Homework 2

Zachary Hightower

1. Reading

2. In $\mathbb{Z}_{20}$ calculate the following. If the answer does not exist, say so and explain why.

a. $17 \oplus 8$

$(17+8) \bmod 20$

$(25) \bmod 20 = 5$

b. $3 \ominus 7$

$(3-7) \bmod 20$

$(-4) \bmod 20 = 16$

c. $5 \otimes 9$

$(5 \times 9) \bmod 20$

$(45) \bmod 20 = 5$

d. 3^{-1}

For $k \in \mathbb{Z}_{20}$, $\gcd(20, k)$ when $k = (1, 3, 7, 9, 11, 13, 17, 19)$

$(3 \times 7) \bmod 20$

$(21) \bmod 20 = 1$

So, $3^{-1} = 7$

e. $5 \oslash 3$

$5 \otimes 3^{-1}$

$5 \otimes 7$

$(5 \times 7) \bmod 20$

$(35) \bmod 20 = 15$

f. 4^{-1} does not exist, because 4 is not a part of the gcd(20, k) list. This means it is not usable in our definition of ~~[illegible]~~ reciprocal.

3. In $\mathbb{Z}_{20}$ solve the following equations for x (find all the solutions or state that none exist)

g. $(9 \otimes x) \oplus 4 = 1$

$9 \otimes x = 1 \ominus 4$

$9^{-1} \otimes 9 \otimes x = 17 \otimes 9^{-1}$

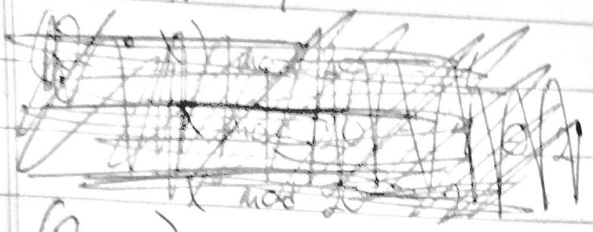
$9 \otimes 9 \otimes x = 17 \otimes 9$

$1 \otimes x = 13$

$x = 13$

HW 2pt 083

b. $2 \otimes x = 4$



$(2 \cdot x) \bmod 20 = 4$

$(2 \cdot 2) \bmod 20 = 4$

~~$(2 \cdot 2) \bmod 20 = 4$~~

$(2 \cdot 12) \bmod 20 = 4$, $(2 \cdot 22) \bmod 20 = 4$

$12 = 10 \cdot 1 + 2$

$x = 10(c_{0,1,2\ldots}) + 2$

c. $2 \otimes x = 3$

$(2 \cdot x) \bmod 20 = 3$

In order for equation to have a solution, it must generate an odd number, however the equation as written will only result in even values for $(2 \cdot x)$. Thus, we cannot get a result $= 3$. So, the equation, has no solutions.

HW 2 Zp11 08 4

4. List all elements of Z_{21} that have a reciprocal

gcd(21, k) when k = (1, 2, 4, 5, 8, 10, 11, , 13, 16, 17 19, 20)
This list covers all elements of Z_{21} that have a reciprocal

5. a.) Find 2 integers such that $111x + 200y = 1$

$200 = 1 \cdot 111 + 89$
$111 = 1 \cdot 89 + 22$
$89 = 4 \times 22 + 1$
$22 = 22 \times 1 + 0$

$1 = 89 - 4 \times 22$
$1 = 89 - 4 \times (111 - 1 \cdot 89)$
$1 = -4 \cdot 111 + 5 \cdot 89$
$1 = -4 \cdot 111 + 5 \cdot (200 - 1 \times 111)$
$1 = 5 \cdot 200 + [-4 + (5 \cdot -1)] 111$
$1 = 5 \cdot 200 + -9 (111)$
So $x = 5$
$y = -9$

HW 2 ZPH P85

b. Find the reciprocal of 111 in $\mathbb{Z}_{200}$

111^{-1}

$(111 \times K) \bmod 200 = 1$

$1 = 5 \cdot 200 + -9 \cdot 111$

$b = -9 \bmod 200 = 191$

$111 \otimes 191 = (111 \cdot 191) \bmod 200 = 21201 \bmod 200 = 1$

Therefore, $111^{-1} = 191$

6. Find all integers x which leave a remainder 4 when divided by 5 and a remainder 7 when divided by 11. That is, solve the following equations simultaneously

$x \bmod 5 = 4$ and $x \bmod 11 = 7$

HW 2 pt 4 for 6

6. cont. $x \bmod 5 = 4$

$x + 5k = 4$

$x = 4 - 5k$

$x \bmod 11 = 7$

$(4 - 5k) \bmod 11 = 7$

$-5k \bmod 11 = 3$

$5^{-1}(5k \bmod 11) = (3)\,5^{-1}$ in $\mathbb{Z}_{11}$ $5^{-1} = 9$

$9 \otimes -5 \otimes k = 3 \otimes 9$ $(9 \times 5) \bmod 11 = 1$

$k = (3 \times 9) \bmod 11$

$k = 6$

$k = 6 + 11j$

$x = 4 - 5k = 4 - 5(6 + 11j) = -26 + (-55j)$

$(\forall j \in \mathbb{Z}$

So the solution set is $\{x \in \mathbb{Z} : x \equiv -26\ (-55)\}$

7. Let $n = 2 \times 3^8 \times 7^6 \times 13^2$ and let $m = 2^2 \times 3^4 \times 5 \times 7^{10}$
Find $\gcd(m, n)$

$\gcd(m, n) = 2^{\min(1,2)} \times 3^{\min(8,4)} \times 5^{\min(1,0)} \times 7^{\min(10,6)} \times 13^{\min(0,2)}$

$\gcd(m, n) = 2^1 \times 3^4 \times 5^0 \times 7^6 \times 13^0$

$\gcd(m, n) = 190\,59138$

8. Prove that $\sqrt{7}$ is irrational

Let us assume that $\sqrt{7}$ is rational

Now, since $\sqrt{7}$ is rational, we write it as $\frac{p}{Q}$ where $p, q \in \mathbb{Z}$ and coprime, their Gcd = 1

$\sqrt{7} = \frac{p}{Q}$

$p = \sqrt{7}\, Q$

$p^2 = 7Q^2$

$\frac{p^2}{7} = Q^2$

#2 Zach pg8

8 cont. 7 is a prime, so, being a prime, it must divide m^2, and so divides m as well. The reverse is also true, m divides 7 and 7^2 So, since we know 7 is a factor of p^2, it must also be the factor of p

So we write $p = 7 \cdot c$, where c is some constant
Sub $p = 7q$ in our equation and,

$$\frac{(7c)^2}{7} = q^2$$

$$\frac{49c^2}{7} = q^2$$

$$q^2 = \frac{q^2}{7}$$

So, 7 will also be the factor of q.
We originally assumed that p and q are the coprimes. Meaning 1 is the only number that can evenly divide both. But here 7 is common factor to p and q, which makes our original assumpeion false.

So, 7 isn't a rational number. Thus, it must be irrational.