7210 HW 9

Duncan Wilkie

8 November 2022

Problem 1 (D&F 8.3.1)**.** *Let $G = \mathbb{Q}^\times$ be the multiplicative group of nonzero rational numbers. If $\alpha = p/q \in G$, where p and q are relatively prime integers, let $\varphi : G \to G$ be the map which interchanges the primes 2 and 3 in the prime power factorizations of p and q (so, for example, $\varphi(2^4 3^{11} 5^1 13^2) = 3^4 2^{11} 5^1 13^2$, $\varphi(3/16) = \varphi(3/2^4) = 2/3^4 = 2/81$, and φ is the identity on all rational numbers with numerators and denominators relatively prime to 2 and 3).*

1. *Prove that φ is a group isomorphism.*
2. *Prove that there are infinitely many isomorphisms of the group G to itself.*
3. *Prove that none of the isomorphisms above can be extended to an isomorphism of the **ring** $\mathbb{Q}$ to itself. In fact, prove that the identity map is the only ring isomorphism of $\mathbb{Q}$.*

Proof. First, φ is a homomorphism:

$$\varphi(ab) = \varphi\left(\frac{2^{\epsilon_1}3^{\epsilon_2}p_3^{\epsilon_3}\cdots p_n^{\epsilon_n}2^{\varepsilon_1}3^{\varepsilon_2}r_3^{\varepsilon_3}\cdots r_m^{\varepsilon_m}}{2^{\sigma_1}3^{\sigma_2}q_3^{\sigma_3}\cdots q_j^{\sigma_j}2^{\varsigma_1}3^{\varsigma_2}s_3^{\varsigma_3}\cdots s_k^{\varsigma_k}}\right)$$

$$= \frac{3^{\epsilon_1}2^{\epsilon_2}p_3^{\epsilon_3}\cdots p_n^{\epsilon_n}3^{\varepsilon_1}2^{\varepsilon_2}r_3^{\varepsilon_3}\cdots r_m^{\varepsilon_m}}{3^{\sigma_1}2^{\sigma_2}q_3^{\sigma_3}\cdots q_j^{\sigma_j}3^{\varsigma_1}2^{\varsigma_2}s_3^{\varsigma_3}\cdots s_k^{\varsigma_k}}$$

$$= \varphi\left(\frac{2^{\epsilon_1}3^{\epsilon_2}p_3^{\epsilon_3}\cdots p_n^{\epsilon_n}}{2^{\sigma_1}3^{\sigma_2}q_3^{\sigma_3}\cdots q_j^{\sigma_j}}\right)\varphi\left(\frac{2^{\varepsilon_1}3^{\varepsilon_2}r_3^{\varepsilon_3}\cdots r_m^{\varepsilon_m}}{2^{\varsigma_1}3^{\varsigma_2}s_3^{\varsigma_3}\cdots s_k^{\varsigma_k}}\right) = \varphi(a)\varphi(b)$$

It is also bijective: it's self-inverse, as swapping 2 and 3 and then swapping them again yields the same prime factorization, so $\varphi(\varphi(a)) = a$; this implies φ is bijective.

The choice of interchanging 2 and 3 was arbitrary; the proof holds for a function interchanging *any* two primes p, p' by replacing the symbols 2 and 3 (when not appearing in a subscript or superscript) by p and p'. Since there are infinitely many primes, there are infinitely many pairs of primes, and so this exhibits infinitely many automorphisms of G.

Suppose $\phi : \mathbb{Q} \to \mathbb{Q}$ is a ring isomorphism. Then, in particular, $1 \mapsto 1$; since for all integers $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$, $\phi(n) = \underbrace{\phi(1) + \cdots + \phi(1)}_{n \text{ times}} = n$. Additionally, $\phi\big(\frac{n}{m}\big) = \phi\big(n \cdot \frac{1}{m}\big) = \phi(n)\phi(m)^{-1} = nm^{-1} = \frac{n}{m}$, so $\phi = id_{\mathbb{Q}}$. □

Problem 2 (D&F 8.3.5)**.** *Let $R = \mathbb{Z}[\sqrt{-n}]$ where n is a squarefree integer greater than 3.*

1. *Prove that 2, $\sqrt{-n}$, and $1 + \sqrt{-n}$ are irreducible in R.*

2. *Prove that R is not a U.F.D. Conclude that the quadratic integer ring $\mathcal{O}$ is not a U.F.D. for $D \equiv 2, 3 \pmod 4$, $D < -3$ (so also not Euclidean and not a P.I.D.).*

3. *Give an explicit ideal in R that is not principal.*

Proof. Restricting the complex absolute value to $\mathbb{Z}[\sqrt{-n}]$, the norm of $a+b\sqrt{-n}$ is a^2+nb^2. First, note that this norm is positive-definite, and there do not exist elements of R of norm 2: if $N(a+b\sqrt{-n}) = a^2 + nb^2 = 2$, one must have $b = 0$, since a^2, b^2 being positive and $n > 3$ implies that even $b = 1$ yields $a^2 + nb^2 > 3 > 2$. But, neither 0 nor 1 squares to 2, and if $a \geq 2$ then $a^2 \geq 4$. So, there do not exist elements of $\mathbb{Z}[\sqrt{-n}]$ that have norm 2. Similarly, if $N(a + b\sqrt{-n}) = a^2 + nb^2 = 1$, then $a = 1$ and $b = 0$, as if $b \geq 1$ then $n > 3$ makes it too big already. Since the norm is multiplicative on $\mathbb{C}$, it is multiplicative on $\mathbb{Z}[\sqrt{-n}]$. Suppose $2 = (a + b\sqrt{-n})(c + d\sqrt{-n})$; then $N(2) = 4 = N(a + b\sqrt{-n})N(c + d\sqrt{-n})$. The only way to factor 4 as a product of nonnegative integers (which is what the norm will output) is as $1 \cdot 4$, $4 \cdot 1$, or $2 \cdot 2$. In either of the first two cases, the argument about norm-1 elements implies one factor is 1 and therefore a unit, and the last is prohibited by the argument about norm-2 elements; accordingly, 2 is irreducible.

Suppose $\sqrt{-n}$ is reducible. Then, as the norm is multiplicative, there must exist some element whose norm divides that of n; its norm is less than or equal than n. Elements with norm at most n have $a^2 + nb^2 \leq n$; if $b > 1$, then things are already too big, and since n is squarefree, $b \neq 0$, (as otherwise $a^2 \mid n$) so we can only have $b = 1$. In such a case, one rearrange to get $a = 0$ as the only solution; accordingly, $\sqrt{-n}$ is the only element whose norm divides n, and it is on those grounds irreducible.

Suppose $1 + \sqrt{-n}$ is reducible. Then, as the norm is multiplicative, there must exist some element whose norm divides $1 + n$; its norm is less than or equal to $1 + n$. If it's of the form $a + b\sqrt{-n}$, $a^2 + nb^2 \leq n + 1$; if $b > 1$, then the norm is $\geq 4n$—too big already. If $b = 0$, then the factor is a mere integer; if any other element of R is to exist such that $a(c + d\sqrt{-n}) = 1 + \sqrt{-n}$, then $ad = 1$, so $a = d = 1$ or $a = d = -1$. Therefore, $b = 1$ is the only possible choice. Solving the inequality, one gets $a^2 \leq 1 \Rightarrow a = 1$, so the only elements whose norm divides that of $1 + \sqrt{-n}$ are either $1 + \sqrt{-n}$ itself, or have no $\sqrt{-n}$ part and so can't divide $1 + \sqrt{-n}$. This implies $1 + \sqrt{-n}$ is irreducible.

Were R a U.F.D., it would have the property that being irreducible is equivalent to being prime. We've shown that 2 is irreducible, but it is never prime. If n is even, then $2 \mid \sqrt{-n}\sqrt{-n} = -n$, but $\sqrt{-n}$ is irreducible, so $2 \nmid \sqrt{-n}$, so 2 isn't prime. If n is odd, then $2 \mid (1 + \sqrt{-n})(1 + \sqrt{-n}) = (1-n)+2\sqrt{-n}$, since it divides each summand, but $1+\sqrt{-n}$ is irreducible, so $2 \nmid 1+\sqrt{-n}$, meaning 2 isn't prime. Therefore, R isn't a U.F.D.

If n is even, then the ideal $(2, \sqrt{-n})$ is not principal: presuming it had generator d, then for all $x, y \in R$ $2x + y\sqrt{-n} = dz$ for some $z \in R$; in particular, for $x = 1, y = 0$ one has $2 = dz$. Since 2 is irreducible, then exactly one of d, z is a unit. If it's d, then the ideal is the whole ring, so there exist x, y such that $1 = 2x + y\sqrt{-n}$; multiplying by $\sqrt{-n}$, this implies $\sqrt{-n} = 2x\sqrt{-n} + y\sqrt{-n}^2$, and since we showed above that $2 \mid \sqrt{-n}^2 = -n$, the right-hand side is divisible by 2, which would imply $2 \mid \sqrt{-n}$, which is false since $\sqrt{-n}$ is irreducible. If z is a unit, then d is irreducible, and $d = 2z^{-1}$. One can instead choose $x = 0, y = 1$ do deduce that $d \mid \sqrt{-n}$; since $2 \mid d$ by the above, this would also imply $2 \mid \sqrt{-n}$, which is false since $\sqrt{-n}$ is irreducible.

For n odd, merely textually substitute $(1 + \sqrt{-n})$ for $\sqrt{-n}$ in the preceding paragraph. $\square$

Problem 3 (D&F 8.3.10a). *Let R be an integral domain and let $N : R \to \mathbb{Z}^+ \cup \{0\}$ be a norm on R. The ring R is Euclidean with respect to N if for any $a, b \in R$ with $b \neq 0$, there exist elements q and r in R with*

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b).$$

Suppose now that this condition is weakened, namely that for any $a, b \in R$ with $b \neq 0$, there exist elements q, q' and r, r' in R with

$$a = qb + r, b = q'r + r' \text{ with } r' = 0 \text{ or } N(r') < N(b),$$

i.e., the remainder after two divisions is smaller. Call such a domain a ***2-stage Euclidean domain.*** *Prove that iterating the divisions in a 2-stage Euclidean domain produces a greatest common divisor of a and b which is a linear combination of a and b. Conclude that every finitely generated ideal of a 2-stage Euclidean domain is principal.*

Proof. The division algorithm tells us that for any $a, b \in R$ there's a finite (since the norm is decreasing and bounded below) sequence of equations

$$r_{-1} = a = q_0 b + r_0,\ r'_{-1} = b = q'_0 r_0 + r'_0$$

$$r_0 = q_1 r'_0 + r_1,\ r'_0 = q'_1 r_1 + r'_1$$

$$\vdots$$

$$r_{n-2} = q_{n-1} r'_{n-2} + r_{n-1},\ r'_{n-2} = q'_{n-1} r_{n-1} + r'_{n-1}$$
$$r_{n-1} = q_n r'_{n-1} + r_n,\ r'_{n-1} = q'_n r_n + 0.$$

By induction on $0 \leq k \leq n$ indexing the $n+1-k$th statement, with the hypothesis $r_n \mid r_{n-k-1}$ and $r_n \mid r_{n-k-1}$, one has that r_n divides both a and b. For $k = 0$, $r'_{n-1} = q'_n r_n \Rightarrow r_n \mid r'_{n-1}$; accordingly, $r_n \mid q_n r'_{n-1}$, and certainly $r_n \mid r_n$, so $r_n \mid r_{n-1} = q_n r'_{n-1} + r_n$. Suppose it holds that $r_n \mid r_{n-k}$ and $r_n \mid r_n \mid r'_{n-k}$. Then, one has

$$r_{n-(k+1)} = q_{n-k} r'_{n-k-1} + r_{n-k},\ r'_{n-k-1} = q'_{n-k} r_{n-k} + r'_{n-k}$$

In the last equation, one has by the induction hypothesis that $r_n \mid r_{n-k-1}$, since it divides each summand; accordingly, r_n divides each summand in the former equation, and so divides $r_{n-(k+1)}$, proving the statement for any k. Taking $k = n$, one gets the property for the first statement, namely

$$r_n \mid r_{-1} = a,\ r_n \mid r'_{-1} = b.$$

Since r_n is a common divisor of a and b, one has $(a, b) \subseteq (r_n)$.

We next prove that $r_n = ax + by$ for some $x, y \in R$, so that $r_n \in (a, b) \Rightarrow (d) \subseteq (a, b)$. This is done by inducting in the other direction: let $1 \leq k \leq n+2$ be the kth statement, with the hypothesis that $r_{k-2} = ax + by$ and $r'_{k-2} = ax' + by'$. If $k = 1$, then $r_0 = a - q_0 b$ and $r'_0 = b - q'_0 r_0 = b - q'_0(a - q_0 b) = -q'_0 a + (1 + q_0 q'_0)b$, forming a base case. Suppose that the statement holds for some arbitrary k. Then

$$r_k = q_{k+1} r'_k - r_{k+1} \Leftrightarrow r_{k+1} = q_{k+1} r'_k - r_k = q_{k+1}(ax' + by') - (ax + by)$$
$$= a[q_{k+1} x' - x] + b[q_{k+1} y' - y]$$

and

$$r'_k = q'_{k+1} r_{k+1} + r'_{k+1} \Leftrightarrow r'_{k+1} = q'_{k+1} r_{k+1} - r'_k = q'_{k+1}[a(q_{k+1}x' - x) + b(q_{k+1}y' - y)] - (ax' + by')$$
$$= a\big[q'_{k+1}(q_{k+1}x' - x) - x'\big] + b\big[q'_{k+1}(q_{k+1}y' - y) - y'\big].$$

So, the statement holds for arbitrary k; consider in particular the last statement $k = n+1$:

$$r_{n-1} = q_n r'_{n-1} + r_n = ax + by,\ r'_{n-1} = q'_n r_n = ax' + by'$$
$$\Rightarrow r_n = ax + by - q_n r'_{n-1} = ax + by - q_n(ax' + by') = a(x + q_n x') + b(y + q_n y').$$

This proves that r_n is an R-linear combination of a and b; as elements of (a, b) are precisely such combinations, this implies that $r_n \in (a, b)$ and accordingly $(r_n) \subseteq (a, b)$, because multiples of $r_n = ax + by$ remain R-linear combinations of a and b.

The above shows that all ideals generated by two elements are principal. Suppose for induction that all ideals generated by n elements are principal. Any ideal I generated by $a_1, a_2, \ldots, a_n, a_{n+1}$ has elements of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n + a_{n+1}x_{n+1}$, where all $x_i \in R$. The induction hypothesis says that the ideal I_0 generated by $a_1, a_2, \ldots, a_n$ is principal, i.e. our $a_1x_1 + a_2x_2 + \cdots a_nx_n$ can be written dy for some $d \in I_0$ and some $y \in R$. Accordingly, the above arbitrary element of I can be written $dy + a_{n+1}x_{n+1}$, so $I = (d, a_{n+1})$. Once again, such ideals are principal by the main argument, so the arbitrary finitely-generated ideal I is principal. □

Problem 4 (D&F 8.3.11)**.** *Prove that R is a P.I.D iff R is a U.F.D. that is also a Bezout domain, that is, a domain in which every ideal generated by two elements is principal.*

Proof. If R is a P.I.D., then it is immediately a U.F.D., and ideals generated by two elements are principal because all ideals are principal.

Conversely, suppose R is a U.F.D. and a Bezout domain, and consider an arbitrary ideal I of R. Order elements of I according to their number of irreducible factors (a well-defined quantity, by the definition of a U.F.D). This is bounded below by zero, so it must have a least element; call it a. If any element $b \in I$ is not in (a), then $a \nmid b$. Since R is a Bezout domain, $(a, b) = (d)$ for some $d \in I$, and in particular for all $x, y \in R$, $ax + by = zd$ for some $z \in R$. Choosing $x = 1, y = 0$ shows that $d \mid a$, but a has the least number of irreducible factors in I; writing out the prime factorizations in $a = ud$ as $va_1a_2 \cdots a_n = v'u_1u_2 \cdots u_jd_1d_2 \cdots d_k$ where $j + k = n$, v, v' are units, and a_i, u_i, d_i are irreducible, one can see if $k < n$, then d has fewer irreducible factors than a, so u must be a unit.

However, choosing $x = 0, y = 1$ shows that $d \mid b$, but $d = u^{-1}a$, so $cu^{-1}a = b$, a contradiction with $a \nmid b$. So, all elements of I must be elements of (a), proving that I is principal; since I was arbitrary, R is a P.I.D. □

Problem 5 (D&F 9.3.3)**.** *Let F be a field. Prove that the set R of polynomials in $F[x]$ whose coefficient of x is equal to 0 is a subring of $F[x]$ and that R is not a U.F.D.*

Proof. Let $a = p_0 + p_1x + p_2x^2 + \cdots + p_nx^n, b = q_0 + q_1x + q_2x^2 + \cdots + q_nx^n \in R$, n is the greatest of the two polynomials degrees, $p_1 = q_1 = 0$, and where (even leading) coefficients are allowed to be zero. Then $a - b = (p_0 - q_0) + (p_2 - q_2)x^2 + \cdots + (p_n - q_n)x^n \in R$; the ith coefficient of ab is $\sum_{k=0}^{i} p_kq_{i-k}$, and in particular, the 1st coefficient is $\sum_{k=0}^{1} p_kq_{1-k} = p_0q_1 + p_1q_0 = p_0 \cdot 0 + 0 \cdot q_0 = 0$, so $ab \in R$.

The polynomials x^2 and x^3 are irreducible in R, intuitively, because one can't factor out an x. If $x^2 = p(x)q(x)$, then $\deg p(x), \deg q(x) \leq 2$; if either equals 2, then the other must have degree zero, so the only factorization where one of the terms has degree 2 and the other 0 is as $x^2 = (ux^2)(v)$ where $u, v \in F$ are units in R. It can't happen that both are of degree 1, since polynomials of such degree aren't in R, and if one is of degree zero, the other is of degree 2, which is reduces to the first case by commutativity. Thus, x^2 is irreducible. If $x^3 = p(x)q(x)$, then $\deg p(x), \deg q(x) \leq 3$; if either equals 3, then the other must have degree zero, so the only factorization where one of the terms has degree 3 and the other 0 is as $x^3 = (ux^3)(v)$ where $u, v \in F$ are units in R. It can't happen that one of the degrees is two, since then the degree of the other must be 1, and polynomials of such degree aren't in R, which also prohibits the case any of the degrees is zero; again, the case when one of the degrees is 0 reduces to the first case. Then x^3 is also irreducible.

However, this implies that $x^6 = x^3x^3 = x^2x^2x^2$ are two distinct factorizations of an element of R as a product of irreducibles, so R is not a U.F.D. $\square$

Problem 6 (D&F 9.3.4)**.** *Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subseteq \mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.*

1. *Prove that R is an integral domain and its units are ± 1.*
2. *Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1. Prove that these irreducibles are prime in R.*
3. *Show that x cannot be written as the product of irreducibles in R (in particular, x is not irreducible) and conclude that R is not a U.F.D.*
4. *Show x is not prime in R and describe the quotient ring $R/(x)$.*

Proof. Since any subring of an integral domain containing 1 is an integral domain, the ring of polynomials over a field is an integral domain, and R contains the 1 of $\mathbb{Q}[x]$, R is an integral domain. An element of a subring can only be a unit if it is also a unit in the parent ring, as its inverse is necessarily in the parent; the units of $\mathbb{Q}[x]$ are exactly $\mathbb{Q}$, so the only possible units are the constant polynomials in $\mathbb{Q}[x]$, which include the constant polynomials in R. Those constant polynomials form a further subring, $\mathbb{Z}$, in which the only units are ± 1, so these are the only units of R.

Suppose $f(x)$ is irreducible in R, meaning for all $p(x), q(x) \in R$ such that if $f(x) = p(x)q(x)$, one of $p(x), q(x)$ is a unit, i.e. equal to ± 1. Break into cases based on degree: if f has degree zero, $f = pq$ for $f, p, q \in \mathbb{Z}$ implying $p, q = \pm 1$ is precisely the definition of irreducibility in $\mathbb{Z}$, so f is a prime integer $\pm p$ for a positive prime p. If f has degree greater than zero, then it must have constant term equal to ± 1, as otherwise a prime (in $\mathbb{Z}$) divides the constant term; continuing to divide this prime through to the other terms with rational coefficients yields a (non-unit, since it has a non-constant term by the degree assumption) polynomial whose product with the prime divided by (which is also non-unit by definition of prime) equals the supposedly irreducible polynomial one started with. If a polynomial with constant coefficient ± 1 is reducible in $\mathbb{Q}[x]$, then the product of the factors' constant terms must be ± 1; the product formula gives the 0th coefficient of a product as the product of the constant terms of the factors alone. The product of two rational numbers being ± 1 implies that one is $\pm$ the inverse of the other, and since for the integers, the only units are ± 1, if an element of R is reducible in $\mathbb{Q}[x]$ then it must reduce into factors with constant coefficient ± 1, which are again an element of R. Accordingly, we've shown "in R, possibly irreducible constant coefficient, and reducible in $\mathbb{Q}[x] \Rightarrow$ reducible in R," so if an element is not reducible in $\mathbb{Q}[x]$, then it's either not in R, doesn't have a possibly irreducible constant coefficient, or is irreducible in $\mathbb{Q}[x]$; the first two cannot hold, so irreducible elements of R with degree larger than 0 are irreducible in $\mathbb{Q}[x]$ with constant coefficient ± 1. Since $\mathbb{Q}[x]$ is a polynomial ring over a field, it is a Euclidean domain, and so irreducible and prime are equivalent. Accordingly, these elements are also prime in the subring R, as if $a \mid bc \Rightarrow a \mid b \vee a \mid c$ for all b, c in a parent ring, then certainly the same holds when b, c are restricted to R.

If $x = p_1(x)p_2(x)\cdots p_n(x)$ for p_i irreducible, then the above implies that each p_i either is a prime integer or a non-constant polynomial with constant coefficient ± 1; the degrees must match, so that of the right must be 1, but then the only non-constant factor is a single degree-1 polynomial, as adding anything more would make this degree too big. Since all irreducible, degree-1 polynomials must have a constant term ± 1, and, consequently, the product must have a product of the primes making up the rest of the factors as its constant term, it is impossible for x to be factored into irreducibles. This implies R is not a U.F.D.

Since x is also not irreducible, it cannot be prime, as prime implies irreducible in a general integral domain. Accordingly, since R/I is an integral domain iff I is a prime ideal, and (x) is not a prime ideal by definition of a prime element, the quotient ring $R/(x)$ is not an integral domain. □

Problem 7 (D&F 9.4.1)**.** *Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$, p a prime*

1. $x^2 + x + 1$ *in* $\mathbb{F}_2[x]$.
2. $x^3 + x + 1$ *in* $\mathbb{F}_3[x]$.
3. $x^4 + 1$ *in* $\mathbb{F}_5[x]$.
4. $x^4 + 10x^2 + 1$ *in* $\mathbb{Z}[x]$.

Proof. x^2+x+1 has no root in $\mathbb{F}_2$ $(1+1+1 \equiv 0+0+1 = 1 \pmod 2)$, so it is irreducible. x^3+x+1 has root $x = 1$ in $\mathbb{F}_3$ $(1+1+1 \equiv 0 \pmod 3)$, so it is reducible; the linear factor with root 1 divides it, so $x^3+x+1 = (x-1)(x^2+x+2)$ (using $-2 \equiv 1 \pmod 3$); the latter has no roots $(0+0+2 \equiv 2 \pmod 3, 1+1+2 \equiv 1 \pmod 3, 1+2+2 \equiv 2 \pmod 3)$, and so this is a factorization into irreducibles. We have $(x^2+2)(x^2-2) = x^4-4 = x^4+1$ (since $-4 \equiv 1 \pmod 5$); x^2+2 has no root in $\mathbb{F}_5$ $(2 \equiv 2 \pmod 5, 3 \equiv 3 \pmod 5, 6 \equiv 1 \pmod 5, 11 \equiv 1 \pmod 5, 16 \equiv 1 \pmod 5)$ and so is irreducible, and likewise for x^2-2 $(-2 \equiv 3 \pmod 5, -1 \equiv 4 \pmod 5, 2 \equiv 2 \pmod 5, 7 \equiv 2 \pmod 5, 14 \equiv 4 \pmod 5)$.

Taking the quotient ring $\mathbb{Z}/5\mathbb{Z}$, the polynomial reduces to x^4+1 over $\mathbb{F}_5$, which is irreducible by the above; accordingly, it is also irreducible in $\mathbb{Z}[x]$. □

Appendix

This is entirely for my own records and interest. I attempted to argue in problem 8.3.5 that 2 was prime, which required a lot of bookkeeping to handle a bunch of cases. As such, I used notation inspired by Fitch notation for natural deduction to keep track of what's been refuted.

1	$2 \mid (a+b\sqrt{-n})(c+d\sqrt{-n})$	
2	$2 \mid (ac-bdn)+(ad+bc)\sqrt{-n}$	Distributing
3	$(2 \mid ac)$	$a \mid (b+c) \Leftrightarrow a \mid b \wedge a \mid c$ (2)
4	$(2 \mid bdn)$	$a \mid (b+c) \Leftrightarrow a \mid b \wedge a \mid c$ (2)
5	$(2 \mid ad)$	$a \mid (b+c) \Leftrightarrow a \mid b \wedge a \mid c$ (2)
6	$(2 \mid bc)$	$a \mid (b+c) \Leftrightarrow a \mid b \wedge a \mid c$ (2)
7	$2 \mid a \vee 2 \mid c$	2 is prime in $\mathbb{Z}$ (3)
8	$2 \mid b \vee 2 \mid d \vee 2 \mid n$	2 is prime in $\mathbb{Z}$ (4)
9	$2 \mid a \vee 2 \mid d$	2 is prime in $\mathbb{Z}$ (5)
10	$2 \mid b \vee 2 \mid c$	2 is prime in $\mathbb{Z}$ (6)
11	$2 \nmid a$	
12	$2 \mid c$	$\vee$-Elim (7)
13	$2 \mid d$	$\vee$-Elim (9)
14	$2 \mid (c+d\sqrt{-n})$	$a \mid (b+c) \Leftrightarrow a \mid b \wedge a \mid c$ (12, 13)
15	$2 \mid a$	
16	$2 \nmid c$	
17	$2 \mid b$	$\vee$-Elim (10)
18	$2 \mid (a+b\sqrt{-n})$	$a \mid (b+c) \Leftrightarrow a \mid b \wedge a \mid c$ (15, 17)
19	$2 \mid c$	
20	$2 \mid b$	
21	$2 \mid (a+b\sqrt{-n})$	$a \mid (b+c) \Leftrightarrow a \mid b \wedge a \mid c$ (15, 20)
22	$2 \nmid b$	
23	$2 \mid d \vee 2 \mid n$	$\vee$-Elim (8)
24	$2 \mid d$	
25	$2 \mid (c+d\sqrt{-n})$	$a \mid (b+c) \Leftrightarrow a \mid b \wedge a \mid c$ (19, 24)
26	$2 \nmid d$	
27	$2 \mid n$	$\vee$-Elim (23)
28	$4 \mid ad$	Product of two multiples of 2 (15, 19)
29	$4 \mid bdn$	$ac-bdn=2 \Rightarrow ac \pmod 4 = 2+bdn \pmod 4 = 0$

At this point, one is stuck; one might hope to find a modular or linear algebraic argument that leads to contradiction in this last case, but it's to no avail. However, the logical elimination of all of these cases provides a significant computational simplification. An even more naïve algorithm wouldn't be impossible to run, because the first example is pretty small, but this suggests seeking an algorithmic solution may be productive. I did the following, in GNU Guile:

```
(use-modules (srfi srfi-1) (ice-9 pretty-print))


;; Cartesian product of sets, implemented on lists.
(define (cart-product lists)
  (fold-right (lambda (xs ys)
                (append-map (lambda (x)
                              (map (lambda (y)
                                     (cons x y))
                                   ys))
                            xs))
              '(())
              lists))

;; Cartesian power of a single set, implemented on lists.
;; These first two functions
(define (cart-power xs n)
  (if (= n 1)
      (map list xs)
      (cart-product (map (lambda (-) xs)
                         (iota n)))))


;; Check if the 5-tuple of the form (a,b,c,d,n) representing the product
;; (a+b√−n)(c+d√−n) has the desired form.
;; Doesn't check for square-freeness, as that'd add factorization complexity;
;; it's easy enough to do that by inspection.
(define (suitable? five)
  (and
   (= (modulo (car five) 2) 0)
   (not (= (modulo (cadr five) 2) 0))
   (= (modulo (caddr five) 2) 0)
   (not (= (modulo (cadddr five) 2) 0))
   (> (car (cddddr five)) 3)))

;; Run through the pair products in R with entries smaller than ``limit''
;; that satisfy the criteria and check if they multiply to 2.
(define (check target limit start)
(filter (lambda (five)
          (= 2
             (- (* (car five)
                   (caddr five))
                (* (cadr five)
```

```
                  (cadddr five)
                  (car (cddddr five))))))
        (filter suitable?
               (cart-power (iota limit start) 5))))

(check 15 -2)
;; => ((2 1 4 1 6) (4 1 2 1 6) (4 1 8 5 6) (4 5 8 1 6) (8 1 4 5 6) ...)
```