1. a. $20 = 13 + 7$ $\boxed{gcd = 1}$

$13 = 7 + 6$

$7 = 6 + 1$

$6 = 6 \cdot 1$

$1 = 7 - 6 = (20 - 13) - (13 - (20 - 13)) = \boxed{2 \cdot 20 - 3 \cdot 13}$

b. $372 = 5 \cdot 69 + 27$

$69 = 2 \cdot 27 + 15$

$27 = 15 + 12$

$15 = 12 + 3$

$12 = 4 \cdot 3$

$3 = 15 - 12 = 15 - (27 - 15) = 2 \cdot 15 - 27 = 2 \cdot (69 - 2 \cdot 27) - 27$

$= 2 \cdot 69 - 5 \cdot 27 = 2 \cdot 69 - 5(372 - 5 - 69)$

$= \boxed{27 \cdot 69 - 5 \cdot 372}$

c. $779{,}086{,}434{,}385{,}541 = 8 \cdot 91{,}442{,}056{,}588{,}823 + 47{,}549{,}981{,}674{,}957$

$91{,}442{,}056{,}588{,}823 = 47{,}549{,}981{,}674{,}957 + 43{,}892{,}074{,}913{,}866$

$47{,}549{,}981{,}674{,}957 = 43{,}892{,}074{,}913{,}866 + 3{,}657{,}906{,}761{,}091$

$43{,}892{,}074{,}913{,}866 = 11 \cdot 3{,}657{,}906{,}761{,}091 + 3{,}655{,}100{,}541{,}865$

$3{,}657{,}906{,}761{,}091 = 3{,}655{,}100{,}541{,}865 + 2{,}806{,}219{,}226$

$3{,}655{,}100{,}541{,}865 = 1302 \cdot 2{,}806{,}219{,}226 + 1{,}403{,}109{,}613$

$2{,}806{,}219{,}226 = 2 \cdot 1{,}403{,}109{,}613$ $\boxed{g.c.d = 1{,}403{,}109{,}613}$

$a = 779{,}086{,}434{,}385{,}541$

$b = 91{,}442{,}056{,}588{,}823$

$c = 47{,}549{,}981{,}674{,}957$

$d = 43{,}892{,}074{,}913{,}866$

$e = 3{,}657{,}906{,}761{,}091$

$f = 3{,}655{,}100{,}541{,}865$

$g = 1{,}403{,}109{,}613$

$h = 2{,}806{,}219{,}226$

$f = 2605g$

$e = f + 2g = f + h$

$d = 11 \cdot e + f$

$c = d + e$

$b = c + d$

$a = 8b + c$

$2g = e - f = e - (d - 11e) = 12e - d$

$= 12c - 13d$

$= 25c - 13b$

$= 25a - 213b$

$f = 1302h + g$ $g = f - 1302h = f - 1302(25a - 213b)$

$2g = h$

$f = d - 11e = 12d - 11c$

$= 12b - 23c$

$f = 12b - 23(a - 8b)$

6

2. In this calculation, we use the norm $N(a+bi)=a^2+b^2$. To find each q_i, we calculate the element of $\mathbb{Q}[i]$ that is $\frac{r_{i-2}}{r_{i-1}}=a+bi$, and then set $q_i=\lfloor a\rfloor+\lfloor b\rfloor i$.

$$\begin{array}{ll}
85=-6i(1+13i)+(7-6i) & N(1+13i)=170>78=N(7-6i) \checkmark \\
1+13i=i(7-6i)+(-5+6i) & N(7-6i)>61=N(-5+6i) \checkmark \\
7-6i=-1(-5+6i)+2 & N(-5+6i)>4=N(2) \checkmark \\
-5+6i=(-2+3i)2-1 \checkmark & N(2)>1=N(-1) \checkmark \\
-2+3i=(2-3i)(-1) \checkmark & N(-1)>0 \checkmark
\end{array}$$

Thus the (-1) is the greatest common divisor of 85 and $1+13i$ in $\mathbb{Z}[i]$. ✓

$$\begin{array}{ll}
53+56i=i(47-13i)+(40+9i) & N(47-13i)=2378>1681=N(40+9i) \\
47-13i=(40+9i)+(7-22i) & N(47-13i)>533=N(7-22i) \\
40+9i=i(7-22i)+(18+2i) & N(7-22i)>328=N(18+2i) \\
7-22i=-i(18+2i)+(5-4i) & N(18+2i)>41=N(5-4i) \\
18+2i=(2+2i)(5-4i)+0 & N(5-4i)>0
\end{array}$$

Thus the greatest common divisor of $53+56i$ and $47-13i$ is $5-4i$. ✓

Problem 3 5

Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field and let $\mathcal{O}$ be its associated integer ring. Let N be its field norm.

a) Suppose $D = -3$. Prove $\mathcal{O}$ is a Euclidean domain wrt N.

Let $\alpha = a + bw$ where $w = \frac{1+\sqrt{D}}{2}$, so $\alpha, \beta \in \mathcal{O}$.
$\beta = c + dw$

Compute $\frac{\alpha}{\beta} = \frac{a+bw}{c+dw} \cdot \frac{c+d\bar{w}}{c+d\bar{w}}$ where $\bar{w} = \frac{1-\sqrt{D}}{2}$

$$= \frac{ac + ad\bar{w} + bcw + bd\,w\bar{w}}{c^2 + cd\bar{w} + cdw + d^2 w\bar{w}}$$

$$= \frac{ac + bd + \frac{bc+ad}{2} + \frac{bc-ad}{2}\sqrt{D}}{c^2 + cd + d^2}$$

$$= \frac{ac + bd + ad + (bc-ad)\left(\frac{1+\sqrt{D}}{2}\right)}{c^2 + cd + d^2}$$

$$= \underbrace{\frac{ac+bd+ad}{c^2+cd+d^2}}_{r} + \underbrace{\frac{bc-ad}{c^2+cd+d^2}}_{s} w$$

$$= r + s\,w \checkmark$$

Let $q = e + fw$ where e is the closest integer to r and f is the closest integer to s; so $q \in \mathcal{O}$.

$$|e - r| \le \tfrac{1}{2} \quad \text{and} \quad |f - s| \le \tfrac{1}{2}.$$

Let $r = \theta\beta$ where $\theta = (r - e) + (s - f)w$.

e have that $\alpha = q\beta + r$ and since $r = \alpha - q\beta$, and each of $\alpha, q, \beta \in \mathcal{O}$, we have that $r \in \mathcal{O}$. ✓

Claim: $N(r) < N(\beta)$

$$N(r) = N(\theta)\,N(\beta)$$

$$= N(\beta)\left[\left(r - e + \frac{s-f}{2} + \frac{s-f}{2}\sqrt{D}\right)\left(r - e + \frac{s-f}{2} - \frac{s-f}{2}\sqrt{D}\right)\right]$$

$$= N(\beta)\left[\left(r - e + \frac{s-f}{2}\right)^2 - D\left(\frac{s-f}{2}\right)^2\right]$$

$$\le N(\beta)\left[(r-e)^2 + \left(\frac{s-f}{2}\right)^2 + 2|r-e|\left|\frac{s-f}{2}\right| - D\left(\frac{s-f}{2}\right)^2\right]$$

$$\le N(\beta)\left[\frac{1}{4} + \frac{1}{16} + 2\,\frac{1}{2}\,\frac{1}{4} + 3\,\frac{1}{16}\right]$$

$$= \frac{3N(\beta)}{4} < N(\beta)$$ ✓

Thus, we have found $q, r \in \mathcal{O}$ s.t. $\alpha = q\beta + r$ and $N(r) < N(\beta$

So $\mathcal{O}$ is a Euclidean domain

Suppose $D = -163$. Prove $\mathcal{O}$ is not a Euclidean domain wrt. any Norm.

We will prove that $\mathcal{O}$ has no universal side divisors.

First, we identify all units of $\mathcal{O}$.

We know that $\alpha \in \mathcal{O}^{\times}$ iff $N(\alpha) = \pm 1$.

Since $D \equiv 1 \ (4)$, for $\alpha = a + bw$ where $w = \frac{1+\sqrt{D}}{2}$,

$$N(\alpha) = a^2 + ab + \frac{1-D}{4} b^2 = a^2 + ab + 41b^2 = \left(a + \frac{b}{2}\right)^2 + \frac{163 b^2}{4}$$

We look for α s.t. $N(\alpha) = \pm 1$

$$(2a+b)^2 + 163 b^2 = \pm 4$$

Since there is no soln for -4,

$$(2a+b)^2 + 163 b^2 = 4$$

This forces $b = 0$ since $b \in \mathbb{Z}$,

$$(2a)^2 = 4$$

Hence, the only solns are $a = \pm 1$, $b = 0$, meaning

$\mathcal{O}^{\times} = \{\pm 1\}$. ✓

So $\tilde{\mathcal{O}} = \{0, \pm 1\}$.

Now suppose $u \in \mathcal{O}$ is a universal side divison and note That if $a, b \in \mathbb{Z}$ and $b \neq 0$, then

$$N(a + b\omega) = \left(a + \frac{b}{2}\right)^2 + \frac{163}{4} b^2 \geqslant 41$$

So the smallest non zero values of N on $\mathcal{O}$ are 1 (for units ± 1) and 4 (for ± 2).

Taking $x = 2$ in the def of a universal side divisor, it follows that

u divides one of $2 - 0$, or 2 ± 1 in $\mathcal{O}$.

Since u cannot be a unit, u divides 2 or 3 in $\mathcal{O}$. ✓

If $2 = \alpha\beta$, then $4 = N(\alpha)N(\beta)$ and It follows that one of α, β has norm 1 while the other has norm 4.

So the only divisors of 2 in $\mathcal{O}$ are $\{\pm 1, \pm 2\}$.

Similarly, the only divisors of 3 in $\mathcal{O}$ are $\{\pm 1, \pm 3\}$, so

u can be one of $\pm 2, \pm 3$. ✓

Now, let $x = \frac{1+\sqrt{-163}}{2}$. Again u must divide one of $x-0$ or $x\pm1$.

So, $N(u)$ must divide $N(x)$ or $N(x\pm1)$.

$N(x) = 41$ $\quad N(x-1) = 41$ and $N(x+1) = 43$.

41 and 43 are not divisible by ~~$\pm2, \pm3$~~ 4, 9 so none of $\pm2, \pm3$ can be a universal side divison.

Hence $\mathcal{O}$ has no universal side divisors. good.

5

1. Let R be a PID w/ $P \subseteq R$ a prime ideal. ~~By~~ definition of a PID, P is principle. So

ase 1: $P = 0$. Then $R/P = \{r+0 : r \in R\} = R$, so R/P is a PID ✓

se 2: $P \neq 0$. Then P is maximal since R is PID, ~~an ideal containing P~~

hus, R/P is a field. In general, the ideals of a field are (0), and (1), which

e both principle. So R/P is a PID. ∎ good

principle.

oblem 5 (5)

Let R be an integral domain and suppose that every prime ideal in R is principal. We'll prove that R is a PID.

) Assume the set of ideals of R that aren't principal is nonempty } and prove that this set has a maximal element under inclusion. By hypothesis, this maximal ideal is not prime.

Let $P = \{$ ~~set of~~ ideals of R that aren't principal $\} \neq \emptyset$.

Let $\mathcal{C}$ be a chain in P.

Let $B = \bigcup_{c \in \mathcal{C}} c$. I claim that B is an upper bd in P of the ~~ε ideals~~ elements in $\mathcal{C}$. Since each $C \in \mathcal{C}$ is an ideal and they are ~~ordered by~~ inclusion, B is also an ideal.

ny' does

Now, suppose for contradiction that $B = (b)$. Then, $b \in C_j$ for some

mean

$C_j \in \mathcal{C}$. C_j is an ideal in R that isn't principal, but because

$\subseteq$

ideal? it contains b and b generates B, $C_j \supset B$. It's clear that $C_j \subset B$ by def of B, so $C_j = B = (b)$. This is a contradiction because C_j is not principal. ✓

By Zorn's Lemma, P contains a maximal element I. ✓

b) Let I be an ideal which is maximal wrt being non principal and let $a, b \in R$ w/ $ab \in I$ but $a \notin I$ and $b \notin I$.

~~Prove that~~

Let $I_a = (I, a)$ and $I_b = (I, b)$. Define $J = \{r \in R \mid r I_a \subseteq I\}$

Prove $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in R

w/ $I \subsetneq I_b \subseteq J$ and $I_a J = (\alpha\beta) \subseteq I$.

Since $a, b \notin I$, we know that $I \subsetneq I_a$ ✓ and $I \subsetneq I_b$. ✓

Since I is maximal wrt being nonprincipal, it follows that I_a and I_b must be prinicipal ideals because $I \neq I_a, I_b$.

So let $I_a = (\alpha)$ ✓

~~Also, $a \notin I_b$ but $a \in J$ because a~~

Now, $I \subset J$ because $\forall i \in I$, $i I_a = i(I, a) = (I, ai)$ and $ai \in I$, so $i I_a = I$. ✓

Also, $b \in J$ b/c $b I_a = b(I, a) = (I, ab)$ and since $ab \in I$, $b I_a = I$.

It follows that $I \subsetneq I_b \leq J$. Since J contains I and $J \neq I$, by maximality of I, J must be principal. So $J = (\beta)$. ✓

Certainly $I_a J \leq I$ because by def. of J, $\forall j \in J$, $j I_a \subseteq I$.

Now $I_a J = \left\{ \sum_{i=1}^{n} (r\alpha)(r'\beta) \;\middle|\; n \text{ is finite}; r, r' \in R \right\} = \left\{ \sum_{i=1}^{n} \tilde{r}\, \alpha\beta \;\middle|\; \tilde{r} \in R, n \text{ is finite} \right\}$

$= (\alpha\beta)$. ✓

c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce $I = I_a J$ is principal, a contradiction, and conclude that R is a PID.

Since $x \in I \subsetneq I_a$, $x \in I_a$ so $x = r\alpha$ for some $r \in R$.

We must have $r\alpha \in I$. Note that J contains all the elements r such that $r\alpha \in I$. So $x = s\alpha$ for some $s \in J$.

Hence, $I \subseteq I_a J$. Part (a) stated that $I_a J \subseteq I$, so $I = I_a J = (\alpha\beta)$. This is a contradiction because I is not principal. ✓

good.

Problem 6. Let R be a commutative ring with 1 and let a, b be nonzero elements of R. A *least common multiple* of a and b is an element e of R such that

(i) $a \mid e$ and $b \mid e$, and
(ii) if $a \mid e'$ and $b \mid e'$, then $e \mid e'$.

(a) Prove that a least common multiple of a and b (if such exists) is a generator for the unique largest PID contained in $(a) \cap (b)$.

(b) Deduce that any two nonzero elements in a Euclidean domain have a least common multiple which is unique up to multiplication by a unit.

(c) Prove that in a Euclidean domain the least common multiple of a and b is $\frac{ab}{(a,b)}$, where (a, b) is the greatest common divisor of a and b.

Answer:

(a) Given a pair $a, b \in R$ which has a least common multiple e, then since $a \mid e$ and $b \mid e$, $e \in a$ and $e \in b$, and thus $e \in (a) \cap (b)$. Thus $(e) \subseteq (a) \cap (b)$. Let $x \in (a) \cap (b)$, which implies $(x) \subseteq (a) \cap (b)$. Then $a \mid x$ and $b \mid x$. By the definition of least common multiple, $e \mid x$. Thus, $(x) \subseteq (e$. Therefore, there cannot be a principle ideal in $(a) \cap (b)$ that is not contained in (e). Thus, e is the generator of the unique largest principle ideal contained in $(a) \cap (b)$. ✓

(b) Given two non-zero elements a, b in a Euclidean Domain R, since R is a Euclidean Domain and hence a Principle Ideal Domain, the ideal $(a) \cap (b)$ is generated by a single element of R. Denote this generating element e. Since $e \in (a)$, $a \mid e$ and similarly since $e \in (b)$, $b \mid e$. Moreover, for an element $e' \in R$, such that $a \mid e'$ and $b \mid e'$, then $e' \in (a) \cap (b) = (e)$. Thus, $e \mid e'$. Thus, any $a, b \in R$ admit a least common multiple. Moreover, if another element f is also a least common divisor for a and b, the $a \mid f$ and $b \mid f$, which implies $e \mid f$. By the same argument except for swapping the roles of f and e, which we can do since both are least common divisors, $f \mid e$. The first implication implies the gcd(e,f)=e while the second implies gcd(e,f)=f. Since the greatest common divisor in a euclidean domain is unique up to multiplication by a unit, $eu = f$ for some unit $u \in R$. Thus, the least common multiple in a Euclidean Domain is unique up to multiplication by a unit. ✓

(c) First, note that since $(a, b) \mid a$ and $(a, b) \mid b$, $\frac{ab}{(a,b)} = a * \frac{b}{(a,b)} = \frac{a}{(a,b)} * b$, meaning $a \mid \frac{ab}{(a,b)}$ and $b \mid \frac{ab}{(a,b)}$. Since R is a euclidean domain, let l be the lowest common multiple for a and b. By definition of a lowest common multiple, $l \mid \frac{ab}{(a,b)}$. Since $a \mid l$, let $ak = l$. Multiplying both sides by b shows $abk = lb$. Note that since $a \mid ab$ and $b \mid ab$, $l \mid ab$. Thus, we divide by l to demonstrate $\frac{ab}{l}k = b$, which means $\frac{ab}{l} \mid b$. Since R is a commutative ring, a similar proof demonstrates $\frac{ab}{l} \mid a$. By the definition of a greatest common divisor, $\frac{ab}{l} \mid (a, b)$. Since $(a, b) \mid ab$, we ✓

5

Problem 7. Let a and b be nonzero elements of a PID R. Prove that a and b has a least common multiple. Now assume that R is additionally a UFD. Describe the least common multiple of a and b in terms of the prime factorizations of a and b.

The proof in part (b) of the previous problem did not rely on the Euclidean property of the domain except in its use of language implying division. We still have any ideal in $(a) \cap (b)$ principal (for nonzero a and b), and so it is a PID, which means that $(a) \cap (b)$ itself is generated by some element e. Such an element e is a least common multiple because every common multiple is in $(a) \cap (b)$, and e generates that ideal! Every PID is a UFD, so there is no need for an additional assumption. The least common multiple of $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ (include the prime factors of both numbers, so $a_i, b_i \in \mathbb{Z}_{\geqslant 0}$) is $e = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ where $e_i = \max\{a_i, b_i\}$.

✓

Problem 8. (a) Prove that the quotient ring $\mathbb{Z}[i]/(1+i)$ is a field of order 2.

(b) Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \pmod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

(c) Let $p \in \mathbb{Z}$ be a prime with $p \equiv 1 \pmod 4$ and write $p = \pi\bar{\pi}$ for some $\pi \in \mathbb{Z}[i]$. Prove that the hypotheses of the Chinese Remainder Theorem are satisfied, and thus

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi})$$

as rings. Show that the ring $\mathbb{Z}[i]/(p)$ has order p^2 and that each of $\mathbb{Z}[i]/(\pi)$, $\mathbb{Z}[i]/(\bar{\pi})$ is a field of order p.

Answer:

(a) Consider the principal ideal $(1+i) \in R$. Given an element $(c+di) \in R$, we have an element $a+bi \in (1+i)$, $(a+bi) = (1+i)*(c+di) = (c-d)+(c+d)i$, implying $a = (c-d)$ and $b = (c+d)$. Adding these equalities demonstrates $2c = a+b$. Given that $c \in \mathbb{Z}$, it must be the case that if $a+bi \in (1+i)$, then $2 \mid a+b$ or put differently, $a+b$ is even. Note furthermore that given an element $a+bi \in R$ such that $a+b$ is even, then $a+bi = (1+i)*(\frac{a+b}{2}+\frac{a-b}{2}i)$, implying $a+bi \in (1+i)$. Thus, $1+i$ is composed of all elements $a+bi \in R$ such that $2 \mid a+b$. As all ✓

elements that do not have this property, *i.e* those elements $x + yi$ where $x + y$ is odd, if we either add 1 or i, then we get an element of $\mathbb{Z}[i]$ that is in $(1 + i)$. Since $\mathbb{Z}[i]$ is a euclidean domain, and $1 + i$ is an irreducible element of $\mathbb{Z}[i]$, $(1 + i)$ is a prime ideal in R. Thus, $\mathbb{Z}[i]/(1 + i)$ is a field with order 2. ✓

(b) Given a prime number $q \in \mathbb{Z}$ such that $q \equiv 3 \pmod 4$, we know that q is an irreducible element in $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a euclidean domain, (q) is a prime ideal. Thus, $\mathbb{Z}[i]/(q)$ is a field. Furthermore, given $a + bi \in (q)$, then $a+bi = (q)*(c+di) = qc+qdi$. Thus, if $q \mid a$ and $q \mid b$ if $a+bi \in (q)$. Furthermore, given an element $a + bi \in \mathbb{Z}[i]$ such that $qk = a$ and $ql = b$ for some $k, l \in \mathbb{Z}$, then $a + bi = qk + ql = q * (k + l) \in (q)$. Thus, the elements in (q) are all of the elements $a + bi \in \mathbb{Z}[i]$ such that $q \mid a$ and $q \mid b$. Given any $a + bi \in \mathbb{Z}[i]$, since $\mathbb{Z}$ is a euclidean domain, $a = qk + r$ and $b = ql + s$, where $r, s < q$. Thus, $a+bi+(q) = qk+r+(ql+s)i+(q) = r + si + (q)$. As there are q possible values of r and s, there are $q * q = q^2$ possible values $a + bi$ could be. Also, given any $r + si \in \mathbb{Z}[i]/(q)$, note $r+si+(q)$ does not reduce, thus all q^2 possible values in $r+si \in \mathbb{Z}[i]/(q)$ are mapped to by the reduction mapping. Thus, $\mathbb{Z}[i]/(q)$ is a field with order q^2. ✓ Maybe use sun-Zc?

(c) Given a prime number $p \in \mathbb{Z}$ such that $p \equiv 1 \pmod 4$, then there exists $a + bi \in \mathbb{Z}[i]$ such that $p = (a+bi)*(a-bi) = a^2 + b^2$. Note furthermore, from the result the demonstrated the previous that $a + bi$ and $a - bi$ are irreducible elements of $\mathbb{Z}[i]$. Thus, $(a + bi)$ and $(a - bi)$ are both prime ideals in $\mathbb{Z}[i]$, and are thus co-maximal ideals. As these criterion fulfill the hypotheses for the Chinese Remainder Theorem, $\mathbb{Z}[i]/p \cong \mathbb{Z}[i]/((a + bi) * (a - bi)) \cong \mathbb{Z}[i]/(a + bi) \times \mathbb{Z}[i]/(a - bi)$. ✓ To show that the order of $\mathbb{Z}[i]/p$ is p^2, note that in the above proof with a prime $q \equiv 3 \pmod 4$, we made no use of the fact that any other condition aside from the primality of $q \in \mathbb{Z}$ to demonstrate the ring $\mathbb{Z}[i]/(q)$ had order q^2. Thus, the same proof shows $\mathbb{Z}[i]/p$ is a ring with order p^2. Furthermore, since $(a + bi)$ and $(a - bi)$ are prime ideal of $\mathbb{Z}[i]$, $\mathbb{Z}[i]/(a - bi)$ and $\mathbb{Z}[i]/(a + bi)$ are both fields. Furthermore, since $\mathbb{Z}[i]/p \cong \mathbb{Z}[i]/(a + bi) \times \mathbb{Z}[i]/(a - bi)$, $|\mathbb{Z}[i]/p| = p^2 = |\mathbb{Z}[i]/(a + bi)| * |\mathbb{Z}[i]/(a - bi)|$. Since p is irreducible and $\mathbb{Z}$ is a UFD, given $ab = p^2$, either $a = p$ and $b = p$, or either a or b is 1. $|\mathbb{Z}[i]/(a - bi)| = 1$ if and only if $(a - bi)$ is a unit. Since $(a - bi)$ is irreducible, $|\mathbb{Z}[i]/(a - bi)| = 1 \neq 1$. As a similar proof shows $|\mathbb{Z}[i]/(a + bi)| \neq 1$, $|\mathbb{Z}[i]/(a + bi)| = |\mathbb{Z}[i]/(a - bi)| = p$. ✓ good.

Challenge 9. An integral domain R in which every ideal generated by two elements is principal is called a *Bezout domain*.

(a) Prove that the integral domain R is a Bezout domain if and only if every pair of elements $a, b \in R$ has a greatest common divisor d in R that can be written as an R-linear combination of a and b.

(b) Prove that every finitely generated ideal of a Bezout domain is principal.

(c) Prove that R is a PID if and only if R is a UFD that is also a Bezout domain. (We have proven in class that every PID is a UFD, and PIDs are obviously Bezout domains. Thus it only remains for you to prove that UFD's which are Bezout domains are in fact PIDs. Let $0 \neq a \in I \trianglelefteq R$ where a has the minimal number of irreducible factors amongst elements of I. Prove that $I = (a)$ by showing that if there is an element $b \in I$ that is not in (a), then $(a, b) = (d)$ leads to a contradiction.

Answer:

(a) Given an integral domain R, in which all elements $a, b \in R$ have a greatest common divisor, d that can be written as an R-linear combination of a and b, then $d \in (a, b)$. Thus, $(d) \subseteq (a, b)$. Furthermore, since $d \mid a$ and $d \mid b$, $a = dk$ and $b = dl$ for some $k, l \in R$. Then given any R-linear combination $ax + by$, which by definition are the form of all elements of (a, b), $ax + by = dkx + dly = d * (kx + ly) \in (d)$. Thus, $(a, b) \subseteq (d)$, which given the reverse inclusion demonstrates $(a, b) = (d)$. Since R is a ring where there exists a d for any pair a, b, the ideal generated by any pair of elements in R is a principle ideal *i.e* a Bezout domain. ✓

Now suppose an integral domain R is a Bezout domain. Then for all $a, b \in R$, $(a, b) = (d)$ for some $d \in R$. Since $a, b \in (a, b)$, $d \mid a$ and $d \mid b$, meaning d is a common divisor for a and b. Furthermore, since $(d) \subseteq (a, b)$, $d = ax + by$ for some $x, y \in R$. Now suppose an element in R $e' \mid a$ and $e' \mid b$. Then a and b are in (e'), which further implies $ax + by = d \in (e')$.✓Thus, $e' \mid d$, concluding the proof that such a d is a greatest common divisor of a, b, which can be written as an R-linear combination of a and b. As such a d exists for all pairs a, b in R by assumption, the reverse implication holds. ✓ good.

(b) Ideals generated by singleton sets are by definition principle and all ideals generated by two elements in R are principle by the definition of a Bezout domain. Letting these cases be the base case for an inductive proof, suppose that given a finite $n \in (N)$, ideals of R generated by $n - 1$ elements is principle. Then given the ideal $(x_1, x_2, ..., x_{n-1}, x_n)$, ✓ for any $x_i \in R$, this is the set of R-linear combinations $(a_1 * x_1 + a_2 * x_2 + ... + a_{n-1}x_{n-1}) + a_n * x_n$, where $a_i \in R$. Since the inductive hypothesis states that ideals of R generated by $n - 1$ elements are principle, there exists a d in R such that for all R-linear combination $a_1 * x_1 + a_2 * x_2 + ... + a_{n-1}x_{n-1} \in (x_1, x_2, ..., x_{n-1})$, $dk = a_1 * x_1 + a_2 * x_2 + ... + a_{n-1}x_{n-1}$ for some k in R. Thus, $(a_1 * x_1 + a_2 * x_2 + ... + a_{n-1}x_{n-1}) + a_n * x_n = dk + a_n * x_n$. ✓ That is, given any n elements of R, there exists a pair of elements in R such that any linear combination of the n elements can be written as a linear combination of the set of 2 elements, in other words, an ideal generated by a set of n elements of R is also generated by a pair of elements in R. Since R is a bezout domain, these ideals must be principle. Thus by induction, all finitely generated ideals in R are principle. ✓

(c) Suppose R is a UFD as well as a Bezout domain, and let $0 \neq a \in I \trianglelefteq R$, where a has the minimal number of irreducible factors among~~st~~ elements of I. That is, a is an element of I such that there does not exist and element $d \mid a$, for if there were, then d would have a smaller number of irreducible factors. Suppose there were $b \in I$ such that $b \notin (a)$. Since both b and a are in I, $(a, b) \subseteq I$. Since R is a Bezout domain, there exists d such that $(a, b) = (d)$. Notably $d \in I$ since $d \in (a, b)$, which means d is the result of an R-linear combination of a and b. Thus, $d \in I$ and $d \mid a$. As we picked a to have a minimal number of irreducible factors amongst elements of I, we have reached a contradiction. ✓ Thus, there cannot be $b \in I$ such that $b \notin (a)$, which concludes the proof that $I = (a)$ and hence principle for all I in R. Thus, a UFD that is also a Bezout domain is a PID. As the reverse result has been previously demonstrated, R is a PID if and only if R is a UFD as well as a Bezout domain. good.