Last name ______________________

First name ______________________

LARSON—MATH 353–CLASSROOM WORKSHEET 06
Fundamental Theorem of Arithmetic.

Review

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

   (**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 $a = bq + r$.

New

(**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 $a = bq + r$.

1. What is the Division Algorithm? (How can we *find* q and r)?

2. Why does **Lemma 1.1.10** imply that, for $a, b > 0$, with unique integers q, r with $a = bq + r$ $(0 \leq r < b)$, that $\gcd(a, b) = gcd(b, r)$?

3. How can the Division Algorithm be used to compute $\gcd(a, b)$?

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?

7. What is the Fundamental Theorem of Arithmetic?

8. How can we use Euclid's Lemma to prove the Fundamental Theorem of Arithmetic?