# Exam 3

**1)** [20 points] Use the *Euclidean Algorithm* to find the GCD of $f = x^7 + x^6 + 2x^4 + x^3 + x^2 + x + 2$ and $g = x^6 + 2x^5 + x^4 + x^3 + x^2 + 2x + 1$ in $\mathbb{F}_3[x]$.

*Solution.* We have:

$$\begin{aligned} f &= (x+2) \cdot g + (x^5 + 2x^4 + x^3 + 2x) \\ g &= x \cdot (x^5 + 2x^4 + x^3 + 2x) + (x^3 + 2x^2 + 2x + 1) \\ x^5 + 2x^4 + x^3 + 2x &= (x^2 + 2) \cdot (x^3 + 2x^2 + 2x + 1) + (x^2 + x + 1) \\ x^3 + 2x^2 + 2x + 1 &= (x+1) \cdot (x^2 + x + 1) + 0. \end{aligned}$$

Hence, $\gcd(f, g) = x^2 + x + 1$. □

**2)** [20 points] Let $k$ be a field and $p_1, p_2, p_3, p_4 \in k[x]$ be monic irreducible polynomials in $k[x]$. Suppose that

$$f = a \cdot p_1^2 \cdot p_2^r \cdot p_3^s \qquad \text{and} \qquad g = b \cdot p_1^t \cdot p_2^3 \cdot p_4,$$

where $a, b \in k$, $a, b \neq 0$, and $r$, $s$ and $t$ are non-negative integers. If we *know* that

$$\gcd(f, g) = p_1 \cdot p_2^3 \qquad \text{and} \qquad \operatorname{lcm}(f, g) = p_1^2 \cdot p_2^3 \cdot p_3^5 \cdot p_4,$$

then what are $r$, $s$ and $t$?

*Solution.* We have that, by the power of $p_1$ in the GCD, that $1 = \min(2, t)$ and hence $t = 1$. Also, by the powers of $p_2$ in the GCD and LCM, we have that $\min(r, 3) = \max(r, 3) = 3$, and thus $r = 3$. Finally, by the power of $p_3$ in the LCM, we have that $5 = \max(s, 0)$, so $s = 5$. □

**3)** [20 points] Let $k$ be a field and $f$ and $g$ be distinct, monic, irreducible polynomials in $k[x]$. Prove that the polynomials $f^2 \cdot g^3$ and $f^3 \cdot g^2$ are *never* equal.

[**Hint:** If you are having a hard time figuring out, try to see what this would say in terms of integers instead of polynomials.]

*Proof.* If $f^2 \cdot g^3 = f^3 \cdot g^2$, then we would have different factorizations into irreducibles for the same polynomial, which cannot happen. □

**4)** Examples:

(a) [10 points] Give an example of a domain $R$ such that $R$ is a subring of $\mathbb{F}_2(x)$, but $R$ is *not* a field.

*Solution.* $\mathbb{F}_2[x]$ works. □

(b) [10 points] Give an example of a field $F$ that contains $\mathbb{C}(x)$ properly [i.e., a field $F$ that contains $\mathbb{C}(x)$ but is different from $\mathbb{C}(x)$ itself].

*Solution.* $\mathbb{C}(x)(y)$ [i.e., add a new variable $y$ and make a field of rational functions with coefficients in $\mathbb{C}(x)$] works. [This field can be simply denoted by $\mathbb{C}(x, y)$] □

**5)** Determine if the polynomials below are irreducible or not in the corresponding polynomial ring. *Justify each answer!*

(a) [4 points] $f = x^7 + 6x^6 - 27x^4 + 120x^3 - 3x - 15$ in $\mathbb{Q}[x]$.

*Solution.* Irreducible by Eisenstein's Criterion for $p = 3$. □

(b) [4 points] $f = x^4 + x + 1 \in \mathbb{F}_5[x]$.

*Solution.* By "brute force" one can check that 3 is a root. Since $\deg(f) > 1$, the polynomial is reducible. □

(c) [4 points] $f = \pi^2\, x - \sqrt{137}$ in $\mathbb{R}[x]$.

*Solution.* The polynomials has degree one, so it is irreducible. □

(d) [4 points] $f = x^6 - 5x^5 - 2x^4 - 4x^2 + x + 1$ in $\mathbb{Q}[x]$.

*Solution.* Using the *Rational Root Test* we see that $-1$ is a root. Since $\deg(f) > 1$, it is reducible. □

(e) [4 points] $f = 304x^3 + 123x^2 - 34x + 90001$ in $\mathbb{Q}[x]$.

*Solution.* Reducing modulo 3 we get $\bar{f} = x^3 - x + \bar{1}$. Now, $\bar{f}(\bar{0}) = \bar{f}(\bar{1}) = \bar{f}(\bar{2}) = 1$. So, $\bar{f}$ has no roots in $\mathbb{F}_3$, and since $\deg(\bar{f}) = 3$, it is irreducible. So, $f$ is also irreducible. □

**Note:** There was a typo on 5(d) in the original exam. The polynomial was: $f = x^6 - 5x^5 - 2x^4 - 3x^2 + x + 2$ [in $\mathbb{Q}[x]$] instead. This is much harder than what I had planned. But here is a possible solution.

With rational root test we can see it has no rational roots: $f(1) = -6$, $f(-1) = 2$, $f(2) = -136$, $f(-2) = 180$. So, if it factors in $\mathbb{Q}[x]$, no factor has degree one. So, $f$ would then be either a product of two [irreducible] polynomials of degree 3 or a product of polynomials of degree 4 [not necessarily irreducible] and of degree 2 [irreducible]. [So, this takes into account that $f$ is the product of three irreducible polynomials of degree 2.] Moreover, by *Gauss's Lemma*, the coefficients in this factorization must be *integers*. [This is extremely important to the solution presented.]

*Case 1:* Assume it is a product of two polynomials of degree 3. Note that, without loss of generality, we may assume both are monic. [Do you understand why we can do that?] So, let's say:

$$f = (x^3 + ax^2 + bx + c)(x^3 + dx^2 + ex + g),$$

with $a, b, c, d, e, g \in \mathbb{Z}$. Expanding and collecting terms of same power of $x$, we have:

$$\begin{aligned} &x^6 - 5x^5 - 2x^4 - 3x^2 + x + 2 = \\ &\quad x^6 + (a+d)x^5 + (e + ad + b)x^4 + (g + ae + bd + c)x^3 + (ag + be + cd)x^2 + (bg + ce)x + cg. \end{aligned}$$

Comparing the coefficients we get the system:

$$a + d = -5 \tag{1}$$
$$e + ad + b = -2 \tag{2}$$
$$g + ae + bd + c = 0 \tag{3}$$
$$ag + be + cd = -3 \tag{4}$$
$$bg + ce + d = 1 \tag{5}$$
$$cg = 2 \tag{6}$$

Now, since all the unknowns are *integers*, Eq. (6) gives us that either $c = \pm 2$ and $g = \pm 1$, or $c = \pm 1$ and $g = \pm 2$. Since we could switch the two polynomials [as they have the same degree], we may assume, without loss of generality, that $c = \pm 1$ and $g = \pm 2$.

Eq. (5) gives us then that:

$$\pm 2b \pm e = 1 \quad \Longrightarrow \quad e = \pm 1 - 2b.$$

Also, Eq. (1) gives us that $d = -5 - a$. These last two, when replaced in Eq. (4), give us

$$\pm 2a + b(\pm 1 - 2b) \pm (-5 - a) = -3 \quad \Longrightarrow \quad a = \pm 2b^2 - b + (5 \pm 3).$$

Since we have $d = -5 - a$, this last equation allows us to write $d$ in terms of $b$ only. Hence, all unknowns can be expressed in terms of $b$ only. Substituting these values on Eq. (4) gives us two equations, depending on the choice of sign, namely:

$$2b^2 + 2b + 10 = 0 \quad \text{[choosing postive]},$$
$$2b^2 + 4b - 10 = 0 \quad \text{[choosing negative]}.$$

But in either case, $b$ would not be an integer [which you can check using the quadratic formula or rational root test]. So, this factorization is impossible!

*Case 2:* Now we assume it factors as a product of polynomials of degree 4 and 2, say:

$$f = (x^4 + ax^3 + bx^2 + cx + d)(x^2 + ex + g),$$

with $a, b, c, d, e, g \in \mathbb{Z}$. Expanding and collecting terms of same power of $x$, we have:

$$\begin{aligned} x^6 - 5x^5 - 2x^4 - 3x^2 + x + 2 = \\ x^6 + (a+e)x^5 + (g + ae + b)x^4 + (ag + be + c)x^3 + (bg + ce + d)x^2 + (cg + de)x + dg. \end{aligned}$$

Comparing the coefficients we get the system:

$$a + e = -5 \tag{7}$$
$$g + ae + b = -2 \tag{8}$$
$$ag + be + c = 0 \tag{9}$$
$$bg + ce + d = -3 \tag{10}$$
$$cg + de = 1 \tag{11}$$
$$dg = 2 \tag{12}$$

As before, since the unknown are integers, we have that Eq. (12) tells us that either $d = \pm 1$ and $g = \pm 2$, or vice-versa. The problem in here is that since the degrees are different, we can't assume one case without loss of generality. So, we have to look at each case individually.

*Subcase 2(a):* $d = \pm 2$, $g = \pm 1$. Eq. (7) gives us that $e = -5 - a$. Also, Eq. (11) gives us that

$$\pm c + \pm 2e = 1 \quad \Longrightarrow \quad c = \pm 1 - 2e = 2a + 10 \pm 1.$$

Then, Eq. (8) gives us:

$$\pm 1 + a(-5 - a) + b = -2 \quad \Longrightarrow \quad b = a^2 + 5a - (2 \pm 1).$$

So, again, we have all unknowns in terms of $a$. Substituting their values in Eq. (10), we get:

$$\begin{aligned} -a^2 + 24a - 43 = 0 \quad \text{[choosing postive]}, \\ -3a^2 + 16a - 53 = 0 \quad \text{[choosing negative]}. \end{aligned}$$

But, again, in either case, $a$ would not be an integer [which you can check using the quadratic formula or rational root test]. So, this factorization is impossible!

*Subcase 2(b):* $d = \pm 1$, $g = \pm 2$. Again, Eq. (7) gives us that $e = -5 - a$. Also, Eq. (11) now gives us that

$$\pm 2c + \pm e = 1 \quad \Longrightarrow \quad e = \pm 1 - 2c.$$

So, since $e = -5 - a = \pm 1 - 2c$, we get $a = 2c - 5 \mp 1$. Then, Eq. (8) gives us:

$$\pm 2 + (2c - 5 \mp 1)(\pm 1 - 2c) + b = -2 \quad \Longrightarrow \quad b = 4c^2 - (10 \pm 4)c \pm 3 - 1.$$

So now we have all unknowns in terms of $c$. Substituting their values in Eq. (10), we get:

$$\begin{aligned} 6c^2 - 27c + 8 = 0 \quad \text{[choosing postive]}, \\ -10c^2 + 11c + 10 = 0 \quad \text{[choosing negative]}. \end{aligned}$$

But, again, in either case, $c$ would not be an integer [which you can check using the quadratic formula or rational root test]. So, this factorization is also impossible!