UD. Algebra I. Some Exercises. F. Lazebnik.

The symbol * marks harder problems (in my opinion).

1. *Study a proof of the divergence of the series $\sum_p \frac{1}{p}$, where p ranges over the set of all positive primes. It turns out that if we use finitely many primes, all up to n, then their sum is $\sim \ln\ln n$, when $n \to \infty$, a very nice fact. As we know, $\sum_{n\geq 1} \frac{1}{n} \sim \ln n, n \to \infty$. I like Euler's "semi-rigourous" proof: search in Google for "Divergence of the sum of the reciprocals of the primes" in Wikipedia.

   See how this result can be used to show that there are no infinite arithmetic progressions with every elements being a prime number (this part is easy).

2. For numerical experimentation, you can use computer, if you wish. For example, investigate what Mathematica can do for you. Start Mathematica, go to Documentation, search for Number theory, or Diophantine equations, or `Mod`, or `PowerMod`, or Number Theoretic Functions, etc.. Explore.

3. Given $n \geq 3$ integers such that every two are coprime. Are all the integers coprime?

   Given $n \geq 3$ coprime integers. Are any two of them coprime?

4. Let $ab = c^n$, where a, b, c, n are integers, $(a, b) = 1$ and $n \geq 1$. Prove that both a and b are the n-th powers of integers. (This fact will be used later in this course.)

5. Let $p \neq \pm 1$ have the property that for any a, b, $p|ab$ implies that $p|a$ or $p|b$. Prove that this property is equivalent to p being prime.[1]

6. Here are some questions on Fermat's and Euler's theorems. When you do these problems by hand, try to avoid computations with integers that result in numbers larger than 1000.

   (a) Use theorems of Euler and Fermat to find the remainder of the division of

   (i) 6^{342} by 17; (ii) 18^{342} by 25.

   Check your results by using `PowerMod`.

[1]The following definitions make sense for all integral domains R with $1 \neq 0$. An element a of R is called **irreducible** if a is not a unit in R and $a = bc$ implies that either b or c is a unit in R.

A nonzero element p in R is called **prime** if p is not a unit and $p|ab$ implies that $p|a$ or $p|b$. The statement of this problem implies that in $\mathbb{Z}$ the notions of 'irreducible' and 'prime' are equivalent. Later we will see rings, where these notions differ) The only reason that irreducible elements in $\mathbb{Z}$ are called primes, is because of the tradition, in lower level courses.

(b) What are the last three digits in the decimal representation of 2019^{2019}?

Check your results by using `PowerMod`.

(c) *Prove that for every integer a, $a^{1729} \equiv a \pmod{1729}$. Do it without using computer. Explain that this implies that the converse statement to Fermat's Little Theorem is false. If you wish, please check it (which is the same that proving it) with computer.

(d) Show that if $a^{\phi(n)} \equiv 1 \pmod{n}$, then $(a, n) = 1$.

(e) If $(a_1, \ldots, a_n) = 1$, does it imply $\phi(a_1 \cdots a_n) = \phi(a_1) \cdots \phi(a_n)$?

(f) Given $(a, n) = 1$, does it imply that $\phi(n)$ is the smallest positive exponent s such that $a^s \equiv 1 \pmod{n}$? The same question if $n = p$, where p a prime.

(g) Prove that for each $n \geq 2$, the sum of all positive integers smaller than n and relatively prime with n is equal to $n\phi(n)/2$.

(h) *Prove that $\lim_{n\to\infty} \phi(n) = \infty$.

7. (a) Prove an additive recurrence for the Euler's function ϕ: $\sum_{d|n} \phi(d) = n$ by busing the formula for $\phi(n)$ in terms of the prime factorization of n.

(b) Prove the recurrence $\sum_{d|n} \phi(d) = n$ by <u>not</u> using the formula for $\phi(n)$ in terms of the prime factorization of n.

Hint: This fact is presented in many texts in different contexts, like cyclic groups, complex roots of unity, finite fields. The amazingly simple proof is this:[2] Consider all proper fractions of the form a/n. There are n of those. When you consider their reduced forms (which are unique) you get fractions of the form b/d with $d|n$ and $(b, d) = 1$. By definition of ϕ, there are $\phi(d)$ of those. The result follows.

(c) Prove that the additive recurrence above can be used to show that Euler function is multiplicative, i.e., $\phi(1) = 1$ and $\phi(ab) = \phi(a)\phi(b)$ for any relatively prime positive integers a, b.

Parts (b) and (c), together with the obvious fact that $\phi(p^e) = p^e - p^{e-1}$ for p prime, lead to another proof of the formula for $\phi(n)$ in terms of the prime factorization of n.

8. Möbius function $\mu(n)$ is another important number-theoretic function that often appears in algebra. It is defined as follows.

$$\mu(n) = \begin{cases} 1, \text{ if } n = 1, \\ 0, \text{ if } a^2|n \text{ for some integer } a \geq 2 \\ (-1)^k, \text{ if } n = p_1 p_2 \cdots p_k, \text{ where } k \geq 1, \text{ and } p_1, \ldots, p_k \text{ are distinct primes.} \end{cases}$$

Hence, the only values of $\mu(n)$ are $-1, 0, 1$. Prove the following several properties of the Möbius function.

[2] See https://math.stackexchange.com/questions/504063/show-sum-limits-dn-phid-n

(a) (Multiplicativity.) For any two relatively prime positive integers a and b, $\mu(ab) = \mu(a)\mu(b)$.

(b)
$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ for } n = 1, \\ 0 \text{ for } n > 1. \end{cases}$$

The summation is over all distinct positive divisors d of n.)

This property gives an additive recurrence for $\mu(n)$: $\mu(1) = 1$, and for $n > 1$,

$$\mu(n) = \sum_{d|n \text{ and } 1 \le d < n} \mu(d).$$

(c) (The Möbius Inversion Formula.) For any two sequences (a_n) and (b_n),

$$\text{if} \quad b_n = \sum_{d|n} a_{n/d}, \quad \text{then} \quad a_n = \sum_{d|n} \mu(n/d) b_d.$$

The summations are over all distinct positive divisors of n.

(d) Apply the The Möbius Inversion Formula to the additive recurrence $\sum_{d|n} \phi(d) = n$.

9. Since $a^{\phi(n)} = a^{\phi(n)-1} \cdot a \equiv 1 \pmod{n}$, the number $a^{\phi(n)-1}$ can be viewed as an explicit expression of the multiplicative inverse of a modulo n, $(a, n) = 1$. Use this fact to solve the following congruences. Then solve them by using the Euclidean algorithm. Present the answer in the form $x = r + nt$, $t \in \mathbb{Z}$, where $0 \le r < n$. The answers may look different, but they must be equivalent, and you should understand why.

(i) $8x \equiv_{15} 3$; (ii) $8x \equiv_{17} 3$.

Check your solutions by using `Reduce` command.

10. Find a general solutions of the diophantine equation $48x + 621y - 258z = 6$, and explain the way you found it.

Compare your solution with the one obtained with Mathematica. They may look different, but must be equivalent, and you should understand why.

11. Many of you might have seen the description of all integer solutions of the equation $x^2 + y^2 = z^2$, i.e., the famous "Pythagoras triples". One approach for finding all of them, is to parameterize the set of all rational points (except one) of the unit circle $u^2 + v^2 = 1$ by a rational parameter.[3] Use a similar technique to find all solutions in integers of the

[3]It is easy to find this approach in books or on the web. See, e.g., a very thorough Chapter 2,3 in `http://www.math.brown.edu/~jhs/frintdir/frintch2ch3.pdf`. This approach can be considered as a glimpse into algebraic geometry, and it clearly works for any conic section.

equation $x^2 + 2y^2 = 3z^2$, assuming that $\gcd(x, y, z) = 1$. Your final answer should be expressed in terms of integers. (You can use Mathematica to assist you with algebraic manipulations if you wish.)

Check that the expressions you found are indeed solutions by direct substitution.

12. (Optional.) A fast computational scheme for the division with remainder of a polynomial f by $x - c$ is the Horner scheme, also known by the term Synthetic Division. Since $f(c)$ is equal to the remainder of this division, the scheme is a good way of *computing* $f(c)$. Even though the algorithm is named after William George Horner, who described it in 1819, the method was already known to Isaac Newton in 1669, to the Chinese 13th century mathematician Qin Jiushao, to the 12th century Persian Muslim mathematician Sharaf al-Di-n al-Tu-si. The earliest use of Horner's scheme was in The Nine Chapters on the Mathematical Art, a Chinese work of the Han Dynasty (202 BC – 220 AD) edited by Liu Hui (fl. 3rd century). If you do not know the scheme, please check your texts, or just Google the terms.

13. Show that there is a polynomial f over $\mathbb{C}$ distinct from x^2 such that $f(0) = 0$, $f(1) = 1$, $f(2) = 4$ and $f(3) = 9$? Describe all such polynomials f. Justify your answers.

14. The sum of two roots of the equation $2x^3 - x^2 - 7x + \lambda = 0$ is equal to 1. Find λ.

15. One root of the equation $x^3 - 7x + \lambda = 0$ is twice the another root. Find λ.

16. Find the sum of squares of all roots of the equation $2x^7 - 5x^6 - 7x + 1 = 0$.

17. Construct a polynomial whose complex roots are the squares of the roots of the equation $x^3 + x^2 + x + 2 = 0$.

18. Construct a polynomial whose complex roots are the reciprocals of the roots of the equation $x^3 + x^2 + x + 2 = 0$.

19. Let $d = (m, n)$. Prove that $(X^m - 1, X^n - 1) = X^d - 1$. All polynomial are considered over an integral domain R.

20. Find all A and B such that the polynomial $AX^4 + BX^3 + 1$ is divisible by $(X - 1)^2$.

21. Find necessary and sufficient conditions on p, q, m, such that $x^3 + px + q$ is divisible by $x^2 + mx - 1$.

22. Let f be a polynomial (over $\mathbb{C}$) which gives a remainder A when divided by $x - a$, a remainder B when divided by $x - b$, and a remainder C when divided by $x - c$, $a, b, c \in \mathbb{C}$ and are all distinct. Find the remainder of the division of f by $(x - a)(x - b)(x - c)$.

23. Let $\{x_1, \ldots, x_n\}$ be n elements from a field $\mathbb{F}_q$.

(a) Prove that the determinant of the Vandermonde's matrix $V(x_1, x_2, \ldots, x_n)$ is:

$$\det(V(x_1, x_2, \ldots, x_n)) = \det \begin{bmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ {x_1}^2 & {x_2}^2 & \ldots & {x_n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ {x_1}^{n-1} & {x_2}^{n-1} & \ldots & {x_n}^{n-1} \end{bmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

(b) Use the fact from (a) to show that a polynomial of degree $n \geq 1$ has at most n distinct roots.

(c) Use the fact from (a) to show that for every $n+1$ ordered pairs of elements of $\mathbb{F}_q$, $(x_1, y_1), \ldots, (x_{n+1}, y_{n+1})$, all x_i are distinct, there exists a unique polynomial $f \in \mathbb{F}_q[x]$ of degree at most n, such that $f(x_i) = y_i$ for all i (*interpolation* polynomial). Can it happen that $\deg f < n$?

24. Let $x_1, \ldots, x_{n+1}$ be distinct elements of a field $\mathbb{F}_q$, and let $y_1, \ldots, y_{n+1}$ be arbitrary elements of $\mathbb{F}_q$. Define

$$f_n(x) = \sum_{i=1}^{n+1} y_i \cdot \frac{(x - x_1)(x - x_2) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_{n+1})}{(x_i - x_1)(x_i - x_2) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_{n+1})}.$$

This gives $f_0(x) = y_1$, $f_1(x) = y_1 \cdot \frac{x - x_2}{x_1 - x_2} + y_2 \cdot \frac{x - x_1}{x_2 - x_1}$.

(a) Write the expressions for $f_2(x)$ for $n = 2$.

(b) Let $\mathbb{F}_q = \mathbb{Q}$, $x_1 = 1$, $x_2 = 2$, $x_3 = 3$ and $y_1 = -4$, $y_2 = -1$, $y_3 = 2$. Compute $f_2(x)$.

(c) Prove that $f_n(x_k) = y_k$ for all $k = 1, \ldots, n+1$ (so "the curve $y = f_n(x)$ passes through the points $(x_1, y_1), \ldots, (x_{n+1}, y_{n+1})$.")

Polynomial $f_n(x)$ is called the *Lagrange interpolation* polynomial.

(d) What can you say about the degree of $f_n(x)$? Justify.

(e) What is the relation between $f_n(x)$ and the polynomial obtained in part (c) of the previous problem. Justify your answer.

25. Prove that for an arbitrary function $\phi : \mathbb{Z}_p \to \mathbb{Z}_p$, p is prime, there exists a unique polynomial $f \in \mathbb{Z}_p[X]$ of degree at most $p-1$, such that $\phi(a) = f(a)$ for every $a \in \mathbb{Z}_p$. This means that *every (!)* functions on $\mathbb{Z}_p$ to itself can be uniquely represented as polynomial function of degree at most $p - 1$.

Is the same correct if $\mathbb{Z}_p$ is replaced by $\mathbb{Q}$? Justify.

Comment. If you think that this remarkable fact makes the study of functions on $\mathbb{Z}_p$ to itself much simpler than over other fields, you are wrong.

26. (i) Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$, p is prime, be a function. Based on Problem 25, we can assume that $f \in \mathbb{Z}_p[x]$ and $\deg f \leq p-1$. Let $\{x_1, x_2, \ldots, x_p\} = \mathbb{Z}_p$, and $y_i = f(x_i)$, $i = 1, \ldots p$. Show that

$$f(x) = \sum_{i=1}^{p} y(i)[1 - (x - x_i)^{p-1}].$$

(ii) What is the relation of f in part (i) to the Lagrange interpolation polynomial?

27. Let $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{F}_q[X]$, and its (formal) derivative is defined as

$$f' = a_1 + 2a_2 X + 3a_3 X^2 + \cdots n a_n X^{n-1}.$$

Prove that in addition to the properties $(constant)' = 0$ and $(f+g)' = f' + g'$, the following properties also hold.

(i) $(fg)' = f'g + fg'$

(ii) for $g = X^m$, $m \geq 1$, and $g = X^2 + 1$, $(f(g))' = (f'(g))g'$.

(iii)* Of course, the chain rule $(f(g))' = (f'(g))g'$ holds for all $g \in \mathbb{F}_q[X]$. Prove this result.

28. Prove that the roots of a quadratic equation $ax^2 + bx + c = 0$, $a, b, c \in \mathbb{C}$, $a \neq 0$, are in $\mathbb{C}$.

(Do it, of course, without using the fact that $\mathbb{C}$ is algebraically closed.)

29. Let f be a nonzero polynomial in $\mathbb{C}[X]$ and z be a root of f. Will $\bar{z}$ be necessarily a root of f?

30. Suppose f, g are two relatively prime polynomials in $\mathbb{Q}[X]$. Can they share a root in $\mathbb{C}$? Justify your answers.

31. Let $(a + bi)^n = x + yi$, $n \in \mathbb{N}$. Prove that $x^2 + y^2 = (a^2 + b^2)^n$.

32. How does point $1/z$ move (in the complex plane), when z makes one rotation around the circle centered at $a + bi$ and of radius r?

33. Let $n \geq 2$ be a positive integer. Show that the polynomial $X^{2n} - nX^{n+1} + nX^{n-1} - 1$, has 1 as a root of multiplicity at least 3.

34. (i) Prove that the polynomial $X^{334} + X^{29} + X^6$ is divisible by $X^2 + X + 1$.

Hint: roots of $X^2 + X + 1$ are roots of unity of degree 3.

(ii) Find all integers m such that the polynomial $X^{2m} + X^m + 1$ is divisible by $X^2 + X + 1$.

35. Prove that if $g(X) = f(X^n) \in \mathbb{C}[X]$ is divisible by $X - 1$, then it is divisible by $X^n - 1$. Is it true if $\mathbb{C}$ is replaced by an arbitrary field $\mathbb{F}_q$?

36. Represent $X^{18} - 1$ and $X^{18} + 1$ as products of irreducible polynomials over $\mathbb{R}$.

37. Prove that the polynomial $f = 1 + \frac{1}{1!}X + \frac{1}{2!}X^2 + \cdots + \frac{1}{n!}X^n$ has no multiple roots (in $\mathbb{C}$).

38. Is $f = 3x^5 - 4x^4 + 2x^3 + x^2 + 18x + 31$ irreducible in $\mathbb{Z}[x]$? in $\mathbb{Q}[x]$?

39. Is $f = x^4 + 4$ irreducible in $\mathbb{Z}[x]$?

40. Is $f = x^4 + 1$ irreducible in $\mathbb{Z}_5[x]$?

41. Is $f = 2x^4 - 8x^2 + 1$ irreducible in $\mathbb{Z}[x]$?

42. Let p be a prime number. Prove that $f = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible in $\mathbb{Q}[x]$.

    (*Hint:* Consider $g(x) = f(x + 1)$. Prove that f is irreducible in $\mathbb{Q}[x]$ if and only if g is irreducible in $\mathbb{Q}[x]$.)

43. Suppose $f = x^{n-1} + x^{n-2} + \ldots + x + 1$ is irreducible in $\mathbb{Q}[x]$. Does it imply that n is prime?

44. * Show that the polynomial $f = (x - 1)(x - 2)\cdots(x - n) + 1$ is irreducible over $\mathbb{Z}$ for all integer $n \geq 1$ and $n \neq 4$.

45. (i) Find a formula for the number of monic irreducible polynomials of degree $d = 1, 2, 3$ in $\mathbb{Z}_p[x]$, where p is prime. Check that your answer is correct by listing all of them for $p = 2$ and $p = 3$.

    (ii)* Do part (i) for $d = 4$.

46. Consider the polynomial $f = x^4 + 1 \in \mathbb{Z}[x] \subset \mathbb{R}[x]$.

    (a) Factor f into a product of irreducible polynomials in $\mathbb{R}[x]$.

    (b) Show that f is irreducible in $\mathbb{Z}[x]$.

    (c) * Show that $[f]_p = x^4 + 1 \in \mathbb{Z}_p[x]$ is reducible in $\mathbb{Z}_p[x]$ for each prime p.

    (*Hint:* One may first prove the fact that for any prime p, at least one of numbers $2, -2, -1$, considered as elements of $\mathbb{Z}_p$, is a square in $\mathbb{Z}_p$.)

    Comment. We know that in order to show that a monic polynomial g in $\mathbb{Z}[x]$ is is irreducible, it is *sufficient* to find at least one prime p such that $[g]_p$ is irreducible in $\mathbb{Z}_p[x]$. The example above demonstrates that this method may not always work, or, equivalently, that the condition is *not necessary*: $x^4 + 1$ is reducible over all $\mathbb{Z}_p$'s

but is irreducible over $\mathbb{Z}$. There are, actually, infinitely many other polynomials with this property.

47. Express the following polynomials in terms of the elementary symmetric polynomials of x_1, x_2, x_3, x_4:

    (i) $f = (x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3)$

    (ii) $g = x_1^3 + x_2^3 + x_3^3 + x_4^3$.

48. Find a monic cubic polynomial $f \in \mathbb{R}[x]$ whose roots are the sums $x_i + x_j$, $1 \le i < j \le 3$, where x_1, x_2, x_3 are the roots of the polynomial $g = x^3 - x - 1$.

49. Let $f \in \mathbb{C}[x]$ be a monic polynomial of degree n, and let $x_1, \dots, x_n$ be roots of f. Let

$$D(f) = \prod_{1 \le i < j \le n} (x_i - x_j)^2$$

    $D(f)$ is called the **discriminant** of f, and it is clearly a symmetric polynomial of x_i's (considered as indeterminants). It is also clear that f has no multiple roots if an only if $D(f) \neq 0$, but this is not the only important property of this this function.

    Compute $D(f)$ for

    (i) $f = x^2 + bx + c$

    (ii) $f = x^3 + px + q$

    (iii) $f = x^4 + 5x + 2$

50. (i) Compute the discriminant of the polynomial $f = ax^3 - bx^2 + (b - 3a)x + a \in \mathbb{C}[x]$.

    (ii) Describe all pairs $(a, b) \in \mathbb{C}^2$ such that f from part (i) has no multiple roots.

    (iii) Redo part (ii) using the derivative of f.

51. Factor the following polynomials of several variables into irreducible polynomial. You may try to use the ideas discussed in class. You can use computer to assist you, but your final solution should be computer-free.

    (a) $(b - c)^3 + (c - a)^3 + (a - b)^3$ (over $\mathbb{R}$).

    (b) $a^2 + b^2 + c^2 - ab - bc - ca$ (over $\mathbb{C}$). Express the coefficients in terms of the third root of unity $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

    (c) $(x + y)^7 - x^7 - y^7$ (over $\mathbb{R}$).

    (d) $(b - c)(b + c)^4 + (c - a)(c + a)^4 + (a - b)(a + b)^4$ (over $\mathbb{R}$).

52. Find all values of k such that $x^3 + y^3 + z^3 + kxyz$ is divisible by $x + y + z$.

53. (i) Find a greatest common divisor of 85 and $1 + 13i$ in $\mathbb{Z}[i]$.

(ii) Let $x \in \mathbb{Z}$. Find α and β in $\mathbb{Z}[i]$ such that $\alpha(x + i) + \beta(x - i) = 1$.

54. Let $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\} = \{a + b\sqrt{2}i : a, b \in \mathbb{Z}\}$.

It is clearly a subring in the field

$$\mathbb{Q}(\sqrt{-2}) = \mathbb{Q}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Q}\} \subset \mathbb{C}.$$

(a) Show that $N(x+y\sqrt{-2}) = x^2+2y^2$ is a positive multiplicative function on $\mathbb{Q}(\sqrt{-2})$, and, so a positive multiplicative norm on $\mathbb{Z}[\sqrt{-2}]$

(b) Show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean Domain.

Warning: the norm is not the same as the Euclidean norm!

(c) Use the previous part to find all solutions of the diophantine equation $x^2 + 2 = y^3$.

55. Try to find all solutions of the diophantine equation $x^2 - 2 = y^3$? Can you rewrite the equation as $(x - \sqrt{2})(x + \sqrt{2}) = y^3$ and use the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subset \mathbb{R}$?

Hint: Use $N(a + b\sqrt{2}) = |a^2 - 2b^2|$.

56. Describe the units of the ring $\mathbb{Z}[\sqrt{2}]$.

57. Consider two rings:

$$R_1 = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}], \quad \text{and,}$$

$$R_2 = \mathbb{Z}[w] = \{a + bw : a, b \in \mathbb{Z}\}, \quad \text{where } w = -1/2 + \sqrt{-3}/2.$$

Hence w is a primitive root of 1, $w^2 + w + 1 = 0$.

Are R_1 and R_2 Euclidean domains? Are they UFD's?

58. Consider a subring of the Gaussian integers $R = \mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\}$, where $i^2 = -1$.

(i) Check that $2i$ is irreducible but not prime in R. Explain that this implies that R is not a UFD.

(ii) Prove that $R/(2i) \cong \mathbb{Z}/4\mathbb{Z}$. Explain that this implies that $(2i)$ is not a prime ideal (do not use part (i)).

(iii) Is $(2i)$ a maximal ideal in R? If your answer is Yes, prove it. If your answer is No, find a maximal ideal M in R such that $I \subset M$.

59. Let $\mathbb{K}$ be a field, and let R be the set of all polynomials in $\mathbb{K}[x]$ whose coefficient of x is zero.

(i) Check that R is a subring of $\mathbb{K}[x]$.

(ii) Check that x^2 and x^3 are irreducible in R.

(iii) Explain why the equality $x^6 = (x^2)^3 = (x^3)^2$ implies that R is not a UFD.

Comment. Two problems above show that subrings of UFDs do not have to be UFDs. We observed similar phenomena with a subring $\mathbb{Z}[\sqrt{-3}]$ of $\mathbb{Z}[w] = \{a + bw : a, b \in \mathbb{Z}\}$, $w = -1/2 + \sqrt{-3}/2$. Another similar example, is the Hilbert's example for semigroups: $\{4n + 1 : n \in \mathbb{N} \cup \{0\}\}$ and $\mathbb{N}$. In all these examples, having "less" primes results in non-uniqueness of prime factorizations.

60. (i) Is the ring the ring $\mathbb{Z}[i]/(3 + 2i)$ finite or infinite? If it is finite, how many elements does it have?

(ii) Is there and ideal $I \neq (0)$ in $\mathbb{Z}[i]$ such that the ring $\mathbb{Z}[i]/I$ is infinite?

61. Read about Zorn's Lemma, and go over the proof that in a ring with identity every proper ideal is contained in a maximal ideal.

62. An isomorphism of a ring R to itself is called an **automorphism** of R. The automorphisms can be thought as the "symmetries" of R. Find all ring automorphisms $f : R \to R$ for the following rings.

(a) $R = \mathbb{Z}$.

(b) $R = \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}, n \geq 2$.

(c) $R = \mathbb{Q}$.

(d) $R = \mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D}, a, b \in \mathbb{Q}\}$, where D is a square-free integer. Prove that there are exactly two distinct automorphisms of R.

(e) * $R = \mathbb{R}$. In this case prove that f must be the identity map.

Hint: Show that any automorphism f of $\mathbb{R}$ to itself maps positive numbers to positive numbers. Conclude from this that it preserves the order of elements. Conclude from this that f is the identity isomorphism.

(f) An obvious field automorphisms of $\mathbb{C}$ are the identity map and the conjugation. Show that these are the only *continuous* automorphisms of $\mathbb{C}$.

It can be shown that there are infinitely many others. None of them can be presented explicitly.

(g) * Let $\mathbb{Q}(X)$ be the field of all rational functions over $\mathbb{Q}$, i.e., the quotient field of the polynomial ring $\mathbb{Q}[X]$. Find all automorphisms of $\mathbb{Q}(X)$.

63. Find an explicit isomorphism between rings (fields) $\mathbb{Z}_2[x]/(x^3+x+1)$ and $\mathbb{Z}_2[x]/(x^3+x^2+1)$.

64. ** Consider $I = (2^2, 2x, x^2) = \{2^2 f + 2xg + x^2 h : f, g, h \in \mathbb{Z}[x]\}$ – the ideal in $\mathbb{Z}[x]$ generated by three elements $2^2 = 4$, $2x$, and x^2. Prove that I is not generated by two elements of $\mathbb{Z}[x]$.

65. Describe all ideals of the ring $\mathbb{Z}[x]/(2, x^3+1)$.

66. Prove that for any prime p and any non-zero $a \in \mathbb{F}_p$, the polynomial $f(x) = x^p - x + a$ is irreducible over $\mathbb{F}_p$ and has no multiple roots.

Comment. This gives examples of polynomials of degree p irreducible over $\mathbb{F}_p$ for every prime p. Similar *explicit* examples of polynomials of arbitrary degree n irreducible over $\mathbb{F}_p$ for an arbitrary prime p are not known.

67. Let $\mathbb{K} = \mathbb{F}_q(\alpha)$, where α is of degree n over $\mathbb{F}_q$ with minimal polynomial $m_\alpha(x) = a_0 + a_1 x + \cdots + x^n$. Let $\phi = \phi_\alpha : \mathbb{K} \to \mathbb{K}$ such that for every $k \in \mathbb{K}$, $k \mapsto \alpha k$.

(a) Check that ϕ is a linear transformation of $\mathbb{K}$ considered as a vector space over $\mathbb{F}_q$.

(b) Describe the matrix A of ϕ in the basis $1, \alpha, \ldots, \alpha^{n-1}$ (of $\mathbb{K}$ over $\mathbb{F}_q$).

(c) Prove that α is a root of the characteristic polynomial of A.

68. Find the minimal polynomial over $\mathbb{Q}$ for $\beta = 2 - \sqrt[3]{2} + \sqrt[3]{2^2}$.