Solutions to Homework 11

Throughout, all variables represent integers unless otherwise specified.

1. Prove that in \( \mathbb{Z}[\sqrt{10}] \), 3 is irreducible but not prime.

   **Solution:** If \( 3 = \alpha \beta \) is a non-trivial factorization of 3, then \( \text{norm}(\alpha) \mid \text{norm}(3) \), which is 9. Since the factorization is non-trivial, we must have \( \text{norm}(\alpha) = 3 \). Thus for \( \alpha = a + b\sqrt{10} \), we get \( a^2 - 10b^2 = 3 \). Since 3 is not a square mod 10, this has no solution and thus 3 is irreducible.

   Also, we have seen that \( 6 = (4+\sqrt{10})(4-\sqrt{10}) \), so \( 3 \mid (4+\sqrt{10})(4-\sqrt{10}) \). However, from Exercise 1 from the last homework set, we know that \( 3 \not\mid (4 + \sqrt{10}) \) and \( 3 \not\mid (4 - \sqrt{10}) \), so 3 is not prime.

2. **TURN IN:** Prove that if \( p \) is a prime element in an integral domain, then \( p \) is irreducible.

3. **TURN IN:** Prove that cancelation holds in an integral domain: if \( ab = ac \) and \( a \neq 0 \), then \( b = c \).

4. Stillwell 7.3.1-7.3.4.

   **Solution:**

   7.3.1: Suppose that \( x \) is odd and \( y^3 = x^2 + 1 \). Then \( y^3 \equiv 2 \pmod{4} \), which has no solutions since 2 is not a cube mod 4. Thus \( x \) must be even.

   7.3.2: If \( \alpha \mid x + i \) and \( \alpha \mid x - i \), then \( \alpha \mid 2i \) by the Two-Out-Of-Three Theorem. Therefore \( \alpha \mid 2 \), also. On the other hand, if \( \alpha \mid x + i \) and \( \alpha \mid 2 \), then \( \alpha \mid 2i \) and so \( \alpha \mid x + i - 2i \). That is, \( \alpha \mid x - i \). Therefore \( x + i \) and \( x - i \) must have the same gcd as \( x + i \) and 2. Also, \( \text{norm}(x + i) = x^2 + 1 \), which is odd by 7.3.1.

   7.3.3: We have \( \gcd(x + i, x - i) = \gcd(x + i, 2) \). If \( \alpha \mid x + i \) and \( \alpha \mid 2 \), then \( \text{norm}(\alpha) \mid x^2 + 1 \) and \( \text{norm}(\alpha) \mid 4 \). But \( x^2 + 1 \) is odd, so we must have \( \text{norm}(\alpha) = 1 \). That is, only units can divide both \( x + i \) and \( x - i \). Therefore 1 is a gcd of \( x + i \) and \( x - i \).

   7.3.4: Now \( y^3 = (x + i)(x - i) \). Each prime factor of \( y \) appears thrice on the left-hand side and therefore must appear thrice on the right-hand side. Since \( x + i \) and \( x - i \) are relatively prime, all three factors of a given prime must appear in \( x + i \) or all three must appear in \( x - i \). Therefore each one is a cube in \( \mathbb{Z}[i] \).