Name: Shivani Patel GSI: Madeline Brandt DISC #: 103

Math 55, Handout 8.

PRIMES.

1.1. A **prime** is a number that has exactly 2 different positive integer factors; one and itself.

1.2. A **composite** integer is a positive integer that is greater than 1 and not prime

1.3. **Fundamental Theorem of Arithmetic**: Any integer greater than 1 factors as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size

1.4. Any composite integer n has a prime divisor p such that n has a prime divisor less than or equal to $\sqrt{n}$

Q1. Write 770077 as a product of primes.

① $\frac{770077}{7} = 110,011$ ② $\frac{110,011}{11} = 10,001$ $\frac{10,001}{73} = 137$

$7 \cdot 11 \cdot 73 \cdot 137 = 770077$

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 d such that $d \mid a$ and $d \mid$

2.2. Two integers a, b are **relatively prime** if their GCD is 1.

2.3. Let $a, b \in \mathbb{N}$. The **least common multiple** of a and b (denoted lcm(a,b)) is the smallest positive integer that is divisible by both a and b

Q2. What are gcd(770077, 165) and lcm(770077, 165)?

gcd(770077) = 11
lcd(770077) = 1

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

The latter fact is known as . Its corollary is the following Lemma:

let $a = bq + r$, where a, b, q, and r are integers. then $\gcd(a,b) = \gcd(b,r)$

This Lemma, in turn, implies uniqueness in prime factorization of a positive integer

INTEGER REPRESENTATIONS.

3.1. Given any **base** $b \in \mathbb{N} \setminus \{1\}$, any $n \in \mathbb{N}$ can be written as

$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$

where k is a nonnegative integer, $a_0, a_1 \ldots a_k$ are nonnegative ints less than b. and $a_k \neq 0$

3.2. The computation of $b^n \pmod m$ can be done efficiently using $O((\log m)^2 \log n)$ (pg. 268)

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

$27 = 2 \cdot 13 + 1$
$13 = 2 \cdot 6 + 1$
$6 = 2 \cdot 3 + 0$
$3 = 2 \cdot 1 + 1$
$1 = 2 \cdot 0 + 1$

$27 = 8 \cdot 3 + 3$
$3 = 8 \cdot 0 + 3$

$(27)_{10} = (33)_8$

$27 = 16 \cdot 1 + 11$
$1 = 16 \cdot 0 + 1$

$(11\,3)_{16} = (27)_{10}$

$22^{27} \pmod 7 = 22^{(11011)} \pmod 7$ initially, $x = 1$, $i = 0$, power $= 22 \pmod 7 = 22$

i	a_i	x	power
0	1	$1 \cdot 22 = 22$	$22^2 \pmod 7 = 1$
1	1	$22 \cdot 1 = 22$	$1^2 \pmod 7 = 1$
2	0	22	$1^2 \pmod 7 = 1$
3	1	$22 \cdot 1 = 22$	$1^2 \pmod 7 = 1$
4	1	$22 \cdot 1 = 22$	$1^2 \pmod 7 = 1$

SOLVING CONGRUENCES. (274)

4.1. Let $m \in \mathbb{N} \setminus \{1\}$. An inverse of $a \in \mathbb{Z}$ modulo m is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m

If such an inverse exists it is unique up to m

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

SEE WORK for problem on page 3!

Answer $x = 183$

4.2. The **Chinese remainder theorem** says: a system of linear congruences modulo pairwise relatively prime ints has a unique solution modulo the product of these moduli.

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime ints greater than one and $a_1, a_2, \ldots, a_n$ arbitrary ints then the system:

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\vdots$
$x \equiv a_n \pmod{m_n}$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$ (that is, there is a solution x with $0 \leq x < m$, and all other solutions congruent modulo m to this solution.)

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

SEE WORK for problem on page 4!

Answer 46

4.3. **Fermat's little theorem** says: If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod p$$

Furthermore, for every integer a we have

$$a^p \equiv a \pmod p$$

Q4

$462 = 5(101) - 43$

$101 = 2(43) + 15$

$43 = 3(15) - 2$

$15 = 7(2) + 1$

therfore:

$1 = 15 - 7(2)$

$= 15 - 7(3(15) - 43)$

$= 15 - 21(15) + 7(43)$

$= -20(15) + 7(43)$

$= -20(101 - 2(43)) + 7(43)$

$= -20(101) + 47(43$

$= -20(101) + 47(5(101) - 462)$

$= -20(101) + 235(101) - 47(462)$

$1 = 215(101) - 47(462)$

$1 = 215(101) - 47(462) \mod(462) \Rightarrow$

$1 = 215(101) \mod 462$

$101x \equiv 3 \pmod{462}$

$\Rightarrow x = \frac{3}{101} \pmod{462}$

$x \equiv 645 \pmod{462}$

$x = (645 - 462) \pmod{462}$

$x = 183 \pmod{462}$

$\boxed{x = 184}$

Q5: $2x \equiv 1 \pmod 7$, $13x \equiv 2 \pmod{11}$

$2x \equiv 1 \pmod 7 \Rightarrow 2^{-1} \cdot 2x \equiv 2^{-1} \cdot 1 \pmod 7 \Rightarrow x \equiv 2^{-1} \pmod 7$.

But $2^{-1} \bmod 7 = 4$ $(\because 2 \times 4 = 8 = 1 \pmod 7)$

$\Rightarrow x = 4 \pmod 7$

$\Rightarrow 7 / x-4 \Rightarrow x-4 = 7t$, where $t \in \mathbb{Z}$.

$\boxed{\Rightarrow x = 4+7t} \rightarrow (1)$

second congruence, $13x = 2 \pmod{11}$

$13(4+7t) \equiv 2 \pmod{11}$ from (1)

$\Rightarrow 13 \times 4 + 13 \times 7t \equiv 2 \pmod{11} \Rightarrow 52 + 91t = 2 \pmod{11} \Rightarrow 91t = -50 \pmod{11}$

$\Rightarrow 3t \equiv 5 \pmod{11}$ $[\because 91 \bmod (11) = 3,\ 50 \bmod (11) = 5]$

$\Rightarrow 3^{-1} \cdot 3t \equiv 3^{-1} \cdot 5 \pmod{11}$

$\Rightarrow t = 3^{-1} \cdot 5 \pmod{11}$

$\Rightarrow t = 4 \cdot 5 \pmod{11}$ $[\because 3^{-1} \bmod (11) = 4]$

$\Rightarrow t = 20 \bmod (11)$

$\Rightarrow t \equiv 3 \cdot 5 \pmod{11}$

$\Rightarrow t \equiv 4 \cdot 5 \pmod{11}$ $[\because 3^{-1} \bmod (11) = 4]$

$\Rightarrow t \equiv 20 \pmod{11}$

$\Rightarrow t = 9 \pmod{11} \Rightarrow 11 / t-9 \Rightarrow t-9 = 11s$ where $s \in \mathbb{Z}$

$\boxed{t = 9+11s} \rightarrow (2)$

for (1) and (2), we have $x = 4+7(9+11s)$

$x = 4+63+77s$

$x = 67+77s$ where $s \in \mathbb{Z}$

The smallest +ve solution of above, means $s = 0$

$x = 67+0 = 67$

$\boxed{\text{the answer is } 67}$