Answersheet 9 - Yiwei Yang 2018533218

1.

a.

Suppose that p is a prime dividing $4n^2+1$.
Then, if we define $x=2n$:
$x^2 \equiv -1(\bmod p)$
$\left(x^2\right)^{\frac{p-1}{2}} \equiv(-1)^{\frac{p-1}{2}}(\bmod p)$
$x^{p-1} \equiv(-1)^{\frac{p-1}{2}}(\bmod p)$
$(-1)^{\frac{p-1}{2}} \equiv 1(\bmod p)$ by Fermat's theorem
$(-1)^{\frac{p-1}{2}}=1$
And, so: $p \equiv 1(\bmod 4)$ $\square$

b.

For sums of 2 squares, let $n=x^2+y^2=\prod p_i^{e_i} \prod q_j^{f_j} \in \mathbb{N}$, for some $p_i, q_j \in \mathbb{Z}$ where each $p_i \equiv 1 \bmod 4$ and each q_j is 2 or 3 $\bmod 4$.

Suppose n is a sum of two squares, i.e., $n=N(\alpha)$ for some $\alpha \in \mathbb{Z}[i]$. By the above exercises, each p_i is irreducible in $\mathbb{Z}[i]$ and an irreducible factorization of any q_j looks like $q_j=\pi_j \bar{\pi}_j$ where π_j is an element of norm q_j in $\mathbb{Z}[i]$. So an irreducible factorization of n in $\mathbb{Z}[i]$ looks like

$$n=\prod p_i^{e_i} \prod \pi_j^{f_j} \prod \bar{\pi}_j^{f_j} \tag{1}$$

Now write an irreducible factorization of $\alpha \in \mathbb{Z}[i]$ as

$$\alpha=u \prod r_i^{h_i} \prod \phi_j^{k_j} \tag{2}$$

where u is a unit and,, we may assume each r_i is a prime of $\mathbb{N}$ with $r_i \equiv 1 \bmod 4$ and each ϕ_j is an element of $\mathbb{Z}[i]$ of s_j, where s_j is a prime of $\mathbb{N}$ which is 2 or 3 mod 4 . Then, by multiplicativity of the norm,

$$n=N(\alpha)=N(u) \prod N\left(r_i\right)^{h_i} \prod N\left(\phi_j\right)^{k_j}=\prod r_i^{2 h_i} \prod s_j^{k_j} \tag{3}$$

Now, by unique factorization in $\mathbb{Z}$, we have up to reordering each $r_i=p_i, 2 h_i=e_i, s_j=q_j$ and $k_j=f_j$. Hence each e_i is even, which is precisely the latter condition in the theorem.

$\rightarrow$: If rs is a sum of two squares then r and s must each be sums of two squares. This is obviously not true if $r=s$, but it turns out to be true if r and s are relatively prime. By the above lemma,

$\leftarrow$: If each e_i is even. Then $\prod p_i^{e_i}$ is a square, whence a sum of two squares. Also, by (a), we know each q_j is a sum of two squares. Then by the composition law, n is a sum of two squares.$\square$

2.

$20 x^3+42 x^2+48 x+45=(2 x+3) \frac{20 x^3+42 x^2+48 x+45}{2 x+3}=(2 x+3)\left(10 x^2+6 x+15\right)$

$x^5-x^3 y^2-x^2 y^2+y^4=x^3(x+y)(x-y)+y^2(y+x)(y-x)=(x+y)(x-y) x^3-(x+y)(x-y) y^2=(x+y)(x-y)\left(x^3-y\right.$

3.

a.

For each pair of polynomials f, g in $A\left[x_1, \ldots, x_n\right]$,

$$\operatorname{cont}(f g) \subset \operatorname{cont}(f) \operatorname{cont}(g) \subset \sqrt{\operatorname{cont}(f g)} \tag{4}$$

where $\sqrt{\cdot}$ denotes the radical of an ideal. Moreover, if R is a GCD domain then

$$\operatorname{gcd}(\operatorname{cont}(f g))=\operatorname{gcd}(\operatorname{cont}(f)) \operatorname{gcd}(\operatorname{cont}(g)) \tag{5}$$

where $\operatorname{gcd}(I)$ denotes the unique minimal principal ideal containing a finitely generated ideal I.

So given $g(x) \in A[x]$, first write it as $g(x) = cG(x)$, where c is a constant and $G(x)$ is primitive. Then show that a primitive polynomial in $A[x]$ is irreducible if and only if it is irreducible when viewed as a polynomial in $A[x]$, where k is the field of fractions of A. Then use this to take an arbitrary polynomial in $A[x]$, and factor it by "factoring out the content, then factoring it over $A[x]$,
Since A is a UFD, then by this argument so is $A\left[x_1\right]$; which means that so is $A\left[x_1\right]\left[x_2\right] \cong A\left[x_1, x_2\right]$. Which means that so is $A\left[x_1, x_2\right]\left[x_3\right] = A\left[x_1, x_2, x_3\right]$. $\square$

b.

A standard example of a non-Noetherian domain is the ring $R = \{f(x) \in \mathbb{Q}[x] : f(0) \in \mathbb{Z}\}$; that is, the ring of rational polynomials with integer constant term. The units of R are just ± 1. The polynomial x is reducible, since it factors as $2 \cdot \frac{1}{2}x$, but is not a product of irreducibles, since one of the factors would have to be qx for some rational q, and again this factors as $2 \cdot \frac{q}{2}x$.

4.

Let $p = 7$ The norm $N(p) = p^2 = p \cdot p$. There does not exist an element in $\mathbb{Z}[\sqrt{-5}]$ with norm p, thus a rational prime p that is congruent to 7 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, but not a prime element in $\mathbb{Z}[\sqrt{-5}]$.

Similarly, Let $p = 13$. Then $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{5}{p}\right) = \left(\frac{5}{p}\right)$ and so $\left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{20k+13}{5}\right) = \left(\frac{3}{5}\right) = -1$. In this case, since -5 is not a square $\bmod p$, p is irreducible in $\mathbb{Z}\sqrt{-5}$, because If p is a rational prime and reducible, then -5 is a square modulo p. Because let p be reducible. If $p = \alpha\beta$ where α, β are not units, then $p^2 = N(p) =$ $N(\alpha\beta) = N(\alpha)N(\beta)$ and $N(\alpha) = p$. If $\alpha = a + b\sqrt{-5}$, then $a^2 + 5b^2 = p$. Then $a^2 + 5b^2 \equiv 0 \bmod p$ which implies $a^2 \equiv -5b^2 \bmod p$. Thus $\left(ab^{-1}\right)^2 \equiv -5 \bmod p$ since b is a unit in $\mathbb{Z}_p$. 13 is also a prime element in $\mathbb{Z}[\sqrt{-5}]$