.1 Further remarks and examples

Problem .1.1. Generalize the CRT for two ideals, as follows. Let I, J be ideals in a commutative ring R; prove that there is an exact sequence of R-modules

$$0 \longrightarrow I \cap J \longrightarrow R \xrightarrow{\varphi} \tfrac{R}{I} \times \tfrac{R}{J} \longrightarrow \tfrac{R}{I+J} \longrightarrow 0$$

where φ is the natural map. (Also, explain why this implies the first part of Theorem 6.1, for $k = 2$.)

Solution. Let the map for $I \cap J \to R$ be the inclusion. Since it is injective, its kernel is 0 and the first part of the sequence is exact. Furthermore, its image is merely $I \cap J$. Now consider the map φ which sends $r \in R$ to $(r + I,\ r + J)$. Certainly the kernel of this map is the set of elements in R which are in both I and J; that is, the kernel is $I \cap J$. The image of this map is merely the set $\{r+I,\ r+J) \mid r \in R\}$. Note that this may not be the entirety of $(R/I) \times (R/J)$. Define a map from $(R/I) \times (R/J)$ to $R/(I + J)$ which sends $(a + I, b + J)$ to $a - b + (I + J)$. One can easily verify that this is indeed a homomorphism of modules. Note that the kernel of this image is precisely the image of φ. Furthermore, the homomorphism is surjective; and arbitrary $a + (I + J)$ is mapped to by $(a + I, 0 + J)$. With these homomorphisms, we have shown the existence of such an exact sequence of R-modules.

In the case where $I + J = (1)$, then the map φ is surjective. This can be seen by noting that there exist $i \in I$, $j \in J$ such that $i+j = 1$. Then for all $(r+I, s+J)$, we have

$$\begin{aligned}\varphi(rj + si) &= (rj + I, si + J)\\ &= (rj + ri + I, si + sj + J)\\ &= (r(j + i) + I, s(i + j) + J)\\ &= (r + I, s + J).\end{aligned}$$

Thus, we have recovered the desired statement. □

Problem .1.2. Let R be a commutative ring, and let $a \in R$ be an element such that $a^2 = a$. Prove that $R \cong R/(a) \times R/(1 - a)$.

Show that the multiplication in R endows the ideal (a) with a *ring* structure, with a as the identity. Prove that $(a) \cong R/(1 - a)$ as rings. Prove that $R \cong (a) \times (1 - a)$ as rings.

Solution. Consider the natural homomorphism φ from R to $R/(a) \times R/(1 - a)$ which sends r to $(r + (a), r + (1 - a))$. The kernel of this homomorphism is the set of elements in $(a) \cap (1 - a)$. Let $x \in (a) \cap (1 - a)$ so $x = ra = s(1 - a)$ for some $r, s \in R$. Multiplying both sides by a yields $ra^2 = sa - sa^2$. But then we have

$$x = ra = sa - sa = 0.$$

Thus, $(a) \cap (1-a) = 0$ so φ is injective. To see that it is surjective, note that $(a) + (1-a) = (1)$. By Exercise 6.1, the natural homomorphism is surjective. Therefore, φ is a bijective ring homomorphism and thus an isomorphism.

The ideal (a) is already an abelian group under addition. To see that it is also a ring under multiplication in R with a as an identity, note that for $ax \in (a)$, we have $a \cdot ax = a^2x = ax$. Distributivity is inherited from R, making (a) a ring.

Consider the natural map from (a) to $R/(1-a)$ which sends ax to $ax + (1-a)$. This map is surjective as any $x+(1-a) = ax+(x-ax)+(1-a) = ax+(1-a) = \varphi(ax)$. Furthermore, the kernel of this map is the set of elements $ax \in (1-a)$. But $ax = (1-a)y \implies a(x+y) = y \implies a(x+y) = ay \implies ax = 0$ so $x = 0$ and the homomorphism is injective. Thus, we have a bijective homomorphism from $(a) \to R/(1-a)$ so the rings are isomorphic. The third isomorphism is relatively similar to show. □

Problem .1.3. Recall (Exercise III.3.15) that a ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Let R be a finite Boolean ring; prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$.

Solution. Suppose R has only two elements; then $R \cong \mathbb{Z}/2\mathbb{Z}$. If R has more than two elements, then there is some idempotent $e \notin \{0, 1\}$. Per Exercise 6.2, we can split R into $(e) \times (1-e)$, both of which have strictly fewer elements than R. Repeating this process will eventually yield a direct product in which each component is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. □

Problem .1.4. Let R be a finite commutative ring, and let p be the smallest prime dividing $|R|$. Let $I_1, \ldots, I_k$ be proper ideals such that $I_i + I_j = (1)$ for $i \neq j$. Prove that $k \leq \log_p |R|$. (Hint: Prove $|R|^{k-1} \leq |I_1| \cdots |I_k| \leq (|R|/p)^k$.)

Solution. To do. □

Problem .1.5. Show that the map $\mathbb{Z}[x] \to \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x)$ is not surjective.

Solution. Consider the element $(1, 2) \in \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x)$. Suppose some polynomial $f \in \mathbb{Z}[x]$ is sent to this element. Since $f \equiv 2 (\mod x)$, this forces the constant term of f to be 2. However, if this were the case then the constant term of $f \mod 2$ would be 0, a contradiction. Thus, there is no polynomial mapped to this element and the mapping is not surjective. □

Problem .1.6. Let R be a UFD.

- Let $a, b \in R$ such that $\gcd(a, b) = 1$. Prove that $(a) \cap (b) = (ab)$.
- Under the hypotheses of Corollary 6.4 (but only assuming that R is a UFD) prove that the function φ is injective.

Solution. Certainly $(ab) \subseteq (a) \cap (b)$ since any element $r \cdot ab = (rb) \cdot a = (ra) \cdot b$. To show the other direction, consider the least common multiple m of a and b. That is, for any other multiple n of a and b, we have $m \mid n$. Certainly $(a) \cap (b) \subseteq (m)$ so we must show that $m = ab$. Indeed, suppose $ab \nmid m$. Then we find $x = ab/m \neq 1$. But then we have

$$a = \frac{ab}{m} \cdot \frac{m}{b} = x \cdot \frac{m}{b}.$$

Similarly, $x \mid b$ so $\gcd(a, b) \neq 1$, a contradiction. Thus, it must be the case that $m = ab$ and $(a) \cap (b) = (ab)$.

For the second part, note that the kernel of φ is clearly $(a_1) \cap \cdots \cap (a_k)$. But by the first part, this ideal is equal to $(a1 \cdots a_k) = (a)$. Thus, the kernel of φ is equal to the identity in $R/(a)$ and the function is injective. □

Problem .1.7. Find a polynomial $f \in \mathbb{Q}[x]$ such that $f \equiv 1 \mod (x^2+1)$ and $f \equiv x \mod x^{100}$.

Solution. First note that $x^{100} \equiv 1 \mod (x^2+1)$. From this, consider the polynomial $f(x) = x + x^{100}(1-x) = x + x^{100} - x^{101}$. We find that $f \equiv x \mod x^{100}$ and $f \equiv x + 1 - x \equiv 1 \mod (x^2+1)$. □

Problem .1.8. Let $n \in \mathbb{Z}$ be a positive integer and $n = p_1^{a_1} \cdots p_r^{a_r}$ its prime factorization. By the classification theorem for finite abelian groups (or, in fact, simplier considerations; cf. Exercise II.4.9)

$$\frac{\mathbb{Z}}{(n)} \cong \frac{\mathbb{Z}}{(p_1^{a_1})} \times \cdots \times \frac{\mathbb{Z}}{(p_r^{a_r})}$$

as abelian groups.

- Use the CRT to prove that this is in fact a *ring* isomorphism.
- Prove that
$$\left(\frac{\mathbb{Z}}{(n)}\right)^* \cong \left(\frac{\mathbb{Z}}{(p_1^{a_1})}\right)^* \times \cdots \times \left(\frac{\mathbb{Z}}{(p_r^{a_r})}\right)^*$$
(recall that $(\mathbb{Z}/n\mathbb{Z})^*$ denotes the group of units of $\mathbb{Z}/n\mathbb{Z}$).
- Recall (Exercise II.6.14) that *Euler's ϕ-function* $\phi(n)$ denotes the number of positive integers $\leq n$ that are relatively prime to n. Prove that
$$\phi(n) = p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1).$$

Solution. To do. □

Problem .1.9. Let I be a nonzero ideal of $\mathbb{Z}[i]$. Prove that $\mathbb{Z}[i]/I$ is finite.

Solution. Note that $\mathbb{Z}[i]$ is a Euclidean domain so it is a PID. That is, there exists some $\alpha \in \mathbb{Z}[i]$ such that $I = (\alpha)$. Let $a + bi + I$ be an element of $\mathbb{Z}[i]/I$. By the Division Algorithm, there exist $q, r \in \mathbb{Z}[i]$ such that

$$a + bi = q\alpha + r$$

with $N(r) < N(\alpha)$. But then $a + bi - r = q\alpha \in I$ so $a + bi + I = r + I$. That is, every element of the quotient ring is represented by some element r with norm less that $N(\alpha)$. There are only finitely many elements with such a norm (since there are only finitely many integers a, b such that $a^2 + b^2 < N(\alpha)$. Thus, the quotient ring $\mathbb{Z}[i]/I$ is finite. □

Problem .1.10. Let $z, w \in \mathbb{Z}[i]$. Show that if z and w are associates, then $N(z) = N(w)$. Show that if $w \in (z)$ and $N(z) = N(w)$, then z and w are associates.

Solution. Recall that z and w are associates if and only if $z = uw$ for some unit $u \in \mathbb{Z}[i]$. But then we have $N(z) = N(uw) = N(u)N(w) = N(w)$ (since $N(u) = 1$).

Now suppose $w \in (z)$ and $N(z) = N(w)$. Let $w = uz$. Clearly $N(u) = 1$. But by Lemma 6.6, this implies that u is a unit so w and z are associates. □

Problem .1.11. Prove that the irreducible elements in $\mathbb{Z}[i]$ are, up to associates: $1 + i$; the integer primes congruent to 3 mod 4; and the elements $a \pm bi$ with $a^2 + b^2$ an integer prime congruent to 1 mod 4.

Solution. Let $q \in \mathbb{Z}[i]$ be irreducible. Certainly $N(q) \neq 1$ so $N(q)$ is a product of primes in $\mathbb{Z}$. First consider the case where $N(q)$ is prime. If it is even, then it must be that case that $N(q) = 2$, in which case we have $q = 1 + i$ or one of its associates (there are only four solutions to $a^2 + b^2 = 2$. If $N(q)$ is odd then by the classification of primes which split in $\mathbb{Z}[i]$ we must have $N(q) \equiv 3 \mod 4$. Now suppose $N(q)$ is not prime. If there is a prime $p \equiv 3 \mod 4$ which divides $N(q) = \bar{q}q$ then $p \mid q$. But since q is irreducible, it must be the case that $(p) = (q)$ and the elements are associate. We are reduced to the case where $N(q)$ is a product of primes $p \equiv 1 \mod 4$. Let p be one such prime. Then p splits in $\mathbb{Z}[i]$ as $z\bar{z}$ for some prime element z. Therefore $z \mid q$ and $(z) = (q)$ so $N(q) = N(z) = p$, a contradiction. □

Problem .1.12. Prove Lemma 6.5 without any 'visual' aid. (Hint: Let $z = a + bi$, $w = c + di$ be Gaussian integers with $w \neq 0$. Then $z/w = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$. Find integers e, f such that $|e - \frac{ac+bd}{c^2+d^2}| \leq \frac{1}{2}$ and $|f - \frac{bc-ad}{c^2+d^2}| \leq \frac{1}{2}$, and set $q = e + if$. Prove that $|\frac{z}{w} - q| < 1$. Why does this do the job?)

Solution. Denote $c^2 + d^2$ by $N(w)$ since they are equivalent. By Euclidean division in the integers, there exist $e, r_1 \in \mathbb{Z}$ such that

$$ac + bd = eN(w) + r_1$$

where $|r_1| \leq \frac{N(w)}{2}$. The inequality follows from the fact that if $r_1 > 0$ then $e > 1$ so we are at least dividing by 2. Similarly, we have $bc - ad = fN(w) + r_2$ with $|r_2| \leq \frac{N(w)}{2}$. Now note that

$$\left| e - \frac{ac + bd}{c^2 + d^2} \right| \leq \frac{1}{2},$$
$$\left| f - \frac{bc - ad}{c^2 + d^2} \right| \leq \frac{1}{2}$$

and let $q = e + if$. Then we have

$$\frac{z}{w} = q + \frac{r_1 + r_2 i}{N(w)}.$$

which can be rearranged to yield

$$\left| \frac{z}{w} - q \right| = \left| \frac{r_1 + r_2 i}{N(w)} \right| \leq 1$$

where the last inequality follows from the division algorithm in $\mathbb{Z}$. I don't know why this is sufficient, or if I even did this correctly. However, we can see that

$$z = qw + \frac{r}{\bar{w}}$$

where $r = r_1 + r_2 i$. Furthermore, we have

$$N\left(\frac{r}{\bar{w}}\right) = \frac{r_1^2 + r_2^2}{N(w)} \leq \frac{\frac{N(w)^2}{4} + \frac{N(w)^2}{4}}{N(w)} = \frac{N(w)}{2} < N(w)$$

proving that this is in fact a Euclidean valuation. □

Problem .1.13. Consider the set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

- Prove that $\mathbb{Z}[\sqrt{2}]$ is a ring, isomorphic to $\mathbb{Z}[t]/(t^2 - 2)$.
- Prove that the function $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ defined by $N(a + b\sqrt{2}) = a^2 - 2b^2$ is multiplicative: $N(zw) = N(z)N(w)$. (Cf. Exercise III.4.10.)
- Prove that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.
- Prove that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain, by using the absolute value of N as valuation. (Hint: Follow the same steps as in Exercise 6.12.)

Solution. It is easy to verify that $\mathbb{Z}[\sqrt{2}]$ is a ring. The isomorphism sends $a + bt \in \mathbb{Z}[t]/(t^2 - 2)$ to $a + b\sqrt{2}$. The map is clearly surjective. Furthermore, the kernel is the set of polynomials such that $a = b = 0$. But then $f \in (t^2 - 2)$ so the kernel is trivial in the quotient ring, making the map injective and hence an isomorphism.

Given the norm function and letting $z = a_0 + b_0\sqrt{2}, w = a_1 + b_1\sqrt{2}$, we have

$$\begin{aligned}
N(zw) &= (a_0a_1 + b_0b_1d)^2 - 2(a_0b_1 + a_1b_0) \\
&= \left((a_0a_1)^2 + 2(a_0a_1)(b_0b_1d) + (b_0b_1d)^2\right) - \left((a_0b_1)^2 + 2(a_0b_1)(a_1b_0) + (a_1b_0)^2\right) d \\
&= (a_0a_1)^2 + (b_0b_1d)^2 - (a_0b_1)^2d - (a_1b_0)^2d \\
&= (a_0^2 - b_0^2d)(a_1^2 - b_1^2d) \\
&= N(z)N(w)
\end{aligned}$$

showing that N is multiplicative.

Recall that if u is a unit in $\mathbb{Z}[\sqrt{2}]$ then $N(u)$ is a unit in $\mathbb{Z}$. Thus, we should consider solutions to $N(u) = a^2 - 2b^2 = \pm 1$. It is clear that the solution set is nonempty as $a = 1, b = 1$ produces a solution. Now suppose that $a + b\sqrt{2}$ is a unit in in $\mathbb{Z}[\sqrt{2}]$ so that $a^2 - 2b^2 = \pm 1$. Consider $z = (a + 2b) + (a + b)\sqrt{2}$. We have

$$\begin{aligned}
N(z) &= (a + 2b)^2 - 2(a + b) \\
&= a^2 + 4ab + 4b^2 - 2a^2 - 4ab - 2b^2 \\
&= 2b^2 - a^2 \\
&= -(a^2 - 2b^2) = \pm 1
\end{aligned}$$

so we can construct a distinct solution, proving that there are infinitely many units.

Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$. We have

$$\frac{x}{y} = \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2} = r + s\sqrt{2}.$$

Let n be the closest integer to r and m be the closest integer to s so that $|r - n| \leq \frac{1}{2}$ and $|s - m| \leq \frac{1}{2}$. Define $t = (r - n) + (s - m)\sqrt{2}$ so that we have

$$t = r + s\sqrt{2} - (n + m\sqrt{2}) = \frac{x}{y} - (n + m\sqrt{2}).$$

Multiplying by y and rearranging yields

$$x = yt + (n + m\sqrt{2})y$$

where

$$\begin{aligned} N(yt) &= N(y)N(t) \\ &= N(y)\left|(r-n)^2 - 2(s-m)^2\right| \\ &\leq N(y)\left(\left|\frac{1}{4}\right| + 2\left|\frac{1}{4}\right|\right) \\ &= \frac{3}{4}N(y) \end{aligned}$$

Thus, the valuation of the remainder is less than that of the divisor, proving the valuation is Euclidean. □

Problem .1.14. Working as in Exercise 6.13, prove that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain. (Use the norm $N(a+b\sqrt{-2} = a^2 + 2b^2$.)

If you are particularly adventurous, prove that $\mathbb{Z}[(1+\sqrt{d})/2]$ is also a Euclidean domain for $d = -3, -7, -11$. (You can still use the norm defined by $N(a+b\sqrt{d}) = a^2 - db^2$; note that this is still an integer on $\mathbb{Z}[(1+\sqrt{d})/2]$, if $d \equiv 1 \mod 4$.)

The five values $d = -1, -2$, resp., $-3, -7, -11$, are the only ones for which $\mathbb{Z}[\sqrt{d}]$, resp., $\mathbb{Z}[(1+\sqrt{d})/2]$, is Euclidean. For the values $d = -19, -43, -67, -163$, the ring $\mathbb{Z}[(1+\sqrt{d})/2]$ is still a PID (cf. §2.4 and Exercise 2.18 for $d = -19$); the fact that there are no other negative values for which the ring of integers in $\mathbb{Q}(\sqrt{d})$ is a PID was conjectured by Gauss and only proven by Alan Baker and Harold Stark around 1966. Also, keep in mind that $\mathbb{Z}[\sqrt{-5}]$ is not even a UFD, as you have proved all by yourself in Exercise 1.17.

Solution. We proceed in the same manner as in Exercise 6.13. Let $x = a+b\sqrt{-2}$ and $y = c + d\sqrt{2}$. We have

$$\frac{x}{y} = \frac{(ac+2bd) + (bc-ad)\sqrt{2}}{c^2+2d^2} = r + s\sqrt{2}.$$

Let n be the closest integer to r and m be the closest integer to s so that $|r-n| \leq \frac{1}{2}$ and $|s-m| \leq \frac{1}{2}$. Now define $t = (r-n) + (s-m)\sqrt{-2}$ so that we have

$$t = r + s\sqrt{-2} - (n + m\sqrt{-2}) = \frac{x}{y} - (n + m\sqrt{-2}).$$

We can transform this into the equation

$$x = yt + (n - m\sqrt{-2})y$$

where

$$\begin{aligned} N(yt) &= N(y)N(t) \\ &= N(y)\left((r-n)^2 + 2(s-m)^2\right) \\ &\leq N(y)\left(\frac{1}{4} + 2\frac{1}{4}\right) \\ &= \frac{3}{4}N(y) \\ &< N(y) \end{aligned}$$

Thus, the valuation of the remainder is less than the valuation of y so we have a Euclidean valuation.

I am not feeling particularly adventurous so I will not show the rings of integers are in fact Euclidean domains but I imagine the proofs are incredibly similar. □

Problem .1.15. Give an elementary proof (using modular arithmetic) of the fact that if an integer n is congruent to 3 modulo 4, then it is not the sum of two squares.

Solution. Consider the ring $\mathbb{Z}/4\mathbb{Z}$. Squaring each element in this ring yields the elements 0 and 1. Suppose $n = a^2 + b^2$. Clearly if $n \equiv 3 \mod 4$ then $a^2 + b^2 \equiv 3 \mod 4$. But we cannot add two elements among 0 and 1 to get 3. Thus, n cannot be the sum of two squares. □

Problem .1.16. Prove that if m and n are two integers, both of which can be written as sums of two squares, then mn can also be written as the sum of two squares.

Solution. Suppose $m = a^2 + b^2$ and $n = c^2 + d^2$. Then we have

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d^2) \\ &= (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 \\ &= (ac)^2 + 2abcd(bd)^2 + (ad)^2 - 2abcd + (bc)^2 \\ &= (ac + bd)^2 + (ad - bc)^2 \end{aligned}$$

so mn is also a sum of squares. □

Problem .1.17. Let n be a positive integer.

- Prove that n is a sum of two squares if and only if it is the norm of a Gaussian integer $a + bi$.

- By factoring $a^2 + b^2$ in $\mathbb{Z}$ and $a + bi$ in $\mathbb{Z}[i]$, prove that n is a sum of two squares if and only if each integer prime factor p of n such that $p \equiv 3 \mod 4$ appears with an even power in n.

Solution. Suppose $n = N(a + bi)$. Clearly $N(a + bi) = a^2 + b^2 = n$ so n is the sum of two squares. Now suppose $n = a^2 + b^2$ and consider $z = a + bi$. Then $N(z) = a^2 + b^2 = n$ so n is the norm of a Gaussian integer.

Consider the factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. First suppose that each prime factor $p_i \equiv 3 \mod 4$ has a corresponding even power α_i. Then we can write $n = s^2 m$ where m is not divisible by any squares. Therefore, all primes p which divide m must satisfy $p \equiv 1 \mod 4$ so each p is the sum of two squares and hence their product m is the sum of two squares, say $x^2 + y^2$. But then we have $n = s^2(x^2 + y^2) = (sx)^2 + (sy)^2$ so it is the sum of two squares.

Now suppose $n = x^2 + y^2$ is the sum of two squares. Again, consider the factorization of n over $\mathbb{Z}$. If all of the primes in this factorization are congruent to 1 modulo 4 then we are done so suppose there is a prime $p \equiv 3 \mod 4$. We must show that the largest power of p dividing n, call it α, is even. Indeed, we have $p^\alpha \mid n = (x + iy)(x - iy)$. But since p does not split in $\mathbb{Z}[i]$, it is prime over this ring and hence we have $p \mid x + yi$ or $p \mid x - yi$, both of which imply that $p \mid x$ and $p \mid y$. That is, $x = p^{\beta_1} a$ and $y = p^{\beta_2} b$. But then $x^2 = p^{2\beta_1} a^2$ and $y^2 = p^{2\beta_2} b^2$ so the power of p dividing $x^2 + y^2 = n$ must be even. □

Problem .1.18. One ingredient in the proof of Lagrange's theorem on four squares is the following result, which can be proven by completely elementary means. Let $p > 0$ be an odd prime integer. Then there exists an integer n, $0 < n < p$, such that np may be written as $1 + a^2 + b^2$ for two integers a, b. Prove this result, as follows:

- Prove that the numbers a^2, $0 \leq a \leq (p-1)/2$, represent $(p+1)/2$ distinct congruence classes mod p.
- Prove the same for numbers of the form $-1 - b^2$, $0 \leq b \leq (p-1)/2$.
- Now conclude, using the pigeon-hole principle.

Solution. Let $c = a^2 \mod p$. Then a is a root of the polynomial $x^2 - c$ over $\mathbb{Z}/p\mathbb{Z}$, as is $p - a$ (which is distinct from a since p is odd). Since a polynomial of degree n over an integral domain can have at most n solutions, these two roots are all of the solutions of this polynomial. As a ranges from 0 to $(p-1)/2$, we have $1 + (p-1)/2$ distinct congruence classes represented by a^2 (we add 1 to account for $a = 0$). Thus, a^2 represents $(p+1)/2$ distinct congruence classes modulo p.

Similarly, the integers b^2 are distinct, so the integers $-1 - b^2$ are also distinct and represent $(p+1)/2$ congruence classes.

By the pigeonhole principle, there are a and b in this range such that a^2 and $-1-b^2$ are congruent modulo p. That is, there exist $a, b \in \mathbb{Z}$ such that

$$p \mid a^2 + b^2 + 1 \iff np = 1 + a^2 + b^2$$

proving the desired result. □

Problem .1.19. Let $\mathbb{I} \subseteq \mathbb{H}$ be the set of quaternions (cf. Exercise III.1.12) of the form $\frac{a}{2}(1+i+j+k) + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$.

- Prove that $\mathbb{I}$ is a (noncommutative) subring of the ring of quaternions.
- Prove that the norm $N(w)$ (Exercise III.2.5) of an integral quaternion $w \in \mathbb{I}$ is an integer and $N(w_1 w_2) = N(w_1)N(w_2)$.
- Prove $\mathbb{I}$ has exactly 24 units in $\mathbb{I}$: $\pm 1, \pm i, \pm j, \pm k$, and $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$.
- Prove that every $w \in \mathbb{I}$ is an associate of an element $a + bi + cj + dk \in \mathbb{I}$ with $a, b, c, d \in \mathbb{Z}$.

The ring $\mathbb{I}$ is called the ring of *integral quaternions.*

Solution. It is clear that $\mathbb{I}$ is closed additively and has an additive identity, namely 0. Furthermore, we can verify that $\mathbb{I}$ is closed under multiplication by writing down the product of two quaternions and substituting the coefficients of $1, i, j, k$ by half-integers (elements of the set $\mathbb{Z} + \frac{1}{2}$. Doing so shows that the product is still composed of half integers and is thus an element of $\mathbb{I}$. The multiplicative identity is 1. Thus, $\mathbb{I}$ is a subring of $\mathbb{H}$.

Recall that the norm of a quaternion $w = a + bi + cj + dk$ is given by $N(w) = a^2 + b^2 + c^2 + d^2$. Given an element $w \in \mathbb{I}$, we have

$$\begin{aligned} N(w) &= \frac{a^2}{4} + \left(\frac{a}{2} + b\right)^2 + \left(\frac{a}{2} + c\right)^2 + \left(\frac{a}{2} + d\right)^2 \\ &= a^2 + b^2 + c^2 + d^2 + ab + ac + ad \end{aligned}$$

which is an integer. The multiplicativity of the norm is inherited from $\mathbb{H}$.

Recall that if $u \in \mathbb{I}$ is a unit then there is some element $v \in \mathbb{I}$ such that $uv = 1$. But then $N(uv) = N(u)N(v) = 1$ so $N(u)$ is a unit in $\mathbb{Z}$ and we must have

$$a^2 + b^2 + c^2 + d^2 + ab + ac + ad = \pm 1.$$

Clearly $\pm 1, \pm i, \pm j, \pm k$ satisfy this, as do $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. I'm not sure how to verify that these are the *only* units but they are certainly units.

Now we show that every $w \in \mathbb{I}$ is associate to a quaternion with integer coefficients. First note that if a is even then $a/2$ is an integer and we are done. Now suppose a is odd. Then we can multiply by $\frac{1}{2}(1 \pm i \pm j \pm k)$ where the sign is positive if the associated coefficient is odd and even if the associated coefficient is negative. It is tedious to show this case by case so just trust me. Since we are multiplying by a unit, the ideal generated by this product and w are the same, so the two are associate. □

Problem .1.20. Let $\mathbb{I}$ be as in Exercise 6.19. Prove that $\mathbb{I}$ shares most good properties of a Euclidean domain, notwithstanding the fact that it is noncommutative.

- Let $z, w \in \mathbb{I}$, with $w \neq 0$. Prove that $\exists q, r \in \mathbb{I}$ such that $z = qw + r$, with $N(r) < N(w)$. (This is a little tricky; don't feel too bad if you have to cheat and look it up somewhere.)
- Prove that every left-ideal in $\mathbb{I}$ is of the form $\mathbb{I}w$ for some $w \in \mathbb{I}$.
- Prove that every $z, w \in \mathbb{I}$, not both zero, have a 'greatest common right-divisor' d in $\mathbb{I}$, of the form $\alpha z + \beta w$ for $\alpha, \beta \in \mathbb{I}$.

Solution. Consider the element $x = z/w$ and construct x_0 with each component of x rounded to the nearest integer so that $x \in \mathbb{I}$. Then we have $|x - x_0| \leq (1/2)^2 \cdot 4 = 1$. Let $r = x - x_0$. If $|r| < 1$ then we have $z = wx_0 + wr$, where $N(wr) = N(w)N(r) < N(w)$. If $|r| = 1$, then each component of r has absolute value $\frac{1}{2}$ so r is a unit in $\mathbb{I}$. But then $x' = x + r \in \mathbb{I}$ and we find

$$x = r + x_0 = x' \Longrightarrow z = wx' + 0.$$

Since $N(0) = 0$, we are done.

Let I be an ideal of $\mathbb{I}$. Clearly if $I = 0$, then $w = 0$ so assume $I \neq 0$. Then pick $w \in I$ with minimal norm. Clearly $(w) \subseteq I$. Now let $z \in I$. By division in $\mathbb{I}$, there exist $q, r \in \mathbb{I}$ such that $z = qw + r$. If $r = 0$ then $z \in (w)$ and we are done. Otherwise, we have $r = z - qw \in I$ and $N(r) < N(w)$. However, we assumed w had minimal norm in I, a contradiction. Thus, $r = 0$ is the only case. That is, $I = (w)$.

Given $z, w \in \mathbb{I}$, consider an application of division with remainder.

$$\begin{aligned} z &= q_1 w + r_1 \\ w &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \end{aligned}$$

where $N(r_i) < N(q)$. Clearly this process must terminate so for some r_{n+1}, we have $N(r_{n+1}) = 0 \Longrightarrow r_{n+1} = 0$, or $r_{n-1} = q_{n+1} r_n$. We claim that $d = r_n$. It is easy to see that $r_n \mid z$ and $r_n \mid w$ so assume that x is any divisor of both z and w. We have $x \mid z - q_1 w = r_1$. Repeating this process for each step in the 'Euclidean algorithm' shows that $x \mid r_n$. Thus, r_n is the greatest common right-divisor for z and w. Furthermore, it can easily be rewritten in the form $\alpha z + \beta w$ by reversing the steps of the algorithm and substituting values for the remainders. □

Problem .1.21. Prove Lagrange's theorem on four squares. Use notation as in Exercise 6.19 and 6.20.

- Let $z \in \mathbb{I}$ and $n \in \mathbb{Z}$. Prove that the greatest common right-divisor of z and n in $\mathbb{I}$ is 1 if and only if $(N(z), n) = 1$ in $\mathbb{Z}$. (If $\alpha z + \beta n = 1$, then $N(\alpha)N(z) = N(1 - \beta n) = (1 - \beta n)(1 - \bar{\beta} n)$, where $\bar{\beta}$ is obtained by changing the signs of the coefficients of i, j, k. Expand, and deduce that $(N(z), n) \mid 1$.)
- For an odd prime integer p, use Exercise 6.18 to obtain an integral quaternion $z = 1 + ai + bj$ such that $p \mid N(z)$. Prove that z and p have a common right-divisor that is not a unit and not an associate of p.
- Say that $w \in \mathbb{I}$ is *irreducible* if $w = \alpha\beta$ implies that either α or β is a unit. Prove that integer primes are *not* irreducible in $\mathbb{I}$. Deduce that every positive prime integer is the norm of some integral quaternion.
- Prove that every positive integer is the norm of some integral quaternion.
- Finally, use the last point of Exercise 6.19 to deduce that every positive integer may be written as the sum of four perfect squares.

Solution. First assume $(N(z), n) = 1$ and let w be a common divisor of z and n. Then $N(w) \mid N(z)$ and $N(w) \mid N(n) = n$ so $N(w) \mid 1$ and $N(w) = 1$. Thus, w is a unit in $\mathbb{I}$ and is associate to 1. Now suppose the gcrd of z and n is 1. By Problem 6.20, we can write $1 = \alpha z + \beta n$ for $\alpha, \beta \in \mathbb{I}$. Then we find

$$N(\alpha)N(z) = N(1 - \beta n) = (1 - \beta n)(1 - \bar{\beta} n),$$

where $\bar{\beta}$ is obtained by reversing the signs of i, j, k. Expanding this yields

$$N(\alpha)N(z) = 1 - bn + N(\beta)n^2$$

where b is the real component of β. Since $N(\alpha)$ and $N(\beta)n - b$ are elements of $\mathbb{Z}$, we can find $a_1, a_2 \in \mathbb{I}$ to represent them. Thus, we can rearrange the above equation to yield

$$a_1 N(z) + a_2 n = 1,$$

implying that $\gcd(N(z), n) = 1$.

By Exercise 6.18, there is some n, $0 < n < p$ such that $np = 1 + a^2 + b^2$. That is, $p \mid 1 + a^2 + b^2$. Now consider the integral quaternion $z = 1 + ai + bj$. Clearly $N(z) = 1 + a^2 + b^2$ so $p \mid N(z)$. By the above point, the greatest common right-divisor of p and z is not 1 because $\gcd(p, N(z)) = p$. Furthermore, since z is a proper integral quaternion, $p \nmid z$ and the two are not associate.

As shown above, an odd integer prime p divides the norm of some integral quaternion z, and the two have a common right-divisor, say w. Then we can write $p = wx$ for some $x \in \mathbb{I}$ where neither are units. For every positive prime integer, we have $p \mid 1 + a^2 + b^2$. Let $\alpha = 1 + ai + bj$ and w be the gcd of p and α. Then $p = z_1 w$ and $\alpha = 1 + ai + bj = z_2 w$ and we can write

$$N(p) = N(z_1)N(w) = p^2.$$

Since $N(w) \neq 1$ and $N(w) \neq p^2$, we must have $N(z_1) = N(w) = p$. Thus, p is the norm of some integral quaternion.

To see that every postitive integer is the norm of some integral quaternion, it suffices to show that the product of any two primes is the norm of an integral quaternion. Indeed, if $p_1 = N(z_1)$ and $p_2 = N(z_2)$, then

$$p_1 p_2 = N(z_1)N(z_2) = N(z_1 z_2)$$

so $p_1 p_2$ is the norm of an integral quaternion. Since any postive integer n has a decomposition into primes, n is the norm of some integral quaternion.

Finally, let n be a positive integer and suppose $n = N(z)$ for some $z \in \mathbb{I}$. By Exercise 6.19, z is associate to some integral quaternion w of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$. But then $N(z) = N(w)$ so

$$n = a^2 + b^2 + c^2 + d^2$$

proving that every positive integer is a sum of four perfect squares. $\square$