HOMEWORK 3
DUE: 10/3

For reference, consult sections 3.1, 3.2, 4.1 and 4.2 of J&J. Numbered examples/exercises refer to examples/exercises from J&J. For problems which partially or fully appear in J&J, or anywhere else, please do not look at solutions; feel free to look at all other solved problems.

Problem 1. Find all solutions to the following congruences in \( \mathbb{Z} / n \):
   (a) \( 4x \equiv 10 \mod 11 \) (\( n = 11 \)).
   (b) \( 7x \equiv 2 \mod 14 \) (\( n = 14 \)).
   (c) \( 6x \equiv 4 \mod 14 \) (\( n = 14 \)).

Problem 2. Let \( p \) be a prime, \( a, b \in \mathbb{Z} \). Show that \( (a + b)^p \equiv a^p + b^p \mod p \) by using the binomial theorem. (Hint: what is \( \binom{p}{k} \mod p \)?)

Problem 3. For \( k \) a field, we have seen that the ring \( k[t] \) of polynomials in \( t \) with coefficients in \( k \) is a Euclidean domain. A polynomial \( f \) is monic if its leading coefficient is 1. Since \( k[t]^{\times} = k \setminus 0 \), any \( f \in k[t] \) is an associate of a monic one of the same degree just by multiplying by the inverse of the leading coefficient. Note that \( f \in k[t] \) of degree 2 or 3 is not irreducible if and only if it is divisible by a linear factor.
   (a) Find all monic irreducible polynomials of degree 2 in \( (\mathbb{Z}/5)[t] \).
   (b) Find all monic irreducible polynomials of degree 3 in \( (\mathbb{Z}/3)[t] \).
   (c) Prove that \( f = t^2 + 6t - 4 \) and \( g = t^3 + 4t^2 + 8t - 2 \) have no roots in \( \mathbb{Z} \) (for the first don’t use the quadratic formula).

Problem 4. Find all the roots of \( 3x^{25} + x^{19} + 2x^{14} - x^{12} + 1 \)
   (a) in \( \mathbb{Z}/5 \).
   (b) in \( \mathbb{Z}/7 \).

Problem 5. Fermat’s little theorem can also be used as a primality test. Prove that \( n \in \mathbb{N} \) is prime if and only if \( x^{n-1} \equiv 1 \mod n \) for all \( x \in \mathbb{Z} \) with \( x \neq 0 \mod n \).

Problem 6. Recall that a pseudoprime base \( a \) is a composite number \( n \) such that \( a^{n-1} \equiv 1 \mod n \).
   (a) Perform the base 2 test on the number 391.
   (b) Show that if \( n \) is an odd pseudoprime base \( a \), it is also a pseudoprime base \( n - a \).
   (c) Show that if \( n \) is a pseudoprime base \( a \) and \( \gcd(a,n) = 1 \), then it is a pseudoprime base \( c \) for any \( c \) such that \( ac \equiv 1 \mod n \).
   (d) Show that if \( n \) is a pseudoprime base \( a \) and \( b \), then it is a pseudoprime base \( ab \).

Problem 7. For \( a, b, c \in \mathbb{Z} \), \( n \in \mathbb{N} \), let \( d = \gcd(a,b,n) \). Show that \( ax + by \equiv c \mod n \) has solutions if and only if \( d|c \). Prove that there are precisely \( dn \) solutions in \( \mathbb{Z}/n \) if there are solutions.

Problem 8. We can just as easily consider arithmetic mod \( \pi \) for \( \pi \in \mathbb{Z}[i] \) a Gaussian integer. We say \( a \equiv b \mod \pi \) if \( \pi|a - b \) just as for \( \mathbb{Z} \) (and indeed the same works for any Euclidean domain). A congruence class mod \( \pi \) is a set of the form \( [a] = \{ b \in \mathbb{Z}[i] | a \equiv b \mod \pi \} \).

The set of congruence classes mod \( \pi \) is denoted \( \mathbb{Z}[i]/\pi \) and similarly forms a ring.
   (a) Prove that there are exactly \( |\pi|^2 \) congruence classes mod \( \pi \). (Hint: Consider the tessellation of the plane by squares whose vertices are multiples of \( \pi \).)
   (b) Prove that if \( \pi \) is a Gaussian prime then \( \mathbb{Z}[i]/\pi \) is a field.
   (c) Compute representatives for the elements of \( \mathbb{Z}[i]/2, \mathbb{Z}[i]/3, \mathbb{Z}[i]/(2+i) \).
Problem 9. An addition (multiplication) table for a ring \( R \) is a table showing the sums (products) of all possible pairs of elements of \( R \). For example, the addition and multiplication tables of \( \mathbb{Z}/5 \) are:

\[
\begin{array}{ccccc}
+ & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 0 \\
2 & 2 & 3 & 4 & 0 & 1 \\
3 & 3 & 4 & 0 & 1 & 2 \\
4 & 4 & 0 & 1 & 2 & 3 \\
\end{array}
\quad
\begin{array}{ccccc}
\cdot & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 \\
2 & 0 & 2 & 4 & 1 & 3 \\
3 & 0 & 3 & 1 & 4 & 2 \\
4 & 0 & 4 & 3 & 2 & 1 \\
\end{array}
\]

It’s possible for two rings to look the same as far as addition and multiplication are concerned, but have differently named elements. For example, the addition and multiplication tables of \( \mathbb{Z}/5 \) and \( \mathbb{Z}/9 \) are isomorphic. For example, the addition and multiplication tables of \( Z[i]/(2 + i) \) are

\[
\begin{array}{ccccc}
+ & 0 & 1 & 2 & i & 1+i \\
0 & 0 & 1 & 2 & i & 1+i \\
1 & 1 & 2 & i & 1+i & 0 \\
2 & 2 & i & 1+i & 0 & 1 \\
i & i & 1+i & 0 & 1 & 2 \\
1+i & 1+i & 0 & 1 & 2 & i \\
\end{array}
\quad
\begin{array}{ccccc}
\cdot & 0 & 1 & 2 & i & 1+i \\
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & i & 1+i \\
2 & 0 & 2 & 1+i & 1 & i \\
i & 0 & i & 1 & 1+i & 2 \\
1+i & 0 & 1+i & i & 2 & 1 \\
\end{array}
\]

which are clearly the same as those of \( \mathbb{Z}/5 \). In this case we say \( \mathbb{Z}/5 \) and \( \mathbb{Z}[i]/(2 + i) \) are isomorphic.

(a) Compute the multiplication table of \( \mathbb{Z}/4 \) and \( \mathbb{Z}/9 \).

(b) Find representatives for each congruence class mod 2 of \( \mathbb{Z}[i] \). (Use the fact that there are \( |x|^2 \) distinct congruence classes.)

(c) Compute the multiplication table of \( \mathbb{Z}/2 \).

(d) Find representatives for each congruence class mod 3 of \( \mathbb{Z}[i] \).

(e) Compute the multiplication table of \( \mathbb{Z}/3 \).

(f) Show that the multiplication tables of \( \mathbb{Z}/4 \) and \( \mathbb{Z}[i]/2 \) are the same after rearranging the elements (in fact, \( \mathbb{Z}[i]/2 \) and \( \mathbb{Z}/4 \) are still not isomorphic because they’re addition tables are different); show that \( \mathbb{Z}/9 \) and \( \mathbb{Z}[i]/3 \) are not.