Kyle Kloberdanz
21 February 2022

Exercise 2.3.3: Let $f = x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2$ and $g = 4x^4 + 16$. Find $gcd(f, g)$ and express it as $uf + vg$

I spent too much time trying to show long division in LaTex. I gave up, and inserted a scanned image of my notes instead to show the process of calculating the GCD using the Euclidean Algorithm below. From those results, we can see that the monic form of the $GCD(f, g) = x^2 + 2x + 2$.

$f = x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2$

$g = 4x^4 + 16$

$$\frac{1}{4}x + \frac{1}{2}$$

$$4x^4 + 16 \,\big|\, x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2$$

$$-(x^5 + 0 + 0 + 0 + 4x)$$

$$2x^4 + 2x^3 - x^2 - 6x - 2$$

$$-(2x^4 + 0 + 0 + 0 + 8)$$

$$2x^3 - x^2 - 6x - 10$$

$f = x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2 = (4x^4 + 16)\underbrace{\left(\frac{1}{4}x + \frac{1}{2}\right)}_{q_1} + \overset{r_1}{(2x^3 - x^2 - 6 - 10)}$

$$2x + 1$$

$$2x^3 - x^2 - 6x - 10 \,\big|\, 4x^4 + 0x^3 + 0x^2 + 0x + 16$$

$$-(4x^4 - 2x^3 - 12x^2 - 20x)$$

$$2x^3 + 12x^2 + 20x + 16$$

$$-(2x^3 - x^2 - 6x - 10)$$

$$13x^2 + 26x + 26 \quad r_2$$

$g = 4x^4 + 16 = (2x^3 - x^2 - 6x - 10)(2x + 1) + (13x^2 + 26x + 2$

$$\frac{2}{13}x - \frac{5}{13}$$

$$13x^2 + 26x + 26 \,\big|\, 2x^3 - x^2 - 6x - 10$$

$$-(2x^3 + 4x^2 + 4x)$$

$$-5x^2 - 10x - 10$$

$$-5x^2 - 10x - 10$$

$$0$$

Exercise 2.3.5: Prove that a polynomial $f \in \mathbb{F}[x]$ of degree 3 is irreducible in $\mathbb{F}[x]$ if it does not have a root in $\mathbb{F}$.

Proof. Recall, for a polynomial f to be irreducible, one must be able to write $f = uv$ where either u or v is a nonzero constant polynomial, i.e., either $deg(u) = 0$ or $deg(v) = 0$.

We will demonstrate a proof by contrapositive where we will show that a polynomial $f \in \mathbb{F}[x]$ of degree 3 has a root in $\mathbb{F}$ if f is not irreducible (i.e., f is reducible) in $\mathbb{F}[x]$

Because we are assuming that f is reducible, then we can write $f = uv$ where $deg(u) > 0$ and $deg(v) > 0$. Because $deg(uv) = deg(u) + deg(v)$ and $deg(f) = 3$ (as per the problem statement), then we have two cases, either $deg(u) = 1$ and $deg(v) = 2$ or $deg(u) = 2$ and $deg(v) = 1$.

Let's start by assuming that $deg(u) = 1$. This means that $u = a_0 + a_1x$ where $a_0, a_1 \in \mathbb{F}$. Because $\mathbb{F}$ is a field, and $a_1 \neq 0$ (because if $a_1 = 0$ then $deg(u) = 0$, which would be a contradiction to the statement that $deg(u) = 1$) then there exists a multiplicative inverse for a_1 in $\mathbb{F}$, namely a_1^{-1}, such that $u(-a_0a_1^{-1}) = a_0 + a_1(-a_0a_1^{-1}) = a_0 + (-a_0) = 0$ therefore f has the root $-a_0a_1^{-1} \in \mathbb{F}$.

Since we have shown that a polynomial $f \in \mathbb{F}[x]$ of degree 3 has a root in $\mathbb{F}$ if f is reducible in $\mathbb{F}[x]$, by the contrapositive we see that a polynomial $f \in \mathbb{F}[x]$ of degree 3 is irreducible in $\mathbb{F}[x]$ if it does not have a root in $\mathbb{F}$. □

Exercise: Come up with a polynomial $g \in \mathbb{Q}[x]$ that has no roots in $\mathbb{Q}$ but is *not* irreducible.

let $g = x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$

We can see that g is not irreducible.

To avoid having to apply the quartic equation, by factoring this polynomial, we see that all of the roots will be x such that $x^2 + 1 = 0$. Hence we can apply the quadratic equation to find the roots like so.

$$\frac{-0 \pm \sqrt{0^2 - 4(1)(1)}}{2(1)} = \frac{\pm\sqrt{(-4)}}{2} = \frac{\pm 2\sqrt{-1}}{2} = \pm\sqrt{-1} = \pm i \notin \mathbb{Q}$$

Hence, we see that the roots to $g = x^4 + 2x^2 + 1$ are i and $-i$, which do not exist in Q, and is therefore an example of a polynomial $g \in \mathbb{Q}[x]$ that has no roots in $\mathbb{Q}$ but is not irreducible.

Exercise 2.3.6: Consider the polynomial $f(x) = x^3 - x + 2 \in \mathbb{Z}_5[x]$ (more precisely, $f(x) = [1]x^3 - [1]x + [2]$). Prove that f is irreducible in $\mathbb{Z}_5$. *Hint: Use Exercise 2.3.5.*

Proof. Recall that we have proven in Exercise 2.3.5 that if a polynomial $f \in \mathbb{F}[x]$ of degree 3 does not have a root in $\mathbb{F}$, then f is irreducible in $\mathbb{F}[x]$.

We will therefore show that $f \in \mathbb{Z}_5[x]$ does not have a root in $\mathbb{Z}_5$, and is therefore irreducible.

Because $\mathbb{Z}_5$ is the finite set $\{0, 1, 2, 3, 4\}$, we can show that given any $x \in \mathbb{Z}_5$, $x^3 - x + 2 \neq 0$ as follows.

$f(0) = 2 \neq 0$
$f(1) = 1 - 1 + 2 = 2 \neq 0$
$f(2) = 2^3 - 2 + 2 = 8 - 2 + 2 \equiv 8 \pmod 5 = 3 \neq 0$
$f(3) = 3^3 - 3 + 2 = 8 - 2 + 2 = 27 - 3 + 2 \equiv 26 \pmod 5 = 1 \neq 0$
$f(4) = 4^3 - 4 + 2 = 64 - 4 + 2 \equiv 62 \pmod 5 = 2 \neq 0$

We have exhausted every possible value for $x \in \mathbb{Z}_5$, and found that no such value for x is a root for f, i.e., where $f(x) = 0$, hence there does not exist a root for f in $\mathbb{Z}_5$, therefore by Exercise 2.3.5, we conclude that f is irreducible in $\mathbb{Z}_5$. □

Exercise: Consider the polynomial $p(x) = 3x^3 + 2x^2 + 4x + 2 \in \mathbb{Z}_7[x]$ (more precisely, $f(x) = [3]x^3 + [2]x^2 + [4]x + [2]$). Prove that f is *not* irreducible in $\mathbb{Z}_7[x]$.

Proof. Recall Corollary 2.3.16: For every $f \in \mathbb{F}[x]$ and $\alpha \in \mathbb{F}$, there exists a polynomial $q \in \mathbb{F}[x]$ so that $f = (x - \alpha)q + f(\alpha)$. In particular, α is a root of f if and only if $(x - \alpha)|f$.

If α is a root of f, then by corollary 2.3.16, $f = (x - \alpha)q + 0 = (x - \alpha)q$, and therefore f is reducible if there exits a root for f.

We will show that f has a root in $\mathbb{F}$.

$f(0) = 2 \neq 0$
$f(1) = 3 + 2 + 4 + 2 \equiv 11 \pmod 7 = 2 \neq 0$
$f(2) = 24 + 8 + 8 + 2 \equiv 42 \pmod 7 = 0$

We have found a root $2 \in \mathbb{Z}_7$ for $f \in \mathbb{Z}_7[x]$. Therefore, because the polynomial $f \in \mathbb{Z}_7[x]$ of degree 3 has a root in $\mathbb{Z}_7$, f is not irreducible. □

As a bonus, by using the Computer Algebra System, sage mathematics, one can find that factors for this polynomial are $(3x + 1)(x^2 + 5x + 2)$, therefore $p(x)$ is not irreducible.

```
sage: x = PolynomialRing(RationalField(), ’x’).gen()
sage: f = (3*x^3 + 2*x^2 + 4*x + 2)
sage: f.factor_mod(7)
(3) * (x + 5) * (x^2 + 5*x + 2)
```

Exercise 2.5.1: Suppose $T : R^n \to R^n$ is a linear transformation. Prove that T is an isometry if and only if $T(v) \cdot T(w) = v \cdot w$. Recall that an isometry is a *bijection* that preserves distance.

Note: when proving that if $T(v) \cdot T(w) = v \cdot w$ then T is an isometry, make sure you verify that T is a bijection.

Proof. Given the definition of an isometry, We must show that

$$|T(v) - T(w)| = |v - w| \iff T(v) \cdot T(w) = v \cdot w$$

First we will show that T is injective by contradiction. Let's assume that there is some $a_1, a_2 \in \mathbb{R}^n$ such that $a_1 \neq a_2$ and $T(a_1) = T(a_2)$. Therefore we can write:

$$a_1 \cdot a_2 = T(a_1) \cdot T(a_2) = T(a_1) \cdot T(a_1) = a_1 \cdot a_1$$

Which would imply that $a_1 = a_2$, a contradiction.

We will also demonstrate that T is surjective by contradiction. Let's assume that $a \in \mathbb{R}$ such that $a \neq x \cdot y$ where $x, y \in \mathbb{R}^n$ We could write a as the sum of products of some numbers $x_1y_1 + x_2y_2 + ... + x_ny_n$ where $n \in \mathbb{Z}, n > 0$, $x_1, .., x_n \in \mathbb{R}$, and $y_1, .., y_n \in \mathbb{R}$. But then $a = x_1y_1 + x_2y_2 + ... + x_ny_n = x \cdot y = T(x) \cdot T(y)$ which contradicts that $a \neq x \cdot y$, and therefore T is surjective.

By showing that T is both injective and surjective, we have therefore shown that T is bijective.

(i) To demonstrate what happens if $v = w$

$$T(v) \cdot T(v) = v \cdot v = |v|$$

The norm for some vector $x \in \mathbb{R}^n$ is $|x| = \sqrt{x \cdot x}$. We can replace the norm in this equation with this definition.

$$|T(v) - T(w)| = |v - w|$$

$$\sqrt{(T(v) - T(w)) \cdot (T(v) - T(w))} = \sqrt{(v - w) \cdot (v - w)}$$

Squaring both sides we find

$$(T(v) - T(w)) \cdot (T(v) - T(w)) = (v - w) \cdot (v - w)$$

$$T(v) \cdot T(v) - 2(T(v) \cdot T(w)) + T(w) \cdot T(w) = v \cdot v - 2(v \cdot w) + w \cdot w$$

By (i), we can show:

$$v \cdot v - 2(T(v) \cdot T(w)) + w \cdot w = v \cdot v - 2(v \cdot w) + w \cdot w$$

$$|v| - 2(T(v) \cdot T(w)) + |w| = |v| - 2(v \cdot w) + |w|$$

By subtraction of $|v|$ and $|w|$

$$-2(T(v) \cdot T(w)) = -2(v \cdot w)$$

By division of -2

$$T(v) \cdot T(w) = v \cdot w$$

By algebraic manipulation we can see that

$$|T(v) - T(w)| = |v - w| \implies T(v) \cdot T(w) = v \cdot w$$

By performing this same procedure in reverse, we can see that

$$T(v) \cdot T(w) = v \cdot w \implies |T(v) - T(w)| = |v - w|$$

Therefore:

$$|T(v) - T(w)| = |v - w| \iff T(v) \cdot T(w) = v \cdot w$$

□