18.781, Fall 2007 Problem Set 7

Solutions to Selected Problems

Problem 1 First, observe that $N(13) = 13^2 - 13 \cdot 0 + 0^2 = 169 = 13^2$. If $ab = 13$ for some nonunit $a, b \in R$, then $N(a)N(b) = 13^2$ and $N(a) = N(b) = 13$ since 13 is a prime number in $\mathbb{Z}$ and $N(a), N(b) > 1$.

For any $a = r + s\omega$, we have $N(a) = (r - s)^2 + rs$. By some computations, we can find the set of (r, s) which gives $N(a) = 13$. (Actually, they are $(4, 1), (-4, -1), (4, 3), (-4, -3)$). And we can easily find that

$$13 = (3 + 4\omega)(-1 - 4\omega).$$

Each element of left hand side is clearly non-unit in R since the value by N is not 1. $\square$

Problem 2 For any element $a = s + ti$ in $\mathbb{Z}[i]$, define the function λ by$\lambda(a) = s^2 + t^2$. Since $s + ti = 0$ if and only if both s and t are 0, we see that $\lambda(s + ti) \geq 1$ when $s + ti \equiv 0$. It is easy to find that $\lambda(ab) = \lambda(a)\lambda(b)$ for $a, b \in \mathbb{Z}[i]$. Then when $b \neq 0$ we have

$$\lambda(a) = \lambda(a) \cdot 1 \leq \lambda(a)\lambda(b) = \lambda(ab).$$

If $b \neq 0$, it is also easy to verify that $\frac{a}{b}$ is a complex number that can be written in the form $c + di$, where $c, d \in \mathbb{Q}$. Since $c \in \mathbb{Q}$, it lies between two consecutive integers; and similarly for d. Hence,there are integers m and n such that $\mid m - c \mid \leq \frac{1}{2}$ and $\mid n - d \mid \leq \frac{1}{2}$. Since $\frac{a}{b} = c + di$.

$$\begin{aligned} a &= b[c + di] = b[(c - m + m) + (d - n + n)i] \\ &= b[(m + ni) + ((c - m) + (d - n)i)] \\ &= b[m + ni] + b[(c - m) + (d - n)i] \\ &= bq + r, \end{aligned}$$

where $q = m + ni \in \mathbb{Z}[i]$ and $r = b[(c - m) + (d - n)i]$. Since $r = a - bq$ and $a, b, q \in \mathbb{Z}[i]$, we see that $r \in \mathbb{Z}[i]$. Therefore,

$$\begin{aligned} \lambda(r) &= \lambda(b)\lambda[(c - m) + (d - n)i] = \lambda(b)[(c - m)^2 + (d - n)^2] \\ &\leq \lambda(b) \left[\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \right] = \left(\frac{1}{2}\right) \cdot \lambda(b) < \lambda(b). \end{aligned}$$

This implies that $\mathbb{Z}[i]$ is a Euclidean domain. $\square$

Problem 3 We need to find elements $a = s + ti \in \mathbb{Z}[i]$ such that $\lambda(a) = s^2 + t^2 = 1$. Clearly, $s^2 + t^2 = 1$ if and only if $(s,t) = (1,0), (-1,0), (0,1), (0,-1)$. Thus all the units of $\mathbb{Z}[i]$ are

$$1, -1, i, -i.$$

$\square$

Problem 4 It is easy to find that

$$2 = (1+i)(1-i)$$

and $1+i, 1-i$ are irreducible because $\lambda(1+i) = \lambda(1-i) = 2$ is a prime number in $\mathbb{Z}$. $\square$

Problem 5 For any $\alpha = a + b\omega \in R$, we have $\alpha = a + b\omega = (a+b) + (-b)(1-\omega)$. Since $a+b$ is an integer, $a + b \equiv 0, 1$ or 1 in modulus 3. This implies that $a + b = 3k + r$ for some integer k and $r = 0, 1$ or 1. Note that $3 = (2+w)(1-w)$. Therefore, we have

$$\alpha = (a+b) + (-b)(1-\omega) = (3k+r) + (-b)(1-\omega) = r + (k(2+w) - b)(1-\omega).$$

Since $k(2+w) - b \in R$, we can conclude that α must be congruent to r, which is one of $0, 1$, or -1 mod $1-\omega$. $\square$

Problem 6 Suppose that 1 and ω are same in $R/\wp R$. Then $(1-\omega) = a\wp$ for some $a \in R$. Take the norm, we have $3 = N(1-\omega) = N(a)N(\wp)$. Hence $N(\wp) = 1$ or 3, but by assumption, $N(\wp) \neq 3$, so we have $N(\wp) = 1$. But this implies that $\wp$ is an unit in R, which is a contradiction because $\wp$ is a prime element. Therefore, 1 and ω are distinct in $R/\wp R$.

Similarly, $N(1-\omega^2) = N(2+\omega) = 2^2 - 2\cdot 1 + 1 = 3$ and $N(\omega - \omega^2) = N(1+2\omega) = 3$ implies that, together with the above observation, $1, \omega$ and ω^2 are distinct in $R/\wp R$.

Hence, for any nonzero element r in $R/\wp R$, $r, r\omega, r\omega^2$ are all distinct. since $\omega^3 = 1$, we can say

$$\text{Nonzero elements of } R/\wp R = \bigsqcup \{r, r\omega, r\omega^2\}$$

where $\bigsqcup$ means disjoint union.

This implies that $N(\wp) = \sharp$ of elements of $R/\wp R = 1+ \sharp$ of nonzero elements of $R/\wp R = 1 + 3k$. Thus we can conclude that $3 \mid N(\wp) - 1$. $\square$

If you have any question, please contact me : Yoonsuk Hyun (yshyun@math.mit.edu)