Math 3110: Number Theory

Exploration 2: Number systems

March 9, 2016

1 Questions and constructions involving the integers

Question 1. For a fixed positive integer n, what are the integers x, y, and z that satisfy Equation (F)?

$$x^n + y^n = z^n \tag{F}$$

Question 2. Which integers can be expressed as $x^2 + y^2$ for some integers x and y?

Question 3. What proportion of integers between 0 and N are prime?

Question 4. Can every integer be factored into irreducibles? Is this factorization unique?

Question 5. Which integers can be expressed as $10x + 6y$ for some integers x and y?

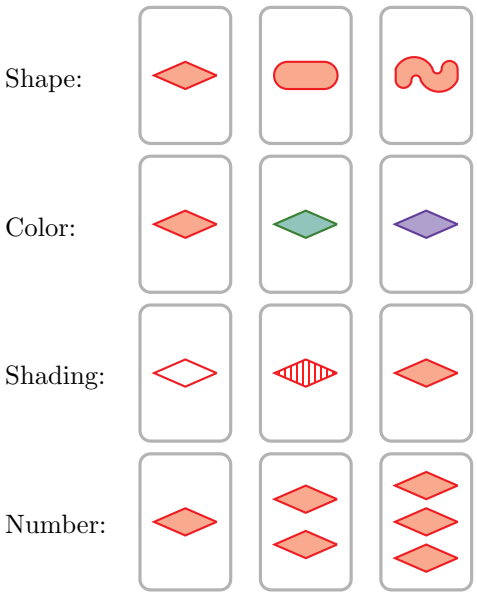
A number system is a setting where can try to ask the same questions, or maybe similar ones. This is necessarily an imprecise definition, and we might not be able to ask every one of these questions in every number system we want to study.

Even if we are only interested in the integers, other number systems can still be very helpful. For example, some of these questions might get easier in other number systems, and that can give us clues about the integer solutions.

Question 6. What features of the integers make it possible to ask these questions?

2 The game of set

SET is a card game in which each card contains an image with 4 characteristics:



Since this page has probably been printed in black and white, we'll play 3-characteristic SET and ignore color. There are a lot of questions we can ask about SET:

Question 7. How many cards are there in a SET deck? What if we had n characteristics?

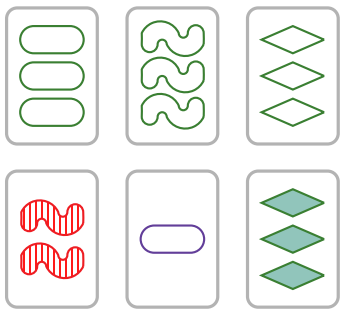
A SET is a collection of 3 cards such that, in each one of the characteristics, all 3 cards are the same or all 3 cards are different. Here it is more notationally:

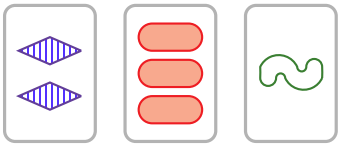
> A set of cards S is a SET if $|S| = 3$ and, for every characteristic C, either
>
> (i) for every $x, y \in S$ we have $C(x) = C(y)$, or
>
> (ii) for every $x, y \in S$ with $x \neq y$ we have $C(x) \neq C(y)$.

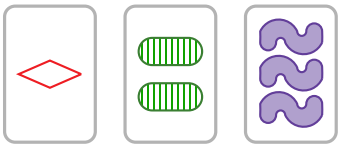
Question 8. Which of the following are SETs?

(1)

(2)



(3) 

(4) 

Can you find any more SETs by picking cards from different rows?

Question 9. How many possible SETs are there?

Of course, it's not important that the characteristics of set cards actually be numbers, colors, shapes, and shades. We may as well have chosen to represent cards as vectors whose entries are 1, 2, or 3. For example, here are vector representations of the cards in the last question:

$(3,1,2,2)$	$(3,1,2,3)$	$(3,1,2,1)$
$(2,3,1,1)$	$(1,1,3,2)$	$(3,2,2,2)$
$(2,2,3,1)$	$(3,3,1,2)$	$(1,1,2,3)$
$(1,1,1,1)$	$(2,2,2,2)$	$(3,3,3,3)$

Question 10. How can we tell *numerically* whether 3 cards form a SET?

3 Points on lines

Question 11. Suppose that $P = (x_1, y_1)$, $Q = (x_2, y_2)$, and $R = (x_3, y_3)$ are three points in the plane. How can you tell, in terms of their coordinates, if they lie on the same line?

Question 12. Can you generalize your criterion from the last question to characterize triples of points that lie on a line in a Euclidean space of arbitrary dimension?

Theorem 13. *Suppose that $P = (x_1, \ldots, x_n)$, $Q = (y_1, \ldots, y_n)$, and $R = (z_1, \ldots, z_n)$ are points in $\mathbb{R}^n$. They lie on the same lie if and only if every 2×2 minor of the matrix*

$$\begin{pmatrix} Q - P & R - P \end{pmatrix}$$

has determinant zero.

Restated, the condition in the theorem is that, for every pair of integers i and j in the range $1 \leq i < j \leq n$, the determinant

$$\det \begin{pmatrix} y_i - x_i & z_i - x_i \\ y_j - x_j & z_j - x_j \end{pmatrix}$$

is zero.

Question 14. Try computing these determinants for some SETs, written as vectors. What do you get?

Question 15. Find analogies between geometry and the game of SET in which points correspond to cards and lines correspond to SETs.

Question 16. Why were you able to find so many SETs in the bottom 3 rows of Question 8?

4 Résumé of equivalence relations

Definition 17. Let S be a set. An equvialence relation on S is a subset $R \subset S \times S$ with the following properties:

(i) *reflexivity*: if $x \in S$ then $(x, x) \in R$;

(ii) *symmetry*: if $(x, y) \in R$ then $(y, x) \in R$;

(iii) *transitivity*: if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

A subset $E \subset S$ is called an *equivalence class* (of the equivalence relation R) if it has the following properties:

(i) $E \neq \varnothing$;

(ii) if $x \in E$ and $(x, y) \in R$ then $y \in E$;

(iii) if $x \in E$ and $y \in E$ then $(x, y) \in R$.

Remark 18. Here is a cute way of phrasing these conditions. First define some operations on subsets of $S \times S$. For $Q, R \subset S \times S$, we define:

$$\begin{aligned} \Delta &= \{(x, x) \,\big|\, x \in S\} \\ R^{-1} &= \{(y, x) \,\big|\, (x, y) \in R\} \\ Q \circ R &= \{(x, z) \,\big|\, \exists\, y \in S,\ (x, y) \in R \text{ and } (y, z) \in Q\} \end{aligned}$$

Then reflexivity of R means $\Delta \subset R$; symmetry of R means $R^{-1} \subset R$; transitivity of R means $R \circ R \subset R$. (In fact, you can check that $R \circ R = R$ and $R^{-1} = R$.)

Here are a few formal statements about equivalence relations that you should know:

Theorem 19. *(i) If R is an equivalence relation on S then for every $x \in S$ there is a unique equivalence class of R containined x. This is often denoted $\overline{x}$ or $[x]$.*

(ii) If two equivalence classes of R intersect then they are equal.

(iii) If $f : S \to T$ is a function, let

$$R = \{(x, y) \in S \times S \,\big|\, f(x) = f(y)\}.$$

Then R is an equivalence relation on S.

(iv) If R is an equivalence relation on S, let T be the set of equivalence classes of R. There is a surjective function $f : S \to T$ such that $f(x) = \overline{x}$.

5 Modular arithmetic

Question 20. What time will it be in 189 hours?

Question 21. I was born on a Tuesday in 1981. What day of week was my birthday in 1982? What about 1983? Can you figure out what it was in 1984?

If two times of day differ by a multiple of twelve hours, they register the same on a 12-hour clock. From the point of view of the clock, they are equivalent. If two dates differ by a multiple of 7 days, they are the same day of the week. From the point of view of a weekly calendar, they are equivalent.

Definition 22. Let n be an integer. Integers a and b are said to be *congruent* modulo n if $b - a$ is an integer multiple of n.

This is an example of an *equivalence relation*:

Theorem 23. *Let n be an integer and let R be defined as follows:*

$$R = \{(x, y) \in \mathbb{Z}^2 \ : \ x - y \in n\mathbb{Z}\}$$

Then R is an equivalence relation on $\mathbb{Z}$.

The equivalence classes of the equivalence relation in Theorem 23 are called *congruence classes modulo n*. We write $a \bmod n$ or $\overline{a}$ for the congruence class of a modulo n. We also write $a \equiv b \pmod{n}$ to mean that a and b are congruent modulo n, or equivalently that $a \bmod n = b \bmod n$.

Since congruence modulo n is the same as congruence modulo $-n$, the different congruence relations on $\mathbb{Z}$ really correspond to *ideals* in $\mathbb{Z}$. For that reason, we also write $a \bmod n\mathbb{Z}$ for the congruence class of a, and $a \equiv b \pmod{n\mathbb{Z}}$ to mean that a and b are congruent modulo n.

The set of congruence classes of integers modulo n is denoted $\mathbb{Z}/n\mathbb{Z}$ and read '$\mathbb{Z}$ mod $n\mathbb{Z}$'.

Remark 24. Many people think that $a \bmod n$ is the remainder of a when divided by n. *This is not correct.* The remainder is an integer, whereas $a \bmod n$ is an set of integers. It turns out if r is the remainder of a when divided by n then $a \bmod n = r \bmod n$, and that $a \equiv r \pmod{n}$, but this is different from saying $a \bmod n = r$.

It is quite common to drop the mod$n$ once we get comfortable with arithmetic modulo n, but you still need to remember when you are talking about equivalence classes of integers and when you are talking about integers.

Question 25. Which of the following formulas are correct for any integers a, b, c, d, and n such that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$?

(i) $a + b \equiv c + d \pmod{n}$

(ii) $a - b \equiv c - d \pmod{n}$

(iii) $ab \equiv cd \pmod{n}$

(iv) $a^b \equiv c^d \pmod{n}$.

Question 26. Let R be as in Theorem 23. Suppose that $(a, c) \in R$ and $(b, d) \in R$. Which of the following formulas are correct?

(i) $(a + b, c + d) \in R$

(ii) $(a - b, c - d) \in R$

(iii) $(ab, cd) \in R$

(iv) $(a^b, c^d) \in R$

What is the relationship between this question and the previous one?

One good sign that $\mathbb{Z}/n\mathbb{Z}$ deserves to be called a number system is that some of the familiar features of the integers reappear in $\mathbb{Z}/n\mathbb{Z}$:

Question 27. Adapt the definitions of primes and units to $\mathbb{Z}/n\mathbb{Z}$. Can you describe the prime elements of $\mathbb{Z}/n\mathbb{Z}$ in terms of the number n? What are the units? What are the irreducible elements? Does unique prime factorization still hold?

Question 28. Find all solutions $x, y, n \in \mathbb{Z}/n\mathbb{Z}$ to $x^2 + y^2 = n$. What does this tell you about solutions to $x^2 + y^2 = n$ in $\mathbb{Z}$?

Question 29. Do the following for some small values of n:

(i) Draw the full multiplication table for $\mathbb{Z}/n\mathbb{Z}$.

(ii) Use one color to mark the rows that contain more than one 0.

(iii) Use another color to mark the rows that contain a 1.

What observations can you make? Is every row marked in one color or the other? Is any row ever marked in both colors? Can you make a prediction about when row k will be marked, based on the relationship between k and n? Can you prove your observation is correct?

Theorem 30. *An element* $k \bmod n$ *is a divisor of* 0 *in* $\mathbb{Z}/n\mathbb{Z}$ *if and only if* $\gcd(k, n) > 1$. *An element* $k \bmod n$ *is a unit of* $\mathbb{Z}/n\mathbb{Z}$ *if and only if* $\gcd(k, n) = 1$.

6 The Chinese remainder theorem

In this section, we are going to study systems of equations, like this:

$$x \equiv a \pmod{n} \tag{1}$$
$$x \equiv b \pmod{m} \tag{2}$$

Here we are thinking of a, b, m, and n as fixed integers and x as a variable for which we would like to solve.

Question 31. Try the following special cases of Equations (1):

(i) $x \equiv 3 \pmod{5}$ and $x \equiv 4 \pmod{7}$

(ii) $x \equiv 3 \pmod{6}$ and $x \equiv 0 \pmod{9}$

(iii) $x \equiv 3 \pmod{6}$ and $x \equiv 1 \pmod{9}$

Make up some examples of your own. When can the equations be solved? How many solutions are there?

Solving $x \equiv a \pmod{n}$ is the same as solving $x = a + kn$. Likewise, solving $x \equiv b \pmod{m}$ is the same as solving $x = b + \ell m$. Thus we are really trying to solve these equations:

$$a + kn = x = b + \ell m$$

We could forget about x and just try to find k and ℓ solving this equation:

$$a + kn = b + \ell m \tag{3}$$

If we know either k or ℓ, we can recover x so solving the above equation is equivalent to our task.

Question 32. How can you tell if Equation (3) has a solution? How can you find all solutions?

Theorem 33 (Chinese remainder theorem)**.** *Equations* (1) *have a solution if and only if* $a - b$ *is divisible by the greatest common divisor of* m *and* n*. In that case, the solution set is an element of* $\mathbb{Z}/\operatorname{lcm}(m, n)\mathbb{Z}$*.*

Question 34. Solve the following congruences for $x \in \mathbb{Z}$:

(i) $x \equiv 2 \pmod{5}$ and $x \equiv 3 \pmod{7}$ and $x \equiv 1 \pmod{3}$

(ii) $x \equiv 4 \pmod{6}$ and $x \equiv 2 \pmod{3}$ and $x \equiv 0 \pmod{4}$

(iii) $x \equiv 5 \pmod{20}$ and $x \equiv 15 \pmod{30}$ and $x \equiv 3 \pmod{6}$

(iv) $x \equiv 5 \pmod{20}$ and $x \equiv 15 \pmod{30}$ and $x \equiv 5 \pmod{6}$

Theorem 35. *Suppose that m and n are relatively prime integers. Let*

$$\pi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

be the function defined by

$$\pi(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z}).$$

Then π is a bijection.

Question 36. Generalize the Chinese remainder theorem to a statement involving more than two congruences.

7 Fields

In the last section, you discovered that addition, subtraction, and multiplication all make sense in modular arithmetic, for any modulus n. We will say that *division is possible* modulo n if, for any *nonzero* $x \in \mathbb{Z}/n\mathbb{Z}$, there is some $y \in \mathbb{Z}/n\mathbb{Z}$ such that $xy = 1 \bmod n$.

Definition 37. A *field* is a set with special elements 0 and 1 and addition, subtraction, multiplication, and division (except by zero) operations satisfying all of the familiar properties:

(i) (nontriviality) $0 \neq 1$

(ii) (additive identity) $a + 0 = a$

(iii) (multiplicative identity) $1a = a$

(iv) (subtraction is inverse to addition) $a + (b - a) = b$

(v) (division is inverse to multiplication) $a(b/a) = b$ for any $a \neq 0$

(vi) (associativity of addition) $a + (b + c) = (a + b) + c$

(vii) (commutativity of addition) $a + b = b + a$

(viii) (associativity of multiplication) $a(bc) = (ab)c$

(ix) (commutativity of multiplication) $ab = ba$

(x) (distributivity of multiplcation over addition) $a(b + c) = ab + ac$

Question 38. You should already be familiar with a few fields. Identify as many of them as you can.

Question 39. Determine whether $\mathbb{Z}/n\mathbb{Z}$ is a field for a few small values of n (for example, do it for all n between 1 and 10). Can you predict whether $\mathbb{Z}/n\mathbb{Z}$ will be a field based on the value of n? Work out more examples if it helps you make a conjecture.

Theorem 40. *$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is irreducible.*

Definition 41. When p is a positive prime number, we use the notation $\mathbb{F}_p$ for the field $\mathbb{Z}/p\mathbb{Z}$.

Theorem 42 (Wilson's theorem)**.** *For any finite field F, the product of the nonzero elements of F is -1.*

Theorem 43 (Fermat's little theorem)**.** *Let F be a finite field of size q and let a be a nonzero element of F. Then $a^{q-1} = 1$.*

Question 44. Are there any more finite fields, or do we have a complete list? Can you build a field with 4 elements? (Remember: $\mathbb{Z}/4\mathbb{Z}$ is not a field!)

Theorem 45. *Suppose that E is a field and $p(x)$ is a polynomial with coefficients in E. Then there is a field F and an element $\alpha \in F$ such that E is a subfield of F and $p(\alpha) = 0$.*

We will not prove this theorem in this class because it would require a lot of notation. You can try to prove it yourself, or you can find a proof in any abstract algebra text or class.

Theorem 46. *If E is a finite field then there is a prime p and a positive integer n such that $|E| = p^n$.*

Question 47. Can you build a field with 9 elements? A field with 8 elements? What about 16, 25, 27, and 32 elements? Can you build more than one field with the same number of elements?

Question 48. The last question asked you if you could build more than one field with the same number of elements. But what does that mean? If I build a field with 4 elements by adding a new element called x to $\mathbb{F}_2$ satisfying $x^2+x+1 = 0$ and you build a field with 4 elements by adding a new element called y to $\mathbb{F}_2$ satisfying $y^2 + y + 1 = 0$, are those the same field, or are they different? Come up with a definition of what it means for two fields to be 'the same'.

Theorem 49. *If F is a finite field of size q then $x^q - x = \prod_{a \in F}(x - a)$ as polynomials with coefficients in F.*

Proof. For any nonzero $a \in F$, we know by Fermat's little theorem that $a^{q-1} = 1$. Therefore $a^q = a$. Likewise, it is clear that if $a = 0$, we also have $a^q = a$, so that $a^q = a$ for all $a \in F$.

This means that a is a root of the polynomial $x^q - x$, so it is possible to factor $(x - a)$ out of $x^q - x$: There is some polynomial f of degree $q - 1$ such that

$$x^q - x = (x - a)f(x).$$

Now if b is another element of F, not equal to a, then $b^q - b = 0$, so $(b-a)f(b) = 0$. Since $b - a \neq 0$, this means $f(b) = 0$. Therefore we can factor $x - b$ out of $f(x)$ and get

$$x^q - x = (x - a)(x - b)g(x)$$

for some polynomial g of degree $q-2$. Now pick $c \in F$ with $c \neq a$ and $c \neq b$... By induction, we find that

$$x^q - x = \prod_{a \in F} (x - a).$$

□

Theorem 50. *Any two finite fields with the same number of elements are isomorphic.*

Theorem 51. *If q is a power of a prime then there is a field of size q.*

8 The Gaussian integers

Recall that the complex numbers consist of all symbols $a + bi$, where $a, b \in \mathbb{R}$, with the rules:

$$0 = 0 + 0i$$
$$1 = 1 + 0i$$
$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

The set of complex numbers is denoted $\mathbb{C}$. We won't check explicitly that 0 is an additive identity, 1 is a multiplicative identity, addition is associative and commutative, additive inverses exist, multiplication is associative and commutative, and multiplication distributes over addition.

Question 52. Is $\mathbb{C}$ a field? That is, if $a + bi \neq 0$ can you find $c + di$ such that $(c + di)(a + bi) = 1$?

Definition 53. Let $\mathbb{Z}[i]$ be the set of complex numbers $a + bi$ such that both a and b are integers. It is called the ring of *Gaussian integers*.

You should check that the sum, difference, and product of elements of $\mathbb{Z}[i]$ is still in $\mathbb{Z}[i]$.

Question 54. Is $\mathbb{Z}[i]$ a field?

Question 55. Is $1 + i$ an irreducible element of $\mathbb{Z}[i]$? What about 2? What about other integer primes? Is there a pattern?

Question 56. Find a factorization into irreducible Gaussian integers of some small integer primes. Can you make a prediction about which integer primes are also prime in the Gaussian integers? When integer primes are not Gaussian integer primes, how do they factor?

Question 57. Does $\mathbb{Z}[i]$ have unique factorization into irreducibles?

Theorem 58. *Let z and d be elements of $\mathbb{Z}[i]$, with $d \neq 0$. Then there are $q, r \in \mathbb{Z}[i]$ such that $z = qd + r$ and $|r| \leq \frac{|d|}{2}$.*

Theorem 59. *Let a and b be any two elements of $\mathbb{Z}[i]$. Define:*

$$I = \{ax + by \ : \ x, y \in \mathbb{Z}[i]\}$$

Then $I = d\mathbb{Z}[i]$ for some $d \in \mathbb{Z}[i]$.

Theorem 60. *Every nonzero Gaussian integer can be factored into irreducibles in a way that is unique up to reordering and multiplication by units.*

9 Gaussian modular arithmetic

Definition 61. Suppose that ζ is a Gaussian integer. We call two Gaussian integers α and β *equivalent* or *congruent* modulo ζ if $\alpha - \beta$ is a multiple of ζ by a Gaussian integer.

You might like to try to prove this theorem. It's a lot like the proof in the case of the regular integers.

Theorem 62. *If ζ is a Gaussian integer, then congruence modulo ζ is an equivalence relation.*

If α and ζ are Gaussian integers, the equivalence class of α modulo ζ is sometimes denoted in the following ways:

$\alpha + \zeta\mathbb{Z}[i]$	$\overline{\alpha}$
$\alpha \bmod \zeta$	$[\alpha]$

We will stick to the first two. The set of equivalence classes of congruence modulo ζ is denoted $\mathbb{Z}[i]/\zeta\mathbb{Z}[i]$.

Question 63. Suppose that ζ is an integer (not a Gaussian integer). How many equivalence classes are there in $\mathbb{Z}[i]/\zeta\mathbb{Z}[i]$?

Question 64. Which of the following are fields?

(i) $\mathbb{Z}[i]/2\mathbb{Z}[i]$	(v) $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$
(ii) $\mathbb{Z}[i]/3\mathbb{Z}[i]$	(vi) $\mathbb{Z}[i]/(1+2i)\mathbb{Z}[i]$
(iii) $\mathbb{Z}[i]/4\mathbb{Z}[i]$	(vii) $\mathbb{Z}[i]/(1+3i)\mathbb{Z}[i]$
(iv) $\mathbb{Z}[i]/5\mathbb{Z}[i]$	(viii) $\mathbb{Z}[i]/(2+3i)\mathbb{Z}[i]$

Make up more examples of your own.

Question 65. For which $\zeta \in \mathbb{Z}[i]$ is $\mathbb{Z}[i]/\zeta\mathbb{Z}[i]$ a field? What properties of ζ determine whether $\mathbb{Z}[i]/\zeta\mathbb{Z}[i]$ is a field? (Hint: Think about what properties of integers n determine whether $\mathbb{Z}/n\mathbb{Z}$ is a field.)

Question 66. For which prime *integers* (ordinary, not Gaussian) p is $\mathbb{Z}[i]/p\mathbb{Z}[i]$ a field? Can you find a pattern?

Theorem 67. *Suppose that p is a nonzero prime integer. Then p is prime in $\mathbb{Z}[i]$ if and only if -1 is a square in $\mathbb{F}_p$. The following conditions are equivalent:*

(i) There are integers x and y such that $x^2 + y^2 = p$.

(ii) -1 is a square in $\mathbb{F}_p$.

(iii) $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is not a field.

10 Sums of squares

Question 68. For which primes p does $x^2 + 1 = 0$ have a solution in $\mathbb{F}_p$? Can you detect a pattern?

Question 69. How would you find all integer solutions to the equation $xy = n$?

Question 70. Find all integer solutions to the following equation:

$$x^2 + y^2 = n$$

The Guassian integers give a very useful perspective on this equation. We can factor it into:

$$(x + iy)(x - iy) = n$$

If we called the first factor z and the second factor $\overline{z}$ then it becomes:

$$z\overline{z} = n$$

This equation is a lot like the equation $xy = n$, except z is allowed to be a Gaussian integer.

Question 71. Adapt the method you used to solve Question 69 to solve $z\overline{z} = n$ for a Gaussian integer z and an integer n.

11 Polynomials

Suppose we already have a number system A. We can build a new number system $A[x]$ whose elements are *polynomials* with coefficients in A:

Definition 72. Let A be a number system. A *polynomial* in the variable x with coefficients in A is a symbol of the following form:

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + 0x^{n+1} + 0x^{n+2} + \cdots$$

Usually, we don't both to write the zeroes and just write:

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

Here n is an integer, $n \geq 0$, and a_i is an element of A for every $i = 0, \ldots, n$. The set of all polynomials in x with coefficients in A is denoted $A[x]$. The integer n is called the *degree* of the polynomial.

Theorem 73. *Polynomials with coefficients in A can be added, subtracted, and multiplied. The zero polynomial is an additive identity. The polynomial $1 + 0x + 0x^2 + \cdots$ is a multiplicative identity. Addition and multiplication are commutative and associative, and multiplication distributes over addition.*

Question 74. Suppose that E is a field and that $a, b, n \in E[x]$. Can you solve the equation

$$ax + by = n \tag{4}$$

for $x, y \in E[x]$?

Try this question in a few examples:

(i) $E = \mathbb{Q}$, $a = x^2 + 1$, $b = x - 1$, $n = 1$

(ii) $E = \mathbb{Q}$, $a = x^2 - 1$, $b = x - 1$, $n = 1$

(iii) $E = \mathbb{F}_5$, $a = x^2 + 1$, $b = x - 2$, $n = 1$

(iv) $E = \mathbb{F}_7$, $a = x^2 + 1$, $b = x - 2$, $n = 1$

Question 75. How did we solve Equation (4) in the integers? How much of that solution makes sense in $E[x]$?

Theorem 76 (Division algorithm)**.** *Suppose that E is a field and that n and d are elements of $E[x]$, with $d \neq 0$. Then there are unique elements q and r of $E[x]$ such that $n = qd + r$ and the degree of r is less than the degree of d.*

12 Extensions of the integers

13 The p-adics