Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

ALGEBRA I

1. Lecture 41: Ring problems

We have seen in the lectures that Euclidean division works for Gaussian integers. So, what we know is that given m and n which are Gaussian integers, there exist Gaussian integers q and r such that $n = qm + r$ and the size of r is strictly less than the size of m. So, here for a Gaussian integer, recall that the size is $a^2 + b^2$.

So, here is the first problem . Find q and r, given $n = 15 + 7i$ and $m = 3 + 2i$. So, what we will do is, we will first use division of complex numbers to find a solution that is rational the the rational quotient of this that will not be a Gaussian integer , but let us just do that and see what happens. So, $\frac{n}{m} = \frac{15+7i}{3+2i} = \frac{(15+7i)(3-2i)}{13} = \frac{59-9i}{13}$. This q is not going to work for us, because we want a q that is a Gaussian integer. So, what we will do is, we will take a Gaussian integer that is really close to this. So, the nearest integer is 5. So, take q to be 5 and the nearest integer to - 9 by 13 i is - 9 by 13 is - 1. So, let us take 5 - i and so, so now, we try to write n equals 5 - i into 3 - 2 3 + 2 i + r, then we can solve this to get , so 5 + 3 i that is 15 - + 2 that is 17 and - 3 i + ; so, - 3 i + 10 i which is 7 i , so what we get is , r = 2 r = well. So, n is 15 + 7 i. So, we get r = - 2 . So, what we have is n = q is now, we have taken q to be 5 - i into 3 + 2 i - 2 . So, q equals 5 - i and r equals - 2 and indeed, we see that the size of r is 4 , which is less than the size of 3 + 2 i , which we saw was 13 . Now, let us see why this always works . So, so the algorithm for dividing Gaussian integers finding the integral you know with quotient and remainder for Gaussian integers is this, you just do the complex division and then, you find round off the real and imaginary parts of the quotient to the nearest integer and you use that as q . And then, you multiply that q by m and you compute r and the fact is that this r will always have size smaller than m and why is that the case. So, let us just do a little bit of analysis. So, n by m is q + α and we know that the real and imaginary parts of α are each less than or = half. So, what we know is that real part of α . This is what is we are taking q to be the what we get when we take n by m and round off the real and imaginary part to the nearest integer. So, real part of α is less than or = half and imaginary part of α is less than or = half . So, what we get is α d of α is less than or = half squared +

half squared which = 1 by 4 + 1 by 4 , which is half . So, d of α is less than or = half and now, r is taken to be α times m . So, so d of r is going to; because of the multiplicativity of this d function which just holds for Gaussian integers, d of r turns out to be d of α times d of m which is then, less than or = half d of m which is strictly less than d of m . So, this is why this method I have described for doing Euclidean division of Gaussian integers actually, always works ok. Let us move on to problem 2.

Example 1.1. *Is 3 a Gaussian prime? Suppose that 3 is not a prime and try to see if we can find a factorization of it . So, suppose not , then we would be able to write* $3 = (a + bi)(c + di)$*, where* $a + bi, c + di$ *are Gaussian integers.*

So, what that means is, for for Gaussian integers, the only units are 1 i - i and - 1. And so basically; that means, that $a^2 + b^2 > 1$*; that is d of a + bi and c squared + d squared is greater than 1, because if they were = 1, then they would be 1 of a 1 i - 1 and - i, which are the units . Now, let us use the multiplicativity of this norm or absolute value of complex numbers this is the squared absolute value. So, that is also multiplicative. So, we have that* $9 = (a^2 + b^2)(c^2 + d^2)$*. Therefore, we must have* $a^2 + b^2 = 3$ *and so is* $c^2 + d^2$*. But since 3 cannot be written as a sum of two squares; such a b c d do not exist therefore, 3 is a prime in* $\mathbb{Z}[i]$*.*

Example 1.2. *Is 5 a prime in* $\mathbb{Z}[i]$*? I can take* $a = 2, b = 1$*. And so, you you are getting 5 = 2 + i and into what? Now, easily see that 2 - i works . And you can also do it another way, which is you can take a equals a equals 1 and b equals 2 and so, you will also get i + 2 into i sorry that is the same what I meant to say is ; 1 + 2 i into 1 - 2 i and this will also be = 5 . So, here are two factorizations of 5 and these are not units; however, these two factorizations are equivalent in the sense that if you take 2 + i and multiply it by i, then you will get - 1 . So, if you multiply it by say - i perhaps , then you will get 1 + 2 i. So, this this prime is a unit multiplied by this prime so, they are associates. And this prime is a unit multiplied by this prime. So, in some sense, these two factorizations of 5 into smaller primes are equivalent. Anyway, the answer to our problem is no 5 is not a prime in* $\mathbb{Z}[i]$*.*

In fact, what these two problems show you is that a prime number is is not a prime in the Gaussian integers, if and only if it can be written as a sum of two squares. And if it cannot be written as a sum of two squares, it will be a prime number in the Gaussian integers. And it is a result in number theory that a prime number can be written as a sum

of two squares, if and only if it is congruent to 1 mod 4. There is a very beautiful discussion of this in Michael Artin's Algebra book . I think you have to look at chapter 11, section 5 of Michael Artin's Algebra book. And you will find a complete description of which prime's in the integers are primed in Gaussian integers, how they decompose etcetera. We will end this problem session by looking at a problem which I had promised we will discuss later on . And this is the following. Show that the ideal generated by 2 and x in polynomials with integer coefficients is not a principal idea . We have seen that if we take polynomials with rational coefficients or coefficients in any field, then they form a Euclidean domain. And so, every ideal in this ring of polynomials with entries in a field would be a Euclidean domain and hence, a principal ideal domain. However, when you take polynomials with integers then, they do not form a principal ideal domain and this solution is not very difficult. Maybe, you can take a few minutes to try it out yourself . If not, you can follow the solution that I will give you now . So, suppose this were a principal ideal . So, it would be generated by some polynomial $f(x)$. So, this would again be a polynomial with integer coefficients . What we would have is that then, 2 is in the ideal generated by $f(x)$. So, $2 = f(x)g(x)$. So, the degree of 2 which is 0 would be the sum of the degrees of f and g therefore, f would have to be of degree 0 which means that f would have to be a constant polynomial ok . And moreover, f would be = 1 or f would be = 2, because it would have to divide 2. And now, x is going to be = f x times h x for some polynomial h x . This implies that , so f has a coefficient 1. So, you cannot have you cannot have f = 2. So, this implies that f = 1 . So, if this were a principal ideal that have to be generated by 1, but 1 does not even belong to the polynomial ring generated the ring generated by 2 and x . Why is that ? Because if you take something in this , any element of the ideal generated by 2 and x is of the form 2 times h x + x times g x for h x g x in Z x. And so, if you substitute x equals 0 , so we have that 1 is 2 h x + x g x. Substitute h equals 0 you get 1 = 2 h 0 + 0; which would mean that 1 has to be an even number, which is clearly false . So, we get a contradiction . So, we see that the ideal generated by 2 and x in the ring of polynomials with integer coefficients is not a principal ideal.