[03.1] Let $R = \mathbb{Z}/13$ and $S = \mathbb{Z}/221$. Show that the map

$$f : R \to S$$

defined by $f(n) = 170 \cdot n$ is *well-defined* and is a ring homomorphism. (Observe that it does not map $1 \in R$ to $1 \in S$.)

The point is that $170 = 1 \bmod 13$ and $170 = 17 \cdot 10 = 0 \bmod 17$, and $221 = 13 \cdot 17$. Thus, for $n' = n + 13\ell$,

$$170 \cdot n' = 17 \cdot 10 \cdot n + 10 \cdot 17 \cdot 13 = 17 \cdot 10 \cdot n \bmod 13 \cdot 17$$

so the map is well-defined. Certainly the map respects addition, since

$$170(n + n') = 170n + 170n'$$

That it respects multiplication is slightly subtler, but we verify this separately modulo 13 and modulo 17, using unique factorization to know that if $13|N$ and $17|N$ then $(13 \cdot 17)|N$. Thus, since $170 = 1 \bmod 13$,

$$170(nn') = 1 \cdot (nn') = nn' = (170n) \cdot (170n') \bmod 13$$

And, since $17 = 0 \bmod 17$,

$$170(nn') = 0 \cdot (nn') = 0 = (170n) \cdot (170n') \bmod 17$$

Putting these together gives the multiplicativity.

[03.2] Let p and q be distinct prime numbers. Show directly that there is no field with pq elements.

There are several possible approaches. One is to suppose there exists such a field k, and first invoke Sylow (or even more elementary results) to know that there exist (non-zero!) elements x, y in k with (additive) orders p, q, respectively. That is, $p \cdot x = 0$ (where left multiplication by an ordinary integer means repeated addition). Then claim that $xy = 0$, contradicting the fact that a field (or even integral domain) has no proper zero divisors. Indeed, since p and q are distinct primes, $\gcd(p, q) = 1$, so there are integers r, s such that $rp + sq = 1$. Then

$$xy = 1 \cdot xy = (rp + sq) \cdot xy = ry \cdot px + sx \cdot qy = ry \cdot 0 + sx \cdot 0 = 0$$

[03.3] Find all the idempotent elements in $\mathbb{Z}/n$.

The idempotent condition $r^2 = r$ becomes $r(r-1) = 0$. For each prime p dividing n, let p^e be the exact power of p dividing n. For the image in $\mathbb{Z}/n$ of an ordinary integer b to be idempotent,, it is necessary and sufficient that $p^e | b(b-1)$ for each prime p. Note that p cannot divide both b and $b-1$, since $b - (b-1) = 1$. Thus, the condition is $p^e | b$ *or* $p^e | b - 1$, for each prime p dividing n. Sun-Ze's theorem assures that we can choose either of these two conditions for each p as p various over primes dividing n, and be able to find a simultaneous solution for the resulting family of congruences. That is, let $p_1, \ldots, p_t$ be the distinct primes dividing n, and let $p_i^{e_i}$ be the exact power of p_i dividing n. For each p_i choose $\varepsilon_i \in \{0, 1\}$. Given a sequence $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_t)$ of 0s and 1s, consider the collection of congruences $p_i^{e_i} | (b - \varepsilon_i)$, for $i = 1, \ldots, t$. Sun-Ze guarantees that there is a solution, and that it is unique mod n. Thus, each of the 2^t choices of sequences of 0s and 1s gives an idempotent.

[03.4] Find all the nilpotent elements in $\mathbb{Z}/n$.

For each prime p dividing n, let p^e be the exact power of p dividing n. For the image in $\mathbb{Z}/n$ of an ordinary integer b to be nilpotent,, it is necessary and sufficient that for some n sufficiently large $p^e | b^n$ for each prime p. Then surely $p | b^n$, and since p is prime $p | b$. And, indeed, if every prime dividing n divides b, then a sufficiently large power of b will be 0 modulo p^e, hence (by unique factorization, etc.) modulo n. That is, for b to be nilpotent it is necessary and sufficient that every prime dividing n divides b.

[03.5] Let $R = \mathbb{Q}[x]/(x^2-1)$. Find e and f in R, neither one 0, such that

$$e^2 = e \quad f^2 = f \quad ef = 0 \quad e+f = 1$$

(Such e and f are **orthogonal** idempotents.) Show that the maps $p_e(r) = re$ and $p_f(r) = rf$ are ring homomorphisms of R to itself.

Let ξ be the image of x in the quotient. Then $(\xi-1)(\xi+1) = 0$. Also note that

$$(\xi-1)^2 = \xi^2 - 2\xi + 1 = (\xi^2-1) - 2\xi + 2 = -2\xi + 2$$

so

$$\left(\frac{\xi-1}{2}\right)^2 = \frac{\xi^2-2\xi+1}{4} = \frac{(\xi^2-1)-2\xi+2}{4} = \frac{-\xi+1}{2}$$

Similarly,

$$\left(\frac{\xi+1}{2}\right)^2 = \frac{\xi^2+2\xi+1}{4} = \frac{(\xi^2-1)+2\xi+2}{4} = \frac{\xi+1}{2}$$

Thus, $e = (-\xi+1)/2$ and $f = (\xi+1)/2$ are the desired orthogonal idempotents.

[03.6] Prove that in $(\mathbb{Z}/p)[x]$ we have the factorization

$$x^p - x = \prod_{a\in\mathbb{Z}/p} (x-a)$$

By Fermat's Little Theorem, the left-hand side is 0 when x is replaced by any of $0, 1, 2, \ldots, p-1$. Thus, by unique factorization in $k[x]$ for k a field (which applies to $\mathbb{Z}/p$ since p is prime), all the factors $x-0$, $x-1$, $x-2$, …, $x-(p-1)$ divide the left-hand side, and (because these are mutually relatively prime) so does their product. Their product is the right hand side, which thus at least *divides* the left hand side. Since degrees add in products, we see that the right hand side and left hand side could differ at most by a unit (a polynomial of degree 0), but both are *monic*, so they are identical, as claimed.

[03.7] Show that $\mathbb{Z}[x]$ has non-maximal non-zero prime ideals.

(See Notes for examples and discussion.)

[03.8] Show that $\mathbb{C}[x, y]$ has non-maximal non-zero prime ideals.

(See Notes for examples and discussion.)

[03.9] Let $\omega = (-1+\sqrt{-3})/2$. Prove that

$$\mathbb{Z}[\omega]/p\mathbb{Z}[\omega] \approx (\mathbb{Z}/p)[x]/(x^2+x+1)(\mathbb{Z}/p)[x]$$

and, as a consequence, that a prime p in $\mathbb{Z}$ is expressible as x^2+xy+y^2 with integers x, y if and only if $p = 1 \bmod 3$ (apart from the single anomalous case $p = 3$).

If a prime is expressible as $p = a^2+ab+b^2$, then, modulo 3, the possibilities for p modulo 3 can be enumerated by considering $a = 0, \pm1$ and $b = 0, \pm1 \bmod 3$. Noting the symmetry that $(a, b) \to (-a, -b)$ does not change the output (nor does $(a, b) \to (b, a)$) we reduce from $3 \cdot 3 = 9$ cases to a smaller number:

$$p = a^2+ab+b^2 = \begin{cases} 0^2+0\cdot 0+0^2 & = & 1 & \bmod 3 \\ 1^2+1\cdot 1+1^2 & = & 0 & \bmod 3 \\ 1^2+1\cdot(-1)+(-1)^2 & = & 1 & \bmod 3 \end{cases}$$

Thus, any prime p expressible as $p = a^2 + ab + b^2$ is either 3 or is 1 mod 3.

On the other hand, suppose that $p = 1 \bmod 3$. If p were expressible as $p = a^2 + ab + b^2$ then

$$p = (a + b\omega)(a + b\overline{\omega})$$

where $\omega = (-1 + \sqrt{-3})/2$. That is, p is expressible as $a^2 + ab + b^2$ if and only if p factors in a particular manner in $\mathbb{Z}[\omega]$.

Let $N(a + b\omega) = a^2 + ab + b^2$ be the usual (square-of) norm. To determine the units in $\mathbb{Z}[\omega]$, note that $\alpha \cdot \beta = 1$ implies that

$$1 = N(\alpha) \cdot N(\beta)$$

, and these norms from $\mathbb{Z}[\omega]$ are integers, so units have norm 1. By looking at the equation $a^2 + ab + b^2 = 1$ with integers a, b, a little fooling around shows that the only units in $\mathbb{Z}[\omega]$ are ± 1, $\pm\omega$ and $\pm\omega^2$. And norm 0 occurs only for 0.

If $p = \alpha \cdot \beta$ is a proper factorization, then by the multiplicative property of N

$$p^2 = N(p) = N(\alpha) \cdot N(\beta)$$

Thus, since neither α nor β is a unit, it must be that

$$N(\alpha) = p = N(\beta)$$

Similarly, α and β must both be irreducibles in $\mathbb{Z}[\omega]$, since applying N to any proper factorization would give a contradiction. Also, since p is its own complex conjugate,

$$p = \alpha \cdot \beta$$

implies

$$p = \overline{p} = \overline{\alpha} \cdot \overline{\beta}$$

Since we know that the (Eisenstein) integers $\mathbb{Z}[\omega]$ are Euclidean and, hence, have unique factorization, it must be that these two prime factors are the same *up to units*.

Thus, either $\alpha = \pm\overline{\alpha}$ and $\beta = \pm\overline{\beta}$ (with matching signs), or $\alpha = \pm\omega\overline{\alpha}$ and $\beta = \pm\omega^2\overline{\beta}$, or $\alpha = \pm\omega^2\overline{\alpha}$ and $\beta = \pm\omega\overline{\beta}$, or $\alpha = u\overline{\beta}$ with u among $\pm 1, \pm\omega, \pm\omega^2$. If $\alpha = \pm\overline{\alpha}$, then α is either in $\mathbb{Z}$ or of the form $t \cdot \sqrt{-3}$ with $t \in \mathbb{Z}$. In the former case its norm is a square, and in the latter its norm is divisible by 3, neither of which can occur. If $\overline{\alpha} = \omega\alpha$, then $\alpha = t \cdot \omega$ for some $t \in \mathbb{Z}$, and its norm is a square, contradiction. Similarly for $\alpha = \pm\omega^2\overline{\alpha}$.

Thus, $\alpha = u\overline{\beta}$ for some unit u, and $p = uN(\beta)$. Since $p > 0$, it must be that $u = 1$. Letting $\alpha = a + b\omega$, we have recovered an expression

$$p = a^2 + ab + b^2$$

with neither a nor b zero.

Thus, a prime integer $p > 3$ is expressible (properly) as $a^2 + ab + b^2$ of two squares if and only if it is *not prime* in $\mathbb{Z}[\omega]$. From above, this is equivalent to

$$\mathbb{Z}[\omega]/\langle p \rangle \text{ is not an integral domain}$$

We grant that for $p = 1 \bmod 3$ there is an integer α such that $\alpha^2 + alf + 1 = 0 \bmod p$. [1] That is, (the image of) the polynomial $x^2 + x + 1$ factors in $(\mathbb{Z}/p)[x]$.

---

[1] If we grant that there are primitive roots modulo primes, that is, that $(\mathbb{Z}/p)^\times$ is cyclic, then this assertion follows from basic and general properties of cyclic groups. Even without knowledge of primitive roots, we can still give a special argument in this limited case, as follows. Let $G = (\mathbb{Z}/p)^\times$. This group is abelian, and has order divisible by 3. Thus, for example by Sylow theorems, there is a 3-power-order subgroup A, and, thus, at least one element of order exactly 3.

Note that we can rewrite $\mathbb{Z}[\omega]$ as

$$\mathbb{Z}[x]/\langle x^2 + x + 1\rangle$$

Then

$$\mathbb{Z}[\omega]/\langle p\rangle \approx \left(\mathbb{Z}[x]/\langle x^2+1\rangle\right)/\langle p\rangle \approx \left(\mathbb{Z}[x]/\langle p\rangle\right)/\langle x^2+1\rangle \approx (\mathbb{Z}/p)[x]/\langle x^2+1\rangle$$

and the latter is *not* an integral domain, since

$$x^2 + x + 1 = (x-\alpha)(x-\alpha^2)$$

is not irreducible in $(\mathbb{Z}/p)[x]$. That is, $\mathbb{Z}[\omega]/\langle p\rangle$ is not an integral domain when p is a prime with $p = 1 \bmod 3$. That is, p is not irreducible in $\mathbb{Z}[\omega]$, so factors properly in $\mathbb{Z}[\omega]$, thus, as observed above, p is expressible as $a^2 + ab + b^2$. ///