CS203: Abstract Algebra
Assignment 3 Solutions

Ayush Bansal

September 1, 2017

1. Problem 1 Solution

1.1 Part 1.

I have to find and prove whether the following equation has integral solutions or not:

$$x^3 = y^2 + 3 \tag{1.1}$$

For proving the above fact, I will first prove the following lemma.

Lemma 1. *If p is an odd prime number then $\exists x \in \mathbb{Z}$ such that $(x^2+1) mod p = 0$ if and only if p is of the form $4n+1$*

Proof. Consider p, a prime number and $p \neq 2$, then p will be of the form $4n+1$ or $4n+3$ and $\frac{p-1}{2} = 2n$ and $\frac{p-1}{2} = 2n+1$ respectively in either cases.
Now consider the value of $(p-1)!$, I will do some computations on this as follows:

$$(p-1)! = 1*2*3\ldots\frac{p-1}{2}*(p-\frac{p-1}{2})\cdots*(p-1) \tag{1.2}$$

$$(p-1)! = (\frac{p-1}{2})!*(p-\frac{p-1}{2})\cdots*(p-1) \tag{1.3}$$

The terms beyond $(\frac{p-1}{2})!)$ will form a polynomial in p whose constant term will not be divisible by p, rest will be divisible by p.
Now if $\frac{p-1}{2} = 2n$, then the constant term will be **positive**, so using this:

$$(p-1)! = (\frac{p-1}{2})!*(\frac{p-1}{2})! \quad mod p \tag{1.4}$$

$$(p-1)! = ((\frac{p-1}{2})!)^2 \quad mod p \tag{1.5}$$

By using **Wilson's Theorem** (Proved in **2.1 Part 1**) we can say:

$$(x^2+1) mod p = 0, \quad x = (\frac{p-1}{2})!$$

If $\frac{p-1}{2} = 2n+1$, then the constant term will be **negative**, and since x^2 cannot be negative for integral x, such x will not exist, hence our lemma is proved. □

Consider a second lemma as follows.

Lemma 2. *The square of any odd number is of the form $8n+1$.*

Proof. Any odd number can be written in 4 forms which are $8n+1, 8n+3, 8n+5, 8n+7$, considering each one by one.

8n+1: $(8n+1)^2 = 8(8n^2+2n)+1$ which is of the form $8n+1$.
8n+3: $(8n+3)^2 = 8(8n^2+2n+1)+1$ which is of the form $8n+1$.
8n+5: $(8n+3)^2 = 8(8n^2+2n+3)+1$ which is of the form $8n+1$.
8n+7: $(8n+3)^2 = 8(8n^2+2n+6)+1$ which is of the form $8n+1$.

Thus, the lemma is proved. □

Now coming to the equation (1.1) and proving the existence or non-existence of it's solutions.

Proof. Consider x as even then $(y^2+3)mod8 = 0$ but this is not possible as y is odd and $y^2 mod8 = 1$ by **Lemma 2**.
Thus, x must be **odd** and due to this y must be **even**.
Doing following computations on the equation and putting $y = 2a$:

$$x^3 + 1 = y^2 + 4 \tag{1.6}$$

$$(x+1)(x^2 - x + 1) = 4(a^2 + 1) \tag{1.7}$$

Notice that $(x^2 - x + 1)$ is **odd**, let p be a prime factor of $(x^2 - x + 1)$, then p must of the form $4n+1$, as $(a^2+1)modp = 0$, by **Lemma 1**.
Thus all prime divisors of the number $(x^2 - x + 1)$ will be of the form $4n+1$.
$\therefore (x^2 - x + 1)mod4 = 1$, which shows $4 \mid x^2 - x$ and since x is odd, $4 \mid x - 1$.
By using above results we can see that, $(x+1)mod4 = 2$ which means **LHS** in equation (1.7) is not divisible by 4 but **RHS** is, which means there is no possible integral solution for the equation (1.1). □

1.2 Part 2.

I have to find and prove whether the following equation has integral solutions or not:

$$x^3 = y^2 + 1 \tag{1.8}$$

For proving this, I will assume that $\mathbb{Z}[i]$ is a **Unique Factorization Domain**.

Proof. We can re-write the above equation as:

$$x^3 = (y+i)(y-i) \tag{1.9}$$

Now there are 2 possible cases:
Case 1: $(y+i)$ and $(y-i)$ does not have a common factor.
If there is no common factor between $(y+i)$ and $(y-i)$, then both of have will be a cube of a certain element in $\mathbb{Z}[i]$ since **LHS** in (1.9) is a perfect cube of some element in $\mathbb{Z}[i]$, which means:

$$y + i = (a+ib)^3$$
$$y + i = a^3 - 3ab^2 + i(3a^2b - b^3)$$
$$3a^2b - b^3 = 1$$

Since $a, b \in \mathbb{Z}$, the only possible solution for this case is $a = 0, b = -1$.
Case 2: $(y+i)$ and $(y-i)$ have a common factor.
If 2 numbers have a common factor, then their difference and their sum will also have that number as a factor, using their difference we get that the only possible common factors they can have are $(1+i)$ and $(1-i)$, also $(1-i)(1+i) = 2$.
Now we can write $y + i = (1+i)^{f_1}(1-i)^{f_2}(a+ib)^{3k}$ such that $3 \mid f_1 + f_2$ but $3 \nmid f_1$ and $3 \nmid f_2$ because net sum of powers in $(x+i)(x-i)$ must remain multiple of 3 and these both are **Conjugates** of each other.
Assuming $f_1 < f_2$, we can write $x + i = 2^{f_1}(1-i)^{f_2-f_1}(a+ib)^{3k}$, this gives $x + i = 2(p+qi)$ or $1 = 2q$ but $q \in \mathbb{Z}$ which means this case has no possible solution.
Thus, by above 2 cases, it is clear that an integral solution of equation (1.8) exists which is $x = 1, y = 0$. □

2. Problem 2 Solution

2.1 Part 1.

In this part I have to prove the following theorem:

Theorem 1 (Wilson's Theorem)**.** *Suppose p is a prime number then:*

$$(p-1)! = -1 \quad mod p \tag{2.1}$$

The proof will be in 2 cases, $p = 2$ and $p \geq 3$. Let's first suppose $p = 2$, we can see that $(2-1)! = 1$ and $(-1)mod(2) = 1$, thus results holds for $p = 2$.
Now we consider that p is a prime number such that $p \geq 3$. Since p is a prime number, the numbers $\{1,2,3\ldots,p-1\}$ form a group called $\mathbb{Z}_p$ under binary operation **multiplication mod p** and since it forms a group, every element will have an inverse.

Lemma 3. *Every number in group $\mathbb{Z}_p$ has a unique inverse unequal to itself except for 1 and $p-1$, where p is an odd prime number.*

Now, I will prove the above lemma using **Division Algorithm**.

Proof. Assume some number a in group $\mathbb{Z}_p$ is inverse of itself, thus $a^2 mod(p) = 1$, and by division algorithm $a^2 = np + 1, n \in \mathbb{Z}$.
Since a is an integer we can rewrite the above equation as $a^2 = (kp \pm 1)^2$ and thus $a = (\pm 1)mod(p)$ which gives us 2 values of a which are 1 and $p-1$. □

Now going for the main proof:

Proof. Since $p \geq 3$, p will be an odd prime number and thus by **Lemma 3** for the group $\mathbb{Z}_p$.
Since every element a_i in the group can be paired with unique unequal element a_j which is it's inverse such that $(a_i * a_j)mod(p) = 1$ except for 1 and $p-1$, we get:

$$(p-1)! = [1 * (p-1)].[a_i * a_j]\ldots \tag{2.2}$$
$$(p-1)! = (p-1)mod(p) \tag{2.3}$$
$$(p-1)! = (-1)mod(p) \tag{2.4}$$

By (2.4), **Wilson's Theorem** is proved. □

2.2 Part 2.

Now we take p, a prime number of the form $4n+1$ and have to prove that:

$$x^2 \equiv -1 \quad mod p \tag{2.5}$$

Proof. $p = 4n+1, n \in \mathbb{N}$, and thus $\frac{p-1}{2} = 2n$.
Using the result proved in **Lemma 1**, I can say $x = (\frac{p-1}{2})!$. □

2.3 Part 3.

Consider a prime number p of the form $4n+1$, p is prime in $\mathbb{Z}$.

Lemma 4. *p is not prime in $\mathbb{Z}[i]$ if p is of the form $4n+1$.*

Proof. Since p is of the form $4n+1$, by (2.5) we have some x such that $(x^2+1) mod p = 0$, or we can say that $x^2+1 = kp, k \in \mathbb{N}$.
Now assume p is a prime number in $\mathbb{Z}[i]$.
We can write $x^2+1 = (x+i)(x-i)$ and since $p \mid x^2+1$, by definition of prime in $\mathbb{Z}[i]$, $p \mid x+i$ or $p \mid x-i$.
Case 1. $p \mid x+i$

Since $p \mid x+i$, $\frac{x}{p} + \frac{i}{p} \in \mathbb{Z}[i]$ but since we know that i is a unit in $\mathbb{Z}[i]$, $\frac{i}{p} \notin \mathbb{Z}[i]$, thus our statement is a **Contradiction**.

Case 2. $p \mid x-i$

Same argument as that of **Case 1**.

By above 2 cases, our lemma is proved. □

Now we will prove that there exists integers x, y and c such that $x^2+y^2 = cp$ and $gcd(c,p) = 1$.

Proof. Since we have proved that p is not a prime in $\mathbb{Z}[i]$, we consider that it is product of 2 numbers from $\mathbb{Z}[i]$.
Let $p = (x+iy)(a+ib)$, doing computations on it and equating imaginary part to 0, we get:

$$p = (ax-by) + i(ay+bx) \tag{2.6}$$
$$ay+bx = 0 \tag{2.7}$$
$$\frac{a}{b} = -\frac{x}{y} \tag{2.8}$$
$$kp = x^2+y^2, k = \frac{x}{a} \tag{2.9}$$

Putting $k=1$ in the above equation, we get $p*1 = x^2+y^2, x, y \in \mathbb{Z}$ and $gcd(1,p) = 1$ and so the proof is complete □

2.4 Part 4.

We are given that p is prime number such that $x^2+y^2 = cp$, where x, y and c are integers and $gcd(c,p) = 1$.
I have to prove that p is not a prime in $\mathbb{Z}[i]$.

Proof. Assume that p is a prime in $\mathbb{Z}[i]$.
Since $cp = x^2+y^2$, we can write it as $cp = (x+iy)(x-iy)$, since $p \mid (x+iy)(x-iy)$, by definition of prime in $\mathbb{Z}[i]$, either $p \mid (x+iy)$ or $p \mid (x-iy)$.
Considering either of the both cases we get that $\frac{x}{p}, \frac{y}{p} \in \mathbb{Z}[i]$ and since $x, y \in \mathbb{Z}$, also units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$, and $p \mid x$ and $p \mid y$.
Using above result, $x = ap$ and $y = bp$, $a, b \in \mathbb{Z}$, putting these values in our original equation we get:

$$cp = b^2p^2 + a^2p^2 \tag{2.10}$$
$$c = p(b^2+a^2) \tag{2.11}$$

Since equation (2.11) is a **Contradiction** to the fact that $gcd(c,p) = 1$, thus p is not a prime in $\mathbb{Z}[i]$. □

2.5 Part 5.

We are given a prime number p which is prime in $\mathbb{Z}$ but not in $\mathbb{Z}[i]$.
I have to prove that $p = a^2 + b^2$ and $a, b \in \mathbb{Z}$.

Proof. Since p is not a prime in $\mathbb{Z}[i]$, we can write p as $p = (a + ib)(x + iy)$, where a, b, x, y are integers.
Now doing the same computations done in (2.6),(2.7),(2.8) and (2.9), putting $k = 1$, we get:

$$p = x^2 + y^2, \quad x, y \in \mathbb{Z}$$

The above equation is the one which I had to prove and so my proof is complete. □

2.6 Part 6.

We are given that p is a prime number in $\mathbb{Z}$ and is of the form $4n + 1$.
I have to prove that $p = a^2 + b^2$, where $a, b \in \mathbb{Z}$.

Proof. Using **Lemma 2**, we can say that since p is of the form $4n + 1$, p will not be a prime in $\mathbb{Z}[i]$. Since p is not a prime in $\mathbb{Z}[i]$, from the proof of **2.5 Part 5.** we can say that $p = a^2 + b^2$ for some integers a and b, which concludes our proof. □

3. Problem 3 Solution

3.1 Part 1.

We are given a ring R such that $x^2 = x, \forall x \in R$.
I have to prove that the ring R is commutative i.e. $\forall a, x \in R$ we have $ax = xa$.

Proof. Let $a, x \in R$ be two elements then, $a + x$ and $(a + x)^2$ will also lie in the ring and they will satisfy:

$$(a + x)^2 = a + x \tag{3.1}$$

$$a^2 + xa + ax + x^2 = a + x \tag{3.2}$$

$$xa = -ax \tag{3.3}$$

Now take some element $-m$ and since we know that $x^2 = x, \forall x \in R$, we have $(-m)^2 = -m$, also $(-m)^2 = m^2 = m, \therefore m = -m$.
By combining above result with (3.3), we have $ax = xa$ and the ring R is **Commutative**. □

3.2 Part 2.

For the proof of this part, I will first prove the following **Lemma 5**:

Lemma 5. *$Z/2Z \cong Z_2$, i.e. there are 2 elements in $Z/2Z$ which are $\{0, 1\}$.*

Proof. Z is the group of all integers under operation "+", and $2Z$ is the group of all **even** integers under same operation which we can get my multiplying each and every integer in $\mathbb{Z}$ by 2.
Thus we can write set O of all **odd** integers as $O = \{1 + x \mid x \in 2Z\}$ and set E of all even integers as $E = \{0 + x \mid x \in 2Z\}$ and set $E + O = \mathbb{Z}$.
Thus, the **quotient group** $Z/2Z$ contains 2 elements $\{0, 1\}$ and operation for this group is **addition mod 2**. □

Now I will prove that for the type of ring specified in **3.1 Part 1**, the only possible ring which is also an integral domain is $Z/2Z$.

Proof. Consider an element $x \in R$, then we know that $x^2 = x$, taking 1 as the multiplicative identity of the ring R and doing some computations we have:

$$x^2 = x.1$$

$$x^2 - x.1 = 0$$

Since "Addition" is distributive over "Multiplication" in a ring, we can write above equation as:

$$x(x - 1) = 0 \tag{3.4}$$

$$\therefore x = 0, 1 \tag{3.5}$$

Since, only 2 elements i.e $\{0, 1\}$ can be in this ring, by **Lemma 3**, the ring is $Z/2Z$ or Z_2. □