Solutions 12

P12.1. Euclid proves that there are infinitely many prime integers in the following way: if $p_1, p_2, \dots, p_k$ are positive prime integers, then any prime factor of $1 + p_1\, p_2 \cdots p_k$ must be different from p_j for any $1 \leqslant j \leqslant k$.

i. Adapt this argument to show that the set of prime integers of the form $4\,n - 1$ is infinite.

ii. Adapt this argument to show that, for any field $\mathbb{K}$, there are infinitely many monic irreducible polynomials in $\mathbb{K}[x]$.

Solution.

i. By considering their remainder upon division by 4, we see that every positive prime integer, except for 2, has the form $4\,n \pm 1$ for some nonnegative integer n. Suppose that there are only finitely many primes $p_1, p_2, \dots, p_k$ of the form $4\,n - 1$. The integer $m := 4\,(p_1\, p_2 \cdots p_k) - 1$ is a product of positive prime integers. Since the product of two primes of the form $4\,n + 1$ also has the form $4\,n + 1$, the odd number m must be divisible by at least one prime of the form $4\,n - 1$. This prime factor of m is necessarily distinct from all p_j, because otherwise it would divide -1. Therefore, the set of prime integers of the form $4\,n - 1$ is infinite.

ii. Consider a nonempty finite set $\{f_1, f_2, \dots, f_k\}$ of monic irreducible polynomials in $\mathbb{K}[x]$. Since the principal ideal domain $\mathbb{K}[x]$ is also a unique factorization domain, the polynomial $1 + f_1 f_2 \cdots f_k$, which is not a unit, is a product of a unit and monic irreducible polynomials. Any monic irreducible factor is necessarily distinct from all the f_j, because otherwise it would divide 1. No finite set of monic irreducible polynomials includes all the monic irreducible polynomials, so we conclude that the set of monic irreducible polynomials in $\mathbb{K}[x]$ is infinite. □

P12.2. **i.** Let $f := a_3\, x^3 + a_2\, x^2 + a_1\, x + a_0$ be a polynomial in $\mathbb{Z}[x]$ having degree 3. Assume that a_0, $a_1 + a_2$, and a_3 are all odd. Prove that f is irreducible in $\mathbb{Q}[x]$.

ii. Prove that the polynomial $g := x^5 + 6\,x^4 - 12\,x^3 + 9\,x^2 - 3\,x + k$ in $\mathbb{Q}[x]$ is irreducible for infinitely many integers k.

iii. Prove that $h := x^5 + x^4 + x - 1$ is irreducible in $\mathbb{Q}[x]$ using the Eisenstein criterion.

Solution.

i. Since $a_1 + a_2$ is odd, one of these coefficients is even and the other is odd. As a_0 and a_3 are odd, the image of f in $\mathbb{F}_2[x]$ is either $x^3 + x^2 + 1$ or $x^2 + x + 1$. Our illustration of sieve methods for polynomials established that both of these polynomials are irreducible in $\mathbb{F}_2[x]$. It follows that f is also irreducible in $\mathbb{Q}[x]$.

ii. Observe that 3 does not divide 1, but 3 does divide 6, -12, 9, and -3. Hence, the Eisenstein criterion implies that the polynomial g is irreducible in $\mathbb{Q}[x]$ whenever 3 divides k and 9 does not divide k. It follows that g is irreducible if $k = 9\,n + 3$ or $k = 9\,n + 6$ for some integer n. In particular, the polynomial g is irreducible in $\mathbb{Q}[x]$ for infinitely many integers k.

iii. Consider the ring isomorphism $\varphi\colon \mathbb{Q}[x] \to \mathbb{Q}[x]$ defined by $\varphi(x) = x - 1$. It follows that the polynomial h is irreducible in $\mathbb{Q}[x]$ if and only if the polynomial $\varphi(h)$ is irreducible in $\mathbb{Q}[x]$. Since

$$\begin{aligned}\varphi(h) &= (x-1)^5 + (x-1)^4 + (x-1) - 1 \\ &= (x^5 - 5\,x^4 + 10\,x^3 - 10\,x^2 + 5\,x - 1) + (x^4 - 4\,x^3 + 6\,x^2 - 4\,x + 1) + x - 2 \\ &= x^5 - 4\,x^4 + 6\,x^3 - 4\,x^2 + 2\,x - 2\end{aligned}$$

we see that 2 does not divide 1, 2 does divide -4, 6, 4, 2, and -2, and 4 does not divide -2. Thus, the Eisenstein criterion establishes that the polynomial $\varphi(h)$ is irreducible in $\mathbb{Q}[x]$. $\square$

P12.3. Let R be a principal ideal domain and let K be its field of fractions.

i. Suppose $R = \mathbb{Z}$. Write the rational number $r = \frac{7}{24}$ in the form $r = \frac{b}{3} + \frac{a}{8}$ for some integers a and b.

ii. Let $g := p\,q \in R$ where p and q are coprime. Prove that every fraction $f/g \in K$ can written in the form
$$\frac{f}{g} = \frac{u}{q} + \frac{v}{p}$$
for some elements u and v in R.

iii. Let $g := p_1^{e_1}\,p_2^{e_2} \cdots p_m^{e_m} \in R$ be the factorization of g into irreducible elements p_j, for all $1 \leqslant j \leqslant m$, such that the relation $p_j = u\,p_k$ for some unit $u \in R$ implies that $j = k$. Prove that every fraction $f/g \in K$ can be written in the form
$$\frac{f}{g} = \sum_{j=1}^{k} \frac{h_j}{p_j^{e_j}}$$
for some elements $h_1, h_2, \dots, h_m$ in R.

Solution.

i Since $(-1)(8) + (3)(3) = 1$, we have
$$r = \frac{7}{24} = \frac{7\big((-1)(8) + (3)(3)\big)}{24} = \frac{-7}{3} + \frac{21}{8}\,.$$

ii Since $\gcd(p, q) = 1$, there exists elements s and t in R such that $s\,p + t\,q = 1$. Hence we obtain
$$\frac{f}{g} = \frac{f(s\,p + t\,q)}{p\,q} = \frac{f\,s}{q} + \frac{f\,t}{p}\,.$$

iii We proceed by induction on m. For the base case, when $m = 1$, the assertion is trivial. For the induction step, set $p := p_1^{e_1}$ and $q := p_2^{e_2}\,p_3^{e_3} \cdots p_m^{e_m}$. By hypothesis, we have $\gcd(p, q) = 1$, so there exists elements s and t in R such that $s\,p + t\,q = 1$. It follows that
$$\frac{f}{g} = \frac{f(s\,p + t\,q)}{p\,q} = \frac{f\,s}{q} + \frac{f\,t}{p} = \frac{f\,s}{p_1^{e_1}} + \frac{f\,t}{p_2^{e_2}\,p_3^{e_3} \cdots p_m^{e_m}}$$
The induction hypothesis establishes that
$$\frac{f\,t}{p_2^{e_2}\,p_3^{e_3} \cdots p_m^{e_m}} = \sum_{j=2}^{m} \frac{h_j}{p_j^{e_j}}$$
for some elements $h_2, h_3, \dots, h_m$ in R. Setting $h_1 := f\,s$ gives $f/g = \sum_{j=1}^{m} h_j/p_j^{e_j}$. $\square$