Math 323: Homework 5

1. Prove that the quotient ring \( \mathbb{Z}[i]/I \) is finite for every ideal \( I \).

Solution: Note that every ideal is principal, since it is a Euclidean ring, so 
\( I = (\alpha) \) for some \( \alpha \in \mathbb{Z}[i] \). Then, since we know that \( \mathbb{Z}[i] \) is Euclidean with respect 
to the norm \( N(a+bi) = a^2 + b^2 \), every element \( \beta \in \mathbb{Z}[i] \) can be written as \( \beta = \alpha q + r \) 
with \( N(r) < N(\alpha) \) or \( r = 0 \). Therefore, every congruence class modulo \( I \) has a 
representative of norm less than \( N(\alpha) \). Note that there are only finitely many 
elements of a given norm in \( \mathbb{Z}[i] \). Therefore, the quotient \( \mathbb{Z}[i]/I \) is finite.

Remark: If you draw the Gaussian integers as the lattice \( \mathbb{Z}^2 \) on the complex 
plane, then \( I \) can be thought of as a sub-lattice. Take a "fundamental parallelo-
gram" for the lattice \( I \) (that is, a parallelogram with one vertex at 0 and such that 
its other vertices are in \( I \), and it does not have any points of \( I \) inside). Then the 
cardinality of the quotient \( \mathbb{Z}[i]/I \) is precisely the number of integral points strictly 
inside this parallelogram. Make some example of \( I \), draw this picture, and think 
about why this claim is true!

2. Prove that in a Principal Ideal Domain two ideals \((a)\) and \((b)\) are comaximal 
if and only if a greatest common divisor of \( a \) and \( b \) is 1 (in which case \( a \) and \( b \) 
are said to be coprime or relatively prime).

Solution: Suppose \( R \) is a Principal Ideal Domain. Two ideals \((a)\) and \((b)\) are 
comaximal in \( R \) if and only if \((a) + (b) = R \) (by definition). Now \((a) + (b) = R \) if 
and only if \((a) + (b) = (1) \) if and only if 1 \( \in (a) + (b) \) if and only if 1 = \( ax + by \) for 
some \( x, y \in R \), if and only if \( \gcd(a, b) = 1 \) as desired.

3. Prove that a quotient of a P.I.D by a prime ideal is again a P.I.D.

Solution: Suppose \( R \) is a Principal Ideal Domain. Assume \( I \) is a prime ideal 
in \( R \). Since \( R \) is a P.I.D, it follows that \( I = (p) \) for some \( p \in R \). If \( p = 0 \), 
then \( R/I = R/(0) \cong R \) which is a P.I.D. Assuming \( p \neq 0 \), we have \( (p) \neq (0) \).

Proposition 7 in page 280 in Dummit & Foote states that every nonzero prime 
ideal in a P.I.D is a maximal ideal. Since \((p)\) is prime, and \((p) \neq (0)\), we know that 
\((p)\) is a maximal ideal. Hence \( R/I = R/(p) \) is a field, and consequently, a P.I.D.

Problem 4.

(a) Draw the picture for the ideal \((2)\) in the ring of Eisenstein integers \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}] \).

Picture will be posted separately.

(b) Describe the quotient \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}]/(2) \) and determine whether \((2)\) is a prime ideal 
in this ring.

Solution. Since Eisenstein integers is a Euclidean ring, exactly as in prob-
lem 1, every element has a remainder of norm less than \( N(2) = 4 \), and therefore, 
the quotient ring cannot have more than 4 elements. Note that the elements 
0, 1, \( \frac{1 + \sqrt{-3}}{2} \), and \( \frac{1 - \sqrt{-3}}{2} = (\frac{1 + \sqrt{-3}}{2})^{-1} \) are pairwise non-congruent modulo \((2)\), 
and therefore they are the four representatives of all equivalence classes. Note 
that all these elements are units, and thus the quotient \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}]/(2) \) is the 
field of 4 elements!

(Compare this with the picture and see why this makes sense).

Since the quotient is a field, \((2)\) is a maximal ideal (and thus it is a prime 
ideal).
(c) Explain why the existence of two factorizations

\[ 4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}) \]

proves that \( \mathbb{Z}[\sqrt{-3}] \) is not a PID, and at the same does not contradict the fact that \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}] \) is a PID.

**Solution.** In \( \mathbb{Z}[\sqrt{-3}] \), the elements 2 and \((1 \pm \sqrt{-3})\) are irreducible: to prove that they are irreducible, look at their norm. Both have Norm 4, and so if they factored, the factors would have had norm 2: since the norm of the factors would have to divide 4, and if an element has norm 1, it is a unit, the only possibility for non-unit factors would be to have norm 2. But there are no elements of norm 2 in this ring (it is not possible to have \( a^2 + 3b^2 = 2 \) for integers \( a, b \)). Thus we have two factorizations of 4 as a product of irreducibles, and note that the elements 2 and \((1 \pm \sqrt{-3})\) are not associate (i.e. one of them is not a unit times another). This proves that \( \mathbb{Z}[\sqrt{-3}] \) is not a UFD, and therefore not a PID.

What happens to the two factorizations if we think of them as elements of \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}] \) instead? Well, now they become associate: \( \frac{1 + \sqrt{-3}}{2} \) is a unit in \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}] \), and thus the factorizations \( 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2 \) are now the same factorization up to units! So there is no contradiction with the fact that \( \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}] \) is a PID.

5. Prove that in \( \mathbb{Z}[-\sqrt{5}] \), the ideal \( (3) \) is the product of two prime ideals \( I_1 = (3, 2 + \sqrt{-5}) \) and \( I_2 = (3, 2 - \sqrt{-5}) \). (You need to include the proof that these ideals are prime; you can do it for just one of them).

**Solution:** We need to show that \((3) \subseteq I_1 I_2 \), and that \( I_1 I_2 \subseteq (3) \).

The first inclusion: Note that \((2 - \sqrt{-5})(2 + \sqrt{-5}) = 9 \), so \( 9 \in I_1 I_2 \). On the other hand, \( 12 = 3 \cdot 2 \), so it is also in \( I_1 I_2 \). Then \( 3 = 12 - 9 \in I_1 I_2 \), hence \((3) \subseteq I_1 I_2 \).

The second inclusion: the ideal \( I_1 \) is generated by two elements: \( 3 \) and \( 2 + \sqrt{-5} \), and similarly \( I_2 \). Then the ideal \( I_1 I_2 \) (which, by definition, consists of finite sums \( \sum_i x_i y_i \) with \( x_i \in I_1, y_i \in I_2 \)), is generated by their pairwise products: \( 3 \cdot 3, 3 \cdot (2 + \sqrt{-5}), (2 + \sqrt{-5}) (2 - \sqrt{-5}) \). To show that \( I_1 I_2 \subseteq (3) \), we just need to show that these four generators are contained in the ideal \((3) \). For the first three of them, it is obvious, and the last one equals 9, so it is also obvious.

Let us show that \( I_1 = (3, 2 + \sqrt{-5}) \) is a prime ideal. For that we need to find the quotient \( R/I_1 \). I claim this quotient is the ring of 3 elements with representatives 0, 1, 2. There are several ways to see it. One idea is to use the equality:

\[ a + b\sqrt{-5} = (a - 2b) + b(2 + \sqrt{-5}), \]

and thus every element \( a + b\sqrt{-5} \) is congruent to \( a - 2b \in \mathbb{Z} \) modulo \( I_1 \). Now we use the other generator of \( I_1 \) (namely, 3), and reduce \( a - 2b \mod 3 \).

Another way to see it: draw a picture (will post it separately).

Yet another way to see it: use Third Isomorphism Theorem and do the quotient in stages: first note that \( R/(3) \) has 9 elements. Indeed, given \( a + b\sqrt{-5} \in R \), reducing the coefficients mod 3, we get \( \overline{a} + \overline{b}\overline{\sqrt{-5}} \in R/(3) \) where \( \overline{a} \) is canonical mod 3 map. Since \( \overline{a} \) and \( \overline{b} \) each has three choices, and so \( R/(3) \) has 9 elements. Next, we claim that \( I_1/(3) \) has three elements. Indeed, it has to be a subgroup with respect to addition, so it can only have order 1, 3, or 9. We proved in class that it is not 1 (we know the ideal \( I_1 \) is not principal – not the same as the ideal \((3)\)), and we also
know this ideal is not the whole ring, so 9 is also impossible. Then it has to have order 3. Thus the quotient \( R/(3)/(I_1/(3)) \) has to have 3 elements; then it has to be a field of 3 elements (the only ring of order \( p \) for \( p \) prime is \( \mathbb{Z}/p\mathbb{Z} \)). (or you can directly see that 0, 1, 2 are not congruent to each other \( \mod I_1 \), so they are the distinct representatives of the congruence classes, and they are invertible \( \mod I_1 \), so we get a field of 3 elements. ) Thus \( I_1 \) is prime (in fact, maximal).