Last name ______________________

First name ______________________

LARSON—MATH 353–CLASSROOM WORKSHEET 19
Chinese Remainder Theorem.

Review

1. (**Proposition 2.1.22, Wilson's Theorem**). An integer $p > 1$ is prime if and only if $(p-1)! \equiv -1 \mod p$.
2. **Algorithm 2.3.7 (Extended Euclidean Algorithm)** Suppose a and b are integers and let $g = gcd(a, b)$. This algorithm finds g, x and y such that $ax + by = g$.
3. **Algorithm 2.3.8 (Inverse Modulo n)**. Suppose a and n are integers and $\gcd(a, n) = 1$. This algorithm finds an x such that $ax \equiv 1 \mod n$.
4. **Resolved claim:** For an integer $x \geq 2$, the number of distinct prime factors of x is no more than $\frac{1}{2}$ the number of divisors of x.

New

Open Conjectures

1. Have these been resolved?

```
count_prime_divisors(x) <= digits10(x)
count_prime_divisors(x) <= ceil(sqrt(count_divisors(x)))
```

Chinese Remainder Theorem

2. Does this system have a solution?

$$x \equiv 2 \mod 3$$

$$x \equiv 3 \mod 5$$

(**Theorem 2.2.2, Chinese Remainder Theorem**). Let $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{N}$ such that $\gcd(n, m) = 1$. Then there exists $x \in \mathbb{Z}$ such that

$$x \equiv a \mod m,$$

$$x \equiv b \mod n.$$

Moreover x is unique modulo mn.

3. Why is the Chinese Remainder Theorem true?

4. Does this system have a solution?

$$x \equiv 2 \mod 3$$
$$x \equiv 3 \mod 5$$
$$x \equiv 2 \mod 7$$

Multiplicative functions

5. What is a *multiplicative function*?

6. Is Euler's ϕ function multiplicative?