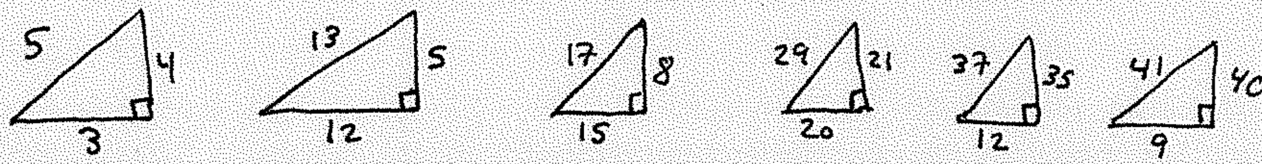
MATH 307 : TEST 2 SOLUTION

PROBLEM 1 Find integer right-angled triangles with hyptotenuses 5, 13, 17 and 29, 37, 41



PROBLEM 2 Find sol^{n} of $x^2 - 65y^2 = 1$ by 1st solving $x^2 - 65y^2 = -1$.

Observe $y = \pm 1 \Rightarrow x^2 - 65y^2 = -1 \hookrightarrow x^2 = -1 + 65 = 64 \therefore \underline{x = \pm 8}$

Hence $(8,1), (-8,1), (8,-1), (-8,-1)$ all sol^{n}'s of $x^2 - 65y^2 = -1$.

Recall, $x_1^2 - 65y_1^2 = -1$ and $x_2^2 - 65y_2^2 = -1$ yields

$$(x_1^2 - 65y_1^2)(x_2^2 - 65y_2^2) = (-1)(-1) = 1$$

$$x_1^2 x_2^2 - 65 y_1^2 x_2^2 - 65 x_1^2 y_2^2 + 65^2 y_1^2 y_2^2 = 1$$

$$\Rightarrow (\underbrace{x_1 x_2 + 65 y_1 y_2}_{x_3})^2 - 65(\underbrace{x_1 y_2 + y_1 x_2}_{y_3})^2 = 1$$

adding zero, grouping, algebra.

Hence, using $x_1 = x_2$, $y_1 = y_2$ where $x_1 = 8$, $y_1 = 1$

$$x_3 = 8^2 + 65 = 64 + 65 = 129.$$
$$y_3 = 8(1) + (1)(8) = 16.$$

$\boxed{(129, 16) \text{ solves } x^2 - 65y^2 = 1}$

Notice, $129^2 - 65(16)^2 = 16{,}641 - 16{,}640 = 1.$

This we did in hwk. Alternatively, (this is better way to see it)

$$x^2 - 65y^2 = (x + y\sqrt{65})(x - y\sqrt{65})$$

Thus, $x_1^2 - 65y_1^2 = (x_1 + y_1\sqrt{65})(x_1 - y_1\sqrt{65})$ and,

$$(x_1^2 - 65y_1^2)(x_2^2 - 65y_2^2) = (x_1 + y_1\sqrt{65})(x_1 - y_1\sqrt{65})(x_2 + y_2\sqrt{65})(x_2 - y_2\sqrt{65})$$
$$= z_1 \bar{z}_1 z_2 \bar{z}_2 = (z_1 z_2)(\overline{z_1 z_2})$$

← not complex conjugate. Rather the natural one here.

But, $z_1 z_2 = (x_1 + y_1\sqrt{65})(x_2 + y_2\sqrt{65})$

$$= (\underbrace{x_1 x_2 + 65 y_1 y_2}_{x_3}) + (\underbrace{x_1 y_2 + y_2 x_1}_{y_3})\sqrt{65}$$

$\boxed{\text{PROBLEM 3}}$ Suppose d is squarefree and $a, b, x, y \in \mathbb{Z}$.
Prove: If $a + b\sqrt{d} = x + y\sqrt{d}$ then $a = x$ & $b = y$

Suppose $a, b, x, y \in \mathbb{Z}$ and $a + b\sqrt{d} = x + y\sqrt{d}$ where $d \neq 0$ and $d \neq \pm n^2$ $\forall n \in \mathbb{N}$. Observe

$$a + b\sqrt{d} = x + y\sqrt{d} \Rightarrow \underline{a - x = (-b + y)\sqrt{d} = (y - b)\sqrt{d}} \quad *$$

Thus, for $y - b \neq 0$ we find

$$\sqrt{d} = \frac{a - x}{y - b} \Rightarrow \sqrt{d} \in \mathbb{Q}$$

But, as d is squarefree we can argue $\sqrt{d} \notin \mathbb{Q}$. Suppose $\sqrt{d} \in \mathbb{Q}$ then $\sqrt{d} = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$ whence $d = \frac{p^2}{q^2}$, and as $d \in \mathbb{Z}$ was assumed from the outset, the prime factorizations of p^2 & q^2 must coincide in the sense $q^2 = (\underbrace{\pi_1 \pi_2 \cdots \pi_r}_{\text{possible repeats}})^2$

$$\Rightarrow p^2 = (\pi_1 \pi_2 \cdots \pi_r \, \zeta_1 \zeta_2 \cdots \zeta_s)^2 \text{ which yields}$$

$$\frac{p^2}{q^2} = (\zeta_1 \zeta_2 \cdots \zeta_s)^2 = d \Rightarrow d = n^2 \text{ for } n = \zeta_1 \zeta_2 \cdots \zeta_s$$

a $\rightarrow\leftarrow$, thus $\sqrt{d} \notin \mathbb{Q}$ and we find $y - b = 0$ which shows $\underline{y = b}$. Returning to $*$ we find

$$a - x = 0\sqrt{d} = 0 \Rightarrow \underline{a = x}. //$$

$\boxed{\text{PROBLEM 4}}$ Find 4 distinct units in $\mathbb{Z}[\sqrt{5}]$. How many units in $\mathbb{Z}[\sqrt{5}]$?

$a + b\sqrt{5}$ has $\text{norm}(a + b\sqrt{5}) = a^2 - 5b^2$. For a unit we have $uu^{-1} = 1 \Rightarrow \text{norm}\, u \; \text{norm}\, u^{-1} = 1 \Rightarrow \text{norm}\, u = \pm 1$.
We wish to solve $x^2 - 5y^2 = 1$ or $\underline{x^2 - 5y^2 = -1}$

$x = 2,\ y = 1$ easy to see.

But, using technique of $\boxed{\text{PROBLEM 2}}$

$$(2 + \sqrt{5})^2 = 4 + 4\sqrt{5} + 5 = 9 + 4\sqrt{5}$$

$$(2 + \sqrt{5})^3 = (9 + 4\sqrt{5})(2 + \sqrt{5}) = 18 + 17\sqrt{5} + 10 = 28 + 17\sqrt{5}$$

continued ↩

PROBLEM 4 to solve $x^2-5y^2=\pm 1$ we simply read off coefficients of $(2+\sqrt{5})^k$ for $k=1,2,3,4,\dots$ where

$k=1,3,5,\dots$ correspond to sol$^{\underline{n}}$s of $x^2-5y^2=-1$

$k=2,4,6,\dots$ correspond to sol$^{\underline{n}}$s of $x^2-5y^2=1$

We calculated

$$(2+\sqrt{5})^k = \underbrace{2+\sqrt{5},\ 9+4\sqrt{5},\ 38+17\sqrt{5},\ 161+72\sqrt{5}}_{\text{units of } \mathbb{Z}[\sqrt{5}]},\dots$$

Of course, we could also include ± 1 there are also units!
— (you could be lazier) —

PROBLEM 5 Consider $p=13$. Discuss primality of p in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}[i]$, $\mathbb{Z}[i,j,k]$.

(a.) yes we know $p=13$ is prime in $\mathbb{Z}$.

(b.) $\mathbb{Q}$ is a <u>field</u>, no element is prime, 13 is not prime as $13 = \left(\frac{13}{7}\right)7$ for example ($13, \frac{13}{7}$ are not associates.)

(c.) In Chapter 6 we proved the following theorem: §6.3

$$\left\{\begin{matrix}\text{An ordinary prime } p\in\mathbb{N} \text{ is} \\ \text{Gaussian prime}\end{matrix}\right\} \Longleftrightarrow \left\{p \neq a^2+b^2 \ \underset{\text{some}}{\text{for}}\ a,b\in\mathbb{N}\right\}$$

But, we also learned in §6.5 if $p=4n+1$ then $p=a^2+b^2$ for some $a,b\in\mathbb{N}$.

Observe, $13 = 4+9 = 2^2+3^2 = \underline{(2+3i)(2-3i) = 13}$

Moreover, $\text{norm}(2\pm 3i) = 4+9 = 13 < \text{norm}(13) = 169$.

Clearly 13 is <u>not</u> prime in $\mathbb{Z}[i]$.

(d.) once again $13 = (2+3i)(2-3i)$ in context of $\mathbb{Z}[i,j,k]$

Hence, 13 is not prime. (we know $2\pm 3i$ not associates of 13 since $\text{norm}(2\pm 3i)\neq \text{norm}(13)$)

$\boxed{\text{PROBLEM 6}}$ Calculate $\gcd(10+7i,\ 2-3i)$ in $\mathbb{Z}[i]$ and find $a, b \in \mathbb{Z}[i]$ such that $a(10+7i)+b(2-3i) = \gcd(10+7i, 2-3i)$

Notice $\dfrac{10+7i}{2-3i} = \dfrac{(10+7i)(2+3i)}{(2-3i)(2+3i)} = \dfrac{20+30i+14i-21}{13} = \dfrac{-1+44i}{13}$

thus $\dfrac{10+7i}{2-3i} \approx 3i$ (could also use $-1+3i$, that's also close)

This calculation above guides my work below

$$(10+7i,\ 2-3i) = (z, w)$$
$$(2-3i,\ 10+7i-3i(2-3i)) = (2-3i,\ 1+i) = (w,\ z-3iw)$$
$$(1+i,\ \underbrace{2-3i+2i(1+i)}_{*}) = (1+i,\ -i) = (z-3iw,\ \underbrace{w+2i(z-3iw)}_{7w+2iz})$$
$$\Rightarrow\ -i = 2iz + 7w$$

Thus, $\boxed{\gcd(10+7i,\ 2-3i) = -i = 2i(10+7i)+7(2-3i)}$.

Remark: the Euclidean Algorithm stopped when we obtained remainder $-i$ as $-i$ is a unit of $\mathbb{Z}[i]$.

Remark: as we discussed earlier, it is natural to think of gcd as a set. With ideals we again recover that view,

$$\underbrace{(10+7i)+(2-3i)}_{\substack{\text{gcd-ideal} \\ \text{of } (10+7i)\ \&\ (2-3i).}} = (-i) = (1) = \mathbb{Z}[i]$$

Remark: $\dfrac{2-3i}{1+i}\left(\dfrac{1-i}{1-i}\right) = \dfrac{2-5i-3}{2} = \dfrac{-1-5i}{2} \approx -\dfrac{4i}{2} = -2i$

this is why in the last step we did $\underline{2-3i-(-2i)(1+i) = -i}_{*}$

Maybe you can guess $-2i$ w/o all the calculation?
I'm not sure how plausible guessing is here.

PROBLEM 7 Suppose $a, b \in \mathbb{Z}$ and $a+ib$ is a Gaussian prime. Show $a-ib$ is a Gaussian prime

Assume $a+ib$ is a Gaussian prime. Suppose towards a $\rightarrow\leftarrow$ that $a-ib = \gamma_1\gamma_2$ where $\text{norm}(\gamma_1), \text{norm}(\gamma_2) \neq \text{norm}(a-ib)$. Of course we know $\text{norm}(z) = \text{norm}(\bar{z})$ hence $\text{norm}(\bar{\gamma}_1), \text{norm}(\bar{\gamma}_2) \neq \text{norm}(a+ib)$. Also by conjugation,

$$a+ib = \bar{\gamma}_1\bar{\gamma}_2 \Rightarrow a+ib \text{ not a Gaussian prime}$$

which <u>contradicts</u> our initial assumption. Thus $a-ib$ is also a Gaussian prime.//

PROBLEM 8 Find a Gaussian prime factorization of 102 in $\mathbb{Z}[i]$

$$102 = 6(17) = 2(3)(17) \quad 2 = 1^2+1^2 \ \& \ 17 = 4^2+1^2$$

$$\boxed{102 = (1+i)(1-i)(3)(1+4i)(1-4i)}$$

Observe $\text{norm}(1 \pm i) = 2$, $\text{norm}(1 \pm 4i) = 17$ thus $1 \pm i, 1 \pm 4i$ have no nontrivial (non associate) divisors as 2, 17 have no divisors except $\pm 2, \pm 17$ and ± 1. To see 3 is prime in $\mathbb{Z}[i]$ Notice $\text{norm}(3) = 9$ and 1, 3, 9 are divisors of 9. However, $\text{norm}(a+ib) \neq 3 \ \forall a, b \in \mathbb{Z}$; $\text{norm}(a+ib) = a^2+b^2$

PROBLEM 9 I'm sure many examples exist to show how prime divisor property breaks down for complex primes. ~~I stole this from [illegible]~~

~~($\beta = \frac{1+i+j+k}{2} + i + j$ has norm~~ ~~(nope, almost right)~~

$$\alpha = i+j+k \qquad \alpha\beta = (i+j+k)(-i-j-k)$$
$$\beta = -i-j-k \qquad = -i^2-j^2-k^2 - \cancel{ij} - \cancel{ji} - ik - ki - \cancel{jk} - \cancel{kj}$$
$$= 3.$$

Observe $\text{norm}(\alpha) = \text{norm}(\beta) = 3$ hence α, β are Hurwitz primes. Further, $p = \frac{i+j+k}{2} + 1 = \frac{3+i+j+k}{2}$ has $\text{norm}(p) = \frac{9+1+1+1}{4} = \frac{12}{4} = 3$ is a prime and $p\bar{p} = 3 \Rightarrow p \mid 3$ or $p \mid \alpha\beta$ more to the point. Yet, $p \nmid \alpha$ and $p \nmid \beta$ as $\alpha \ \& \ \beta$ are primes of Hurwitz #s.

—(thanks to Jess Gregory for this)—

PROBLEM 10

$$\mathcal{M}(a+bj) = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \quad \& \quad \mathcal{M}(zw) = \mathcal{M}(z)\mathcal{M}(w)$$

(a.) $\mathcal{M}(a+bj)\mathcal{M}(c+dj) = \begin{bmatrix} a & b \\ b & a \end{bmatrix}\begin{bmatrix} c & d \\ d & c \end{bmatrix}$

$$= \left[\begin{array}{c|c} ac+bd & ad+bc \\ bc+ad & bd+ac \end{array}\right]$$

$$= \mathcal{M}\left(ac+bd + j(ad+bc)\right)$$

Hence $\underline{(a+bj)(c+dj) = ac+bd + j(ad+bc)}$.

or $c_1 = ac+bd \quad \& \quad c_2 = ad+bc$.

(b.) $jj = 1 \qquad (a=c=0, \quad b=d=1) \quad$ so, $\boxed{j^2=1}$

Remark: $j^2=1 \Rightarrow (j-1)(j+1)=0$ ZERO DIVISORS !!

(c.) If $N = \{x+yj \mid x,y \in \mathbb{R}\}$ then find all sol^{n}s in N to the quadratic eq^{n} $\underbrace{z^2+\alpha z = 0}$ where $\alpha = a+jb \in N$.

$$z(z+\alpha) = 0$$

Clearly $\boxed{z_0 = -\alpha}$ is a ~~possible~~ sol^{n} (no matter what α looks like)

If $\alpha = 0$ then $z^2=0$ and $z=0$ is sol^{n} no example.

Let $z = x+jy$ and $\alpha = a+jb$, assume $\alpha \neq 0$.

$$(x+jy)(x+jy + a+jb) = 0$$

$$(x+jy)(x+a + j(y+b)) = 0$$

$$x(x+a) + y(y+b) + j(x(y+b) + y(x+a)) = 0$$

We face two eq^{n}s:

① $x(x+a) + y(y+b) = 0 \Rightarrow x^2+y^2+ax+by = 0$.

② $2xy + bx + ay = 0$

If $z = x+yj \neq -(a+bj)$ then at least one of $x+a$, $y+b$ is nonzero. In particular, if both $x+a, y+b \neq 0$ then $x(x+a)+y(y+b) = 0 \Rightarrow \underline{x=0, y=0}$. or $\boxed{z=0}$

— (in the following pages I show $\exists$ two more sol^{n}s if $\alpha = bj$ for $b \neq 0$. I have not proved these are <u>all</u> the sol^{n}s possible, but, I think that is true) —

$Z^2 + \alpha z = 0$ where $\alpha = a + jb$ and $z = x + jy \in \mathcal{H}$

$$Z^2 = (x+jy)(x+jy) = x^2 + 2jxy + j^2y^2 = x^2 + y^2 + 2xyj$$

$$\alpha Z = (a+jb)(x+jy) = ax + by + j(ay + bx)$$

Hence,

$$Z^2 + \alpha Z = x^2 + y^2 + ax + by + j(2xy + ay + bx)$$

To solve $Z^2 + \alpha Z = 0$ is to simultaneously solve

$$\underline{x^2 + y^2 + ax + by = 0}_{\text{I}} \quad \& \quad \underline{2xy + ay + bx = 0}_{\text{II.}}$$

On the other hand, $\mathcal{H}$ is a $\underbrace{\underline{\text{commutative}}\ \underline{\text{algebra}}}$

thus $Z^2 + \alpha Z = Z(Z + \alpha) = 0$

oh, this calculation works with less than commutative ---

Clearly $\boxed{Z = 0}$ and $\boxed{Z = -\alpha}$ are sol$^{\underline{n}}$'s. going back to I and II we verify these claims in real notation with $z = 0 \iff \underbrace{x = 0, y = 0}_{\text{clearly solves I \& II.}}$

Also, $Z = -\alpha \Rightarrow x + jy = -a - bj$

$$\Rightarrow x = -a, \ y = -b$$

$$\Rightarrow \begin{cases} (-a)^2 + (-b)^2 + a(-a) + b(-b) = 0 & \text{(solves I.)} \\ \quad \& \\ 2(-a)(-b) + a(-b) + b(-a) = 0 & \text{(solve II.)} \end{cases}$$

Of course, even w/o I and II it was evident that $Z = 0$ and $Z = -\alpha$ solved $Z^2 + \alpha Z = Z(Z + \alpha) = 0$ since $0 \cdot w = 0 \ \ \forall w \in \mathcal{H}$. The novel feature of this problem is the possibility of zero-divisor sol$^{\underline{n}}$'s in addition to $Z = 0$ & $Z = -\alpha$.

Notice $j^2 = 1 \Rightarrow 1^2 - j^2 = 0 \Rightarrow (1-j)(1+j) = 0$

Multiply by k^2 for $k \neq 0$ to see $(k - jk)(k + jk) = 0$

Thus $z(z + \alpha) = 0$ when $\underline{Z = k - jk \ \ \& \ \ z + \alpha = k + jk}_{\text{III.}}$

Continuing,

III. $z = k - jk$ & $z + \alpha = k + jk$

$\Rightarrow \cancel{k} - jk + \alpha = \cancel{k} + jk$

$\Rightarrow \alpha = 2jk$

$\Rightarrow a + bj = 2jk$

$\Rightarrow \underline{a = 0}$, $\underline{b = 2k}$ aka $k = \frac{b}{2}$

Thus, $z = k(1 - j)$ for $k \neq 0$ provided $\alpha = 2kj$. Or we could say $\boxed{\alpha = bj \Rightarrow z = \frac{b}{2}(1-j)}$

Check it: $z^2 + \alpha z = \left[\frac{b}{2}(1-j)\right]^2 + bj\left[\frac{b}{2}(1-j)\right]$

$= \frac{b^2}{4}(1 - 2j + j^2) + \frac{b^2}{2}(j - 1)$

$\neq 0.$

We likewise may have $z = k + jk$ & $z + \alpha = k - jk$

$\Rightarrow \cancel{k} + jk + \alpha = \cancel{k} - jk$

$\alpha = -2jk = a + bj \rightarrow a = 0$, $b = -2k$ or $k = \frac{-b}{2}$

This gives sol^n $z = k(1+j) = \frac{-b}{2}(1+j)$ when $\alpha = bj$

That is, if $\boxed{\alpha = bj \text{ we have sol}^n\ z = \frac{-b}{2}(1+j)}$

In summary, $z^2 + \alpha z = 0$ where $\alpha = a + bj$ has sol$^{\underline{n}}$'s of $z_1 = 0$ and $z_2 = -\alpha$ in all cases. However, if $a \neq 0$ then $\nexists$ any additional sol$^{\underline{n}}$'s. If $a = 0$ then there are two additional sol$^{\underline{n}}$'s of the form $z_3 = \frac{b}{2}(1-j)$ and $z_4 = \frac{-b}{2}(1+j)$ (if $b = 0$ then $z_3 = z_4 = 0$ so these are only really new sol$^{\underline{n}}$'s when $a = 0$ but $b \neq 0$)

<u>Remark</u>: I used the result that for $zw = 0$ either we had $z = 0$ or $w = 0$. Or, the zero-divisor case $z = k(1+j)$, $w = k(1-j)$. If there are additional zero divisors we'd need to consider those. Moreover, it is possible that I've missed something. My current sol$^{\underline{n}}$ <u>conjectures</u> we can compare factors, but, I have not shown numbers of the form $x + jy$ permit nice factorization... for example of the danger, in $\mathbb{Z}_{60}$ if I have $zw = \bar{0} = (\bar{2})(\overline{30}) = (\bar{6})(\overline{10}) = (\bar{4})(\overline{15})$