 Name:______________________________

Instructions: Complete as many of the following problems as you can during class time.

1. The following activity is designed to introduce you to the concept of **modular arithmetic** in a natural way.

   (a) What day will it be 4 days from now? How about 11 days from now? 18 days from now?

   (b) Find 6 other integers k for which the answer to the question "What day will it be k days from now?" is the same as in part (a) above. Make sure that two of them are negative (do negative values make sense?).

   (c) Pick any two numbers that you found in either part (a) or (b) and subtract them. Do this several times. What pattern (if any) do you notice? Why do you think this happens?

Definition 2.9: Let n be a natural number and let a and b be integers. Then a is **congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$ provided that n divides $a - b$.

Theorem 2.10 Let n be a natural number, and let a and b be integers. Then $a \equiv b \pmod{n}$ if and only if a and b yield the same remainder when divided by n.

Note: Activity 2.11 in your textbook gives an outline of the proof of this theorem. Make sure to read through this sometime between now and class on Monday.

2. Let n be a natural number, and let $a, b, c,$ and d be integers.

   (a) Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

   (b) Prove that if $a \equiv b \pmod{n}$ and $m \in \mathbb{N}$, then $a^m \equiv b^m \pmod{n}$.

   (c) Prove that $\equiv$ is an equivalence relation on the set $\mathbb{Z}$.

3. Let a and b be integers with $a > 0$, and let r be the remainder when b is divided by a. Prove that if an integer d divides both a and b, then d also divides r.

Definition 3.3: Let a and b be integers, not both zero. A **common divisor** of a and b is any integer that divides both a and b. The largest integer that divides both a and b is called the **greatest common divisor** of a and b, denoted $\gcd(a, b)$.

4. Find the gcd of each of the following pairs of integers:

   (a) 60 and 95 (b) 540 and 765 (c) 180 and 0

5. You may have observed that finding the gcd of a pair of integers can be a tedious process. The following steps are meant to suggest a way to use the Division Algorithm to find the gcd of a given pair of integers more efficiently.

   (a) Find the quotient and remainder that results from dividing 765 by 540.

   (b) Let r denote the remainder you found in part (a). Find $\gcd(540, r)$.

   (c) How does this answer compare to your answer for part (b) in the previous problem? How can this be used to find the gcd more efficiently?

6. A factor tree is a common method used to find the prime factorization of a natural number.

   (a) On page 25 in your textbook, you will see the factor trees for 396 and 780. Copy these down and use them to find $\gcd(396, 780)$.

   (b) Next, use the method in part (c) of the previous problem to find the gcd of 396 and 780 using the division algorithm. Which method do you prefer?

Theorem 3.4: Let a and b be integers, not both zero, and suppose that $b = aq + r$ for some integers q and r. Then $\gcd(b, a) = \gcd(a, r)$.