

Homework 5 Solutions.

§4.2 #1 d. Use the division algorithm to find the quotient and remainder when $f(x) = 2x^4 + x^3 - 6x^2 - x + 2$ is divided by $g(x) = 2x^2 - 5$ over \mathbb{Q} .

Solution: Long division gives:

$$f(x) = g(x) \left(x^2 + \frac{1}{2}x - \frac{1}{2} \right) + \frac{3}{2}x - \frac{1}{2}.$$

§4.2 #2 b. Use the division algorithm to find the quotient and remainder when $f(x) = x^5 + 4x^4 + 2x^3 + 3x^2$ is divided by $g(x) = x^2 + 3$ over \mathbb{Z}_5 .

Solution: Long division gives:

$$f(x) = g(x)(x^3 + 4x^2 + 4x + 1) + 3x + 2.$$

§4.2 #2 d. Use the division algorithm to find the quotient and remainder when $f(x) = 2x^4 + x^3 + x^2 + 6x + 2$ is divided by $g(x) = 2x^2 + 2$ over \mathbb{Z}_7 .

Solution: Long division gives:

$$f(x) = g(x)(x^2 + 4x + 3) + 5x + 3.$$

§4.4, #4 Use Eisenstein's Criterion to show that each of the following polynomials is irreducible in $\mathbb{Q}[x]$.

- (a) The polynomial $f(x) = x^4 - 12x^2 + 18x - 24$ is 3-Eisenstein, hence irreducible.
- (b) The polynomial $f(x) = 4x^3 - 15x^2 + 60x + 180$ is 5-Eisenstein, hence irreducible.
- (c) The polynomial $f(x) = 2x^{10} - 25x^3 + 10x^2 - 30$ is 5-Eisenstein, hence irreducible.
- (d) The polynomial $f(x) = x^2 + 2x - 5$ is irreducible in $\mathbb{Q}[x]$ since it has no roots in \mathbb{Q} . Alternatively, note that $f(x+1) = (x+1)^2 + 2(x+1) - 5 = x^2 + 4x - 2$ is 2-Eisenstein, implying that $f(x)$ is irreducible.

§4.4, #5 Use Eisenstein's Criterion to show that each of the following polynomials is irreducible in $\mathbb{Q}[x]$.

- (a) Let $f(x) = x^4 + 1$. Observe that $f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$ is 2-Eisenstein. Hence, $f(x)$ is irreducible.
- (b) Let $f(x) = x^6 + x^3 + 1$. Observe that

$$\begin{aligned} f(x+1) &= (x+1)^6 + (x+1)^3 + 1 \\ &= (x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1) + (x^3 + 3x^2 + 3x + 1) + 1 \\ &= x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3 \end{aligned}$$

is 3-Eisenstein. Hence, $f(x)$ is irreducible.

- (c) Let $f(x) = x^3 + 3x^2 + 5x + 5$. One can use the Rational Root Theorem to verify that $f(x)$ has no roots in \mathbb{Q} , and hence, is irreducible. Alternatively, observe that

$$\begin{aligned} f(x+1) &= (x+1)^3 + 3(x+1)^2 + 5(x+1) + 5 \\ &= (x^3 + 3x^2 + 3x + 1) + (3x^2 + 6x + 3) + (5x + 5) + 5 \\ &= x^3 + 6x^2 + 14x + 14 \end{aligned}$$

is 2-Eisenstein. Hence, $f(x)$ is irreducible.

- (d) Let $f(x) = x^3 - 3x^2 + 9x - 10$. One can use the Rational Root Theorem to verify that $f(x)$ has no roots in \mathbb{Q} , and hence, is irreducible. Alternatively, observe that

$$\begin{aligned} f(x+1) &= (x+1)^3 - 3(x+1)^2 + 9(x+1) - 10 \\ &= (x^3 + 3x^2 + 3x + 1) - (3x^2 + 6x + 3) + (9x + 9) - 10 \\ &= x^3 + 6x - 3 \end{aligned}$$

is 3-Eisenstein. Hence, $f(x)$ is irreducible.

§4.4, #7 Let $f(x) = x^2 + 100x + n$.

- (a) Give an infinite set of integers n such that $f(x)$ is reducible in $\mathbb{Q}[x]$.

Solution: Let $t \in \mathbb{Z}$. Then

$$f(x) = x^2 + 100x + (50^2 - t^2) = (x^2 + 100x + 50^2) - t^2 = (x+50)^2 - t^2 = (x+50-t)(x+50+t).$$

Alternatively, compute

$$f(x) = x^2 + 100x + t(100 - t) = (x - t)(x - 100 + t).$$

- (b) Give an infinite set of integers n such that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Solution: Let n be of the form $n = 2(2j + 1) = 4j + 2$. Then for all $j \in \mathbb{Z}$, $f(x)$ is 2-Eisenstein, hence irreducible. Alternatively, let $n = 5(5t + r) = 25t + 5r$ with $1 \leq r \leq 4$. Then for all $t \in \mathbb{Z}$, $f(x)$ is 5-Eisenstein, hence irreducible.

§4.4, #15 Find the irreducible factors of $x^8 - 1$ in $\mathbb{Q}[x]$.

Solution:

$$x^8 - 1 = (x^4 - 1)(x^4 + 1) = (x^2 - 1)(x^2 + 1)(x^4 + 1) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1).$$

This is a factorization of $x^8 - 1$ into irreducibles in $\mathbb{Q}[x]$. The first two factors are linear; therefore they are irreducible. The third factor has roots $\pm i \notin \mathbb{Q}$; hence, it is irreducible. The last factor was shown to be irreducible in problem 5 a.

§4.4, #16

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1).$$

This is a factorization into irreducibles. The first factor is linear and therefore irreducible in $\mathbb{Q}[x]$. The second factor has no roots in \mathbb{Q} ; it must be irreducible since it has degree 2. The third factor was shown to be irreducible in problem 5 b.

§5.3, #24 Let I be the smallest ideal of $\mathbb{Z}[x]$ that contains both 2 and x . Show that I is not a principal ideal.

Proof. We note that $(2) \not\subseteq (x)$ and that $(x) \not\subseteq (2)$. Suppose that there exists $\alpha \in \mathbb{Z}[x]$ for which $(2, x) = (\alpha)$. Then we have $2 \in (\alpha)$ and $x \in (\alpha)$ from which we deduce that $\alpha \mid 2$ and $\alpha \mid x$. But if $\alpha \mid 2$, then $\alpha \in \{\pm 1, \pm 2\}$. However, we observe that $\pm 1 \notin (2, x)$ and $\pm 2 \nmid x$, a contradiction. \square

§4.2, #13 Find all monic irreducible polynomials of degree ≤ 3 over \mathbb{Z}_3 .

Solution:

- Degree one: $x, x + 1, x + 2$.
- Degree two: $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$.
- Degree three: $x^3 + 2x^2 + 1, x^3 + x^2 + 2x + 1, x^3 + 2x^2 + x + 1, x^3 + 2x + 1, x^3 + 2x^2 + 2x + 2, x^3 + x^2 + 2, x^3 + x^2 + x + 2, x^3 + 2x + 2$.

Write each of the following polynomials as a product of irreducibles in $\mathbb{Z}_3[x]$.

- (a) $f(x) = x^2 - 2x + 1 \equiv (x + 2)^2 \pmod{3}$.
 (b) $f(x) = x^4 + 2x^2 + 2x + 2 \equiv (x + 1)^2(x^2 + x + 2) \pmod{3}$.
 (c) $f(x) = 2x^3 - 2x + 1 \equiv -(x^3 + 2x + 2) \pmod{3}$.
 (d) $f(x) = x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2) \pmod{3}$.
 (e) $f(x) = x^9 - x \equiv x(x + 1)(x + 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2) \pmod{3}$.

Note: Observe that $x^9 - x$ factors as a product of all irreducibles in $\mathbb{Z}_3[x]$ of degree ≤ 2 . This phenomenon persists: for all positive integers n , the polynomial $x^{3^n} - x$ factors as a product of all irreducibles in $\mathbb{Z}_3[x]$ with degree $d \mid n$.

§4.2, #14 Let $p \in \mathbb{Z}$ be prime. Show that there are exactly $(p^2 - p)/2$ irreducible polynomials of degree 2 in $\mathbb{Z}_p[x]$.

Proof. Let $f(x) = x^2 + bx + c$. We fix $b \in \mathbb{Z}_p$; there are p choices for b . Now, we will show that there are $\frac{p-1}{2}$ non-zero values of $c \in \mathbb{Z}_p$ for which $f(x) \equiv 0 \pmod{p}$ has a solution in \mathbb{Z}_p . From this we deduce that there must be $\frac{p-1}{2}$ values of $c \in \mathbb{Z}_p$ for which $f(x) \equiv 0 \pmod{p}$ has no solution, and is therefore irreducible.

We develop a criterion for determining whether not $f(x) \equiv 0 \pmod{p}$ has a solution as follows:

$$\begin{aligned} f(x) \equiv 0 \pmod{p} &\iff 4x^2 + 4bx + 4c \equiv 0 \pmod{p} \\ &\iff (4x^2 + 4bx + b^2) + 4c - b^2 \equiv 0 \pmod{p} \\ &\iff (2x + b)^2 \equiv b^2 - 4c \pmod{p}. \end{aligned}$$

Therefore, $f(x) \equiv 0 \pmod{p}$ has a solution mod p if and only if $d = b^2 - 4c$ is a square mod p .

Observe that

$$(2x + b)^2 \equiv (2y + b)^2 \pmod{p} \iff 2x + b \equiv 2y + b \text{ or } 2x + b \equiv -2y - b \pmod{p}.$$

In the first case, $2x + b \equiv 2y + b \pmod{p}$ implies that $x \equiv y \pmod{p}$. In the second case, $2x + b \equiv -2y - b \pmod{p}$ implies that $y \equiv -x - b \pmod{p}$. Hence, as x ranges from 0 to $p - 1$ in \mathbb{Z}_p , $(2x + b)^2 \pmod{p}$ assumes $\frac{p+1}{2} = 1 + \frac{p-1}{2}$ values, including the value b^2 when $x \equiv 0 \pmod{p}$. Furthermore, for each such value d , the congruence $d \equiv b^2 - 4ac \pmod{p}$ has a unique solution, $c \equiv 4^{-1}(b^2 - d) \pmod{p}$. Noting that $c \equiv 0 \pmod{p}$ gives the square $b^2 \pmod{p}$, we find that there are $\frac{p-1}{2}$ non-zero values of $c \in \mathbb{Z}_p$ for which $b^2 - 4ac$ is a square mod p .

We conclude, for fixed $b \in \mathbb{Z}_p$, that there are $\frac{p-1}{2}$ values of $c \in \mathbb{Z}_p$ for which $f(x) = x^2 + bx + c$ is irreducible mod p ; we must have $p(p-1)/2 = \frac{p^2-p}{2}$ monic irreducible quadratics in $\mathbb{Z}_p[x]$. \square

An alternative (and simpler) proof is as follows. A reducible quadratic mod p can arise in the form $(x - a)^2$ or $(x - a)(x - b)$. There are p of the first type and $\binom{p}{2}$ of the second type. Therefore, the total number for reducible quadratics mod p is $p + \binom{p}{2} = \frac{p(p+1)}{2}$. Hence, the total number of irreducible quadratics mod p is $p^2 - \frac{p(p+1)}{2} = \frac{p^2-p}{2}$.