

SOLUTIONS TO HOMEWORK 3
Math 104B - Dr. Evans
UCSD Spring 2004

1. Problem 26 from the book: *Prove Lemma 2.1.3:*

Lemma 2.1.3 For all x and $y \in \mathbb{Q}$, we have

- i. $v_p(xy) = v_p(x) + v_p(y)$
- ii. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

First suppose that x and y are integers. Let $x = p^m x'$ and $y = p^n y'$ where $p \nmid x'$ and $p \nmid y'$. Then

$$xy = (p^m x')(p^n y') = p^{m+n}(x'y')$$

Since $p \nmid x'y'$, $v_p(xy) = m + n = v_p(x) + v_p(y)$.

Now suppose $x = \frac{a}{b}$ and $y = \frac{c}{d}$. Then

$$v_p(xy) = v_p\left(\frac{ac}{bd}\right) = v_p(ac) - v_p(bd) = (v_p(a) - v_p(b)) + (v_p(c) - v_p(d)) = v_p(x) + v_p(y)$$

since $v_p(ac) = v_p(a) + v_p(c)$ and $v_p(bd) = v_p(b) + v_p(d)$ by the integer case.

2. Problem 27 from the book: *Let $k = \mathbb{Q}$, $p = 7$, and let $|\cdot| = |\cdot|_7$ be the 7-adic absolute value. Compute $|35|$, $|56/12|$, $|177553|$, and $|3/686|$.*

$$\begin{aligned} |35| &= |5 \cdot 7| = \frac{1}{7} \\ \left|\frac{56}{12}\right| &= \left|7 \cdot \frac{2}{3}\right| = \frac{1}{7} \\ |177553| &= 1 \text{ since } 177553 \text{ is a prime} \\ \left|\frac{3}{686}\right| &= \left|\frac{1}{7^3} \cdot \frac{3}{2}\right| = 7^3 = 343 \end{aligned}$$

3. Problem 39 from the book: *Let $k = \mathbb{Q}(i)$ be the field obtained by adjoining $i = \sqrt{-1}$ to the rational numbers, so that any element of k can be written as $a + bi$ with $a, b \in \mathbb{Q}$. The "integers" in k are the elements $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. It is not too hard to check that this is a unique factorization domain, so that its properties are much like the usual integers. The primes of $\mathbb{Z}[i]$ are of three kinds:*

- i. $1 + i$ is prime,
- ii. if $p \in \mathbb{Z}$ is a prime number and $p \equiv 3 \pmod{4}$, then p is a prime in $\mathbb{Z}[i]$,
- iii. for each prime $p \in \mathbb{Z}$ which is congruent to 1 modulo 4, there are two primes $x + yi$ and $x - yi$ in $\mathbb{Z}[i]$ satisfying $(x + yi)(x - yi) = x^2 + y^2 = p$.

In each case, we can use the prime $\pi \in \mathbb{Z}[i]$ to construct a π -adic valuation v_π and (from it) a π -adic absolute value $|\cdot|_\pi$ on k as before:

$$|\alpha|_\pi = c^{-v_\pi(\alpha)}.$$

Check that this works, and explore the resulting situation. For example, since \mathbb{Q} is contained in k , this induces an absolute value on \mathbb{Q} ; describe the induced absolute value. In particular, for a fixed π , can you compute $v_\pi(p)$ as p ranges through the primes of \mathbb{Z} ? (Hint: $\pi = 1 + i$ may be a little different.)

The fact that $|\alpha|_\pi = c^{-v_\pi(\alpha)}$ works as an absolute value follows immediately from unique factorization. This would not work in $\mathbb{Z}[\sqrt{-5}]$, for example. ($2^2 \cdot 3 = 12 = 2(1 + \sqrt{-5})(1 - \sqrt{-5})$; what would $|12|_2$ be?)

To explore the situation, let's compute a few absolute values. Let $\pi = 2 + i$ and $\alpha = 5$. Note that $5 = (2 + i)(2 - i)$ and that $2 + i$ does not divide $2 - i$ in $\mathbb{Z}[i]$. (Suppose it did. Then $(2 - i) = (2 + i)(c + di)$ for some $c, d \in \mathbb{Z}$. Multiplying by conjugates on all sides results in $5 = 5(c^2 + d^2) \implies c + di = \pm 1, \pm i$. Checking these four cases shows that this is not the case.) Hence, $v_\pi(5) = 1$ and $|5|_\pi = c^{-1}$.

Now let $\pi = 1 + i$ and $\alpha = 2$. Once again, $2 = (1 + i)(1 - i)$. This time, however, $1 + i$ does divide $1 - i$ in $\mathbb{Z}[i]$: $1 - i = -i(1 + i)$. So $2 = -i(1 + i)^2$, $v_\pi(2) = 2$, and $|2|_\pi = c^{-2}$.

These two examples allows us to calculate $v_\pi(p)$ as p ranges through the primes of \mathbb{Z} . Suppose for some fixed prime $\pi = a + bi$ in $\mathbb{Z}[i]$, π divides the integer prime p . Then $p = (a + bi)(c + di)$ for some $c + di \in \mathbb{Z}[i]$. Multiplying by conjugates on both sides results in $p^2 = (a^2 + b^2)(c^2 + d^2)$, and so $a^2 + b^2$ is either 1, p , or p^2 . $a^2 + b^2$ cannot be 1, otherwise $a + bi = \pm 1, \pm i$ which is not a prime (it's a unit). So we have shown that $a + bi$ must divide exactly one integer prime p .

We now go through the three kinds of primes in $\mathbb{Z}[i]$. In case (i.) when $\pi = 1 + i$, we have already shown that $v_\pi(2) = 2$. From the previous paragraph, π does not divide any other prime p besides 2, so $v_\pi(p) = 0$ for all $p \neq 2$. In case (ii.) when $\pi = p$, then $v_\pi(p) = 1$ and $v_\pi(q) = 0$ for all primes $q \neq p$. In case (iii.) when $\pi = a + bi$ and $a^2 + b^2 = p$, one can show that $a + bi$ and $a - bi$ are distinct primes in $\mathbb{Z}[i]$. (If $a - bi = (a + bi)(c + di)$, then $c + di = \pm 1, \pm i$ just as before. However, $a - bi \neq \pm(a + bi)$ and $a - bi \neq \pm i(a + bi)$ since $a \neq b$ unless $a = b = 1$.) Hence, $p = (a + bi)(a - bi)$ is the unique factorization of p in $\mathbb{Z}[i]$, and $v_\pi(p) = 1$. For any prime $q \neq p$, $v_\pi(q) = 0$.

4. Let $p = 5$. Using the technique shown in class, find the p -adic expansion of $-\frac{2}{4}$ and $-\frac{3}{6}$ without reducing the fractions first. You should get two different expansions; show that they are actually the same.

Since $5^1 \equiv 1 \pmod{4}$,

$$-\frac{2}{4} = \frac{2 \left(\frac{5^1 - 1}{4} \right)}{1 - 5} = \frac{2}{1 - p} = 2(1 + p + p^2 + p^3 + \dots) = 2 + 2p + 2p^2 + 2p^3 + \dots$$

Since $5^2 \equiv 1 \pmod{6}$,

$$-\frac{3}{6} = \frac{3 \left(\frac{5^2 - 1}{6} \right)}{1 - 5^2} = \frac{12}{1 - p^2} = (2 + 2p)(1 + p^2 + p^4 + \dots) = (2 + 2p) + (2 + 2p)p^2 + \dots$$

5. Let $a = 1$, $b = 15$, $c = 50$.

(a) Find the distances between each pair of these three points using the 7-adic absolute value $|\cdot|_7$. Notice that two of three distances are the same, so that a , b , and c form an “isosceles triangle.”

The distance between a and b is $|b - a|_7 = |14|_7 = \frac{1}{7}$. The distance between a and c is $|c - a|_7 = |49|_7 = \frac{1}{49}$. The distance between b and c is $|c - b|_7 = |35|_7 = \frac{1}{7}$. The first and last distances are equal, so the triangle is isosceles.

(b) Since $|a|_7 = |b|_7 = |c|_7 = 1$, a , b , and c lie on the “unit circle” $\{x \in \mathbb{Q}_7 \mid |x|_7 = 1\}$. Show that 7 and $\frac{98}{15}$ are both “inside” the unit circle, i.e., their absolute value is less than 1. Show that 7 and $\frac{98}{15}$ both have distance 1 from a , b , and c . These are examples of the statement “every point inside the circle is the center of the circle.”

$|7|_7 = \frac{1}{7} < 1$ and $|\frac{98}{15}|_7 = \frac{1}{49} < 1$, so both 7 and $\frac{98}{15}$ are inside the unit circle. Now we calculate the distances between the points $\{7, \frac{98}{15}\}$ and the points $\{a, b, c\}$:

$$\begin{aligned} |a - 7|_7 &= |-6|_7 = 1 \\ |b - 7|_7 &= |8|_7 = 1 \\ |c - 7|_7 &= |43|_7 = 1 \\ \left|a - \frac{98}{15}\right|_7 &= \left|-\frac{83}{15}\right|_7 = 1 \\ \left|b - \frac{98}{15}\right|_7 &= \left|\frac{127}{15}\right|_7 = 1 \\ \left|c - \frac{98}{15}\right|_7 &= \left|\frac{652}{15}\right|_7 = 1 \end{aligned}$$

These all follow from the fact that 6, 8, 43, 83, 127, 652, and 15 are not divisible by 7. Therefore, 7 and $\frac{98}{15}$ both are distance one from the three points $\{a, b, c\}$ on the unit circle.