1. A friend comes to you and asks if a particular polynomial $p(x)$ of degree 16 in $\mathbb{F}_3[x]$ is irreducible. The friend explains that he has tried dividing $p(x)$ by every polynomial in $\mathbb{F}_3[x]$ of degree from 1 to 10 and has found that $p(x)$ is not divisible by any of them. He is getting tired of doing all these divisions and wonders if there’s an easier way to check whether or not $p(x)$ is irreducible. You surprise your friend with the statement that he need not do any more work: $p(x)$ is indeed irreducible!

Prove this; that is, use the fact that no polynomial of degree between 1 and 10 divides $p(x)$ to prove that $p(x)$ is irreducible. Do not simply quote a theorem that makes this problem trivial; rather, provide an argument “from scratch” using the given information. You may use the fact that the degree of a product of two polynomials is the sum of the degrees of the two polynomials.

**Solution.** In order to show that $p(x)$ is irreducible, I need to show (according to the definition) that every factorization of $p(x)$ is trivial. Suppose $p(x)$ factors as a product of polynomials in $\mathbb{F}_3[x]$, $p(x) = g(x)h(x)$; I want to show that this must be a trivial factorization. Let $\deg g(x) = n$; then since the degree of a product is the sum of the degrees, $16 = n + \deg h(x)$, so $\deg h(x) = 16 - n$.

Note also that if either $g(x)$ or $h(x)$ is zero, then their product is zero. Their product has degree 16, while the zero polynomial has degree $-\infty$; hence neither $g(x)$ nor $h(x)$ equals zero. Thus both of their degrees are greater than or equal to zero, and so both are less than or equal to 16: $0 \leq n \leq 16$ and $0 \leq 16 - n \leq 16$.

By our friend’s computations, we know that no polynomial of degree between 1 and 10 divides $p(x)$. Therefore neither $n$ nor $16 - n$ is between 1 and 10. If $10 < n < 16$, then $6 > 16 - n > 0$, but $16 - n$ can’t be between 1 and 10, so this can’t happen. This leaves two possibilities: Either $n = 0$ and $16 - n = 16$, or $n = 16$ and $16 - n = 0$. In other words, the only way to factor $p(x)$ is if one of the factors has degree zero. But the degree zero polynomials are the units in $K[x]$, and any factorization $p(x) = g(x)h(x)$ where one factor is a unit is a trivial factorization. Therefore every factorization of $p(x)$ is trivial, and so $p(x)$ is irreducible.

(A slight variant on this approach: I could assume that $p(x)$ factors nontrivially as $p(x) = g(x)h(x)$. “Nontrivially” means that neither of the factors is zero and one of the two factors is a unit. Since the units in $\mathbb{F}_3[x]$ are precisely the degree zero polynomials, this means that I am assuming that neither $g(x)$ nor $h(x)$ is a unit, which is the same as saying that both $g(x)$ and $h(x)$ have positive degree. From this point, I would proceed as above, eventually getting a contradiction. Thus my assumption that there is a nontrivial factorization was wrong, so $p(x)$ must be irreducible.)
2. Suppose that $f(x)$ is the cubic polynomial $x^3 - 6x + 4$ in $\mathbb{R}[x]$. Using standard graphing techniques from calculus, one can easily show that the graph of $y = f(x)$ crosses the $x$-axis three times. (You don’t have to prove this.) This tells us that $f(x)$ has three real roots.

(a) Use Cardano’s Formula to write down an expression for one of the roots of $f(x)$ and observe that the expression you obtained is the sum of the cube roots of two non-real complex numbers.

(b) Explain how it is possible for this expression to be a real number even though it involves non-real numbers.

**Solution.**

(a) Cardano’s Formula says that one root of the cubic polynomial $x^3 + px + q$ is given by the formula

$$\sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \sqrt[3]{-\frac{q}{2} - \sqrt{R}},$$

where

$$R = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2.$$

In this case, $p = -6$ and $q = 4$, so $R = (-6/3)^3 + (4/2)^2 = -8 + 4 = -4$, so the root is

$$\sqrt[3]{-\frac{4}{2} + \sqrt{-4}} + \sqrt[3]{-\frac{4}{2} - \sqrt{-4}} = \sqrt[3]{-2 + 2i} + \sqrt[3]{-2 - 2i}.$$

Note that this is the sum of the cube roots of two (non-real) complex numbers.

(b) The two complex numbers are conjugates of each other, though, and I claim that the cube root of the conjugate of some number is the conjugate of the cube root of that number. We know that, if $z_1$ and $z_2$ are complex numbers, then $\overline{z_1z_2} = \overline{z_1}\overline{z_2}$, and therefore $\overline{z^3} = \overline{z}^3$. Take cube roots of both sides: $\sqrt[3]{\overline{z^3}} = \sqrt[3]{\overline{z}^3} = \overline{z}$. Make the substitution $r = z^3$ (and so $z = \sqrt[3]{r}$); then this equality becomes $\sqrt[3]{r} = \overline{\sqrt[3]{r}}$. This is exactly my claim: the cube root of the conjugate of $r$ is the conjugate of the cube root of $r$.

In the particular case in question, the cube root of $r = -2 + 2i$ will be some complex number, say $z = a + bi$. By the argument in the previous paragraph, the cube root of its conjugate $-2 - 2i$ will be the conjugate of its cube root, which is $a - bi$. So their sum, which is the root of the cubic in question, is $(a + bi) + (a - bi) = 2a$, a real number.

(It turns out that you can compute the cube roots in this case; one way is to use Euler’s formula $e^{i\theta} = \cos \theta + i \sin \theta$. You can compute $\sqrt[3]{-2 + 2i} = 1 + i$ and $\sqrt[3]{-2 - 2i} = 1 - i$, so the root given by Cardano’s formula is $(1 + i) + (1 - i) = 2$. At this point, it doesn’t hurt to verify that 2 is indeed a root of $x^3 - 6x + 4$. Once you have this root, you can compute the other roots; divide $x^3 - 6x + 4$ by $x - 2$ to get $x^2 + 2x - 2$. Then the quadratic formula gives the other two roots: $-1 + \sqrt{3}$ and $-1 - \sqrt{3}$.)
3. Prove that the polynomial

$$4x^{24} + 9x^5 + 15$$

does not factor in $\mathbb{Z}[x]$ as the product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ whose degrees are both less than 24. (Do not simply quote and apply a major theorem. Rather, give a proof from scratch.)

**Solution.** Suppose this polynomial does factor as the product $g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ with degree less than 24. I want to derive a contradiction. The idea is to follow the proof of Eisenstein’s criterion for this particular example.

Let $k = \deg g(x)$ and $\ell = \deg h(x)$ (so that $k + \ell = 24$ and both $k$ and $\ell$ are less than 24). Let

$$g(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0,$$

$$h(x) = b_\ell x^\ell + b_{\ell-1} x^{\ell-1} + \cdots + b_1 x + b_0.$$

Then for any $j$, the coefficient of $x^j$ in the product $g(x)h(x)$ is

$$a_0 b_j + a_1 b_{j-1} + \cdots + a_{j-1} b_1 + a_j b_0.$$

For example, the constant term is $15 = a_0 b_0$.

Since 3 divides 15, 3 must divide one of $a_0$ and $b_0$. Since $3^2$ does not divide 15, 3 does not divide both $a_0$ and $b_0$. Without loss of generality, I’ll suppose that 3 divides $a_0$ and not $b_0$.

I claim that as a result, 3 divides all of the coefficients of $g(x)$. I’ll prove this by induction. Suppose that 3 divides $a_0$, $a_1$, ..., $a_{j-1}$. Since $g(x)$ is of degree $k < 24$, I can assume that $j - 1 < k < 24$. (If $j - 1 = k$, then I have already accounted for all of the coefficients of $g(x)$.)

To understand $a_j$, where $j \leq k < 24$, I’ll look at the coefficient of $x^j$ in $g(x)h(x)$. By the formula above, this is

$$a_0 b_j + a_1 b_{j-1} + \cdots + a_{j-1} b_1 + a_j b_0.$$

Also, since $j < 24$, this is not the leading term of the original polynomial, and all the coefficients except the leading one are divisible by 3. Thus I can write the coefficient of $x^j$ in the original polynomial as $3r$ for some number $r$. This equals the above expression, so I can almost isolate $a_j$:

$$a_j b_0 = 3r - a_0 b_j - a_1 b_{j-1} - \cdots - a_{j-1} b_1.$$

Since each coefficient $a_i$, $0 \leq i \leq j - 1$, is divisible by 3, the entire right side is divisible by 3, and therefore 3 divides $a_j b_0$. Since 3 is prime, it must divide either $a_j$ or $b_0$. By assumption, $b_0$ is not divisible by 3, and so $a_j$ is divisible by 3. So I deduce, by induction, that all of the coefficients of the polynomial $g(x)$ are divisible by 3.

Now look at the highest-degree term of my polynomial. On one hand, it’s equal to $4x^{24}$. On the other hand, it’s equal to $a_k x^k b_\ell x^\ell$. I already knew that $k + \ell = 24$, so I get this equality: $4 = a_k b_\ell$. By the previous argument, $a_k$ is divisible by 3. 4 is not divisible by 3, and this is a contradiction. Hence the assumed factorization cannot exist, and that’s what I wanted to show.
4. Prove that the polynomial
\[ 21x^4 - 16x^2 + 11x + 63 \]
does not factor in \( \mathbb{Z}[x] \) as the product of two polynomials \( g(x) \) and \( h(x) \) whose degrees are both less than 4. (You may use theorems for this problem, as long as you explain what you’re using.)

**Solution.** I will use “reduction mod \( p \)”. One of our theorems says this: suppose \( f(x) \) is a polynomial in \( \mathbb{Z}[x] \), and \( p \) is a prime number. If the highest degree term in \( f(x) \) is not divisible by \( p \), and if the mod \( p \) reduction of \( f(x) \) is irreducible in \( \mathbb{F}_p[x] \), then \( f(x) \) cannot be factored as a product of two polynomials of smaller degree.

I will apply this theorem to the polynomial \( f(x) = 21x^4 - 16x^2 + 11x + 63 \), with \( p = 2 \) – note that 2 does not divide 21, the leading term. The mod 2 reduction of \( f(x) \) is \( \overline{f}(x) = x^4 + x + 1 \), and if I can show that \( \overline{f}(x) \) is irreducible in \( \mathbb{F}_2[x] \), then by the theorem, I can conclude that \( f(x) \) doesn’t factor as a product \( g(x)h(x) \) of polynomials of degree less than 4.

To show that \( \overline{f}(x) = x^4 + x + 1 \) is irreducible in \( \mathbb{F}_2[x] \), I will consider the possible ways it can factor. Since its degree is 4, it can only factor as the product of a degree 1 factor and a degree 3 factor, or as the product of two degree 2 factors.

Having a linear factor is equivalent to having a root in \( \mathbb{F}_2 \), and I check that \( \overline{f}(x) \) has no roots by just plugging in the elements of \( \mathbb{F}_2 \): \( \overline{f}(0) = 1 \) and \( \overline{f}(1) = 1 + 1 + 1 = 1 \). Neither 0 nor 1 is a root, so \( \overline{f}(x) \) has no roots, so \( \overline{f}(x) \) has no linear factors.

Since it has no linear factors, the only other way it could factor is as a product of two quadratics. In this case, the two quadratics must be irreducible – if they factored into linear terms, then those linear terms would divide \( \overline{f}(x) \), and we know that this doesn’t happen.

I can list all of the degree two polynomials in \( \mathbb{F}_2[x] \), because the only possible coefficients are 0 and 1:
\[ x^2, \ x^2 + 1, \ x^2 + x, \ x^2 + x + 1. \]
I am only interested in the irreducible ones of these, and the only way a quadratic can factor nontrivially is into linear terms. That means that a quadratic factors if and only if it has roots, so it’s irreducible if and only if it has no roots. Note that 0 is a root of both \( x^2 \) and \( x^2 + x \), and 1 is a root of \( x^2 + 1 \). \( x^2 + x + 1 \) has no roots – you can check this by plugging in 0 and 1 – so it is the only irreducible degree 2 polynomial in \( \mathbb{F}_2[x] \).

As I said earlier, since \( \overline{f}(x) = x^4 + x + 1 \) has no linear factors, the only possible way for it to factor is as a product of two irreducible degree 2 polynomials. Since there is only one such irreducible, the only way for it to factor is like this:
\[ x^4 + x + 1 \equiv (x^2 + x + 1)(x^2 + x + 1). \]
This is not an equality: the right side is \( x^4 + x^2 + 1 \). Therefore \( x^4 + x + 1 \) is indeed irreducible in \( \mathbb{F}_2(x) \), and so \( 21x^4 - 16x^2 + 11x + 63 \) cannot be factored in \( \mathbb{Z}[x] \) as a product of lower degree polynomials.

(Alternatively, you can just divide \( x^4 + x + 1 \) by \( x^2 + x + 1 \) and show that there is a nonzero remainder – it happens to be 1 – and therefore \( x^4 + x + 1 \) is not divisible by the only degree two irreducible, and so it’s irreducible.)
5. Let $K$ be a field.

(a) State Bezout’s Theorem for a pair of polynomials $a(x)$ and $b(x)$ in $K[x]$.

**Solution.** Let $K$ be a field, let $a(x)$ and $b(x)$ be elements of $K[x]$, and let $d(x)$ be the greatest common divisor of $a(x)$ and $b(x)$ produced by the Euclidean algorithm. Then there exist $r(x)$ and $s(x)$ in $K[x]$ such that
\[ a(x)r(x) + b(x)s(x) = d(x). \]

(Note that, first of all, greatest common divisors in $K[x]$ are not unique, and that, second of all, this theorem is a statement about a particular one of those greatest common divisors. I’ll say more about this in class.)

(b) Prove the statement below.

Suppose that $a(x)$ and $b(x)$ are relatively prime polynomials in $K[x]$ and $a(x)$ divides the product $b(x)c(x)$ in $K[x]$. Then $a(x)$ divides $c(x)$.

You may use Bezout’s theorem in your proof. If you do, be sure to make clear where and how you are using it.

**Solution.** Since $a(x)$ and $b(x)$ are relatively prime, then any of their greatest common divisors $d(x)$ has degree zero – it’s a nonzero constant. Indeed, every nonzero constant is a greatest common divisor. The Euclidean algorithm will produce one of these, so it will give some particular constant, say $d$. So by Bezout’s theorem, there exist polynomials $r(x)$ and $s(x)$ so that
\[ a(x)r(x) + b(x)s(x) = d(x). \]

Since $d$ is a nonzero constant, it has an inverse in $K$, because $K$ is a field. Multiply by that inverse:
\[ a(x)r(x)d^{-1} + b(x)s(x)d^{-1} = 1. \]

Multiply this equation by $c(x)$:
\[ a(x)r(x)c(x)d^{-1} + b(x)c(x)s(x)d^{-1} = c(x). \]

By assumption, $a(x)$ divides $b(x)c(x)$, which means that there is some polynomial $q(x)$ so that $b(x)c(x) = a(x)q(x)$. Make this substitution:
\[ a(x)r(x)c(x)d^{-1} + a(x)q(x)s(x)d^{-1} = c(x). \]

Therefore
\[ c(x) = a(x)\left(d^{-1}r(x)c(x) + d^{-1}q(x)s(x)\right). \]

So $c(x)$ is some polynomial times $a(x)$, and therefore $c(x)$ is divisible by $a(x)$. 