

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

SOLUTIONS FOR HOMEWORK 1: GAUSSIAN INTEGERS I

This homework was due at the start of class on Wednesday Sep 13.

1. Recall that an ordered pair (a, b) of real numbers determines a complex number $z = a + bi \in \mathbb{C}$ of modulus $|z| = \sqrt{a^2 + b^2}$ which is just the distance from z to 0 in the complex plane. Prove that for $z, w \in \mathbb{C}$, $|zw| = |z||w|$.

Let $z = a + bi$, $w = c + di$. We compute $zw = (ac - bd) + (ad + bc)i$, thus

$$|zw|^2 = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2.$$

That simplifies to

$$|zw| = \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2}.$$

On the other hand,

$$|z||w| = \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} = \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2}.$$

We see that we've obtained the same expression for $|zw|$ and $|z||w|$. As you've noticed, this is a fact we will be using over and over again.

2. Prove that if $r, s \in \mathbb{Z}$ and $rs = 1$, then either $r = s = 1$ or $r = s = -1$.

Let's do it by contradiction. Suppose $rs = 1$ for integers r, s and that the pair (r, s) is neither $(1, 1)$ nor $(-1, -1)$. It is clear that $r \neq 0$ and $s \neq 0$ and also we can't have $r = 1, s = -1$ or $r = -1, s = 1$ because rs is positive. Thus, at least one of the numbers $|r|, |s|$ is greater than 1 because all other possibilities for (r, s) , namely $(0, \pm 1), (\pm 1, 0), (\pm 1, \pm 1)$ have been eliminated. So, let's say $|r| > 1$. Then $0 < |s| = 1/|r| < 1$. But $|s|$ is an integer, and there are no integers strictly between 0 and 1. This is a contradiction.

3. Let $\mathbb{G}^\times = \{\alpha \in \mathbb{G} \mid \alpha\beta = 1 \text{ for some } \beta \in \mathbb{G}\}$ be the set of units (or invertible elements) in \mathbb{G} . Show that $\mathbb{G}^\times = \{\pm 1, \pm i\}$.

Hint: Show that $\alpha \in \mathbb{G}^\times \Rightarrow |\alpha|^2 = 1$, and then think geometrically about what this means.

Suppose $\alpha \in \mathbb{G}^\times$. Then there is $\beta \in \mathbb{G}$ such that $\alpha\beta = 1$. Taking norms and using problem 1, we have $|\alpha||\beta| = 1$. But now we use problem 2 to conclude that $|\alpha| = 1$ since $|\alpha|$ is a positive integer so cannot be -1 . Therefore units have distance exactly 1 from 0. Geometrically, it's clear that the only points on the integer lattice that close to 0 are ± 1 and $\pm i$. Algebraically we can argue like this: if $\alpha = x + iy$ and $|\alpha| = 1$, then we have $x^2 + y^2 = 1$. If $|x| > 1$, then $|x^2 + y^2| \geq |x|^2 > 1$ which gives $|x^2 + y^2| > 1$ contradicting $|x^2 + y^2| = 1$. Thus, $|x| \leq 1$. By the same argument, $|y| \leq 1$. Now we can't have $|x| = |y| = 1$ because that would give $x^2 + y^2 = 1 + 1 = 2$, nor can we have $x = y = 0$, so we must have $x = 0$

and $y = \pm 1$ or $x = \pm 1$ and $y = 0$. In other words, $x + iy \in \{\pm 1, \pm i\}$. Note that we already know $\pm 1, \pm i$ are indeed units.

4. Recall that $\gamma \in \mathbb{G}$ is a *Gaussian prime* if there do not exist $\alpha, \beta \in \mathbb{G} - \mathbb{G}^\times$ (i.e. α and β are non-invertible elements of \mathbb{G}) such that $\gamma = \alpha\beta$. Prove that $1 + i, 1 + 2i, 2 + 3i$ are Gaussian primes, and that $1 + 3i, 3 + 4i$ are **not** Gaussian primes.

Let's prove a useful result.

Lemma. If $\pi = a + bi \in \mathbb{G}$ and $N(\pi) = |\pi|^2 = a^2 + b^2$ is an ordinary prime, then π is a Gaussian prime.

Proof of Lemma: Say $p = N(\pi)$ is a prime number. Suppose $\alpha, \beta \in \mathbb{G}$ and $\pi = \alpha\beta$ is a factorization of π . Then taking norms, we have $N(\pi) = p = N(\alpha)N(\beta)$ using problem 1 again. So letting $a = N(\alpha)$ and $b = N(\beta)$, we have $p = ab$. Since p is a prime, and since a, b are positive integers, we must have $a = 1$ or $b = 1$. In other words, in any factorization $\pi = \alpha\beta$, either α or β has norm 1. Recalling the previous problem, that means α or β is a unit. That means π does not a factorization into two non-units. That means π is a Gaussian prime. Here endeth the proof of the Lemma.

Now note $N(1 + i) = 2$, $N(1 + 2i) = 5$, $N(2 + 3i) = 13$ are all primes, so $1 + i, 1 + 2i, 2 + 3i$ are all GP by the Lemma.

On the other hand, $N(1 + 3i) = 10$ is not prime, it factors as $2 \cdot 5$ so we will try to factor $1 + 3i$ into a factor of norm 2 times a factor of norm 5. Let's check $(1 + 3i)/(1 + i)$ and we get $(1 + 3i) = (1 + i)(2 + i)$ a non-trivial factorization of $1 + 3i$ showing it is not a Gaussian prime. Now $(3 + 4i)$ has norm 25 so we try $(3 + 4i)/(2 - i)$ or $(3 + 4i)/(2 + i)$. We find $(3 + 4i) = (2 + i)^2$.

5. Prove that 3, 7, and 103 are not sums of two integer squares. Is 1989 a sum of two integer squares? How about 2006?

If $3 = x^2 + y^2$, then $|x| < 2$ else $x^2 + y^2 \geq x^2 \geq 4$. By the same argument, $|y| < 2$. But $0^2 + 1^2$ and $0^2 + 0^2$ and $1^2 + 1^2$ do not give 3. So 3 is not the sum of two integer squares. Similarly, if $7 = x^2 + y^2$, then $|x| < 3$ because else $x^2 + y^2 \geq 9$. We then check $1 + 4, 4 + 4, 1 + 1, 0 + 1, 0 + 4$ don't give 7, so we're done. For 103, let's do something more sophisticated. Let's write $103 = 4k + 3$ with $k = 25$. If $103 = a^2 + b^2$, then one of the pair a, b is even (if both a, b are odd, then $a^2 + b^2$ is even!, and if they're both odd, then $a^2 + b^2$ is even again). So let's assume without loss of generality that a is odd and b is even. Let us write $a = 2m + 1$ and $b = 2n$ with integers m, n . Then $a^2 + b^2 = (2m + 1)^2 + (2n)^2 = 4m^2 + 4m + 1 + 4n^2 = 4\ell + 1$ with the integer $\ell = m^2 + m + n^2$. But now we get $103 = 4k + 3 = 4\ell + 1$. Subtracting the last two equations we get $2 = 4(\ell - k)$. Since $\ell - k$ is an integer, we get 2 is a multiple of 4. This is absurd! So we're done: 103 is not a sum of two squares.

Moving right along: 1989 is a sum of two squares: a little experimentation gives, for example, $1989 = 15^2 + 42^2$ or $1989 = 30^2 + 33^2$. We could find these by noting: $1989 = 3^2 \cdot 13 \cdot 17$ and then noting that $3, 2 + 3i, 1 + 4i$ have norms 3, 13, 17 respectively. Thus, $3(2 + 3i)(1 + 4i)$ has norm 1989. That's the ticket. If we use $3(2 + 3i)(4 + i)$ say we get the other decomposition of 1989 as a sum of two squares.

As for trying to write 2006 as a sum of two squares, in the words of a previous President, "not gonna do't ... wouldn't be prudent." You can just take square roots of $2006 - 0^2, 2006 - 1^2$, etc. and check that none of $2006 - a^2$ is ever a square in \mathbb{Z} . This has to do with

the fact that a prime number of the form $4k+3$ (namely 59) divides 2006 exactly once. We'll see this later on.

6. Suppose you have access to a computer that given an integer k can decide quickly whether k is a perfect square or not. Devise and describe an algorithm (a procedure) for deciding whether a given natural number n is a sum of two integer squares.

As we were just discussing, we could try the following: if $k = a^2 + b^2$, with say $a \leq b$, then $k \leq 2b^2$ and $k \geq 2a^2$ so $a \in [0, \sqrt{k/2}]$. So it suffices to check $\text{ISPERFECTSQUARE}(k - j^2)$ for $j = 0, \dots, \sqrt{k/2}$. If it ever is, we get a decomposition of k as $a^2 + b^2$. If not, then k is not the sum of two integer squares. In practice, it's probably wiser to start your checking with $j = k/\sqrt{2}$ and working down toward 0.

Extra Credit Problem

A. Prove that if $m = a^2 + b^2$ and $n = c^2 + d^2$, with $a, b, c, d \in \mathbb{N}$, then there exist $e, f \in \mathbb{N}$ such that $mn = e^2 + f^2$. In other words, the product of two integers expressible as a sum of two squares is also expressible as a sum of two squares.

Most extra credit problems I assign take you further than the confines of the material I have in mind for the course. Thus, I usually will not give extra credit solutions until the end of the term so you can still work on them. However, here the problem is actually part of the main stream of thought of the course, so I'll give the solution.

We interpret $m = a^2 + b^2$ and $n = c^2 + d^2$ as saying there exist $\mu = a + bi$ and $\nu = c + di \in \mathbb{G}$ such that $N(\mu) = m$ and $N(\nu) = n$. To find an element of norm mn is quite simple. Take $\alpha = \mu\nu$. Then by problem 1, $N(\alpha) = N(\mu\nu) = mn$. We compute $\alpha = (a + bi)(c + di) = (ac - bd) + i(ad + bc)$, so with $e = ac - bd$ and $f = ad + bc$, we get $e^2 + f^2 = mn$.

This is called Euler's identity:

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2).$$

It shows that the product of two sums of two squares is a sum of two squares.