Solutions to Midterm Exam 1

Math 401

October 7, 2014

It is possible to do well even if you didn’t finish.

1. **(20 points)** Show by induction on \( n \) that

\[
1^4 + 2^4 + \cdots + n^4 = \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}.
\]

**Solution:** For \( n = 1 \) the claim is that \( \frac{1}{5} + \frac{1}{2} + \frac{1}{3} - \frac{1}{30} = 1 \), which is true. Suppose the claim holds for \( n \); then we have

\[
\begin{align*}
\frac{(n + 1)^5}{5} &+ \frac{(n + 1)^4}{2} + \frac{(n + 1)^3}{3} - \frac{n + 1}{30} \\
&= \frac{n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1}{5} \\
&+ \frac{n^4 + 4n^3 + 6n^2 + 4n + 1}{2} + \frac{n^3 + 3n^2 + 3n + 1}{3} - \frac{n + 1}{30} \\
&= \frac{1}{5} n^5 + \left( 1 + \frac{1}{2} \right) n^4 + \left( 4 + \frac{1}{3} \right) n^3 + 6n^2 + \left( 4 - \frac{1}{30} \right) n^2 + 1 \\
&= \left( \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30} \right) + (n^4 + 4n^3 + 6n^2 + 4n + 1) \\
&= (1^4 + 2^4 + \cdots + n^4) + (n + 1)^4,
\end{align*}
\]
so the claim holds for \( n+1 \). Alternatively, you might prefer to assume the claim for \( n-1 \) and prove it for \( n \):

\[
1^4 + 2^4 + \cdots + (n-1)^4 + n^4
= \left( \frac{(n-1)^5}{5} + \frac{(n-1)^4}{2} + \frac{(n-1)^3}{3} - \frac{n-1}{30} \right) + n^4
= \left( \frac{n^5 - 5n^4 + 10n^3 - 10n^2 + 5n - 1}{5} \right.
+ \frac{n^4 - 4n^3 + 6n^2 - 4n + 1}{2} + \frac{n^3 - 3n^2 + 3n - 1}{3} - \frac{n - 1}{30} \left. \right) + n^4
= \left( \frac{n^5}{5} - \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30} \right) + n^4
= \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}.
\]

2. (10 points)

(a) Solve this system of congruences:

\[
x \equiv 1 \pmod{2} \quad x \equiv 2 \pmod{3} \quad x \equiv 3 \pmod{5}
\]

**Solution:** Rewriting the first two as \( x \equiv -1 \pmod{2} \) and \( x \equiv -1 \pmod{3} \) we see that they are equivalent to \( x \equiv -1 \pmod{6} \). Now writing \( 1 = 6 - 5 \) we see that \( 6 \cdot 3 - 5 \cdot (-1) = 23 \) is a solution to all three, so

\[
x \equiv 23 \pmod{30}
\]

is the general solution.

(b) Which of these can be solved? Solve it.

(i) \( x \equiv 5 \pmod{6} \) and \( x \equiv 1 \pmod{9} \).

(ii) \( x \equiv 5 \pmod{6} \) and \( x \equiv 2 \pmod{9} \).

(iii) \( x \equiv 5 \pmod{6} \) and \( x \equiv 3 \pmod{9} \).

**Solution:** Observe that \( \gcd(6,9) = 3 \), and that \( x \equiv 5 \pmod{6} \) implies \( x \equiv 2 \pmod{3} \). Now \( x \equiv 1 \pmod{9} \) implies \( x \equiv 1 \pmod{3} \), so (i) is impossible. Similarly, \( x \equiv 3 \pmod{9} \) implies \( x \equiv 0 \pmod{3} \), so (iii) is impossible. But (ii) can be solved, and the solution is

\[
x \equiv 11 \pmod{18}.
\]
3. (40 points) Let \( \omega = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2} \) be the usual primitive cube root of unity. Recall that \( \omega^2 = \omega^{-1} = \bar{\omega} \). This problem is about my favorite ring, the Eisenstein integers:

\[ \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\} \]

(a) Roughly plot \( a + b\omega \) on the complex plane for \(-2 \leq a, b \leq 2\).

Solution:

(b) Show that \( \bar{\omega} \in \mathbb{Z}[\omega] \). Deduce that if \( z \in \mathbb{Z}[\omega] \) then \( \bar{z} \in \mathbb{Z}[\omega] \). Label 1, \( \omega \), and \( \bar{\omega} \) on your answer to part (a).

Solution: We have \( \bar{\omega} = \frac{-1 - \sqrt{3}i}{2} = -\omega - 1 \). Thus if \( z = a + b\omega \) then

\[ \bar{z} = a + b\bar{\omega} = a + b(-\omega - 1) = (a - b) - b\omega \in \mathbb{Z}[\omega]. \]

(c) Show that if \( z \in \mathbb{Z}[\omega] \) then \( |z|^2 \) is a positive\(^*\) integer.

Solution: We know that \( |z|^2 \) is positive\(^*\) for any \( z \in \mathbb{C} \), so we need only show that it is an integer for \( z \in \mathbb{Z}[\omega] \). If \( z = a + b\omega \) then

\[ |z|^2 = z\bar{z} = (a + b\omega)(a + b\bar{\omega}) = a^2 + ab(\omega + \bar{\omega}) + b^2\omega\bar{\omega} = a^2 - ab + b^2, \]

which is an integer because \( a \) and \( b \) are integers.

(d) Show that an element \( z \in \mathbb{Z}[\omega] \) is a unit if and only if \( |z|^2 = 1 \).

Solution: First suppose that \( z \in \mathbb{Z}[\omega] \) is a unit. Then there is a \( z' \in \mathbb{Z}[\omega] \) such that \( zz' = 1 \). Taking \( |\cdot|^2 \) on both sides we get \( |z|^2|z'|^2 = 1 \); but \( |z|^2 \) and \( |z'|^2 \) are positive integers, so \( |z|^2 = |z'|^2 = 1 \).

Conversely, suppose that \( |z|^2 = 1 \). Then \( z\bar{z} = 1 \), and we have seen that \( \bar{z} \in \mathbb{Z}[\omega] \), so \( z \) is a unit.

\(^*\)Correction 10/15/14: This should have been “non-negative.”
(e) List all the units in $\mathbb{Z}[\omega]$. (Hint: Refer to your answer to part (a). There are finitely many.)

**Solution:** They are the six points lying on the unit circle, namely $\pm 1$, $\pm \omega$, and $\pm \bar{\omega} = \mp 1 \mp \omega$. (In contrast, the ring $\mathbb{Z}[\sqrt{3}]$ has infinitely many units: $\pm (2 + \sqrt{3})^n$ for any $n \in \mathbb{Z}$.)

(f) Are there any zero-divisors in $\mathbb{Z}[\omega]$?

**Solution:** No, because there are no zero-divisors in $\mathbb{C}$.

(g) Show that $z = 3 + 2\omega$ is not a unit, and if it can be factored as $z_1 z_2$ for some $z_1, z_2 \in \mathbb{Z}[\omega]$ then one of $z_1, z_2$ is a unit. Such an element is called *irreducible*.

**Solution:** We have $|z|^2 = 3^2 - 3 \cdot 2 + 2^2 = 7$, so $z$ is not a unit. If $z = z_1 z_2$ then $|z|^2 = |z_1|^2 |z_2|^2$. Since $|z|^2 = 7$ is prime, we either have $|z_1|^2 = 1$ and $|z_2|^2 = 7$, so $z_1$ is a unit, or $|z_1|^2 = 7$ and $|z_2|^2 = 1$, so $z_2$ is a unit. (It is interesting to note that while 7 is prime in $\mathbb{Z}$, it factors as $z \bar{z} = (3 + 2\omega)(1 - 2\omega)$ in $\mathbb{Z}[\omega]$.)

4. (15 points) This problem is about Cardano’s formula for the roots of the cubic polynomial $x^3 + px + q$, $p \neq 0$.

Let 

$$A = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad B = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

be the roots of the quadratic polynomial

$$y^2 + qy - \frac{p^3}{27}.$$

(a) Find $AB$.

**Solution:** Since $A$ and $B$ are the roots of the quadratic above, $AB$ equals its constant term $-\frac{p^3}{27}$.

(b) Show that for every $v$ with $v^3 = A$ there is a $w$ with $w^3 = B$ such that

$$w - \frac{p}{3w} = v - \frac{p}{3v}.$$  

(Hint: $B = \frac{AB}{A}$.)

**Solution:** We want

$$w^3 = B = \frac{AB}{A} = \frac{-p^3/27}{v^3} = \left(-\frac{p}{3v}\right)^3,$$

so we take $w = -\frac{p}{3v}$. This implies that $v = -\frac{p}{3w}$, so

$$w - \frac{p}{3w} = -\frac{p}{3v} + v$$

as desired.
(The point was to show that either square root of $\frac{q^2}{4} + \frac{p^3}{27}$ suffices to give all three roots of $x^3 + px + q$.)

5. (15 points)

(a) Show that $f = x^2 + x - 1$ and $g = x^3 + x^2 - 1$ are irreducible in $\mathbb{Z}_3[x]$.

**Solution:** Since $f$ is quadratic and $g$ is a cubic, it is enough to show that they don’t have any roots in $\mathbb{Z}_3$:

$$
\begin{array}{c|c|c}
    x & f(x) & g(x) \\
    \hline
    0 & -1 & -1 \\
    1 & 1 & 1 \\
    -1 & -1 & -1 \\
\end{array}
$$

Note that $x^3 \equiv x \pmod{3}$ by Fermat’s little theorem, which explains why $f$ and $g$ take the same values.

(b) Find $a, b \in \mathbb{Z}_3[x]$ such that $af + bg = 1$.

**Solution:** Divide $g$ by $f$ to get a quotient $x$ and a remainder $x - 1$, so

$$g = xf + (x - 1).$$

Divide $f$ by $x - 1$ to get a quotient $x - 1$ and a remainder 1, so

$$f = (x - 1)(x - 1) + 1.$$ 

Rewrite the first as

$$(x - 1) = g - xf$$

and the second as

$$1 = f - (x - 1)(x - 1)$$

$$= f - (x - 1)(g - xf)$$

$$= (x^2 - x + 1)f - (x - 1)g,$$

so we can take $a = x^2 - x + 1$ and $b = -x + 1$. There are many other solutions, so yours may be different, but this is the simplest.