If $a \mid b$ and $b \mid c$, then $a \mid c$.
  3. If $a \mid c$ and $b \mid d$, then $ab \mid cd$.
  4. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any integers x and y.
- Know the definition of the *greatest common divisor* d of the integers a and b (notation: $d = (a, b)$).

  Different, equivalent formulations (or characterizations) of $d = (a, b)$:

  1. $d \mid a$ and $d \mid b$, and if $c \mid a$ and $c \mid b$, then $c \leq d$. (This is the definition of (a, b).)
  2. d is the smallest *positive* number that can be written as $d = ax + by$ with $x, y \in \mathbb{Z}$.
  3. $d = (a, b)$ if and only if $d > 0$, $d \mid a$, $d \mid b$, and $f \mid d$ for every common divisor f of a and b.
- The set of all integer linear combinations $ax + by$ consists of the set of all multiples of (a, b). That is, if a and b are integers (with at least one nonzero), then

$$\{ax + by : x, y \in \mathbb{Z}\} = (a, b)\mathbb{Z} = \{n \in \mathbb{Z} : n = c(a, b)\}.$$

  (Proved in class.)
- Know the *Euclidean Algorithm* and how to use it to compute the greatest common divisor of integers a and b, and write the greatest common divisor of a and b as an integer linear combination of a and b.
- Know the definition of *relatively prime integers.*
- Know the definition of *prime* number: p if prime if $p \geq 2$ and if $a \mid p$ then $a = \pm 1$ or $a = \pm p$.
- Know Euclid's Lemma: If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$. (Theorem 2.8)
- Also know the special case: If p is a prime, a and b are integers, and $p|ab$, then $p|a$ or $p|b$ (Corollary 2.9).

- Know the fact: If $a \mid c$, $b \mid c$ and $(a, b) = 1$, then $ab \mid c$. (Theorem 2.13)
- Know the definition of the *least common multiple* m of the integers a and b (notation: $m = [a, b]$).

  Different, equivalent formulations (or characterizations) of $m = [a, b]$.

  1. $m = [a, b]$ for $a \neq 0$, $b \neq 0$ if $m > 0$, $a \mid m$, $b \mid m$ and if n is another positive common multiple of a and b, then $m \leq n$. (This is the definition.)
  2. $m = [a, b]$ if and only if $m > 0$, $a \mid m$, $b \mid m$ and $m \mid n$ for every common multiple of a and b. (Theorem 2.18)
- Know the relationship between the greatest common divisor and least common multiple: If $ab \neq 0$, then $(a, b)[a, b] = |ab|$. (Theorem 2.19) Know how to use this formula, together with the Euclidean algorithm, to compute $[a, b]$.
- Know the inductive property of greatest common divisor and least common multiple:

  1. If none of $a_1, a_2, \ldots, a_n$ is zero, then
  $$(a_1, a_2, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n).$$
  2. If none of $a_1, a_2, \ldots, a_n$ is zero, then
  $$[a_1, a_2, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n].$$
- Know the Prime Factorization Theorem (Fundamental Theorem of Arithmetic, Theorem 2.22). Every integer $n > 2$ is either a prime or a product of primes, and the product of primes is unique except for the order in which the factors appear.
- Know the relationship between prime factorization and divisibility: If $a = \Pi_{i=1}^{r} p_i^{a_i}$ with $a_i > 0$ for each i is the canonical representation for a and $b > 0$, then $b \mid a$ if and only if $b = \Pi_{i=1}^{r} p_i^{b_i}$ with $0 \leq b_i \leq a_i$ for each i. (Theorem 2.23)
- Know how to find the prime factorization of (a, b) and $[a, b]$ from the prime factorizations of a and b. (Theorem 2.25)
- Know the basic properties and formulas for the number of divisors of a (denoted $\tau(a)$ and the sum of all the divisors of a, denoted $\sigma(a)$):

  1. If $(a, b) = 1$, then $\tau(ab) = \tau(a)\tau(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$. (Proved in class)
  2. If $a = \Pi_{i=1}^{r} p_i^{a_i}$ with $a_i > 0$ for each i is the canonical representation for a, then
  $$\tau(a) = \Pi_{i=1}^{r}(a_i + 1) \qquad \text{and} \qquad \sigma(a) = \Pi_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$
- Know Euclid's proof that there are infinitely many primes.
- Know the modification of Euclid's proof to prove that there are infinitely many primes of the form $4k - 1$.

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. Prove that
$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\cdots\left(1-\frac{1}{n^2}\right)=\frac{n+1}{2n}$$
for all integers $n \geq 2$.

▶ **Solution.** Let $S(n)$ be the statement
$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\cdots\left(1-\frac{1}{n^2}\right)=\frac{n+1}{2n}$$
for the integer n.

We will use induction to show that $S(n)$ is true for all integers $n \geq 2$.

Base Step. If $n = 2$ the statement $S(2)$ becomes
$$\left(1-\frac{1}{2^2}\right)=\frac{2+1}{2\cdot 2}=\frac{3}{4},$$
which is a true statement.

Inductive Step. For a given integer $n \geq 2$, assume that $S(n)$ is a true statement. Thus we are assuming that
$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\cdots\left(1-\frac{1}{n^2}\right)=\frac{n+1}{2n}$$
for the given integer n. If we multiply both sides of this equation by $\left(1-\frac{1}{(n+1)^2}\right)$ we get
$$\begin{aligned}\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\cdots\left(1-\frac{1}{n^2}\right)\left(1-\frac{1}{(n+1)^2}\right) &= \left(\frac{n+1}{2n}\right)\left(1-\frac{1}{(n+1)^2}\right)\\ &= \frac{n+1}{2n}-\frac{1}{2n(n+1)}\\ &= \frac{(n+1)^2-1}{2n(n+1)}\\ &= \frac{n^2+2n}{2n(n+1)}\\ &= \frac{n+2}{2(n+1)}\\ &= \frac{(n+1)+1}{2(n+1)}.\end{aligned}$$

Therefore, we have shown that if $S(n)$ is true, then so is $S(n+1)$.

By the principle of mathematical induction, $S(n)$ is true for all natural numbers $n \geq 2$. ◀

2. Prove that $4^n + 2$ is divisible by 6, for every positive integer n.

► **Solution.** Let $S(n)$ be the statement: $4^n + 2$ *is divisible by* n *for the integer* n.

We will use induction to show that $S(n)$ is true for all integers $n \geq 1$.

Base Step. If $n = 1$ the statement $S(1)$ becomes: $4^1 + 2$ *is divisible by 6*, which is a true statement.

Inductive Step. For a given integer $n \geq 1$, assume that $S(n)$ is a true statement. Thus we are assuming that $4^n + 2$ is divisible by 6 for the given integer n. That is, we are assuming that, for the given integer n, $4^n + 2 = 6k$ for some integer k. Then

$$\begin{aligned} 4^{n+1} + 2 &= 4^n \cdot 4 + 2 = 4^n \cdot 4 + 8 - 6 \\ &= 4^n \cdot 4 + 2 \cdot 4 - 6 = 4(4^n + 2) - 6 \\ &= 4(6k) - 6 = 6(4k - 1). \end{aligned}$$

Thus, we have shown that if $4^n + 2$ is divisible by 6, then $4^{n+1} + 2$ is also divisible by 6. Therefore, we have shown that if $S(n)$ is true, then so is $S(n + 1)$.

By the principle of mathematical induction, $S(n)$ is true for all natural numbers $n \geq 1$. ◄

3. Prove that $3 \mid (n^3 + 5n)$ for all $n \geq 1$.

► **Solution.** This can be done by induction, as in problem 2. Alternately, one can use the cubic form of the binomial theorem:

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

To apply this, note that by the division algorithm, every integer n can be written in the form $3q + k$ where $0 \leq k \leq 2$. Thus, consider 3 cases.

Case 1. $k = 0$.

In this case $n = 3q$ so $3 \mid n$ and hence $3 \mid (n^3 + 5n)$ in this case.

Case 2. $k = 1$.

In this case, $n = 3q + 1$ so

$$\begin{aligned} n^3 + 5n = (3q + 1)^3 + 5(3q + 1) &= (27q^3 + 9q^2 + 3q + 1) + 5(3k + 1) \\ &= 27q^3 + 9q2 + 18q + 6 \\ &= 3(9q^3 + 3q^2 + 6q + 2). \end{aligned}$$

Thus $3 \mid (n^3 + 5n)$ in this case.

Case 3. $k = 2$.

In this case, $n = 3q + 2$ so

$$\begin{aligned} n^3 + 5n = (3q + 2)^3 + 5(3q + 2) &= (27q^3 + 18q^2 + 12q + 8) + 5(3q + 2) \\ &= 27q^3 + 18q^2 + 27q + 18 \\ &= 3(9q^3 + 6q^2 + 9q + 6). \end{aligned}$$

Thus $3 \mid (n^3 + 5n)$ in this case.

Hence $3 \mid (n^3 + 5n)$ in all three cases, and since these 3 cases cover all possibilities for n, it follows that $n \mid (n^3 + 5n)$ for all integers n. ◄

4. Find the greatest common divisor $d = (803, 154)$ using the Euclidean Algorithm, and write $d = (803, 154)$ in the form $d = s \cdot 803 + t \cdot 154$. Compute the least common multiple $m = [803, 154]$.

   ▶ **Solution.** Use the Euclidean Algorithm:

   $$\begin{aligned} 803 &= 5 \cdot 154 + 33 \\ 154 &= 4 \cdot 33 + 22 \\ 33 &= 1 \cdot 22 + 11 \\ 22 &= 2 \cdot 11 \end{aligned}$$

   Thus, $(803, 154) = 11$ and

   $$\begin{aligned} 11 &= 33 - 22 \\ &= 33 - (154 - 4 \cdot 33) = 5 \cdot 33 - 154 \\ &= 5(803 - 5 \cdot 154) - 154 \\ &= 5 \cdot 803 - 26 \cdot 154. \end{aligned}$$

   Then

   $$[803,\ 154] = \frac{803 \cdot 154}{(803,\ 154)} = \frac{803 \cdot 154}{11} = 11,242.$$

   ◀

5. Find the greatest common divisor $d = (1887, 1295)$ using the Euclidean Algorithm, and write $d = (1887, 1295)$ in the form $d = s \cdot 1887 + t \cdot 1295$. Compute the least common multiple $m = [1887, 1295]$.

   ▶ **Solution.** Use the Euclidean algorithm: Use the technique of problem 4, or alternatively, keep track of the steps in a table as shown in class:

1887	1295		
1	0	1887	
0	1	1295	
1	−1	592	$= 1887 - 1 \cdot 1295$
−2	3	111	$= 1295 - 2 \cdot 592$
11	−16	37	$= 592 - 5 \cdot 111$
−35	51	0	$= 111 - 3 \cdot 37$

   From this, it follows that $(1887, 1295) = 37 = 11 \cdot 1887 + (-16) \cdot 1295$. Then

   $$[1887, 1295 = \frac{1887 \cdot 1295}{37} = 66,045.$$

   ◀

6. Use the *definition of divisibility* to prove that if $a \mid b$ and $b \mid c$, then $a \mid (7b - 5c)$.

   ▶ **Solution.** If $a \mid b$ then $b = ar$ (definition of divide) and if $b \mid c$ then $c = bs$. Then $7b - 5c = 7ar - 5bs = 7ar - 5(ar)s = a(7r - 5rs)$. Since $7r - 5rs$ is an integer, then $a \mid (7b - 5c)$. ◀

7. Let a, b, c, and d be positive integers. Determine if each of the following statements is True or False. If False, provide a counterexample.

   (a) If $a|c$ and $b|c$, then $ab|c$. **False**. Counterexample: $a = b = c = 2$.

   (b) If $c \mid a$ and $c \mid b$ then $c^2 \mid ab$. **True**.

   (c) If $(a, b) = 1$ and $(c, d) = 1$, then $(ac, bd) = 1$. **False**. Counterexample: $a = d = 2$, $b = c = 3$. Then $(a, b) = (c, d) = 1$ but $(ac, bd) = 6$.

   (d) If $d \mid a$ and $d \mid b$, then $(a, b) \mid d$. **False**. Counterexample: $a = b = 2$, $d = 1$. Then $(a, b) = 2$ and $2 \nmid 1$.

   (e) If there exist integers r and s such that $ra + sb = d$, then $d = (a, b)$. **False**. Counterexample: $4 \cdot 3 - 5 \cdot 2 = 2$ but $(3, 2) = 1$.

   (f) If $(a, b) = 3$,then $[a, b] = \frac{a}{3} \cdot \frac{b}{3}$. **False**. Counterexample: $a = b = 3$.

   (g) Every nonempty set of positive integers contains a largest element. **False**. The set of all positive integers does not contain a largest element.

8. What is the smallest positive integer of the form $30x + 6y + 10z$ for integers x, y, z?

   ▶ **Solution.** The smallest positive integer of the form $30x + 6y + 10z$ for integers x, y, z is $(30, 6, 10) = 2$. ◀

9. If n is an integer then $(2n + 3, 3n - 2) = 1$ or k. What is k?

   ▶ **Solution.** If $d \mid (2n + 3)$ and $d \mid (3n - 2)$, then $d \mid (3(2n + 3) - 2(3n - 2))$ and $3(2n + 3) - 2(3n - 2) = 13$ so any common divisor must be a divisor of 13. This means that the only possibilities for the greatest common divisor are 1 and 13 so $k = 13$. Both possibilities can occur. For example, if $n = 0$ then $(2n + 3, 3n - 2) = (3, -2) = 1$ and if $n = 5$ then $(2n + 3, 3n - 2) = (13, 13) = 13$. ◀

10. Let $a = 2^3 3^2 5^2 13$ and $b = 2^2 3^3 13^7 19$.

    (a) What is the prime factorization of (a, b)? **Answer**: $(a, b) = 2^2 3^2 13$

    (b) What is the prime factorization of $[a, b]$? **Answer**: $[a, b] = 2^3 3^3 5^2 13^7 19$

11. (a) Evaluate $\tau(1500)$.

    ▶ **Solution.** $1500 = 2^2 \cdot 3 \cdot 5^3$. Thus $\tau(1500) = 3 \cdot 2 \cdot 4 = 24$. ◀

    (b) Evaluate $\sigma(1500)$.

    ▶ **Solution.**

    $$\sigma(1500) = \sigma(2^2)\sigma(3)\sigma(5^3) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^4 - 1}{5 - 1} = 7 \cdot 4 \cdot 156 = 4,368.$$

    ◀

    (c) What prime factorizations are possible for n if $\tau(n) = 9$?

    ▶ **Solution.** $\tau(n) = 9 = 3 \cdot 3$ so possible prime factorizations of n are $n = p^8$ or $n = p^2 q^2$ for primes p and q. ◀

(d) If p and q are distinct primes then evaluate $\tau(p^2q^5)$. List the divisors of p^2q^5. (table form is fine)

► **Solution.** $\tau(p^2q^5) = \tau(p^2)\tau(q^5) = 3 \cdot 6 = 18$. The divisors are listed in the following table:

	1	q	q^2	q^3	q^4	q^5
1	1	q	q^2	q^3	q^4	q^5
p	p	pq	pq^2	pq^3	pq^4	pq^5
p^2	p^2	p^2q	p^2q^2	p^2q^3	p^2q^4	p^2q^5

◄

12. What is the smallest integer n such that $\tau(n) = 8$? Such that $\tau(n) = 10$?

► **Solution.** Since $8 = 4 \cdot 2 = 2 \cdot 2 \cdot 2$, we can get $\tau(n) = 8$ provided that $n = p^7$, $n = p^3q$, or $n = pqr$ where p, q and r are distinct primes. The smallest primes are 2, 3, and 5, so the smallest possible n would be $2^7 = 128$, $2^3 \cdot 3 = 24$ or $2 \cdot 3 \cdot 5 = 30$. Thus, the smallest possible n with $\tau(n) = 8$ is $n = 24$.

Similarly, $10 = 2 \cdot 5$ so the possible n with $\tau(n) = 10$ are p^9 and p^4q for distinct primes p and q. The smallest n among these is obtained if $p = 2$ and $q = 3$ which gives $n = 16 \cdot 3 = 48$. ◄

13. In 1644, Mersenne asked for a number with 60 divisors. Find one smaller than 10,000. Find infinitely many n with $\tau(n) = 60$.

► **Solution.** We need an n with $\tau(n) = 60 = 2^2 \cdot 3 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 5$. Thus, n will have $\tau(n) = 60$ provided n has one of the factorizations $n = p^3q^2r^4$ or $n = pqr^2s^4$ where p, q, r, s are distinct primes. In the first factorization let $r = 2$, $p = 3$, $q = 5$ to get $n = 2^4 \cdot 3^3 \cdot 5^2 = 10,800$ and in the second possible factorization use $s = 2$, $r = 3$, $p = 5$, and $q = 7$ to get $n = 2^4 \cdot 3^2 \cdot 5 \cdot 7 = 5040$. Thus, the only $n < 10,000$ with $\tau(n) = 60$ is $n = 5040$. Since any choices of primes p, q, r and s will give $\tau(n) = 60$, there are infinitely many n with $\tau(n) = 60$. ◄

14. Give a proof that there are infinitely many primes.

► **Solution.** Use Euclid's proof given in Theorem 3.1 of the text. ◄

15. (a) Find a non-trivial factor of $2^{55} - 1$.

► **Solution.** Since $55 = 5 \cdot 11$, both $2^5 - 1 = 31$ and $2^{11} - 1 = 2047$ are divisors of $2^{55} - 1$. To see this, use the geometric series formula

$$x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$$

with $k = 11$ and $x = 2^5$ or $k = 5$ with $x = 2^{11}$. ◄

(b) Find a non-trivial factor of $18^{101} - 1$.

► **Solution.** Again, use the geometric series formula with $k = 101$ and $x = 18$ to get that $17 = (18 - 1)$ is a divisor of $18^{101} - 1$. ◄

(c) Find a non-trivial factor of $2^{44} + 1$.

► **Solution.** Use the factorization $x^{11}+1=(x+1)(x^{10}-x^9+\cdots-x+1)$ with $x=2^4$ to get that $2^4+1=17$ is a nontrivial factor of $2^{44}+1$. ◄