Name: [redacted] **GSI: Eduardo Reyes** **DISC #:** [redacted]

Math 55, Handout 8.

PRIMES.

1.1. A **prime** is a number **n** whose factors consist of only 1 and itself.

1.2. A **composite** integer is an integer that can be expressed as the product of two integers, both of which are different than itself.

1.3. **Fundamental Theorem of Arithmetic**: Any integer greater than 1 factors as a unique product of prime numbers.

1.4. Any composite integer n has a prime divisor p such that $n = 0 \pmod{p}$

Q1. Write 770077 as a product of primes.

$= 7 \times 11 \times 73 \times 137$

GCD and LCM.

2.1. Let a, $b \in \mathbb{Z}$, not both zero. The **greatest common divisor** of a and b (denoted $\gcd(a, b)$) is the largest integer that simultaneously divides a and b.

2.2. Two integers a, b are **relatively prime** if $\gcd(a, b) = 1$

2.3. Let a, $b \in \mathbb{N}$. The **least common multiple** of a and b (denoted $\text{lcm}(a, b)$) is the smallest integer that a=a and b both can divide without remainder.

Q2. What are $\gcd(770077, 165)$ and $\text{lcm}(770077, 165)$?

$\gcd(770077, 165) = 11$ and $\text{lcm}(770077, 165) = 11551155$

2.4. The **Euclidean algorithm** allows to evaluate $\gcd(a, b)$ and to express it as a product of its prime factors.

The latter fact is known as . Its corollary is the following Lemma: Suppose $sa \equiv sb \pmod{m}$ and $\gcd(s, m) = 1$. Then $a \equiv b \pmod{m}$

This Lemma, in turn, implies uniqueness in the prime factorization of an integer.

INTEGER REPRESENTATIONS.

3.1. Given any **base** $b \in \mathbb{N} \setminus \{1\}$, any $n \in \mathbb{N}$ can be written as $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$ where p_i is a prime number and $\alpha_i \in \mathbb{N}$ $\forall i$

3.2. The computation of $b^n \pmod m$ can be done efficiently using the Euclidean Algorithm

Q3. Write down the binary, octal and hexadecimal representations of 27. What is $22^{27} \pmod 7$?

Binary: 0001 1011

Octal: 33

Hexadecimal: 1b

SOLVING CONGRUENCES.

4.1. Let $m \in \mathbb{N} \setminus \{1\}$. An inverse of $a \in \mathbb{Z}$ modulo m is some r such that $(ar) \equiv 1 \pmod m$

If such an inverse exists it is unique up to $m - 1$

Q4. Find an inverse of 101 modulo 462 and use it to solve the congruence $101x \equiv 3 \pmod{462}$.

4.2. The **Chinese remainder theorem** says: Let m_1, m_2, …, m_n be pairwise prime positive integers greater than one, and a_1, a_2, …, a_n arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ &\cdots \\ &\cdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 \times m_2 \times \ldots \times m_n$

Q5. What is the smallest positive solution to the congruence system $2x \equiv 1 \pmod 7$, $13x \equiv 2 \pmod{11}$?

4.3. **Fermat's little theorem** says: if p is a prime number and $a \in \mathbb{Z}$ is not divisible by p, then $a^{p-1} \equiv 1 \pmod p$. Furthermore, $\forall a \in \mathbb{Z}$ we have $a^p \equiv a \pmod p$.