1. In \( \mathbb{Z}_7[x] \) let \( f(x) = 2x^5 + 3x^4 + 4x + 4 \) and \( g(x) = 3x^2 + x + 5 \). Find \( q(x), r(x) \) with \( f(x) = q(x)g(x) + r(x) \) and either \( r(x) = 0 \) or \( r(x) \) having smaller degree than \( g(x) \).
Solution: Here is the division, writing \( xi \) for \( x^i \)

\[
\begin{array}{ccc}
3x & + & 2x & + & 4 \\
3x^2 & + & 1x & + & 5 \\
2x^5 & + & 3x^4 & + & 0x^3 & + & 0x^2 & + & 4x & + & 4 \\
2x^5 & + & 3x^4 & + & 1x^3 \\
6x^3 & + & 0x^2 & + & 4x \\
6x^3 & + & 2x^2 & + & 3x \\
5x^2 & + & x & + & 4 \\
5x^2 & + & 4x & + & 6 \\
4x & + & 5 \\
\end{array}
\]

so \( q(x) = 3x^3 + 2x + 4 \) and \( r(x) = 4x + 5 \). (You may have learned division of polynomials slightly differently, but if you got the same answer you are OK.)

2. (*) What is the remainder when \( x^{1000000} \) is divided by \( x^3 + x + 1 \) in \( \mathbb{Z}_2[x] \). (There is a pattern!)
Solution: One approach is to consider the remainder when \( x^i \) is divided by \( x^3 + x + 1 \). Starting at \( i = 0 \) this goes \( 1, x, x^2, x + 1, x^2 + x, x^2 + x + 1, x^3 + 1 \) and then starts repeating. Each term may be found from the previous term by multiplying by \( x \) and then dividing by \( x^3 + x + 1 \). So \( x^7 \) gives 1 which means, as \( 1000000 = 7(142857) + 1 \), that \( x^{1000000} \) gives the same as \( x^1 \) which is \( x \).

3. Further problems on \( Z[\omega] \), as in assignment 1.

(a) What are the possible values of \( |\alpha|^2, \alpha \in Z[\omega] \), with \( |\alpha|^2 \leq 11 \).
(Notation: For \( \alpha = a + bi \in C \), \( |\alpha| = \sqrt{a^2 + b^2} \), the distance from \( \alpha \) to the origin on the complex plane.)
**Solution:** Eyeballing it is fine, here is an organized approach that would allow computer calculation for much higher values than 11. Looking at the possible positions of \(\alpha = i + j\omega\) we see that the \(y\)-coordinate is \(j\frac{\sqrt{3}}{2}\) and the \(x\) coordinate is \(\frac{j}{2} + j\). The horizontal lines are of two types. When \(j\) is even the \(x\) coordinates range over the integers and when \(j\) is odd the \(x\) coordinates range over the half-integers, that is, \(\pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{5}{2}, \ldots\). That is, with \(j = 2k\) we points \(s + k\sqrt{3}i\) which have \(|\alpha|^2 = s^2 + 3k^2\). For \(j = (2k + 1)\) we have points \((s + \frac{1}{2}) + (k + \frac{1}{2})\sqrt{3}i\) which have \(|\alpha|^2 = [3(2k+1)^2 + (2s+1)^2]/4\). From the symmetry (which can also be seen geometrically) we need only look at \(s, k \geq 0\). Let's consider each \(j\) separately and take \(s = 0, 1, \ldots\) until the value exceeds 11. For \(j = 0\) we get (as values for \(|\alpha|^2\)) \(s^2 = 0, 1, 4, 9\); for \(j = 2, s^2 + 3 = 3, 4, 7\); for \(j = 1, [3 + (2s + 1)^2]/4 = 1, 3, 7\); for \(j = 3, [27 + (2s + 1)^2]/4 = 7\) and for \(j \geq 4\) we always have \(|\alpha|^2 \geq 12\). So the values are 0, 1, 3, 4, 7, 9.

(b) Factor the numbers 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 into irreducibles in \(\mathbb{Z}[\omega]\). Prove that you do indeed have irreducibles. [One aid: If \(\alpha = \beta\gamma\) then \(|\alpha|^2 = |\beta|^2|\gamma|^2\). Also, \(|\alpha|^2 = 1\) exactly for the six units of assignment 1.]

**Solution:** By Unique Factorization the order in which we factor doesn’t matter so we first factor into integer primes and then the question is the factorization of 2, 3, 5, 7, 11 in \(\mathbb{Z}[\omega]\). Let \(p\) be an integer prime and suppose \(p = \beta\gamma\) in \(\mathbb{Z}[\omega]\). Then \(p^2 = |p|^2 = |\beta|^2|\gamma|^2\). For the factorization to be nontrivial [that is, not a unit times something] we must have \(|\beta|^2 = |\gamma|^2 = p\). From the previous problem this rules out \(p = 2, 5, 11\) so these \(p\) are primes in \(\mathbb{Z}[\omega]\). Conversely, where some \(|\alpha|^2 = p\) we have a factorization \(p = \alpha\overline{\alpha}\) in \(\mathbb{Z}[\omega]\). Taking \(\alpha = 2\omega + 1 = i\sqrt{3}\),

\[
3 = |2\omega+1|^2 = (2\omega+1)(2\overline{\omega}+1) = (2\omega+1)(-2\omega-1) = -(2\omega+1)^2
\]

Taking \(\alpha = 2\omega + 3 = i\sqrt{3} + 2\) we have

\[
7 = (2\omega + 3)(2\overline{\omega} + 3) = (2\omega + 3)(-2\omega + 1)
\]

Are these factors of 3, 7 now prime in \(\mathbb{Z}[\omega]\)? Well, if \(|\alpha|^2\) is an integer prime then \(\alpha\) must be a prime in \(\mathbb{Z}[\omega]\) (for \(\alpha = \beta\gamma\) would imply that either \(|\beta|^2 = 1\) or \(|\gamma|^2 = 1\) which would mean they were units. These factors have square absolute values 3, 7 so they are prime. Here is the final list
i. 2 prime  
ii. 3 = (−1)(2ω + 1)^2  
iii. 4 = 2 · 2  
iv. 5 prime  
v. 6 = 2 · 3 = (−1)^2 · (2ω + 1)^2  
vi. 7 = (2ω + 3)(−2ω + 1)  
vii. 8 = 2 · 2 · 2  
viii. 9 = 3 · 3 = (2ω + 1)^4  
ix. 10 = 2 · 5  
x. 11 prime

(c) Find the minimal positive real $x$ with the following property: For any $\beta \in C$ there exists $\alpha = a + b\omega \in Z[\omega]$ with $|\beta - \alpha| \leq x$. (One approach: use the geometry of $Z[\omega]$.)

**Solution:** $Z[\omega]$ splits the plane into equilateral triangles of unit side. The center of such a triangle is at distance $\frac{\sqrt{3}}{3}$ from all three vertices and any other point is closer to one of them so the minimal $x$ is $\frac{\sqrt{3}}{3}$.

(d) Use the above and following the argument for $Z[i]$, prove that $Z[\omega]$ is a Euclidean Ring under $d(\alpha) = |\alpha|^2$.

**Solution:** First, $d(\alpha) = |\alpha|^2$ so it must be positive for $\alpha \neq 0$ and some calculation gives $d(a + b\omega) = a^2 + b^2 - ab$ so it is indeed a positive integer. As $|\alpha\beta| = |\alpha| \cdot |\beta|$ for any complex $\alpha, \beta$, $d(\alpha\beta) = d(\alpha)d(\beta) \geq d(\alpha)$ when $\alpha, \beta \in Z[\omega] - \{0\}$.

Now for the division. Given $\alpha, \beta \in Z[\omega]$ with $\beta \neq 0$ set $\gamma = \alpha / \beta$. From the above problem there is a $q \in Z[\omega]$ with $|q - \gamma| \leq \frac{\sqrt{3}}{3}$. Take this $q$ so that

$$r = \alpha - q\beta = (\alpha - q\beta) - (\alpha - \gamma\beta) = (\gamma - q)\beta$$

so that

$$|r| \leq |\gamma - q||\beta| \leq \frac{\sqrt{3}}{3} \cdot |\beta|$$

and, squaring both sides,

$$d(r) \leq d(\beta)/3 < d(\beta)$$

(a) In the picture of $\mathbb{Z}[\omega]$ (you can use the picture from the solutions to assignment one) mark (with a little circle) those points which are in the ideal (2).

Solution: See picture file

(b) Describe $\mathbb{Z}[\omega]/(2)$ as $\overline{\alpha_1}, \ldots, \overline{\alpha_r}$ for some specific $\alpha_1, \ldots, \alpha_r$. (You have to figure out what $r$ is!)

Solution: Since 2 and $2\omega$ are in (2) from any $a + b\omega$ we can subtract off the “even part” leaving us with $a, b$ being zero or one. So one set of representatives is $\overline{0}, \overline{1}, \overline{\omega}, \overline{\omega + 1}$.

(c) Give the multiplication table for $\mathbb{Z}[\omega]/(2)$. Is it a field? (It is automatically a ring so to be a field every element has to have a multiplicative inverse.)

Solution: If times anything is $\overline{0}$ and $\overline{1}$ is a multiplicative identity. $\overline{\omega} \cdot \overline{\omega} = \overline{\omega^2}$ and $\omega^2 = -1 - \omega$ which reduces to $1 + \omega$. That is, $\omega\overline{\omega} = \overline{1 + \omega}$. As $\omega(1 + \omega) = -1$, $\overline{\omega} \overline{1 + \omega} = \overline{1}$. Finally as $(1 + \omega)^2 = \omega, \overline{1 + \omega} = \overline{\omega}$. All nonzero elements have inverses so, yes, it is a field.

5. Let's call an integral Domain $D$ together with a function $d : D - \{0\} \rightarrow \{0, 1, 2, \ldots\}$ a Banana Domain (not its real name!) if

(a) $d(\alpha) \leq d(\alpha\beta)$ for all nonzero $\alpha, \beta \in D$

(b) If $\alpha, \beta \in D - \{0\}$ and if there does not exist $q \in D$ with $\alpha = q\beta$ then there exist $a, b \in D$ with $a\alpha + b\beta \neq 0$ and (critically!) $d(a\alpha + b\beta) < d(\beta)$.

Prove that a Banana Domain is a P.I.D. . (Hint: Follow the argument that a Euclidean Domain is a P.I.D.)

Solution: Let $I \subset D$ be an ideal. If $I$ has only the element 0 then trivially $I = (0)$ is principle. Otherwise let $\beta \in I$ be an element with minimal $d(\beta)$. As $I$ is closed under taking multiples, $(\beta) \subset I$. Now let $\alpha \in I$. Either there exists $q \in D$ with $\alpha = q\beta$ (we say $\beta$ divides $\alpha$ in this case) or there doesn’t. In the first case $\alpha \in (\beta)$. In the second case we find $a, b \in D$ given by the Banana property and set $\gamma = a\alpha + b\beta$. As $a, b \in I, \gamma \in I$. But $\gamma \neq 0$ (from the property) and this is impossible as $\beta$ was an element of $I$ with minimal $d(\beta)$.