HW 2

Problem 1.

(a) \[ 4x \equiv 10 \mod 11 \]
Since \( \gcd(4, 11) = 1 \) there exists a solution and it’s unique. We reduce as follows
\[ 12x \equiv 30 \mod 11, \quad 12 \equiv 1 \]
\[ x \equiv 8 \mod 11. \]
So \( x = [8] \) is the unique solution.

(b) Since \( \gcd(7, 14) = 7 \), and 7 does not divide 2, there are no solutions.

(c) \( \gcd(6, 14) = 2 \) so there are two solutions. To find one, let’s reduce to find
\[ 6x \equiv 4 \mod 14, \quad 3x \equiv 2 \mod 7 \]
\[ 6x \equiv 4 \mod 7, \quad -x \equiv 4 \mod 7 \]
\[ x \equiv 3 \mod 7. \]
So one solution is 3 and another is \( 3 + 14/2 = 10 \).

Problem 2. The binomial theorem gives
\[ (a + b)^p = \sum_{i=0}^{p} a^i b^{p-i}. \]
For \( 1 \leq i \leq p - 1 \), each binomial coefficient is of the form
\[ \binom{p}{i} = \frac{p!}{(p-i)!i!} = \frac{(p-1)! \cdots 1}{1 \cdots i}. \]
We know each binomial coefficient is an integer, so the last fraction in the above equation is a number: the denominator cannot divide \( p \), so it must divide the numerator. Hence
\[ \binom{p}{i}a^i b^{p-i} \equiv 0 \mod p \]
for \( i = 1, \ldots, p - 1 \) and the result follows.

Problem 3. Books tend to have perfectly written up solutions. But sometimes it’s nice to see the route to the solution. So I’d like to show you how I approached this problem. I started by building my intuition about the problem, and slowly discovered the facts. This led to a first (ugly) solution by enumeration. As I understood the problem better, I found a more refined approach. I’ll present both.
If \( \deg(f) = 2, 3 \) and it’s not irreducible, then we can write
\[ f = ab \]
where \( a \) and \( b \) are both not units. Then, \( \sigma(ab) > \sigma(a) \) which means that \( \deg(a) = 1 \). So we have at least one linear factor when \( \deg(f) = 2 \) or 3.
(a) Fix \( \deg(f) = 2 \). Any monic quadratic can be written as

\[
f = t^2 + at + b
\]

and since there are 5 possibilities each for \( a \) and \( b \), there are 25 in total. If \( f \) is not irreducible, we can write it as

\[
f = (t - d)(t - c),
\]

for each pair \((d, c)\). Linear factors are always prime, and since \( \mathbb{Z}_5 \) is a Euclidean domain, each pair gives a different polynomial \( f \in \mathbb{Z}_5[t] \). In other words, each \( f \) has a unique prime factorization; \( t - d \equiv t - c \) iff \( d = c \). There are \( 5 \times (5+1)/2 = 15 \) such distinct pairs. It follows that the number of irreducibles in \( \mathbb{Z}_5[t] \) is 10. The ugly way of doing this is now to list all possible polynomials that result from \((t - a)(t - b)\).

The irreducibles are the ones that are not in this form.

Another way of viewing this is as follows. If \( f \) is not irreducible, it can be written as a product of linear factors. So at least one element of \( \mathbb{Z}_5 \) is a root! Therefore, \( f \) is irreducible iff it has a root in \( \mathbb{Z}_5 \). So let us discover the restrictions this imposes on the coefficients \( a \) and \( b \) of

\[
f = t^2 + at + b.
\]

Let \( \mathbb{Z}_5 = \{0, 1, -1, 2, -2\} \). Plugging each value into the equation, we get the following conditions:

\[
\begin{align*}
b &\not\equiv 0, & 1 + a + b &\not\equiv 0, & 1 + b &\not\equiv 0 \\
-1 + 2a + b &\not\equiv 0, & -1 + 2a + b &\not\equiv 0.
\end{align*}
\]

Now we can enumerate the cases. For \( b = 1 \), we get \( a \not\equiv 0, \pm 2 \). The remaining cases can be calculated similarly. In particular, note that

\[
t^2 + t - 1
\]

is irreducible.

(b) Let \( f = t^3 + at^2 + bt + c \) be a monic cubic in \( \mathbb{Z}_5[t] \). As before, the irreducible cubics have no roots in \( \mathbb{Z}_5 \). For \( t = 0 \), we get the condition \( c \not\equiv 0 \). Assuming \( t \not\equiv 0 \), we can use Fermat’s theorem and its corollary (from J&J) to get

\[
t^3 + at^2 + bt + c \equiv (b + 1)t + (a + c).
\]

If \( b + 1 \equiv 0 \), we must have \( c + a \not\equiv 0 \). If \( b + 1 \not\equiv 0 \), then \( \gcd(b + 1, 3) = 1 \) which means that we can always solve \((b + 1)t + (a + c) \equiv 0 \) in \( \mathbb{Z}_3 \) for all values of \( c + a \). Summarizing, we have the conditions

\[
\begin{align*}
b + 1 &\equiv 0 & c &\not\equiv 0 & c + a &\not\equiv 0,
\end{align*}
\]

which gives us six irreducibles. In particular,

\[
t^3 + t^2 - t + 1
\]

is irreducible.

(c) If a polynomial \( f \) has roots in \( \mathbb{Z} \), it must have roots in \( \mathbb{Z}_n \) for any \( n \). If \( f(t) \) has a root \( a \) in \( \mathbb{Z}_n \), it must have be divisible by \( t - a \). This is easy to see via the Euclidean property: \( z \)

\[
f(t) = g(t - a) + r
\]
Since \( \deg(r) < \deg(t - a) \), \( r \) must be a constant. In fact, substituting \( t = a \), we get that \( r \equiv 0 \). So if we show that \( f \) is irreducible in some \( \mathbb{Z}_p[t] \), then it must mean that \( f \) has no roots in \( \mathbb{Z} \).

We’ve shown that

\[
t^3 + 4t^2 + 8t - 2 \equiv t^3 + t^2 - t + 1 \mod 3
\]

is irreducible in \( \mathbb{Z}_3[t] \), and that

\[
t^2 + 6t - 4 \equiv t^2 + t + 1 \mod 5
\]

is irreducible in \( \mathbb{Z}_5[t] \).

**Problem 4.**

(a,b) This is easy using Fermat’s theorem. Treat the case where \( x \equiv 0 \) separately.

I got the polynomials

\[
f \equiv x^3 + 2x^2 + 3x \mod 5,
\]

\[
f \equiv x^2 + 4x \mod 7.
\]

from which it is easy to deduce that \( \mod 5 \) we have no solutions and we have one solution \( \mod 7 \).

**Problem 5.** We’re asked to prove that \( x^{n-1} \equiv 1 \mod n \) \((x \neq 0)\) iff \( n \) is prime. If \( n \) is prime, this is just Fermat’s theorem. Suppose \( n \) is composite, let \( n = p_1 \cdots p_k \) be its prime decomposition with \( k \geq 2 \). We just have to demonstrate one \( x \) for which \( x^{n-1} \neq 1 \mod n \). Choose \( x = p_1 \). Suppose \( n|p_1^{n-1} - 1 \), then every prime factor of \( n \) must divide it. In particular, \( p_1 \) divides both \( p_1^{n-1} - 1 \) and \( p_1^{n-1} \) which implies that \( p_1|1 \) which is a contradiction. We only have to check that \( p_1 \neq 0 \), which is trivial.

**Problem 6.**

(a) This was quite annoying since I didn’t bother reading the textbook, and got by with a little help from my Mathematica.

\[
2^{390} \equiv (2^{13})^{30} \equiv 19^{30} \equiv (19^7)^419^2 \equiv 8^4(-30) \equiv 8319^28
\]

\[
\equiv 121(-30)8 \equiv 3638(-10) \equiv (-28)8(-10) \equiv 575 = 285.
\]

So it fails the base 2 test.

(b) We need to show that \( a^{n-1} \equiv 1 \mod n \) implies \( (n - a)^{n-1} \equiv 1 \). The binomial theorem gives

\[
(n - a)^{n-1} = \sum_{i=0}^{n-2} n^{n-1-i}(-1)^i + (-a)^{n-1}.
\]

The terms in the sum are clearly divisible by \( n \), and since \( n \) is odd, \( (-a)^{n-1} \equiv 1 \).

This gives that \( (n - a)^{n-1} \equiv 1 \).

(c) Since \( n \) is PP base \( a \), we have

\[
a^{n-1} \equiv 1 \mod n.
\]

We also have \((ac)^{n-1} \equiv 1 \) which implies \( e^{n-1} \equiv 1 \) and hence it’s a pseudoprime base \( c \).

(d) If \( n \) is PP base \( a \) and base \( b \). Then \( a^{n-1}, b^{n-1} \equiv 1 \Rightarrow (ab)^{n-1} \equiv 1 \).
Problem 7.

(a) It’s easy to do this problem if you draw a picture. Tesselate the plane with squares of side length $\pi$. The “fundamental” square $S$ is made up of vertices $(0,0), (\pi,0),(0,i\pi),$ and $(\pi,i\pi)$. To be more precise, let

$$S := \{(a + ib) \mid 0 \leq a < \pi, 0 \leq b < \pi \}$$

We can always translate any Gaussian integer $a$ by a multiple of $\pi$ so that it is inside $S$; this is just the Euclidean property. Distinct Gaussian integers inside $S$ are distinct mod $\mathbb{Z}[i]/\pi$. Let $r_1, r_2 \in S$ be distinct, and let $r_1 - r_2 = q\pi$. We must have $|q|^2 \geq 2$, since $q$ is not a unit. But the diagonal of $S$ has length strictly less that $2|\pi|^2$, by our construction. Hence $r_1$ and $r_2$ are in different congruence classes.

On the $x$ axis, the points $(0,0), \ldots, (\lfloor \pi \rfloor - 1, 0)$ are all in $S$; a similar statement applies to the $y$ axis. Hence, it’s clear that there are exactly $|\pi|^2$ Gaussian integers inside $S$.

(b) Here we have to show that every nonzero element of $\mathbb{Z}[i]/\pi$ has an inverse. That is,

$$bx \equiv 1 \mod \pi$$

has a solution $x$ for every $b \in \mathbb{Z}[i]/\pi$. Let $\mathbb{Z}[i]/\pi := \{0, a_1, \ldots, a_{p-1}\}$, where $|\pi|^2 =: p$. If

$$ba_i \equiv ba_j,$$

it must mean that $p|(a_i - a_j)$ since $b$ is coprime to $p$. So it’s clear that the elements \{ba_1, \ldots, ba_{p-1}\} belong to distinct congruence classes. There are $p-1$ of these and none of these are 0, so at least one $ba_j$ must be 1.

(c) This is elementary, and the procedure for picking representatives follows from part (a).

Problem 8. Since this problem is purely computational, I’m going to use Mathematica to do it. I’ll attach a notebook. You can use the cims computers to run the code, and I think that NYU has a university wide license.