18.781, Fall 2007 Problem Set 8

Solutions to Selected Problems

Problem 2 First, observe the following statement.

If a prime integer (in $\mathbb{Z}$) p is of the form $3k+2$, p is a prime element in R.

This can be proved easily using the problem 6 in problem set 7. (Note that if a is a prime factor of p ,then $N(a)$ should be p.) By this, we can conclude that $2, 5, 11$ are still primes in R.

If $x = r + s\omega$ $(r, s \in \mathbb{Z})$,by easy computation, we have $x\bar{x} = N(x)$. It can help us to find the factorization of the prime integer (in $\mathbb{Z}$) p. Once we find r, s such that $r^2 - rs + s^2 = p$, then we have $(r + s\omega)(r + s\bar{\omega}) = (r + s\omega)(r - s - s\omega) = p$. (Each factor has prime integer value by the function N, so they are primes in R.)

By above observation, $2^2 - 2 \cdot 1 + 1^2 = 3$, $3^2 - 3 \cdot 1 + 1^2 = 7$ and $3^2 - 3 \cdot 4 + 4^2 = 13$ implies that $3 = (2+\omega)(1-\omega)$, $7 = (3+\omega)(2-\omega)$ and $13 = (3+4\omega)(-1-4\omega)$ can be the prime factorization.

In conclusion, we can have following prime factorizations.

$$7 = (3 + \omega)(2 - \omega)$$
$$21 = 3 \cdot 7 = (2 + \omega)(1 - \omega)(3 + \omega)(2 - \omega)$$
$$45 = 3^2 \cdot 5 = (2 + \omega)^2(1 - \omega)^2 \cdot 5$$
$$22 = 2 \cdot 11$$
$$143 = 11 \cdot 13 = 11 \cdot (3 + 4\omega)(-1 - 4\omega)$$

□

Problem 3 First, prove the following claim.

For any prime $\pi \in R$ with $N(\pi) \equiv 1$ (3), $\{\pi, -\pi\, \omega\pi, -\omega\pi, \omega^2\pi, -\omega^2\pi\}$ are all distinct in (mod 3). (i.e, in $R/3R$.)

It is not hard to prove that the $\{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$ are all distinct in (mod 3). Also, $\pi X \equiv \pi Y$ in $R/3R$ implies that $3 = (2 + \omega)(1 - \omega) \mid \pi(X - Y)$. But since $N(2 + \omega) = N(1 - \omega) = 3$ and $N(\pi) \equiv 1$ (3), it is clear that $(2 + \omega)$ and $(1 - \omega)$ cannot divide π. Since these are primes in R, we can conclude that $3 = (2 + \omega)(1 - \omega) \mid (X - Y)$. (This is the similar situation with the following. In $\mathbb{Z}$, $d \mid ab$ implies $d \mid b$ when $gcd(d, a) = 1$.) Therefore, we have $\pi X = \pi Y$ in $R/3R$ if and only if $X = Y$ in $R/3R$. With the fact that $\{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$ are all distinct in $R/3R$, we can find that the above claim is true.

For any element α in R, we can say that $\alpha = (3k+r)+(3t+s)\omega$ with $r, s = 0, 1, 2$, and in this case, $\alpha = r + s\omega \pmod 3$. If $3 \nmid N(a)$, then $3 \nmid ((3k+r)^2 - (3k+r)(3t+s) + (3t+s)^2)$. This gives that $(r, s) = (0,1), (1,0), (0,2), (2,0), (1,1), (2,2)$. Also it can be easily verified that $\alpha = r + s\omega$ for $(r, s) = (0,1), (1,0), (0,2), (2,0), (1,1), (2,2)$ are all distinct in (mod 3).

By the claim, the six elements $\{\pi, -\pi\,\omega\pi, -\omega\pi, \omega^2\pi, -\omega^2\pi\}$ are all distinct in (mod 3), and each of their norm (the value by N) is not divisible by 3, hence, in $R/3R$, this set is exactly equal to $\{1, \omega, 2, 2\omega, 1+\omega, 2+2\omega\}$. Therefore, exactly one of these six elements is equivalent to 2. $\square$

Problem 4 We can observe that $5^2 - 5 \cdot 3 + 3^2 = 19$. This gives

$$(5+3\omega)(2-3\omega) = 19.$$

Clearly these two prime factors are primary.
(Remark) In this case, we are lucky. If we choose the factorization $(3+5\omega)(-2+2\omega) = 19$, we need to find the primary element by computation. $\square$

Problem 5 (For this problem, assume that $N(\pi)$ is not 3.) Since π is a prime element, $R/\pi R$ is an integral domain which has finite element. (The number of residue classes in $R/\pi R$ is $N(\pi)$ by the problem 1.) In general, finite integral domain is a field, so $R/\pi R$ is a finite field. Therefore,since the nonzero elements of the finite field $R/\pi R$ is a cyclic group as a multiplicative group, there is a primitive root for $R/\pi R$.

Now let g be the primitive root of $R/\pi R$. Then we can express the all elements of $R/\pi R$ as $\{0, g^1, g^2, \cdots, g^{N(\pi)-1} = 1\}$.

If α is a cubic residue mod π, $\alpha \equiv x^3(\pi)$. Then $\left(\frac{\alpha}{\pi}\right)_3 \equiv x^{N(\pi)-1} = g^{t(N(\pi)-1)} = 1$.

Conversely, $\left(\frac{\alpha}{\pi}\right)_3 = 1$ implies that if $\alpha = g^t$, $g^{\frac{t(N(\pi)-1)}{3}} = 1$. Since g is a primitive root, it is equivalent to $(N(\pi)-1) \mid \frac{t(N(\pi)-1)}{3}$ (in $\mathbb{Z}$), which is same as $3 \mid t$. Therefore, $\alpha = (g^{\frac{t}{3}})^3$, so α is a cubic residue mod π. $\square$

Problem 7 For (a), we already know that 5 is a prime in R by the claim in problem 2. Hence, by the observation in problem 5, any nonzero element can be written as g^t and $g^{24} \equiv 1$ in $R/5R$. Therefore, any nonzero element α in $R/5R$ satisfies $\alpha^{24} = 1$ in $R/5R$. Since the number of nonzero elements in $R/5R$ is exactly $N(5) - 1 = 24$, the factorization of $x^{24} - 1$ in $R/5R$ is

$$x^{24} - 1 = \prod_{\alpha \in (R/5R)^*} (x - \alpha),$$

where $(R/5R)^*$ indicates the set of nonzero elements in $(R/5R)$.

For (b), we already observed that $\alpha = g^t$ is a cubic residue if and only if $3 \mid t$ in $\mathbb{Z}$. Thus, there are 8 cubic residues in $R/5R$.

For (c), we can compute that, in $R/5R$,

$$(\omega(1-\omega))^4 = \omega^4(1-\omega)^4 = \omega \cdot (-3\omega)^2 = 9 = -1 \neq 1$$
$$(\omega(1-\omega))^8 = (-1)^2 = 1$$

implies that $\omega(1-\omega)$ has order 8. Clearly ω has order 3. Since $gcd(3,8) = 1$, $\omega^2(1-\omega) = (\omega)(\omega(1-\omega))$ has order $3 \cdot 8 = 24$. $\square$

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