Prime Numbers and the Fundamental Theorem of Arithmetic.

For these theorems you must use only the Axioms of the integers and the theorems that are consequences of them (except for exercises 5.14 and 5.22 which are applications of the theory of integers to the reals.) The theorems with the * symbol are important theorems needed to prove the Fundamental Theorem of Arithmetic.

Exercise 5.1. If $a|b$ then $a^n|b^n$ for each positive integer n.

Theorem* 5.1. Suppose that each of a and b is a positive number. If $a|b$ and $b|a$ then $a = b$.

Exercise 5.2. Show that if a is an integer then, $3|(a^3 - a)$.

Exercise 5.3. Show that $6|a(a + 1)(a + 2)$ for any integer a.

Exercise 5.4. Show that $5|(a^5 - a)$ for every positive integer a.

Exercise 5.5. The sum of the cubes of three successive integers is divisible by 9.

Exercise 5.6. Show that if $m > 1$ then $F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$.

Exercise 5.7. Show that if $n|m$ then $F_n|F_m$. [Hint: use exercise 5.6.]

Prime Numbers.

Definition. Suppose that n is a positive integer. If n is only divisible by one positive integer then n is called a *unit*; if there are only two positive integers that divide n then n is called a *prime* number; if n is divisible by *three* positive integers then n is called a *composite* number.

Observation. The positive integer p is a prime number iff it is not equal to 1 and it is divisible only by itself and 1.

Theorem* 5.2. If $n > 1$ is a positive integer then there exists a prime number p so that $p|n$.

Theorem* 5.3. The set of prime numbers in infinite.

Historical note, The Prime Number Theorem:

If x is a positive number then let $\pi(x)$ denotes the number of primes less than or equal to x. Then:

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln(n)}} = 1.$$

This is an important theorem in number theory and uses techniques that will not be covered in this course. It tells us something about the density of prime numbers.

Theorem 5.5. If n is a positive integer then at some point in the number system, there exists n consecutive composite integers.

Open problem: Goldbach's Conjecture: If $n > 2$ is an even positive integer then n is the sum of two primes.

Exercise 5.9. Determine the smallest integer n for which the quantity $n^3 + 1$ is prime.

Exercise 5.10. Show that if p is prime, then one of $p + 2$ or $p + 4$ is not prime.

Exercise 5.11. Show that $x^2 - x + 41$ is prime for all positive integers $x < 41$. [Don't do this by hand, use a spreadsheet or something.] Show that for $x = 41$ this polynomial does not produce a prime.

Theorem 5.6. [Generalization of exercise 5.11.] Show that if $P(x)$ is a polynomial with integer coefficients then there is a positive integer n so that $P(n)$ is a composite number.

Exercise 5.12. Show that if $a^n - 1$ is prime then $a = 2$ and n is prime.

Exercise 5.13. Suppose that N is an integer and A is a set of primes less than N and B is the set of primes less than N that are not in A. Then $\prod_{a\in A} a + \prod_{b\in B} b$ is not divisible by a prime less than N.

Exercise 5.14. Suppose that p is the smallest prime factor of the integer n and that $\sqrt[3]{n} < p$ then either n or $\frac{n}{p}$ is prime.

Exercise 5.15. Show that every integer greater than 11 is the sum of two composite numbers.

Exercise 5.16. Suppose that n is a positive integer. Does it follow that $\left(\begin{array}{c} n \\ r \end{array}\right)$ is divisible by n? What if n is prime?

Theorem 5.7. The set $S = \{4k + 3 | k \in \mathbf{Z}^+\}$ contains infinitely many primes.

[Hint: note that if a and b are both in the form $4n + 1$ then so is ab.]

Definition. If each of a and b is an integer then the *greatest common divisor* of a and b is the largest positive integer that divides both a and b.

The common notation for the greatest common divisor d of a and b is: $d = (a, b)$ or $d = gcd(a, b)$. We will use the latter, though you should be aware that the former is also frequently used.

Definition. If each of a and b is an integer then a and b are said to be *relatively prime* iff $gcd(a, b) = 1$.

Definition. The greatest common divisor for a set of numbers $\{a_i\}_{i=1}^n$ is similarly defined: $gcd(\{a_i\}_{i=1}^n)$ is the largest positive integer that divides all the elements of the set $\{a_i\}_{i=1}^n$.

Example: Find three integers so that $gcd(a, b, c) = 1$ but that are pairwise not relatively prime.

Theorem* 5.8. Suppose that each of a and b is a positive integer and $d = gcd(a, b)$. Then there exists integers x and y so that:

$$d = ax + by.$$

Theorem* 5.9. Suppose that each of a and b is an integer and at least one of them is not 0. Let $S = \{na + mb | n \in \mathbf{Z}, m \in \mathbf{Z}, 0 < na + mb\}$. Then $gcd(a, b)$ is the least element of the set S.

Exercise 5.17. Find the gcd of the following pairs:
a. $gcd(a, a^2) =?$,
b. $gcd(a, a + 1) =?$,
c. $gcd(a, a + 2) =?$,
d. $gcd(ca, cb) =?$.

Theorem 5.9.1. If $n > 0$ is a composite number then there exists a prime p with $p^2 \leq n$ so that $p|n$. [May need to consider this after Theorem 5.17.]

Exercise 5.18. Show that if $gcd(a, b) = 1$, then $gcd(a + b, a - b)$ is 1 or 2.

Exercise 5.19. If a and b are even then $gcd(a, b) = 2gcd(\frac{a}{2}, \frac{b}{2})$. If a is even and b is odd then $gcd(a, b) = gcd(\frac{a}{2}, b)$.

Theorem* 5.10. Let a and b be integers at least one of which is not 0. Then a and b are relatively prime if and only if there exist integers x and y so that:

$$ax + by = 1.$$

Theorem 5.11. Let a, b and c be integers so that $a|bc$ and $gcd(a, b) = 1$. Then $a|c$.

Theorem 5.12. [Euclid's lemma.]. Let a, b and c be integers so that $a|c$, $b|c$ and $gcd(a, b) = 1$. Then $ab|c$.

Theorem 5.13. If $gcd(e, f) = 1$, $e|a$ and $f|a$, then $ef|a$.

Exercise 5.20.
a. If $gcd(a, b) = 1$ and $c|(a + b)$ then $gcd(a, c) = 1$.
b. If $a|bc$ then $a|gcd(a, c)gcd(a, b)$.

c. If $gcd(a,b) = 1$ then $gcd(a^n, b^n) = 1$.
d. If $gcd(a,b) = 1$ and $a|bc$ then $a|c$.
e. If $gcd(a,b) = 1$, $a|c$ and $b|c$, then $ab|c$.
f. If $gcd(a,b) = gcd(a,c) = 1$ then $gcd(a,bc) = 1$.
g. $gcd(3k+2, 5k+3) = 1$.

Theorem 5.14. [The Euclidean Algorithm to calculate the Greatest Common Divisor.] Suppose that a and b are two positive integers. Let $r_0 = a$ and $r_1 = b$, then recursively define r_{n+1} and q_n using the division algorithm by:

$$r_{n-1} = r_n q_n + r_{n+1}.$$

Then there exists an integer k so that $r_k = 0$ and if k is the first such integer then $gcd(a,b) = r_{k-1}$.

Definition Let a and b be two positive integers then the *least common multiple* of a and b is the smallest positive integer m so that $a|m$ and $b|m$.

The common notation for the least common multiple m of a and b is: $m = [a,b]$ or $m = lcm(a,b)$. We will use the latter, though you should be aware that the former is common.

Theorem 5.15. Let a and b be two positive integers. Then:

$$ab = lcm(a,b)gcd(a,b).$$

Theorem 5.16. If $gcd(a,b) = 1$ and $a|bc$ then $a|c$.

Theorem* 5.17. If each of a and b is an integer, p is a prime number and $p|ab$, then either $p|a$ or $p|b$.

Theorem 5.18'. Suppose that p is a prime and n is a positive integer greater than one. Then there is a unique non-negative integer k so that $n = p^k q$ for some integer q and $p \nmid q$ (i.e. p does not divide q). [Note that, if not proven separately, this is also a corollary of the Fundamental Theorem of Arithmetic.]

Theorem 5.18. Suppose that p is a prime, that for each $i \leq n$, a_i is a positive number and

$$p \Big| \prod_{i=1}^{n} a_i,$$

then there exists a k so that $p|a_k$.

Theorem* 5.19. [The Fundamental Theorem of Arithmetic.] Every positive integer n greater that 1 has a unique representation as a product of primes:

$$n = p_1 p_2 p_3 ... p_k,$$

such that $p_i \leq p_{i+1}$.

Corollary to theorem 5.19. If a is a positive integer and p is a prime number then there is a unique non-negative integer n so that:

$$a = p^n Q$$

and the prime number p does not divide Q.

Exercise 21. [Applications of the Fundamental Theorem of Arithmetic.] Assume as usual that r, s are positive integers, a, b, ... etc take on reasonable values; assume that p denotes a prime.

a. If $a^3|b^2$ then $a|b$.
b. If $p^r|a$ and $p^s|b$ then $p^{r+s}|ab$.
c. If $p^r|a$ then $p^{nr}|a^n$.
d. If $a^2|b^2$ then $a|b$.
e. If m is a common multiple of a and b then $lcm(a,b)|m$.
f. If $a^r = b^r$ then $a = b$.

Exercise 5.22. [More applications.]

a. Show that $\log_2(3)$ is irrational.
b. Show that $\sqrt{2}$ is irrational.
c. Show that if p is a prime number then $\sqrt{p}$ is irrational.
d. Show that $\sqrt{12}$ is irrational.
e. Show that $\sqrt[3]{2}$ is irrational.

f. Show that $\sqrt[3]{9}$ is irrational.

g. Generalize b - f as much as you can.