Math 100b Winter 2010 Homework 6

Due 2/26/09 in class, or by 5pm in HW box on 6th floor of AP&M

Reading

If you feel rusty on linear algebra, get out whatever book you learned linear algebra from and review a bit of the basics (vector spaces, spanning, linear independence, bases) to prepare for our unit on linear algebra.

The unit on linear algebra will be based on course notes and there will not be a text.

Assigned Problems from text

9.1: #11(a)

Suggestion for #11: construct the isomorphism using the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}[i]/\langle a+bi \rangle$ defined by $\phi(c) = (c+0i) + \langle a+bi \rangle$ and showing that ϕ is surjective and has kernel $\langle n \rangle$. Note that surjectivity is not obvious in this case.

Additional Problems

These are problems related to our study of factorization of Gaussian integers in class, and the theory of sums of two squares.

1. Find a factorization of 442 into irreducibles in the ring $\mathbb{Z}[i]$. Using this, find explicit $a, b \in \mathbb{Z}$ so that $442 = a^2 + b^2$.

2. (Note: the hint for this problem was changed on Tuesday 2/16. The recommendation to factor out a square is useful only in proving one direction.)

In class, we showed that a prime p is a sum of two squares if and only if $p = 2$ or $p \equiv 1 \mod 4$. Using this, prove the following theorem:

Theorem 0.1 *Let $n > 1$ be a positive integer, with prime factorization $n = p_1^{e_1} \dots p_m^{e_m}$ for distinct primes $p_1, p_2, \dots, p_m$. (This is the prime factorization in $\mathbb{Z}$.) Then n is a sum of two squares if*

and only if every for every prime p_i occurring such that $p_i \equiv 3 \mod 4$, then p_i occurs to an even power e_i.

(For example, $(2^3)(3^2)(5)(7^4)$ is a sum of two squares, but $(2^3)(3^2)(5)(7^3)$ is not.)

(Hint: If every prime congruent to 3 mod 4 occurs to an even power in the factorization of n, then write $n = Dt$ where t is a product of primes which are congruent to 2 or 1 mod 4. Use the results we proved to show that t is a sum of 2 squares, and then use that to show that n is a sum of two squares.

Conversely, suppose that n is a sum of 2 squares, say $n = a^2 + b^2$, so that $n = (a + bi)(a - bi)$ in $\mathbb{Z}[i]$. Then just as in problem 3 step 1 below (you only have to do the argument once on your homework), show that if $(a + bi) = s_1 s_2 \dots s_r$ is a factorization of $(a + bi)$ into irreducibles in $\mathbb{Z}[i]$, then $(a - bi) = \overline{s_1}\,\overline{s_2} \dots \overline{s_r}$ is a factorization of $a - bi$ into irreducibles. So $n = s_1 s_2 \dots s_r \overline{s_1}\,\overline{s_2} \dots \overline{s_r}$. On the other hand, we can also factor n into irreducibles by factoring each prime occurring in $n = p_1^{e_1} \dots p_m^{e_m}$ further into irreducibles in $\mathbb{Z}[i]$. Compare the two factorizations using the fact that $\mathbb{Z}[i]$ is a UFD.)

3. Recall that a *pythagorean triple* consists of positive integers a, b, c such that $a^2 + b^2 = c^2$; these are the possible triples of integers that can occur as the side lengths of a right triangle. Such a triple is *primitive* if $\gcd(a, b) = 1$. If a triple is not primitive, say $\gcd(a, b) = d > 1$, then d also divides c, and then one easily checks that $a/d, b/d, c/d$ is again a pythagorean triple. So to understand pythagorean triples it is enough to find the primitive ones; then all others will just be multiples of these by further integers. In addition, an easy argument shows that in any primitive triple, a and b have different parity. (If a and b are both odd, then a^2 and b^2 are both $\equiv 1 \mod 4$; then $c^2 \equiv 2 \mod 4$, which is impossible since an even square is divisible by 4. Clearly a and b cannot both be even, since then they do not have $\gcd(a, b) = 1$.) Thus by switching a and b, it is enough to consider triples in which b is even and a is odd (then c is also odd.)

For example, $5, 12, 13$ and $9, 12, 15$ are pythagorean triples; the first one is primitive but the second one isn't, it is rather obtained by multiplying the primitive triple $3, 4, 5$ by 3.

The point of this problem is to prove the following result:

Theorem 0.2 *Every primitive pythagorean triple a, b, c with b even is of the form $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ for some $m, n \in \mathbb{Z}$.*

The theorem thus gives a way of finding all primitive triples, by letting m, n vary. Caution, though: the theorem does not state that for all integers m and n the triples the theorem produces are primitive, just that all primitive triples arise in this way.

You will prove the theorem as another application of factorization in $\mathbb{Z}[i]$, in the following steps.

Step 1. Suppose that $c^2 = a^2 + b^2$ with $\gcd(a, b) = 1$ and b even. Then $c^2 = (a + bi)(a - bi)$ in $\mathbb{Z}[i]$. Let $(a + bi) = p_1 p_2 \dots p_n$ be a factorization of $(a + bi)$ into irreducibles in $\mathbb{Z}[i]$ (possibly with repeats.) Show that $(a - bi) = \overline{p_1}\,\overline{p_2} \dots \overline{p_n}$ where each $\overline{p_i}$ is also irreducible in $\mathbb{Z}[i]$. Let $c = q_1 \dots q_m$ be a factorization of c into irreducibles in $\mathbb{Z}[i]$ (again, possibly with repeats). Then we have

$$q_1^2 \dots q_m^2 = p_1 p_2 \dots p_n \overline{p_1}\,\overline{p_2} \dots \overline{p_n}.$$

Step 2. In this step, you will show that no irreducible factor of $(a - bi)$ is an associate (in $\mathbb{Z}[i]$) of an irreducible factor of $(a + bi)$.

Suppose that $\overline{p_j}$ is an associate of p_i.

Case (1): If $i = j$ then $\overline{p_i}$ is an associate of p_i itself: show this can only happen if p_i is an associate of $(1 + i)$. But then show that $p_i\overline{p_i} = \pm 2$, so that 2 occurs as a factor of c^2 in $\mathbb{Z}[i]$. Show that this forces c even, which does not happen in a primitive triple, a contradiction.

Case (2): If $i \neq j$, then $\overline{p_j} = up_i$ where $u \in \{\pm 1, \pm i\}$ is a unit, and then $p_j\overline{p_j} = up_ip_j$, where $p_j\overline{p_j} = d \in \mathbb{Z}$. Since p_ip_j is part of the factorization of $(a+bi)$, show this implies that $\gcd(a, b) > 1$, a contradiction again.

Step 3. Since each irreducible factor of c^2 occurs an even number of times, and no irreducible factor of $(a+bi)$ is an associate of an irreducible factor of $(a-bi)$, use the fact that $\mathbb{Z}[i]$ is a UFD to show that $(a + bi) = uz^2$ for some $z = (m + ni) \in \mathbb{Z}[i]$ and some unit u. Now use this to complete the proof of Theorem 0.2.