Numbers and Equations

Andrew D Smith
University College Dublin

7 October 2023

> Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
> Leopold Kronecker (1823 - 1891)

Number Problems

Solving Equations

Solving an equation means finding the *solution set*, that is, the set of numbers for which an equation holds.

	One variable	Two variables
Linear	$5x = 55$	$20x + 23y = 2023$
Quadratic		$x^2 + y^2 = 100$
Quintic	$x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$	

These equations are all examples of polynomials, that is, sums of products of constants and powers. The *coefficients* of a polynomial are the numbers multiplying the powers. For example, the coefficients of $x^5 + 2x^3 - 8x$ are $(5, 0, 2, 0, -8, 0)$. The zeroes arise because there are no even powers in this polynomial.

Number Operations

Mathematically, numbers are not defined in terms of what they *are* but what we can *do* with them.

For a set of numbers $\mathbb{F}$, called a *field*, we have operations of addition, $+$, and multiplication $\times$, which satisfy the following:

Addition

Associative	$(a + b) + c = a + (b + c)$
Identity 0	$a + 0 = 0 + a = a$
Inverse $-a$	$a + (-a) = (-a) + a = 0$
Commutative	$a + b = b + a$

Multiplication

Associative	$(a \times b) \times c = a \times (b \times c)$
Identity 1	$a \times 1 = 1 \times a = a$
Inverse a^{-1}	$a \times a^{-1} = a^{-1} \times a = 1$
	(unless $a = 0$)
Commutative	$a \times b = b \times a$
	(except quaternions, a *skew* field)

Distributive

$(a + b) \times (c + d) = (a \times c) + (a \times d) + (b \times c) + (b \times d)$

In the history of mathematics, these rules were observed, and then proved for integers (except multiplicative inverse), then rational numbers, then real numbers.

Sometimes when no ambiguity arises, we omit the $\times$ sign for a product, so that ab is short-hand for $a \times b$.

The field axioms do not require us to define powers a^b for elements of a field. We can define integer powers a^b for $a \in \mathbb{F}$ and the exponent $b \in \mathbb{Z}$ (where $\mathbb{Z}$ is the set of all integers, positive and negative). For example a^{-3} is short-hand for $a^{-1} \times a^{-1} \times a^{-1}$.

Consequences of Field Axioms

Modern mathematicians start with the axioms and see what they can prove for a general set with operations satisfying the field axioms. Most of what we know about numbers follow from the field axioms and therefore apply to any field.

For example consider the statements:

(i) If $a = 0$ than $a \times b = 0$ for any b.

(ii) If $a \times b = 0$ then either $a = 0$ or $b = 0$ (or both).

Exercise: Statements (i) and (ii) hold for the rational numbers, and for the real numbers. Prove these statements for a general field.

Solution: Take statement (i) first. We have

$$0 \times b = (0 + 0) \times b = (0 \times b) + (0 \times b)$$

Adding $-(0 \times b)$ to each side gives the conclusion.

Now take statement (ii). Suppose $a \times b = 0$ but $b \neq 0$. Then b^{-1} exists and

$$a = a \times 1 = a \times (b \times b^{-1}) = (a \times b) \times b^{-1} = 0 \times b^{-1} = 0$$

Likewise, the *difference of two squares* formula applies for any field, by the distributive law and then the commutative law for multiplication:

$$(x - y)(x + y) = x^2 + xy - yx - y^2 = x^2 - y^2$$

Classes of Numbers

We will consider six important classes of numbers:

Positive integers	$\mathbb{Z}^+$
Integers	$\mathbb{Z}$
Rational numbers	$\mathbb{Q}$
Real numbers	$\mathbb{R}$
Complex numbers	$\mathbb{C}$
Quaternions	$\mathbb{H}$

Inclusion relationships:

$$\mathbb{Z}^+ \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$$

The way we solve equations equations depends on the set of numbers x and y which we consider eligible. For example, we might want solutions in integers, or in real numbers, or rational numbers.

Of these number sets, $\mathbb{Z}^+$ and $\mathbb{Z}$ are not fields, because the inverse x^{-1} of an integer $x \geq 2$ is not an integer. The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all fields. The quaternions form a *skew field* because multiplication does not commute. Plenty of theorems that apply to all fields do not apply to the quaternions.

Equations to Solve

Solving an equation is a combination of the equation and the constraints on allowable numbers. We arrange the equations and number sets into a table:

	$\mathbb{Z}^+$ $\mathbb{Z}$ $\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$ $\mathbb{H}$
$20x + 23y = 2023$ $x^2 + y^2 = 100$ $x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$	

Integers

The *integers* are the whole numbers $\{\ldots -2, -1, 0, 1, 2 \ldots\}$. This set is usually denoted by $\mathbb{Z}$. If x is an integer, we write $x \in \mathbb{Z}$, that is, x is an *element* of the *set* $\mathbb{Z}$.

The *natural numbers* usually means the positive integers, but sometimes includes zero, with the notation $\mathbb{N}$ used in either case. The notation in this table avoids ambiguity:

Set	Name	Notation
$\ldots -2, -1, 0, 1, 2, \ldots$	Integers	$\mathbb{Z}$
$1, 2, 3, \ldots$	Positive Integers	$\mathbb{N}\backslash\{0\}$, $\mathbb{Z}^+$, $\mathbb{Z}_{>0}$
$0, 1, 2, 3, \ldots$	Non-negative Integers	$\mathbb{N} \cup \{0\}$, $\mathbb{Z}_0^+$, $\mathbb{Z}_{\geq 0}$
$\ldots -3, -2, -, 1$	Negative Integers	$\mathbb{Z}^-$, $\mathbb{Z}_{<0}$
$\ldots -3, -2, -1, 0$	Non-positive Integers	$\mathbb{Z}_0^-$, $\mathbb{Z}_{\leq 0}$

Here, $\{0\}$ means the set containing zero. We use the following set notation for operations on sets A and B:

Name	Notation	Meaning
Empty set	$\emptyset$	
Union	$A \cup B$	Elements of A or B or both
Intersection	$A \cap B$	Elements of A and B
Difference	$A \backslash B$	Elements of A not in B

The integers are closed under addition, subtraction and multiplication but not under division.

Primes and Factors

If $c = a \times b$ for positive integers a, b then we say that a and b are *factors* of c. If a is a factor of c we say that a *divides* c, which we can write $a \mid c$.

We can classify positive integers according to how many factors they have.

Class	Number of factors	Examples
Unit	One factor: itself	1
Primes	Two factors: 1 and itself	2, 3, 5, 7, 11
Composite	Three or more	4, 6, 8, 9, 10

We can only define primes because the set $\mathbb{Z}$ of integers is *not* a field. If it were a field, then every element (except zero) divides every other.

It should be obvious that any integer $x \geq 2$ is a product of primes. Just divide it into smaller and smaller bits (how do you know the process has to stop?).

It is not obvious that we get the same list of primes regardless of the order in which we break the original number down into factors. Uniqueness of integer prime factorisation is the *fundamental theorem of arithmetic*.

Relative Primality

For two positive integers a and b, the *greatest common divisor* is the largest positive integer than divides them both, written $\gcd(a, b)$.

If we write a and b as a product of prime powers, then the greatest common divisor is a product of primes with each exponent taken to be the smaller of the respective exponents in a and b.

For example:

$$\begin{aligned} 60 &= 2^2 \times 3^1 \times 5^1 \\ 100 &= 2^2 \times 3^0 \times 5^2 \\ 20 = \gcd(60, 100) &= 2^2 \times 3^0 \times 5^1 \end{aligned}$$

If the greatest common divisor of positive integers a and b is 1, then we say a and b are *relatively prime*. That is equivalent to a and b having no common prime factors.

Euclid's Lemma If an integer n divides the product ab of two integers, and n is relatively prime to a, then n divides b. Euclid was a Greek mathematician who lived in the third century BC.

Remark: Euclid's lemma is obvious if we can assume uniqueness of factorisation into primes. However, most proofs of prime

factorisation uniqueness use Euclid's lemma so, to avoid circular logic, we have to seek other proofs of Euclid's lemma, for example using the Euclidean gcd algorithm (proof not provided here).

Linear Equation in Integers

Equations to be solved in integers are called *Diophantine* equations, after Diophantus of Alexandria who lived in the third century AD.

An example of a Diophantine equation is $20x + 23y = 2023$, to be solved in positive integers.

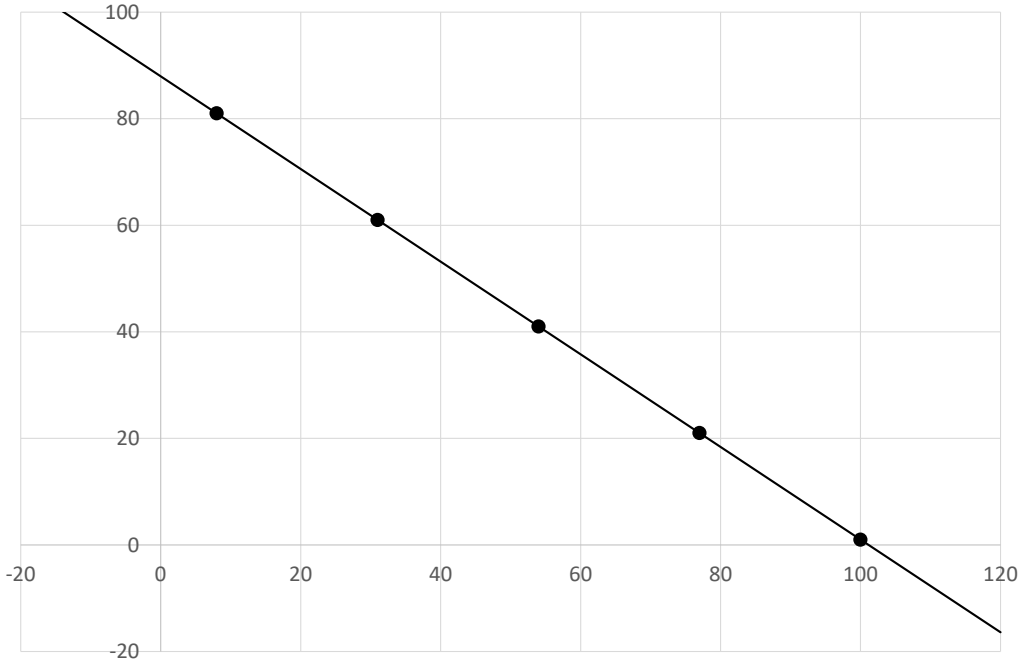
A *brute force* solution means reducing a problem to finitely many cases and then checking them all.

To solve the Diophantine equation $20x+23y = 2023$ in positive integers, make x the subject of the equation:

$$x = \frac{2023 - 23y}{20}$$

This can give positive x and y (in real numbers) only if $0 < y < \frac{2023}{23} = 87\frac{22}{23}$. We can check 87 values of y and see when the corresponding x turns out to be an integer.

Exercise: Why is it more efficient to express x as a function of y and not the other way around?



This gives the solutions:

x	y	$20x + 23y$
100	1	2023
77	21	2023
54	41	2023
31	61	2023
8	81	2023

The need for brute force can sometimes be reduced by some clever maths. For example, we might spot the obvious solution $x = 100, y = 1$ and then subtract that from the original equation:

$$\begin{aligned} 20x + 23y &= 2023 \\ 20 \times 100 + 23 \times 1 &= 2023 \\ 23(y-1) &= 20(100-x) \end{aligned}$$

Using Euclid's lemma, we can conclude that 20 divides $y-1$ and 23 divides $100-x$, and that the two quotients are equal. Let us call their common integer value k. It follows that the general solution is:

$$\begin{aligned} x &= 100 - 23k \\ y &= 1 + 20k \end{aligned}$$

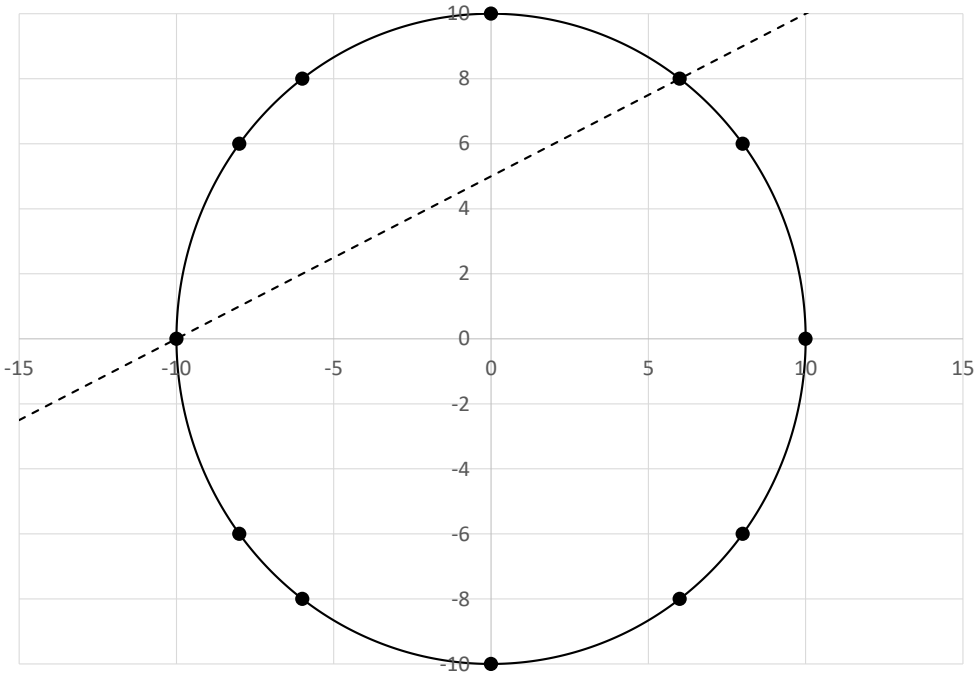
If we want x and y to be positive integers then we choose $0 \leq k \leq 4$. If x and y can be any integer, then the solutions follow the same formula for any $k \in \mathbb{Z}$.

Quadratic Equation in Integers

Likewise, to solve $x^2 + y^2 = 100$ in positive integers x, y, simply test all integers from $x = 1$ to $x = 9$ (inclusive) and check the cases where $100 - x^2$ is a square number. There are only two where $(x, y) = (6, 8)$ or $(8, 6)$.

For solutions in integers we have to add $(0, 10)$ and various other derived points by permuting the co-ordinates or changing sign.

These points are shown in the figure below:



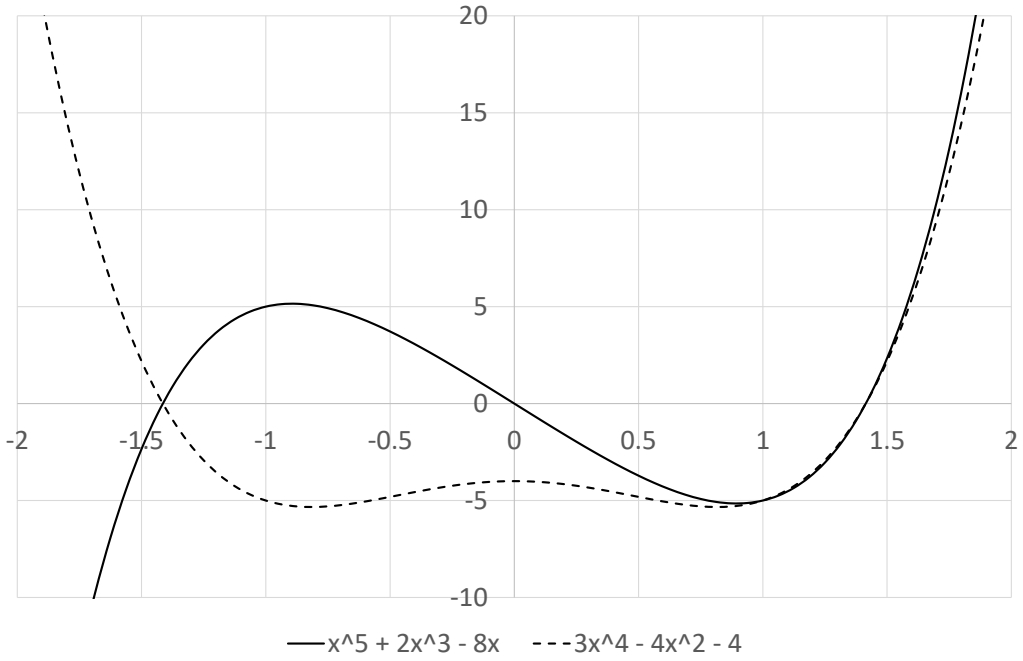
Quintic Equation in Integers

Suppose we want to solve $x^5+2x^3-8x = 3x^4-4x^2-4$ in integers.

For large negative x, the left hand side is large and negative while the right hand side is large and positive. Therefore, there cannot be solutions for large negative x.

For large positive x the term in x^5 grows factor than $3x^4$ and all other terms are small in comparison, which implies that there are no solutions for large positive x.

With some work we can make this argument rigorous to exclude roots outside the range $[-2, 2]$ but we have not done that here.



Status So Far

We have now mostly solved three equations for positive and negative integers, as shown by checks in the table below.

	$\mathbb{Z}^+$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
$20x + 23y = 2023$	✓	✓				
$x^2 + y^2 = 100$	✓	✓				
$x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$	?	?				

Real Numbers

Mathematicians use *real numbers* to describe continuous variables, that might correspond, for example, to the length of a line or the mass of an object.

Decimal Expansions

Real numbers include zero, positive and negative integers, rational numbers and irrational numbers such as $\sqrt{2}$ or π. Real numbers can be expanded in decimals. The decimal expansion of a rational number either terminates or repeats in a cycle. Decimal expansions for irrational numbers do not repeat.

Real number	Decimal Expansion
$\frac{1}{8}$	0.125
$\frac{1}{14}$	$0.0\overline{714285}$
$\sqrt{2}$	$1.41421356237309504880168872420 9\ldots$
π	$3.14159265358979323846264338327 9\ldots$

Intermediate Value Theorem

A function $f : \mathbb{R} \to \mathbb{R}$ is *continuous* if whenever we have a sequence $x_1, x_2, \ldots \to x_\infty$ then $f(x_1), f(x_2), \ldots \to f(x_\infty)$. All polynomials, for example, are continuous functions but there are other continuous functions which are not polynomials.

The *intermediate value theorem*, (sometimes called *Bolzano's theorem*) is an important result regarding the values taken by a

continuous function.

Intermediate Value Theorem: Let $f(x)$ be a continuous real-valued function that takes values of opposite signs within a real interval of values of x. Then there is some x within that interval for which $f(x) = 0$.

The intermediate value theorem might seem obvious by a physical analogy. We can draw the graph of a continuous function without lifting the pencil from the paper, so if the pencil crosses the horizontal axis then it must be on the axis at some time. Proofs by physical analogy do not satisfy mathematicians who require more formal proofs (starting from a formal definition of a continuous function, not included here).

Linear and Quadratic Equations

Finding real solutions to linear and quadratic equations is straightforward by making one variable the subject of the equation. We have seen how $20x + 23y = 2023$ can be written in that form.

Similarly, for the circle $x^2 + y^2 = 100$ we can write (for $|x| \leq 10$):

$$y = \sqrt{100 - x^2}, y = \sqrt{100 = x^2}$$

which together yield all the real points.

Quintic Example

Suppose we want real solutions to $x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$. Subtracting the right-hand-side from the left hand side, we need

$A(x) = 0$ where:

$$A(x) = x^5 - 3x^4 + 2x^3 + 4x^2 - 8x + 4$$

We can calculate values of $A(x)$ as follows:

x	$x^5 + 2x^3 - 8x$	$3x^4 - 4x^2 - 4$	$A(x)$
-1.5	-2.34375	2.1875	-4.53125
-1.3	2.29307	-2.1917	4.48477
-1	5	-5	10
0	0	-4	4
1	-5	-5	0
1.3	-2.29307	-2.1917	-0.10137
1.5	2.34375	2.1875	0.15625

We already knew about the root at $x = 1$. The intermediate value theorem tells us there are (at least) two more real roots x such that $A(x) = 0$, one with $-1.5 < x < -1.3$ and one with $1.3 < x < 1.5$. Direct substitution reveals that those two roots are $\pm\sqrt{2}$.

Bounds on Root Count for Polynomials

Suppose we have a polynomial $p(x)$ of degree $d \geq 1$ (that is, the highest power of x is x^d), over some field $\mathbb{F}$ (ie coefficients of p lie in $\mathbb{F}$) and suppose that $p(x)$ has a root $\lambda \in \mathbb{F}$ with $p(\lambda) = 0$.

Then it can be shown that $p(x)$ factorises as $(x-\lambda)q(x)$ where $q(x)$ is also a polynomial of degree $d-1$. There is a long division algorithm for polynomials that proves this.

It follows that a polynomial of degree d can have at most d real roots. In particular for our quintic polynomial, there can be at most 5 real roots, although we have found only 3 so far.

Status So Far

We have now solved three equations for positive and negative integers, and for real numbers as shown by checks in the table below.

	$\mathbb{Z}^+$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
$20x + 23y = 2023$	✓	✓		✓		
$x^2 + y^2 = 100$	✓	✓		✓		
$x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$	?	?		?		

The question mark is because we have found three real roots but we have not proved there are no more.

Rational Numbers

A *rational* number is the ratio of two integers, for example $1/2$ or $-5/3$. We denote the set of rational numbers by $\mathbb{Q}$.

Farey Sequences

The Farey sequence of order n is the sequence of completely reduced fractions, between 0 and 1, which when in lowest terms have denominators less than or equal to n, arranged in order of increasing size.

For example, the Farey sequence of order 6 is:

$$F_6 = \left\{ \frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1} \right\}$$

There is a clever algorithm to calculate the k^{th} term in the Farey sequence of order n. The zeroth and first terms are:

$$\frac{a_0}{b_0} = \frac{0}{1}; \frac{a_1}{b_1} - \frac{1}{n}$$

The following recurrence formula produces the $(k+1)^{th}$ term from the $(k-1)^{th}$ term and the k^{th} term:

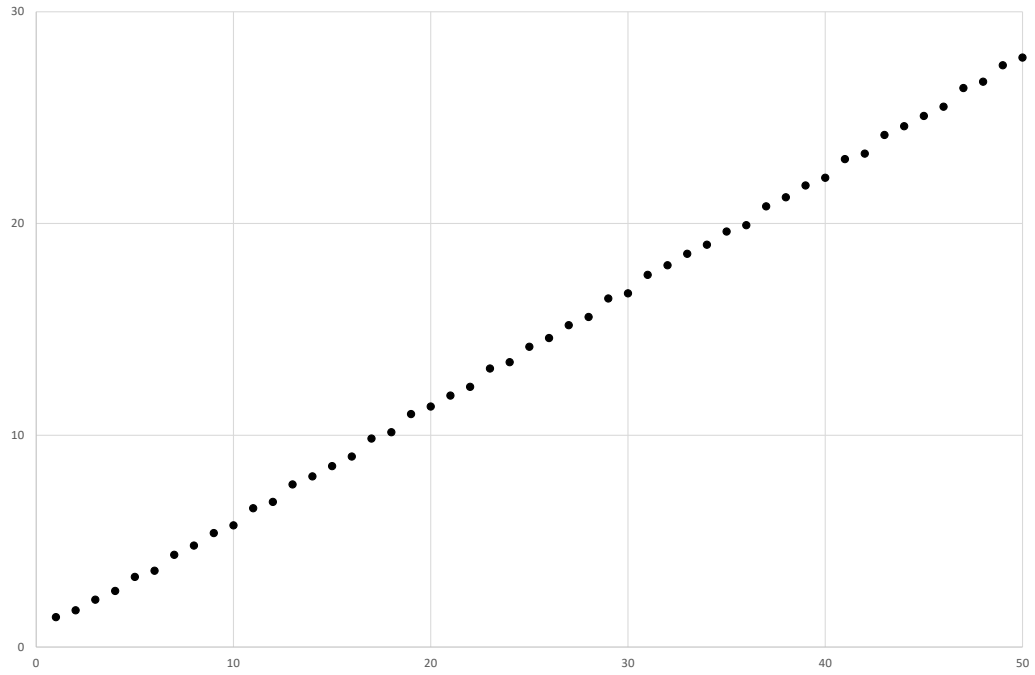
$$a_{k+1} = \left\lfloor \frac{n + b_{k-1}}{b_k} \right\rfloor a_k - a_{k-1}$$
$$b_{k+1} = \left\lfloor \frac{n + b_{k-1}}{b_k} \right\rfloor b_k - b_{k-1}$$

Here $\lfloor x \rfloor$ denotes the greatest integer not exceeding x.

Exercise (easy): Show that $|F_n| \leq 2 + \frac{n(n-1)}{2}$.

Exercise (hard): Prove the recurrence formula works.

The chart shows $\sqrt{|F_n|}$ as a function of n:



Fun Fact: Let $|F_n|$ be the number of terms in the Farey sequence of order n. Then for large n:

$$\lim_{n\uparrow\infty} \frac{\sqrt{|F_n|}}{n} = \frac{\sqrt{3}}{\pi}$$

Irrational Numbers

A real number that is not rational is an *irrational* number. The set of irrational numbers is $\mathbb{R}\backslash\mathbb{Q}$, that is, the elements of R which are not elements of $\mathbb{Q}$.

Exercise: Is the set of irrational numbers closed under addition? Under multiplication? Can you construct a proof or counter-example?

The Rational Root Theorem

Suppose that $p(x)$ is a polynomial of order $d \geq 1$ with integer coefficients, so that:

$$A(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

Suppose that $x = \frac{p}{q}$ is a rational *root* of A, with the fraction in its lowest terms. Then the rational root theorem states that:

- p is an integer factor of the constant term a_0, and
- q is an integer factor of the leading coefficient a_d.

A number x is a root of the polynomial if $A(x) = 0$.

For example, to find rational solutions of $x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$, let us define

$$A(x) = 4 - 8x + 4x^2 + 2x^3 - 3x^4 + x^5$$

Then the numerator p must be a factor of 4, so that p could be -4, -2, -1, 1, 2 or 4. The denominator must be a factor of 1, that is -1 or +1. This the only possible roots are -4, -2, -1, 1, 2 and 4. Checking all the cases, we find that the only rational root is $x = 1$.

This implies that the other real roots, namely $\pm\sqrt{2}$, are irrational.

To prove the rational root theorem, substitute $x = \frac{p}{q}$ into the polynomial and multiply by q^d. This gives:

$$a_d p^d + a_{d-1} p^{d-1} q + \ldots + a_2 p^2 q^{d-2} + a_1 p q^{d-1} + a_0 q^d = 0$$

All the terms except the last are multiples of p, and therefore p must also divide $a_0 q^d$. As p and q are relatively prime, Euclid's lemma implies that $p \mid a_0$. Likewise, all terms except the first are multiples of q, implying that the first term is also a multiple of q so that $q \mid a_d$.

Rational Points on a Circle

We know the integer points on the circle $x^2 + y^2 = 100$, namely $(0, 10)$, $(6, 8)$ and other solutions by permutation or sign changes.

We also know all the real points, namely $\{(x, \pm\sqrt{100 - x^2}) : |x| \leq 10\}$.

But what about rational points? Is there a rational root theorem in two dimensions that allows us to enumerate all the rational points? No: there are infinitely many rational points.

To find them, draw a straight line through the point $(-10, 0)$ and through one other rational point. Let the gradient of that straight line by g, so its equation is:

$$y = g(x + 10)$$

Of course, g is rational as the straight line connects two rational points. Squaring each side and substituting $y^2 = 100 - x^2$ gives:

$$100 - x^2 = g^2(x + 10)^2 = g^2x^2 + 20g^2x + 100g^2$$

Moving all terms to the right hand side gives:

$$0 = (1+g^2)x^2+20g^2x+100(g^2-1) = (x+10)((1+g^2)x+10(g^2-1))$$

The right hand side has two roots; the point we already know at $(-10, 0)$ and a second where:

$$x = 10\frac{1 - g^2}{1 + g^2}$$

Substituting back into the straight line gives:

$$y = 10\frac{2g}{1 + g^2}$$

We can now see that not only does every rational point on the circle, except $(-10, 0)$ implies rational g, but also that any rational g generates a rational point on the circle. Integer points on the curve correspond to

$$t = 0, \pm\frac{1}{3}, \pm\frac{1}{2}, \pm1, \pm2, \pm3$$

Status So Far

We have now mostly solved three equations for positive and negative integers, for the rationals and the reals, as shown by checks in the table below.

	$\mathbb{Z}^+$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
$20x + 23y = 2023$	✓	✓	✓	✓		
$x^2 + y^2 = 100$	✓	✓	✓	✓		
$x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$	✓	✓	✓	?		

Note that by considering rational solutions to the quintic, we are also able to enumerate integer solutions.

Complex Numbers

Square Root of -1

If $x \in \mathbb{R}$, then $x^2 \geq 0$ The equation $x^2 = -1$ has no solution in real numbers.

We can invent new numbers, the *imaginary* numbers, which solve this equation. We write the roots of $x^2 = -1$ as $x = i$ and $x = -i$.

A *complex* number x is a number of the form $a+bi$ where a, b are real and $i = \sqrt{-1}$. We say that $a = \Re(x)$ is the *real* part of x and $b = \Im(z)$ is the *imaginary* part. The set of complex numbers is written $\mathbb{C}$.

Are the Complex Numbers a Field?

To determine whether complex numbers form a field, we have to define addition and multiplication.

To define addition, add the real and imaginary parts separately.

To define multiplication, use the distributive law

$$(a+bi)\times(c+di)=ac-bd+(ad+bc)i$$

It is straightforward but tedious to demonstrate that all the field axioms for $\mathbb{C}$ follow from the statements for $\mathbb{R}$. The trickiest part is the multiplicative inverse, where we have:

$$(a+bi)^{-1}=\frac{a-bi}{a^2+b^2}$$

Square Root of a General Complex Number

Suppose $z=a+bi$ is a complex number. If $b=0$ then z is also real and we know how to calculate its square root. If $b\neq 0$ then z has two square roots, of which one has positive real part:

$$\sqrt{a+bi}=\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}+\mathrm{sgn}(b)\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}i$$

Here $\mathrm{sgn}(b)$ means the sign of b, that is, $+1$ if $b>0$ and -1 if $b<0$. Check this by multiplying out. The square of the right hand side is:

$$\begin{aligned}&\frac{a+\sqrt{a^2+b^2}}{2}-\frac{-a+\sqrt{a^2+b^2}}{2}\\&+2\mathrm{sgn}(b)\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}\times\frac{-a+\sqrt{a^2+b^2}}{2}}i\\&=\frac{a}{2}+\frac{a}{2}+2\mathrm{sgn}(b)\sqrt{\frac{b^2}{4}}i\\&=a+bi\end{aligned}$$

The second square root of $a + bi$ is the negative of the expression above.

Repeated Square Roots

Using this, we can compute square roots of $\pm i$:

$$\sqrt{i} = \frac{1+i}{\sqrt{2}}$$
$$\sqrt{-i} = \frac{1-i}{\sqrt{2}}$$

In total, there are 8 solutions to $x^8 = 1$, namely 1, -1, $\pm i$, the two square rots of i and the two square roots of $-i$. We can keep going to find 16 roots of $x^{16} = 1$ and so on. Critically, we do not need to keep inventing more imaginary numbers every time we need a square root; one invention of i is sufficient.

Complex Solutions to $x^2 + y^2 = 100$

We can find two solutions for y given (almost) any complex number x, namely:

$$y = \pm\sqrt{100 - x^2}$$

Exercise: Can you find a number of x for which there is only one value of y? Are there any values of $x \in \mathbb{C}$ for which no $y \in \mathbb{C}$ exists?

Quadratic Formula

Suppose $a, b, c \in \mathbb{C}$ and $a \neq 0$. Consider the quadratic equation:

$$ax^2 + bx + c = 0$$

You might already know how to solve this. First multiply each side by $4a$:

$$4a^2x^2 + 4abx + 4ac = 0$$

This we can re-arrange by completing the square:

$$(2a + b)^2 = 4a^2x^2 + 4abx + b^2 = b^2 - 4ac$$

Taking the square root of each side implies the well-known quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

The original quadratic can now be factorised as:

$$ax^2 + bx + c = \frac{(2ax + b - \sqrt{b^2 - 4ac})(2ax + b + \sqrt{b^2 - 4ac})}{4a}$$

In general, the factorisation might not work under the real numbers $\mathbb{R}$, because the square root might not exist, but it always works over the complex numbers $\mathbb{C}$.

Polynomial with Given Roots

Let $d \in \mathbb{Z}^+$ and let $\lambda_1, \lambda_2, \ldots \lambda_d \in \mathbb{F}$ where $\mathbb{F}$ is some field. It is easy to find a polynomial for which these are all roots; that

polynomial is the product:

$$p(x) = (x - \lambda_1) \times (x - \lambda_2) \times \ldots \times (x - \lambda_d)$$

Multiplying according to the distributive law, we can see that this polynomial is *monic*, that is, the leading coefficient (the coefficient of x^d) is 1.

Fundamental Theorem of Algebra

The fundamental theorem of algebra is that any *any* monic polynomial of degree d with coefficients in $\mathbb{C}$ factorises as:

$$p(x) = (x - \lambda_1) \times (x - \lambda_2) \times \ldots \times (x - \lambda_d)$$

for some complex numbers $\lambda_1, \lambda_2, \ldots \lambda_d$, not necessarily distinct. In other words, introducing $i = \sqrt{-1}$ does not only mean that all quadratic polynomials split into linear factors, but also cubics, quartics and univariate polynomials of higher degree. We do not have to keep inventing more imaginary numbers to split awkward polynomials.

Exercise: Why does the fundamental theorem of algebra fail over the real numbers?

Quintic Example

We have already considered the polynomial $A(x) = x^5 - 3x^4 + 2x^3 + 4x^2 - 8x + 4$. We know that $x = 1$ is a root, implying that $(x-1)$ is a factor of $A(x)$, and that $\pm\sqrt{2}$ are roots, implying that

$x^2 - 2$ is a factor. Dividing through by those two factors gives the factorisation:

$$A(x) = (x - 1)(x^2 - 2)(x^2 - 2x + 2)$$

We can factorise the last quadratic using the quadratic formula as:

$$x^2 - 2x + 2 = (x - 1 - i)(x - 1 + i)$$

Thus the last two roots of $A(x)$ are revealed as $1 \pm i$ and now we have the full set, by the fundamental theorem of algebra.

We notice that three of these roots are real and only one is an integer, so we have solved the quintic over all the number sets we were concerned with.

Status So Far

We have solved all three equations for positive and negative integers, for the rationals, the reals and the complex numbers, as shown by checks in the table below.

	$\mathbb{Z}^+$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
$20x + 23y = 2023$	✓	✓	✓	✓	✓	
$x^2 + y^2 = 100$	✓	✓	✓	✓	✓	
$x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$	✓	✓	✓	✓	✓	

Note that by considering rational solutions to the quintic, we are also able to enumerate integer solutions.

Advanced Material

Quaternions

William Rowan Hamilton was an Irish mathematician who invented *quaternions* in 1843. A general quaternion is of the form:

$$x = a + bi + cj + dk$$

where $a, b, c, d \in \mathbb{R}$ and i, j, k are three quaternion roots of -1 so that $i^2 = j^2 = k^2 = -1$. Addition of quaternions is performed component-wise.

Hamilton also declared the triple product:

$$i \times j \times k = -1$$

This is not compatible with the field axioms, specifically the commutativity of multiplication. However, if we relax the requirement for multiplication to commute, we can obtain a *skew field*.

Pre-multiplying the triple product by $-i$, or post-multiplying by $-k$, and applying the associative law, gives:

$$j \times k = -i^2 \times j \times k = i; i \times j = -i \times j \times k^2 = k$$

Further calculations in the same vein give the full table for multiplying units:

$$\begin{array}{cccc} 1 \times 1 = 1 & 1 \times i = i & 1 \times j = j & 1 \times k = k \\ i \times 1 = i & i^2 = -1 & i \times j = k & i \times k = -j \\ j \times 1 = j & j \times i = -k & j^2 = -1 & j \times k = i \\ k \times 1 = k & k \times i = j & k \times j = -i & k^2 = -1 \end{array}$$

Products of general quaternions are defined by the distributive law. Quaternions fail many properties of fields, for example in having infinitely many solutions to $x^2 = -1$. The failure occurs because of multiplication not being commutative.

The solution of linear equations with real coefficients is easy with quaternions, but higher order equations are very tricky. Thus our final progress chart is

	$\mathbb{Z}^+$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
$20x + 23y = 2023$	✓	✓	✓	✓	✓	✓
$x^2 + y^2 = 100$	✓	✓	✓	✓	✓	
$x^5 + 2x^3 - 8x = 3x^4 - 4x^2 - 4$	✓	✓	✓	✓	✓	

Finite Fields

Mathematicians who call themselves *algebraists* work with fields in general, proving theorems that apply to any field.

For example, you might think all fields have to contain the positive integers, that is, the sequence 1, $1+1$, $1+1+1$ etc. But none of the field axioms imply that the sequence has to go on for ever without repeating. The sequence could loop back to 0. The number of steps before this happens is called the *characteristic* of the field, and (it turns out) the characteristic always has to be a prime number.

For example, suppose we have a field of characteristic 3, so that in this field $0 = 3$ and $-1 = 2$. Suppose also there is an element i such that $i = \sqrt{-1} = \sqrt{2}$. Then we can compute successive

powers of $1 + i$:

$$\begin{aligned}
(1+i)^2 &= 1 - 1 + 2i = -i \\
(1+i)^3 &= -i(1+i) = 1 - i \\
(1+i)^4 &= (1-i)(1+i) = 2 = -1 \\
(1+i)^5 &= -1 - i \\
(1+i)^6 &= i \\
(1+i)^7 &= -1 + i \\
(1+i)^8 &= 1
\end{aligned}$$

These are the eight solutions of $x^8 = 1$. It turns out that these 8 elements, together with zero, form a finite field. All the field axioms can be checked by brute force as there are only finitely many cases to verify. The field is known as $\mathbb{F}_9$. It can be shown that any field with 9 elements must be isomorphic to this one, that is, any two fields of 9 elements are the same apart from swapping the labels of the elements.

There are not finite fields of all sizes; for example there is no $\mathbb{F}_{10}$.

The field $\mathbb{F}_9$ is not algebraically complete; for example the equation $x^2 = 1 + i$ has no solutions in $\mathbb{F}_9$.

Conclusions

Useful techniques to help you solve equations in different number sets:

$\mathbb{Z}^+$	Fundamental Theorem of Arithmetic
	Brute force search
$\mathbb{Q}$	Rational Root Theorem
	Chord Method
$\mathbb{R}$	Intermediate Value Theorem
$\mathbb{C}$	Quadratic formula
	Fundamental Theorem of Algebra