Math 110A Homework 4

Jiaping Zeng

2/15/2021

1. For each pair of polynomials $f(x)$ and $g(x)$ below, use the Euclidean algorithm to compute the $\gcd(f(x), g(x))$, and to find polynomials $u(x)$ and $v(x)$ with $(f(x), g(x)) = f(x)u(x) + g(x)v(x)$:

   (b) $f(x) = x^5 + x^4 + 2x^3 - x^2 - x - 2$ and $g(x) = x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Q}[x]$.

   Answer: As follows:
   $x^5 + x^4 + 2x^3 - x^2 - x - 2 = (x^4 + 2x^3 + 5x^2 + 4x + 4)(x - 1) + (-x^3 - x + 2)$
   $x^4 + 2x^3 + 5x^2 + 4x + 4 = (-x^3 - x + 2)(-x - 2) + (4x^2 + 4x + 8)$
   $-x^3 - x + 2 = (4x^2 + 4x + 8)(-\frac{1}{4}x + \frac{1}{4}) + 0$
   Therefore $\gcd(f(x), g(x)) = x^2 + x + 2$; now let $u = \frac{1}{4}x + \frac{1}{2}$ and $v = -\frac{1}{4}x^2 - \frac{1}{4}x + \frac{3}{4}$, we have $x^2 + x + 2 = f(x)u(x) + g(x)v(x)$.

   (c) $f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ and $g(x) = 3x^3 + 5x^2 + 6x$ in $(\mathbb{Z}/7\mathbb{Z})[x]$.

   Answer: As follows:
   $4x^4 + 2x^3 + 6x^2 + 4x + 5 = (3x^3 + 5x^2 + 6x)(6x) + (5x^2 + 4x + 5)$
   $3x^3 + 5x^2 + 6x = (5x^2 + 4x + 5)(2x + 5) + (4x + 3)$
   $5x^2 + 4x + 5 = (4x + 3)(3x + 4)$ Since $2(4x + 3) = x + 6$ in $(\mathbb{Z}/7\mathbb{Z}[x])$, $\gcd(f(x), g(x)) = x + 6$; now let $u = 3x + 4$ and $v = 3x^2 + 4x + 2$, we have $x + 6 = f(x)u(x) + g(x)v(x)$.

   (d) $f(x) = x^3 - ix^2 + 4x - 4i$ and $g(x) = x^2 + 1$ in $\mathbb{C}[x]$.

   Answer: As follows:
   $x^3 - ix^2 + 4x - 4i = (x^2 + 1)(x - i) + (3x - 3i)$
   $3x - 3i = 3(x - i)$
   Therefore $\gcd(f(x), g(x)) = x - i$; now let $u = \frac{1}{3}$ and $v = -\frac{1}{3}(x - i)$, we have $x - i = f(x)u(x) + g(x)v(x)$.

2. Express $x^4 - 4$ as a product of irreducibles in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

   Answer:

   $\mathbb{Q}$: $x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x^2 - 2)(x^2 + 2)$

   $\mathbb{R}$: $x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$

   $\mathbb{C}$: $x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{2}i)(x + \sqrt{2}i)$

3. Use unique factorization to find the gcd in $\mathbb{C}[x]$ of $(x - 3)^3(x - 4)^4(x - i)^2$ and $(x - 1)(x - 3)(x - 4)^3$.

   Answer: Since both polynomials are already expressed as products of irreducibles, the gcd is $(x - 3)(x - 4)^3$.

4. (a) Show that $x^2 + 2$ is irreducible in $(\mathbb{Z}/5\mathbb{Z})[x]$.

   Answer: We can show that $x^2 + 2$ has no roots in $\mathbb{Z}/5\mathbb{Z}$ (i.e. $x^2 + 2 = 0$ has no solutions):

x	x^2+2	is solution?
$[0]$	$[0]^2+[2]=[0]+[2]=[2]$	no
$[1]$	$[1]^2+[2]=[1]+[2]=[3]$	no
$[2]$	$[2]^2+[2]=[4]+[2]=[1]$	no
$[3]$	$[3]^2+[2]=[9]+[2]=[1]$	no
$[4]$	$[4]^2+[2]=[16]+[2]=[3]$	no

Since x^2+2 has no roots in $\mathbb{Z}/5\mathbb{Z}$, it is irreducible.

(b) Factor x^4-4 as a product of irreducibles in $(\mathbb{Z}/5\mathbb{Z})[x]$.

Answer: We have $x^4-4=(x^2+2)(x^2-2)$; we can verify that it cannot be reduced further by checking if (x^2+2) and (x^2-2) have roots in $(\mathbb{Z}/5\mathbb{Z})[x]$:

x	x^2+2	is solution?
$[0]$	$[0]^2+[2]=[0]+[2]=[2]$	no
$[1]$	$[1]^2+[2]=[1]+[2]=[3]$	no
$[2]$	$[2]^2+[2]=[4]+[2]=[1]$	no
$[3]$	$[3]^2+[2]=[9]+[2]=[1]$	no
$[4]$	$[4]^2+[2]=[16]+[2]=[3]$	no

x	x^2-2	is solution?
$[0]$	$[0]^2-[2]=[0]-[2]=[3]$	no
$[1]$	$[1]^2-[2]=[1]-[2]=[4]$	no
$[2]$	$[2]^2-[2]=[4]-[2]=[2]$	no
$[3]$	$[3]^2-[2]=[9]-[2]=[2]$	no
$[4]$	$[4]^2-[2]=[16]-[2]=[4]$	no

Since neither has roots in $(\mathbb{Z}/5\mathbb{Z})[x]$, $x^4-4=(x^2+2)(x^2-2)$ cannot be reduced further.

5. Use the factor theorem to show that x^7-x factors in $(\mathbb{Z}/7\mathbb{Z})[x]$ as $x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$, *without* doing any polynomial multiplication.

Answer: We can do so by showing that $x=0,1,2,3,4,5,6$ are all solutions to $x^7-x=0$ in $\mathbb{Z}/\mathbb{Z}$ as follows:

x	x^7-x	is solution?
$[0]$	$[0]^7-[0]=[0]-[0]=[0]$	yes
$[1]$	$[1]^7-[1]=[1]-[1]=[0]$	yes
$[2]$	$[2]^7-[2]=[128]-[2]=[0]$	yes
$[3]$	$[3]^7-[3]=[2187]-[3]=[0]$	yes
$[4]$	$[4]^7-[4]=[16384]-[4]=[0]$	yes
$[5]$	$[5]^7-[5]=[78125]-[5]=[0]$	yes
$[6]$	$[6]^7-[6]=[279936]-[6]=[0]$	yes

Therefore $x=0,1,2,3,4,5,6$ are all roots, so $x,(x-1),(x-2),(x-3),(x-4),(x-5),(x-6)$ are all factors by the factor theorem.

6. Determine if the given polynomial is irreducible:

(a) x^2-7 in $\mathbb{Q}[x]$.

Answer: $x^2-7=0 \implies x^2=7$ which has no solution in $\mathbb{Q}$, therefore x^2-7 is irreducible in $\mathbb{Q}[x]$.

(b) $2x^3 + x^2 + 2x + 2$ in $(\mathbb{Z}/5\mathbb{Z})[x]$.

Answer:

x	$2x^3 + x^2 + 2x + 2$	is solution?
$[0]$	$2[0]^3 + [0]^2 + 2[0] + [2] = [0] + [0] + [0] + [2] = [2]$	no
$[1]$	$2[1]^3 + [1]^2 + 2[1] + [2] = [2] + [1] + [2] + [2] = [2]$	no
$[2]$	$2[2]^3 + [2]^2 + 2[2] + [2] = [16] + [4] + [4] + [2] = [1]$	no
$[3]$	$2[3]^3 + [3]^2 + 2[3] + [2] = [54] + [9] + [6] + [2] = [1]$	no
$[4]$	$2[4]^3 + [4]^2 + 2[4] + [2] = [128] + [16] + [8] + [2] = [4]$	no

Therefore $2x^3 + x^2 + 2x + 2$ is irreducible $(\mathbb{Z}/5\mathbb{Z})[x]$.

(c) $x^4 + x^2 + 1$ in $(\mathbb{Z}/3\mathbb{Z})[x]$.

Answer:

x	$x^4 + x^2 + 1$	is solution?
$[0]$	$[0]^4 + [0]^2 + [1] = [0] + [0] + [1] = [1]$	no
$[1]$	$[1]^4 + [1]^2 + [1] = [1] + [1] + [1] = [0]$	yes
$[2]$	$[2]^4 + [2]^2 + [1] = [16] + [4] + [1] = [0]$	yes

Therefore $x^4 + x^2 + 1$ is not irreducible since $x = 1, 2$ are roots.

7. Let $\varphi : \mathbb{C} \to \mathbb{C}$ be an isomorphism of rings such that $\varphi(a) = a$ for all $a \in \mathbb{Q}$. Suppose that $r \in \mathbb{C}$ is a root of $f(x) \in \mathbb{Q}[x]$. Prove that $\varphi(r)$ is also a root of $f(x)$.
Answer: Since $f(x) \in \mathbb{Q}[x]$ and φ is a ring isomorphism, we have $f(r) = a_0 + a_1 r + \ldots + a_n r^n \implies 0 = \varphi(f(r)) = a_0 + a_1\varphi(r) + \ldots + a_n\varphi(a_n) = f(\varphi(r))$, therefore $\varphi(r)$ is a root by definition.

8. (a) Prove that the following version of the division algoirthm holds in $\mathbb{Z}[i]$: *For any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there is some not necessarily unique $q, r \in \mathbb{Z}[i]$ with $\alpha = \beta q + r$ and $N(r) < N(\beta)$.*
Answer: Let $z = \frac{\alpha}{\beta} \in \mathbb{C}$ such that $\frac{r}{\beta} = z - q$, we want to show that there exists some $q \in \mathbb{Z}[i]$ such that $|z - q| < 1$. We can do so by taking the four points in $\mathbb{Z}[i]$ closest to z as follows: let $z = x + yi$, and let $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ such that $x_1 \leq x < x_2, y_1 \leq y < y_2$ and $x_2 - x_1 = y_2 - y_1 = 1$ (visually, the four points $(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_2)$ form a square that contains z). Now if we divide the square into four smaller squares evenly, z must be in or on one of the smaller squares. Since each of the smaller squares contains a point from $\mathbb{Z}[i]$, the distance between z to a point from $\mathbb{Z}[i]$ must be smaller than the diagonal of the smaller square, which is $\frac{\sqrt{2}}{2} < 1$. Therefore $|z - q| < 1$.

(b) Give an example to show that the q and r you found in part (a) do not need to be unique.
Answer: Let $\alpha = 1 + 2i$ and $\beta = 2 + 4i$, then $\alpha = 1 \cdot \beta + (-1 - 2i)$ with $q = 1$ and $r = -1 - 2i$. Similarly, $\alpha = 0 \cdot \beta + (1 + 2i)$ with $q = 0$ and $r = 1 + 2i$. Therefore q and r do not need to be unique.

(c) If $\alpha, \beta \in \mathbb{Z}[i]$ are irreducibles and $\alpha | \beta$, prove that α and β are associates.
Answer: Since $\alpha | \beta$, there is some $\gamma \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma$. Then since α is irreducible, either β or γ is a unit. Since β is irreducible and therefore cannot be a unit by definition, γ is a unit. Then α and β are associates by definition.

9. Let $p > 0$ be a prime number in $\mathbb{Z}$. Notice that it is possible for a prime in $\mathbb{Z}$ to be no longer be irreducible in $\mathbb{Z}[i]$. For example, $2 = (1 + i)(1 - i)$ or $13 = (2 + 3i)(2 - 3i)$. However, some primes are still irreducible in $\mathbb{Z}[i]$.

(a) Prove that if $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$, then p is reducible in $\mathbb{Z}[i]$.
Answer: We have $p = a^2 + b^2 = (a + bi)(a - bi)$ for $a, b \in \mathbb{Z}$. Note that $a, b \neq 0$ since p is prime (or else

we would have $p = a^2 \implies a|p$ or $p = b^2 \implies b|p$); therefore neither $a + bi$ nor $a - bi$ is a unit so p is reducible into $(a + bi)(a - bi)$.

(b) Prove that if p is prime in $\mathbb{Z}$ but is reducible in $\mathbb{Z}[i]$ then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Answer: Since p is reducible, we have $p = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$ that are not units. Then $N(\alpha)N(\beta) = N(p) = p^2 \implies N(\alpha) = N(\beta) = p$ since $N(\alpha) \neq 1$ and $N(\beta) \neq 1$. Now let $\alpha = a + bi$ where $a, b \in \mathbb{Z}$, then $p = N(\alpha) = N(a + bi) = a^2 + b^2 \implies p = a^2 + b^2$.