Last name _____

First name _____

LARSON—MATH 353–CLASSROOM WORKSHEET 04
Primes.

Review

1. What is $\mathbb{Z}$?
2. **Def.** If $a, b \in \mathbb{Z}$ we say that a divides b, written $a \mid b$, if $ac = b$ for some $c \in \mathbb{Z}$. In this case, we say a is a *divisor* of b. We say that a does not divide b, written $a \nmid b$, if there is no $c \in \mathbb{Z}$ such that $ac = b$.
3. What is a *prime* integer $n > 1$?
4. What is a *composite* integer?
5. What is $\gcd(a, b)$ for integers a, b?
6. Why does $\gcd(a, b) = \gcd(b, a)$?
7. Why does $\gcd(a, b) = \gcd(\pm a, \pm b)$?

New

1. Why does $\gcd(a, b) = \gcd(a, b - a)$?

(**Lemma 1.1.10**) Suppose $a, b, n \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(a, b - an)$.

2. Why is Lemma 1.1.10 true?

(**Proposition 1.1.11**.) Suppose that a and b are integers with $b \neq 0$. Then there exists unique integers q and r such that $0 \leq r < |b|$ and $a = bq + r$.

3. Why is Proposition 1.1.11 true?

(**Algorithm 1.1.12. Division Algorithm**.) Suppose a and b are integers with $b \neq 0$. This algorithm computes integers q and r such that $0 \leq r < |b|$. and $a = bq + r$.

4. Use the division algorithm repeatedly to compute $\gcd(2261, 1275)$.

(Theorem 1.1.19. Euclid). Let p be a prime and $a, b \in \mathbb{N}$. If $p|ab$ then $p|a$ or $p|b$.

5. Why is Euclid's Lemma true?

(Proposition 1.1.20) Every natural number is a product of primes.

6. Why is Proposition 1.1.20 true?