412 Individual HW2

Jack Madden

Februrary 2024

Problem 1

To find all generators in $\mathbb{Z}_{17}^*$, we note that $\mathbb{Z}_{16}$ is isomorphic to it under the map 3^x. We have that the generators in $\mathbb{Z}_16$ are those numbers which are coprime to 16, which are 1, 3, 5, 7, 9, 11, 13, 15. These generators will be isomorphic to the generators in $\mathbb{Z}_{17}^*$, so we therefore have generators 3, 10, 5, 11, 14, 7, 12, 6.

Problem 2

We try to find

$$2^{2^{17}} \ mod \ 19 = 2^{131072} \ mod \ 19$$

Fermat's little theorem gives us that 2^{18} is 1 mod 19. Thus, we now have

$$2^{2^{17}} \ mod \ 19 = 2^{131072} \ mod \ 19 = 2^{18^{7281}} \ mod \ 19 \cdot 2^{14} \ mod \ 19 = 2^{14} \ mod 19$$

We then have that this is equal to

$$2^7 \ mod \ 19 \cdot 2^7 \ mod \ 19 = 14 \cdot 14 \ mod \ 19 = 196 \ mod \ 19 = 6$$

Problem 3

We can apply Euler's theorem to help solve this problem as 5 and 18 are relatively prime. We have

$$\phi(18) = 6$$

and thus

$$5^{1000} \ mod \ 18 = (((5^6)^{166} \ mod \ 18) \cdot (5^4 \ mod 18)) \ mod \ 18$$

Then by Euler's theorem, 5^6 is 1 modulo 18 which gives us:

$$5^{1000} \ mod \ 18 = 5^4 \ mod \ 18$$

which is just 13.

Problem 4

We have:

$$21x = 6 \ mod \ 57$$

We divide this equation by the gcd of 21 and 57, 3, to get

$$7x = 2 \ mod \ 19$$

Since 7 and 19 are coprime, 7 has a multiplicative inverse in $\mathbb{Z}_{19}$, specifically 11.

$$11 \cdot 7x = 2 \cdot 11 \ mod \ 19$$

$$x = 3 \ mod \ 19$$

Thus, we have that the solutions for our original equation are the numbers which are 3 modulo 19 in $\mathbb{Z}_{57}$, which are 3, 22, and 41.

Problem 5

Take a to be a unit in R with a^{-1} being its multiplicative inverse. Take b to be a non-unit in R. We will show by contradiction that neither ab nor ba can be a unit. Suppose ab is a unit. Then, we have c such that $(ab)c = 1$. Using the fact that a is a unit gives us $bc = a^{-1}$, and then $bca = 1$ But then b clearly has an inverse $b^{-1} = ca$, and we claimed that it was not a unit. This is a contradiction. Taking $bac = 1$, we reach the same contradiction, where $b^{-1} = ac$.

Problem 6

If an element $x \in \mathbb{Z}_p$ is its own inverse, we have that

$$x^2 = 1$$

$$x^2 - 1 = 0$$

$$(x + 1)(x - 1) = 0$$

Since $\mathbb{Z}_p$ is an integral domain, we have that either $(x + 1)$ or $(x - 1)$ equal to zero. This is only true for $x = 1, -1$ and $-1 \equiv p - 1$. Thus, this gives us that $1, p - 1$ are the only elements that are their own inverses.

Problem 7

Let's examine the product $2 \cdot 3 \cdots p - 2 = (p - 2)!$. We know that the only elements that are their own inverse are $1, p - 1$. Thus, we have that for any $a \in [2, p - 2]$, $a^{-1} \neq a$ and $a^{-1} \in [2, p - 2]$. We also have that $|[2, p - 2]| = p - 3$, which will be an even number if p is an odd prime. Thus, since $\mathbb{Z}_p$ is an integral domain and therefore commutative, we can rewrite $(p - 2)! \ mod \ p$ as:

$$(1 \cdot 1^{-1}) \cdot (2 \cdot 2^{-1}) \cdots ((p - 2) \cdot (p - 2)^{-1}) = 1 \cdot 1 \cdot \cdots \cdot 1 = 1 \ mod \ p$$

From here, we can see that:

$$(p - 1)! \ mod \ p = (p - 1) \cdot ((p - 2)! \ mod \ p = (p - 1) \cdot 1 \ mod \ p = p - 1 \equiv -1$$

Problem 8

Let $(a,b),(c,d),(e,f) \in K$. Then:

$$((a,b)+(c,d))+(e,f) = (ad+bc,bd)+(e,f) = (f(ad+bc)+ebd,bdf) = (adf+bcf+ebd,bdf)$$

$$(a,b)+((c,d)+(e,f)) = (a,b)+(cf+ed,df) = (b(cf+ed)+adf,bdf) = (adf+bcf+ebd,bdf)$$

Thus we have shown that addition of fraction is associative in field of fractions.

Problem 9

Problem 10

To prove that this is an integral domain, we have to show that there are no zero divisors.

The field of fractions of $\{n+mi|n,m \in \mathbb{Z}\}$ is all pairs $\{(a+bi,n+mi) \in \mathbb{Z}$ with either n or m not equal to zero. It is isomorphic to the subfield described under the map $\phi((x,y)) = \frac{x}{y}$. We show that this map is a bijection first. First, if

$$\phi\left((a+bi,c+di)\right) = \frac{a+bi}{c+di} = \frac{w+xi}{y+zi} = \phi\left((w+xi,y+zi)\right)$$

which then gives us:

$$\frac{a+bi}{c+di} = \frac{w+xi}{y+zi}$$

$$(a+bi)(y+zi) = (w+xi)(c+di)$$

which is the condition for equality in field of fractions, showing us that the function is injective. Likewise, the function is surjective as for any $\frac{a+bi}{c+di}$ we can just choose $\phi((a+bi,c+di))$. The function also follows the homomorphism properties, as the process of adding fractions in complex numbers and obtaining a common denominator is the same as adding fractions in a field of fractions. The same equivalence follows for multiplication.