Melbourne High School Maths Extension Group 2023 Handouts

Nathan Wong Tom Yan

As of August 19, 2023

Contents

Part I

Weekly handouts

Melbourne High School
Maths Extension Group 2023
First Meeting Problems

1. Solve the equation $4t/3 + 2 = 2(t - 2)$.

2. A square circumscribes a circle of radius a. Find the probability that a randomly chosen point in the square is also in the circle.

3. Find a number that is the same when added to 5 as when multiplied by 5.

4. Evaluate
$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{99 \cdot 100}.$$

5. Call an integer to be *gobbus* if every digit is either 0 or 2 and it is divisible by 15. What is the smallest number that is gobbus?

6. I have three jars of cookies. The product of the number of cookies in each jar is 36. Unfortunately, even if I tell you the sum of the number of cookies in each jar, you won't be able to determine how many there are in each jar, but I do know that the jar with the most cookies is currently open. How many cookies are there in each jar?

7. If $1/(a + b) = 4$ and $a^2 + b^2 = 16$ find $1/a + 1/b$.

8. Find all primes less than 100 that are the sum of two squares.

9. Find all solutions in positive integers x and y of the equation $15x^2 + 2y^2 = 100 + 13xy$.

10. Find the last digit of 2^{2023}.

11. If $a, b, c > 0$ and $a + b + c = 1$, prove that $a^2 + b^2 + c^2 + 1 \geq 4(ab + bc + ca)$.

12. Define the *alternating sum* of a set of positive integers as follows: List the elements of the set in decreasing order. Take the first number in the list, subtract the second, add the third, subtract the fourth, and so on. For example, the alternating sum of the set $3, 5, 11, 7$ is $11 - 7 + 5 - 3 = 6$. Find the sum of the alternating sums of all the subsets of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

13. Evaluate $5^{261} \pmod{397}$.

14. Suppose BP and CQ are bisectors of the angles B, C of triangle ABC and suppose AH, AK are the perpendiculars from A to BP, CQ. Prove that KH is parallel to BC.

15. The Fibonacci sequence is defined by the recurrence relation $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Consider the power series
$$\begin{aligned} G(x) &= \sum_{i=0}^{\infty} F_i x^i \\ &= F_0 x^0 + F_1 x^1 + F_2 x^2 + F_3 x^3 + F_4 x^4 + F_5 x^5 + F_6 x^6 + \cdots. \end{aligned}$$
Find a closed-form expression for $G(x)$.

Melbourne High School
Maths Extension Group 2023
Term 1 Week 7 Handout

Introductory note

As this is the first handout of the year in this style, a few notes are in order. The first section consists of problems generally related to the main topic of the meeting—in this handout's case, combinatorics. The second section will contain a range of topics I find interesting that are not directly related to competition problems. The problems in this section require some working knowledge of proof. It is up to you what you work on.

Section A: Problems in combinatorics

1. Find the number of ways I can arrange the letters of: MATHSEXTENSIONGROUP

2. 10 points in the plane are given, with no 3 collinear. 4 distinct segments joining pairs of these points are chosen at random, all such segments being equally likely. Find the probability that some 3 of the segments form a triangle whose vertices are among the 10 given points.

3. Students sit at their desks in three rows of eight. Felix, the class pet, must be passed to each student exactly once, starting with Alex in one corner and finishing with Bryn in the opposite corner. Each student can pass only to the immediate neighbour left, right, in front or behind. How many different paths can Felix take from Alex to Bryn? (AMC Intermediate Q30)

4. Ali, Beth, Chen, Dom and Ella finish a race in alphabetical order: Ali in first place, then Beth, Chen and Ella. They decide to run another race and their placings all change. Two of the runners receive a placing higher than the week before, and the other three runners receive a placing lower than the week before. Given this information, in how many orders could the five runners have finished this second race? (AMC Senior Q30)

5. Each cell of an $m \times n$ board is filled with some nonnegative integer. Two numbers in the filling are said to be adjacent if their cells share a common side. (Note that two numbers in cells that share only a corner are not adjacent). The filling is called a garden if it satisfies the following two conditions:

(i) The difference between any two adjacent numbers is either 0 or 1.
(ii) If a number is less than or equal to all of its adjacent numbers, then it is equal to 0 .

Determine the number of distinct gardens in terms of m and n.

Section B: The higher arithmetic

Number theory, or the higher arithmetic, is the branch of mathematics that studies the natural numbers. It is a wondrous and beautiful subject, full of amazing ideas that will make your study of it worthwhile.[1]

Number theory investigates many different types of natural numbers and the relationships between them. Some are listed below.

- Prime numbers. They are the basic building blocks of all the natural numbers, and thus come up frequently in any arithmetic investigation. Many of number theory's famous solved and unsolved problems have to do with primes, including the Twin Prime Conjecture and the Prime Number Theorem.
- Shapely numbers. These are numbers like the familiar triangular and square numbers. Shapely numbers extend up to pentagonal numbers, hexagonal numbers, etc.
- Powers of numbers. The most famous theorem involving these numbers is *Fermat's Last Theorem*, which asserts that a number raised to a power greater than 2 is not the sum of two like powers.
- Perfect numbers. These are the numbers that are the sum of their proper divisors (all of their divisors except for itself). For example, 6 is a perfect number; its proper divisors, which are 1, 2, and 3, have a sum of 6.

Although number theory is primarily the study of natural numbers, we often have to resort to other number systems, including the integers, rationals, reals, and sometimes even the complex numbers. For the most part, however, we will stick to the natural numbers, the integers, and sometimes the rationals.

For all the interesting numbers of number theory, there are just as many interesting questions. Here are some about the primes; some have been solved while others remain unsolved.

- Which primes are the sum of two squares?
- The sequence 3, 5, 7 is a *prime triplet*. Are there infinitely many prime triplets?
- Are there infinitely many primes of the form $2^n - 1$?
- Are there infinitely many primes of the form $4n + 1$? $4n + 3$?
- Are there infinitely many primes of the form $n^2 + 1$?
- For some given natural number x, how many primes are there less than or equal to x?
- Is every even number greater than or equal to 4 the sum of two primes?

Number theory asks many questions of equations and polynomials too. Generally polynomials in number theory are considered to have integer or rational coefficients. For example, the equation $x^2 - Ny^2 = 1$ for a natural number N that is not a perfect square is known as *Pell's Equation*. Amazingly, such an equation always has infinitely many solutions. What's more, those solutions are related to continued fractions!

Even the simplest equations, linear equations, present difficulties because we often consider them in several variables. Consider the equation $ax - by = n$ for natural numbers a, b, and n. When does this equation have solutions in integers or natural numbers x and y?

Then there are equations of a more elaborate kind, such as the equation $y^2 = x^3 + 17$. It's not at all obvious how to solve such an equation in the integers or rationals. In fact, it is still and unsolved problem in mathematics as to how to determine whether such equations (y^2 equals a cubic in x) have finitely many rational solutions, infinitely many rational solutions, or no rational solutions at all.

We shall consider all the above types of numbers and equations in our journey through number theory.

Pythagorean triples

Let's begin our exploration into number theory by starting with something we already know: Pythagorean triples.

A Pythagorean triple is a triple of positive integers (a, b, c) where $a^2 + b^2 = c^2$. Geometrically, c is the hypotenuse and a and b are the two shorter sides of a right-angled triangle. A natural question is whether there are infinitely many such triples. The answer is yes because if (a, b, c) is a Pythagorean triple, then so is (na, nb, nc) for any natural number n. The simple direct proof follows.

$$\begin{aligned}(na)^2 + (nb)^2 &= n^2(a^2 + b^2)\\ &= n^2c^2\\ &= (nc)^2\end{aligned}$$

Triples that are just multiples of other triples aren't very interesting, so we look mainly at those triples in which a, b, and c share no common factors. These Pythagorean triples are called *primitive*. For example, $(3, 4, 5)$ is a primitive triple, while $(6, 8, 10)$ is not.

[1] Your mileage may vary.

Interlude 1. Write down as many primitive Pythagorean triples as you can and look for patterns.

From our definition of primitive triples, we immediately note that one of a and b has to be even and the other odd. If both a and b were even, then $c^2 = a^2 + b^2$ is even. This means c would also be even, contradicting the assumption that a, b, and c share no common factors. What happens if both a and b are odd?

Interlude 2. Prove that both a and b cannot be odd.

Since either a or b can be even and the other odd, from now on we can assume, without loss of generality, that a is odd and b is even. Note that this implies c must be odd too, because $a^2 + b^2$, being the sum of an even and an odd number, is odd.

A way to generate primitive triples would be quite a useful thing. How might we go about deriving a formula for a, b, and c? First we note that $a^2 = c^2 - b^2$, so $a^2 = (c+b)(c-b)$. The right-hand side, $(c+b)(c-b)$, is a perfect square. Since c and b share no common factors, neither do $c + b$ and $c - b$. Since they share no common factors, both $c + b$ and $c - b$ have to be squares themselves.

Interlude 3. To see why this is true, write down a few primitive Pythagorean triples and check if both $c + b$ and $c - b$ are perfect squares.

Since c is odd and b is even (by assumption), both $c - b$ and $c + b$ are odd. Thus we can let

$$c - b = t^2 \tag{1}$$

and

$$c + b = s^2 \tag{2}$$

for odd integers t and s. Since $c + b > c - b$, we have $s > t$. We can make one further deduction about t and s; they must share no common factors, because $c - b$ and $c + b$ share no common factors.

Interlude 4. Solve equations (1) and (2) to get b and c in terms of t and s.

If you done the above interlude correctly, you should have $b = (s^2-t^2)/2$ and $c = (s^2+t^2)/2$. Now we just need a formula for a. From $a^2 = b^2 - c^2$, we have

$$\begin{aligned} a &= \sqrt{(b+c)(b-c)} \\ &= \sqrt{s^2 t^2}. \end{aligned}$$

This implies $a = st$.

At the end of this long voyage, we have discovered a formula for generating primitive Pythagorean triples:

$$(a, b, c) = \left(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2} \right)$$

where $s > t \geq 1$ and s and t are odd integers that share no common factors. This formula, with slight modifications, is attributed to Euclid.

Interlude 5. Generate as many primitive triples as you can using the above formula to make sure that it works.

Problems

1. Show that the formula derived above is always a solution to $a^2 + b^2 = c^2$. If you can, prove that the formula always generates a primitive triple by showing that st, $(s^2 - t^2)/2$, and $(s^2 + t^2)/2$ share no common factors.

2. What do you notice about the even number in primitive Pythagorean triples? Prove that your conjecture is correct.

3. Show that one of a and b must be a multiple of 3.

4. Given a Pythagorean triple (not necessarily primitive) (a, b, c), consider its *product* to be abc. Prove that one of a, b, and c must be divisible by 5, and hence determine the highest common factor of all products of all Pythagorean triples.

5. Consider a circle of radius 1 centred at the origin with equation $x^2 + y^2 = 1$, and a line with a rational gradient m that passes through the point $(-1, 0)$. Find the coordinates of the other point of intersection between the line and the circle in terms of m. Hence deduce a second formula to generate Pythagorean triples (this one won't just generate primitive triples).

6. Given that the equation $X^4 - Y^4 = Z^2$ has no nonzero solution in integers X, Y, and Z, show that if three square numbers are in an arithmetic progression, their difference cannot also be a square.

7. Hence, or otherwise, show that a right-angled triangle with *rational* side lengths cannot have a square area.

Melbourne High School
Maths Extension Group
Term 1 Week 8 Handout

Problems

1) Find the ratio between the areas of a square and an octagon that are both inscribed in the same circle.
2) A circle of radius $9/2$ circumscribes a triangle ABC such that one of the triangle's sides passes through the centre of the circle; let this side be AB. If the arc length of BC is 3π, find the area of the triangle.
3) Given a rational number x/y, where x and y are positive integers, we define its *size* to be $x + y$. Find the rational number with smallest size that equals π to six decimal places.
4) (This problem requires calculus.) Now you will become Euler and prove the famous identity
$$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots. \tag{1}$$

   a) By instead considering the sum
   $$1 + \frac{1}{1}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{3} + \frac{1}{3}\cdot\frac{1}{4} + \cdots$$
   show that the infinite sum on the RHS of (1) converges to a finite value less than 2.

   b) Assume that $\sin x$ can be written as an infinite polynomial:
   $$\sin x = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + \cdots.$$
   Substitute in $x = 0$ and we get $a_0 = 0$. Differentiating both sides yields
   $$\cos x = a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + 5a_5 x^4 + \cdots.$$
   Put in $x = 0$ again and we have $a_1 = 1$. Repeat this process to find that $a_3 = -1/3!$, $a_4 = 0$, $a_5 = 1/5!$, $a_6 = 0$, $a_6 = -1/7!$ and so on. Hence show that
   $$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots. \tag{2}$$

   c) Divide both sides of (2) by x to get
   $$\frac{\sin x}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots. \tag{3}$$
   The key thing to realise in (3) is that the coefficient of the x^2 term is $-1/3! = -1/6$.

   Note that the roots of $\sin x/x$ are the same as $\sin x$ except that $x = 0$ is excluded. Hence the roots of the LHS of (3) are $x = \pm\pi, \pm 2\pi, \pm 3\pi, \ldots$. We know with normal polynomials that we can express them as a product of their

roots with a scaling factor. Let's do the same with $\sin x/x$; we get the infinite product

$$\frac{\sin x}{x} = a(x^2 - \pi^2)(x^2 - 4\pi^2)(x^2 - 9\pi^2)(x^2 - 16\pi^2)\cdots.$$

Now we just need to know what the scaling factor a is.

As with normal polynomials, we can find the scaling factor by plugging in another point that is not one of the roots. Let's choose $x = 0$. Obviously the LHS is undefined, but we can use a interesting trick that is generally not allowed when we are dealing with finite polynomials. Graphing $\sin x/x$, perhaps using Desmos, we see that

$$\lim_{x\to 0} \frac{\sin x}{x} = 1.$$

(This might be the most important limit in calculus.) Use this limit to find a and hence show that

$$\frac{\sin x}{x} = \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\left(1 - \frac{x^2}{9\pi^2}\right)\cdots.$$

d) If we expand the first two terms, we get

$$\left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right) = 1 - \left(\frac{1}{\pi^2} + \frac{1}{4\pi^2}\right)x^2 + \frac{x^4}{4\pi^4}.$$

Keep expanding the product until you notice a pattern.

e) Comparing coefficients with (3), complete Euler's proof of the Basel Problem.

5) For this problem, we definite a particular function $\zeta(s)$ to be

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots.$$

a) Show that

$$\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{7^s}\right)\cdots\zeta(s) = 1.$$

b) Hence show that

$$\frac{1}{\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\left(1 - \frac{1}{7^2}\right)\cdots} = \frac{\pi^2}{6}.$$

c) Finally, prove that the probability of two randomly chosen integers being coprime to each other is $6/\pi^2$.

d) What is the probability that four randomly chosen integers are all coprime? (Here we mean that the GCD of the four numbers is 1; we don't mean that every pair of those four integers is coprime.)

Melbourne High School
Maths Extension Group 2023
Term 1 Week 9 Handout

§1. More combinatorics problems

1. If 20 boys are on my school's soccer team, 25 boys are on my school's hockey team, and 11 boys play both sports, then how many boys play soccer or hockey?

2. A true-false test has 10 questions. Suppose that if you answer any five questions "true" and the remaining five questions "false", then your score is guaranteed to be at least four. How many answer keys are there for which this is true?

3. Annie the Ant starts at the lattice point $(0, 0)$ and each minute moves 1 space up or 1 space to the right (with equal probability). Benny the Beetle starts at $(5, 7)$ and each minute moves 1 space down or 1 space to the left (with equal probability). What is the probability that they meet?

4. What is the average number of pairs of consecutive integers in a randomly selected subset of 5 distinct integers chosen from the set $\{1, 2, 3, \ldots, 30\}$? For example the set $\{1, 17, 18, 19, 30\}$ has 2 pairs of consecutive integers.

5. There are K boys placed around a circle. Each of them has an even number of sweets. At a command each boy gives half of his sweets to the boy on his right. If, after that, any boy has an odd number of sweets, someone outside the circle gives him one more sweet to make the number even. This procedure can be repeated indefinitely. Prove that there will be a time at which all boys will have the same number of sweets.

§2. Euclid's Algorithm

Divisibility is a most useful concept in mathematics. We will explore this idea and present a famous algorithm for finding the greatest common divisor (GCD) of two numbers.

Our intuitive understanding of divisibility is probably this: an integer b is said to divide another integer a if and only if a is a multiple of b. Another common way to think about it is that dividing a by b leaves no remainder. This definition suffices for most purposes, but sometimes it is useful to have a more formal notion of the concept: b divides a if there is some integer m for which $a = mb$. This is useful in using divisibility information within an algebraic context.

Now that we have established the notion of divisibility, we can turn to the concepts of divisors (which are also called the 'factors' of a number) and the greatest common divisor. The *divisors* of an integer a are all the integers that divide a. For example, the divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$. Note that a divisor must be less than or equal to the number it is a divisor of.

Given two integers, we can ask which divisors they have in common. For example, 2 is a common divisor of any pair of even numbers, and 3 is a common divisor of 9 and 24. The *greatest common divisor* (GCD) of two numbers is the largest of the two numbers' common divisors; in other words, it is the largest number that divides both of them. This value is of such importance that it has its own notation; it is commonly denoted by $\gcd(a, b)$, where a and b are nonzero integers. If $\gcd(a, b) = 1$, then a and b are *coprime* or *relatively prime*.

How do we find the GCD of two numbers? Of course, we could just list the divisors of each and find the greatest number that is in both lists. However this is slow and not convenient for large numbers. Fortunately, there is an elegant algorithm of Euclid's that finds the GCD of two numbers in a much more efficient way.

Suppose we have two positive integers a and b that we want to find the GCD of. The core of the Euclidean algorithm is *Euclidean division*, which means expressing a in the form

$$a = qb + c,$$

where q and c are nonnegative integers and $c < b$. We call q the *quotient* and c the *remainder*. Writing this equation is really the same as dividing a by b with remainder; for example, if $a = 104$ and $b = 24$ we would write

$$104 = 4 \times 24 + 8.$$

Now let d be any common divisor of a and b; we know there must be at least one because 1 divides every positive integer. Note that d divides c too, because $c = a - qb$. To make this conclusion we rely on a simple theorem that you can prove for yourself: if two numbers m and n are both divisible by a third number k, then so is their sum $m + n$ and their difference $m - n$. In our specific case, we assume that d divides both a and qb, and so it must divide their difference $a - qb$, which is c.

By definition d divides b, and we have just shown that d also divides c; it follows from this that d is also a common factor of b and c. We have assumed nothing about d as a common divisor of a and b, so we are justified in saying that the set of common divisors of a and b is the same as the set of common divisors of b and c. Hence the GCD of a and b is equal to the GCD of b and c.

This may not seem like progress, but it is. We have essentially reduced the original problem to a smaller one: finding the GCD of b and c. It is "smaller" because $c < b$, whereas before $b < a$.

So now we just play the game again; we want to find the GCD of b and c and so we write

$$b = q'c + c'$$

where q' and c' are nonnegative integers and $c' < c$. Again we deduce that the GCD of b and c must be the same as that of c and c'.

Obviously we can't just keep going on like this forever, or else we wouldn't be solving the original problem of finding $\gcd(a, b)$. Where does it stop?

Note that the sequence of remainders we obtain by successive use of Euclidean division is a strictly decreasing sequence. The second time we did the division we had $c' < c$, and if we had continued we would have $c'' < c'$, $c''' < c''$, and so on. A decreasing sequence of nonnegative integers must reach 0 at some point. That is, one of the terms in the sequence $c, c', c'', ...$ must be 0. Let the term directly preceding it be t and the term preceding t be s. Recall that each term in the sequence comes from the Euclidean division of the preceding terms: c is the remainder when a is divided by b, the next term c' is the remainder when b is divided by c, and so on.

How did we get this 0 in our list of remainders? We must have used the division algorithm on s and t, the two previous terms. Therefore the relationship between s and t is

$$s = tu + 0$$

for some positive integer u. From this we infer that s is actually a multiple of t. But if s is a multiple of t, then the GCD of s and t must be t.

So we have found the GCD of t and s, but we haven't solved our original problem, which was to find the GCD of a and b. Actually, we have! Recall that we showed the GCD of a and b is the same as

that of b and c. In the same way, the GCD of b and c is the same as that of c and c'. Continuing in this fashion. we find that the GCD of a and b is the same as that of s and t; hence $\gcd(a, b) = t$, the last nonzero remainder in our list of remainders supplied by repeated application of Euclidean division.

That, in a nutshell, is the Euclidean algorithm for finding the GCD of two numbers. To summarise, here is the algorithm in two simple steps. Assume we want to find $\gcd(a, b)$.

1. If a is a multiple of b, then $\gcd(a, b) = b$.
2. Otherwise, let c be the remainder when a is divided by b. Then $\gcd(a, b) = \gcd(b, c)$.

Up until now, we have been using only algebraic symbols, which may have made the process of the algorithm confusing. Let's now do a concrete example and find $\gcd(177, 48)$. We begin by writing

$$177 = 3 \times 48 + 33.$$

Now the problem is reduced to finding $\gcd(48, 33)$, for which we continue with

$$48 = 1 \times 33 + 15.$$

The remainder is not 0 yet so the algorithm continues.

$$33 = 2 \times 15 + 3.$$

It is clear that the next remainder will be 0. One more application of the division algorithm yields

$$15 = 5 \times 3 + 0.$$

We have reached a 0 remainder, so $\gcd(177, 48) = 3$, the last nonzero remainder. Note we could also have deduced this from $\gcd(15, 3) = 3$, because we know that the set of common divisors of each pair of successive remainders is the same as the set of common divisors of 177 and 48. We proved this previously in our exploration of the general case of the algorithm.

The preceding example was small, so you might have been able to do it the naiv́e way (listing the factors of both numbers) or even in your head. Now try finding

$$\gcd(1160718174, 316258250).$$

(Despite the size of the numbers, you can get the answer using only a scientific calculator. Your immediate objection might be that the calculator has no button to give the remainder upon division; how might you get the remainders manually?)

A simple linear equation

In this section, let $g = \gcd(a, b)$.

Surprisingly, Euclid's algorithm answers the question of when the equation

$$ax - by = c \tag{1}$$

has natural number solutions in x and y. It is clear that $ax - by$ is always a multiple of g, because both ax and by are multiples of g. Thus (1) might have natural number solutions only when c is a multiple of g.

Now that we know when (1) might have solutions, the next question is whether there is always a solution when g divides c. It suffices to answer the question for when $c = g$; that is, the question of whether a linear combination of a and b can ever equal their GCD. The answer is yes. To see why the equation $ax - by = g$ always has solutions in natural numbers x and y, we need Euclid's algorithm.

If c is the difference of multiples of a and b (this is the same as saying there are positive integer solutions to $ax - by = c$), we say that c is *linearly dependent* on a and b. We now aim to prove the following results:

1. If c is linearly dependent on a and b, so is kc for any natural number k.
2. If both c and d are linearly dependent on a and b, so are $c + d$ and $c - d$.
3. Both a and b are linearly dependent on themselves.

The first is easy; if $c = ax - by$ then $kc = akx - bky$, so kc is also linearly dependent on a and b with solution (kx, ky). The second is only slightly more difficult. Let

$$c = ax_1 - by_1$$

and

$$d = ax_2 - by_2.$$

Then

$$c + d = (ax_1 - by_1) + (ax_2 - by_2),$$

which implies

$$c + d = a(x_1 + x_2) - b(y_1 + y_2).$$

showing that $c + d$ is also linearly dependent on a and b. Similarly,

$$c - d = (ax_1 - by_1) - (ax_2 - by_2),$$

and so

$$c - d = a(x_1 - x_2) - b(y_1 - y_2).$$

We verify the third statement simply by seeing that $a = a(b + 1) - b(a)$ and $b = b(a + 1) - a(b)$.

Note that we cannot write $a = a \cdot 1 + b \cdot 0$, because x and y are natural numbers.

We are now ready to use Euclid's algorithm to show that the equation $ax - by = g$ is soluble in the natural numbers. Recall that the first line of the algorithm is to write $a = qb + c$, which implies $c = a - qb$. Since a and qb are both linearly dependent on a and b (from the first and third rules), so is their difference, which is c (from the second rule).

Now we know that both b and c are linearly dependent on a and b. We can again rearrange the next line, $b = q'c + c'$, for the remainder: $c' = b - q'c$. Applying the same reasoning as before, we deduce that c' is also linearly dependent on a and b.

In other words, a and b being linearly dependent on themselves implies that each remainder of the Euclidean algorithm is also linearly dependent on them. In particular, $\gcd(a, b)$ is linearly dependent on a and b because it is the last nonzero remainder in the algorithm.

Thus we have accomplished what we set out to show: linear equations of the form $ax - by = \gcd(a, b)$ are always soluble in the natural numbers. Note this also means that the equation $ax - by = c$ always has natural number solutions when a and b are coprime, as every natural number is a multiple of 1.

The preceding logic, although beautiful, only provides us insight as to why equation (1) is always soluble. It doesn't actually give us a way to solve the equation in practice. Fortunately, the process isn't difficult; we illustrate with a concrete example.

Suppose we want to solve the equation $177x - 48y = 3$ (previously we found that $\gcd(177, 48) = 3$). We begin by writing the lines of the Euclidean algorithm. To make things easier, replace 177 by a and 48 by b; the reason will become apparent soon.

$$\begin{aligned} a &= 3b + 33 \\ b &= 1 \times 33 + 15 \\ 33 &= 2 \times 15 + 3 \end{aligned}$$

Rearranging the first line for the remainder, we get $33 = a - 3b$. Substitute this into the next equation, and solve for its remainder again:

$$\begin{aligned} b &= (a - 3b) + 15 \\ 15 &= b - (a - 3b) \\ &= 4b - a \end{aligned}$$

If we keep repeating this process we'll eventually end up with 3, the last remainder, expressed as a combination of a and b. For the third line we substitute in both $33 = a - 3b$ and $15 = 4b - a$.

$$\begin{aligned} a - 3b &= 2(4b - a) + 3 \\ a - 3b &= 8b - 2a + 3 \\ 3 &= 3a - 11b \end{aligned}$$

Finally, read off the coefficients of a and b to find that the solution is $x = 3$ and $y = 11$.

Problems

1. Describe a general procedure for solving the equation $ax - by = n$ in the natural numbers when n is a multiple of $\gcd(a, b)$.

2. Solve the equation

$$1769x - 551y = \gcd(1769, 551)$$

for natural numbers x and y.

3. Try using Euclid's algorithm to solve the equation $7200x - 3132y = \gcd(7200, 3132)$ for positive integers x and y. What seems to be wrong at the end? How can this be fixed?

4. Show that if $a^x \equiv 1 \pmod{n}$ and $a^y \equiv 1 \pmod{n}$, then

$$a^{\gcd(x,y)} \equiv 1 \pmod{n}.$$

5. Let a and b be coprime positive integers. Show that for any integer k, there exists a positive integer N such that N is divisible by a and $N + k$ is divisible by b.

6. Prove that if a prime p divides a product ab, then p divides at least one of a and b. (Do this without relying on the Fundamental Theorem of Arithmetic.)

Melbourne High School
Maths Extension Group 2023
Term 1 Week 10 Handout

§1. Problems relating to combinatorial games

1. A pile of a stones is given. Two players play the following game: each of them in turns takes 1,2 or 3 stones. The player who takes the last stone wins. Determine, in terms of a, who has a winning strategy.

2. In the game *DoubleChess*, the rules of chess are changed so that White and Black alternately make two legal moves at a time. Show that Black doesn't have a winning strategy

3. Two players start with the number 1 and take turns to multiply it by an integer from 2 to 9. The winner is the first player to obtain a number greater than or equal to 1000. Which player has a winning strategy?

4. All cells of a 4×4 table are painted white. In turn two players paint a white cell black. If a player makes a move, after which there is a black square 2×2, the player loses. Who has a winning strategy?

5. Two players in turn write S or O in an empty cell of a 1×2000 table. The first player who produces three consecutive boxes that spell SOS wins. If all boxes are filled without producing SOS then the game is a draw. Prove that the second player has a winning strategy.

§2. Modular arithmetic and congruences

§2.1 Theory and notation

Our previous exploration of Euclid's algorithm has left us perfectly poised on the precipice of the most important theorem in elementary number theory, the Fundamental Theorem of Arithmetic. However, to increase the suspense, we shall delay our study of this theorem until next term. For now, we settle for another core pillar of number theory: modular arithmetic and congruence.

Think of modular arithmetic as cyclic counting, or a system of doing arithmetic in which numbers "wrap" around at a certain value. For example, when we consider the hour of the day on a twelve-hour clock, 13 is the same as 1, 14 is the same as 2, 15 is the same as 3, and so on. In this case the hours wrap around when they get to the number 12. The power of this lies in how we can take an infinity (the positive integers) and reduce it to a finite set of 12 numbers. To illustrate, suppose we start at midnight and add 147 hours. To find the hour of the day at that time, we only need to know how much bigger 147 is than a multiple of 12, because the hours reset every 12 hours. We see that 147 is 3 more than a multiple of 12, so we are at 3 o'clock. Note how this works for an arbitrarily large hour. By subtracting a multiple of 12, we can always reduce the hour to one between 0 and 11; the 12th hour wraps around to 0. Also note how this is the same as finding the remainder after division by 12. The only possible remainders are the numbers $0, 1, 2, \ldots, 11$.

This idea of "wrapping around" is so useful it has its own notation. Given two integers a and b and a third positive integer greater than unity m called the *modulus*, we say that *a is congruent to b modulo m* if b can be obtained by subtracting from a a multiple of m. This relation is denoted

$$a \equiv b \pmod{m}.$$

Another way of saying it is that $a - b$ is a multiple of m. We call a and b *residues* of each other.

The preceding algebraic definition is not intuitive. A more intuitive way to think about it is if a and b are congruent modulo m, then a and b are essentially the same number when viewed from the perspective of divisibility by m; that is, they leave the same remainder when divided by m. That remainder is always a number between 0 and $m - 1$ inclusive, and is called the *least residue* of a and b. Relative to a modulus m, every number is congruent to one number in the set $\{0, 1, 2, \ldots, m-1\}$. This set is called a *complete set of residues*. Any set of m elements in which all elements are incongruent to one another is also called a complete set of residues. For example, relative to the modulus 5, the set $\{-2, -1, 0, 1, 2\}$ is a complete set of residues. Every number is congruent to one of those numbers modulo 5.

The definition of congruence extends naturally to negative integers. For example, $2 \equiv -5 \pmod{7}$ because $2 - (-5)$ is divisible by 7. The main algebraic picture to keep in mind is that of $a - b$ being divisible by m if $a \equiv b \pmod{m}$. This relation can be written

$$a - b = mk$$

for some integer k. Rearranging yields

$$a = mk + b.$$

Recognise that this is Euclidean division of a and m; this proves there exists some $b = b'$ such that $0 \leq b' \leq m - 1$, and hence any number a is congruent to a number in that range, as already mentioned.

The true power of congruence reveals itself when we being treating the congruence symbol $\equiv$ like an equals sign. Here are some of the basic properties of congruences. Assuming that $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then:

- $a + b \equiv a' + b' \pmod{m}$;
- $a - b \equiv a' - b' \pmod{m}$;
- $ab \equiv a'b' \pmod{m}$;
- $ka \equiv ka' \pmod{m}$ for any integer k (this is a special case of the preceding property).

These are fairly simple to prove using the algebraic definition of congruence.

The preceding properties show that congruences are compatible with equations in at least addition, subtraction, and multiplication. We can deduce from this that congruences are also compatible with polynomial evaluation, as long as the polynomial has integer coefficients. For example, if $a \equiv 1 \pmod{4}$, then

$$\begin{aligned} a^2 + 7a + 5 &\equiv 1^2 + 7 + 5 \pmod{4} \\ &\equiv 13 \pmod{4} \\ &\equiv 1 \pmod{4} \end{aligned}$$

Even though the only thing we know about a is that it is 1 more than a multiple of 4, we can tell that $a^2 + 7a + 5$ will also be 1 more than a multiple of 4, regardless of what a actually is. More generally, if $P(x)$ is a polynomial with integer coefficients, then

$$P(a) \equiv P(b) \pmod{m}$$

if $a \equiv b \pmod{m}$.

We have seen that addition, subtraction, and multiplication work with congruences the same way they work with equations. How about division?

A common factor can only be cancelled from both sides of a congruence if it is coprime with the modulus. For example, in the congruence $42 \equiv 12 \pmod{10}$, the factor 3 may be cancelled from both sides to yield the correct congruence $14 \equiv 4 \pmod{10}$ because 3 is coprime with 10. However, dividing both sides by 6 yields the incorrect congruence $7 \equiv 2 \pmod{10}$.

To demonstrate why this is the case, suppose $ax \equiv ay \pmod{m}$. Then, by definition, $a(x-y)$ is divisible by m. By cancelling a from both sides, we assert that $x-y$ is divisible by m, but this might not be the case, because m could divide a and not $(x-y)$. The only way to ensure that m divides $(x-y)$ and not a is if a and m are coprime; hence cancelling a factor from both sides of a congruence is valid only if that factor is relatively prime with the modulus.

What if the two sides of a congruence don't share a common factor? In other words, are fractions allowed in congruences? The answer to this question is slightly more complicated, relating to solving linear congruences. This will be explored in the next section.

§2.2 Exercises

1. Prove the following two properties of congruences (symmetry and transitivity).
   - If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.
   - If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
2. Use modular arithmetic to prove the divisibility test for 3 and 9.
3. Use modular arithmetic to prove the divisibility test for 11. (That is, a number written in decimal notation is divisible by 11 if the alternating sum of its digits is divisible by 11.)
4. Show that if $a \equiv b \pmod{2m}$, then $a^2 \equiv b^2 \pmod{4m}$. If you can, prove the more general statement that if $a \equiv b \pmod{km}$, then $a^k \equiv b^k \pmod{k^2 m}$.

§2.3 Linear congruences

As with normal equations, we can solve congruences. The simplest type is the linear congruence

$$ax \equiv b \pmod{m}.$$

The above equation is soluble for x when a and m are relatively prime. To see why, let's go back to the definition of congruence. If $ax \equiv b \pmod{m}$, then $ax-b$ is divisible by m. Hence let $ax-b = my$ for some integer y. Rearrange to get the equation $ax-my = b$. This is the linear equation we considered when discussing the Euclidean algorithm, and we know that it always has natural number solutions when a and m are coprime. Hence our linear congruence has a solution in x too, since we just need to solve the linear equation and reduce the value of x to its least residue.

To illustrate, let us solve the congruence

$$7x \equiv 5 \pmod{13}.$$

Since 7 and 13 are prime, they are coprime, so this equation has a solution. We use the definition of congruence and let $7x - 5 = 13y$ for some integer y; rearranging we get $7x - 13y = 5$. To solve this equation, we first solve the equation $7x' - 13y' = 1$ using the Euclidean algorithm, which gives us the solution $(x', y') = (2, 1)$. Multiply x' and y' by 5 to get the solution to the desired equation: $(x, y) = (10, 5)$. Since 10 cannot be reduced further modulo 13, we have solved the congruence by obtaining the solution $x \equiv 10 \pmod{13}$.

There are two things to note in our preceding example. Firstly, by finding one solution, we have actually found infinitely many solutions, because any number congruent to 10 modulo 13 is also a solution. However, in finding solutions to congruences, we consider the number of solutions to be the number of incongruent solutions; hence this equation has only one solution. Secondly, solving the congruence gives us an answer as to what the fraction 5/7 means modulo 13; it is congruent to 10. In general, fractions are allowed in congruences as long as the denominator is coprime with the modulus because they are just symbolic of a solution to a linear congruence. The fraction b/a relative to the modulus m represents the solution to the linear equation $ax \equiv b \pmod{m}$, and hence only exists when a and m are coprime because otherwise such a solution would not exist, as we have shown. An interesting parallel between congruences and equations is evident when we consider prime moduli. If m is prime, the only condition is that b is not a multiple of m, as that guarantees b and m are coprime. But that just means $b \not\equiv 0 \pmod{m}$, which is analogous to how dividing both sides of an equation by 0 is not allowed.

Now it is time to generalise. Consider the equation

$$ax \equiv b \pmod{m} \tag{1}$$

where a and m are not necessarily coprime. Let $g = \gcd(a, m)$. If $g = 1$ we have the case described above. So what happens if $g \neq 1$?

As is often the case in mathematics, we start with the definitions. Performing a similar algebraic manipulation as before, we get the equation

$$ax - my = b \tag{2}$$

for some integer y. We know the LHS will always be a multiple of g, and therefore the equation only

has positive integer solutions when b is a multiple of g. This immediately answers our question as to when the congruence (1) has any solutions.

Now the goal is to find how many solutions there are and what they are. As before, the next step is to solve equation (2) for x and y. If we let the solution to $ax' - my' = g$ be $(x', y') = (u, v)$, we obtain a solution to equation (2) by multiplying by b/g, which we know to be an integer because g divides b. Hence the solution we get for equation (2) is

$$(x, y) = \left(\frac{ub}{g}, \frac{vb}{g}\right).$$

Having found one solution, $x \equiv ub/g \pmod{m}$, the natural question is whether there are any more. A key technique that we use here is to assume another solution exists; if we prove that this second solution is congruent to the first, then there are no more solutions. Otherwise, we have found a way of generating all other solutions.

Let's label our first solution x_1 and suppose there is another solution x_2. By definition, $ax_2 \equiv b \pmod{m}$. Using the properties of transitivity and symmetry, we deduce that $ax_2 \equiv ax_1 \pmod{m}$. Now we use the definition of congruence to find that $a(x_2 - x_1)$ is divisible by m, which further implies that $(a/g)(x_2 - x_1)$ is divisible by m/g.

Here is where we use the definition of g. Since $g = \gcd(a, m)$, then a/g and m/g cannot share any common factors, since otherwise we would derive a contradiction in the definition of g. Hence the number m/g cannot divide a/g; it must divide $x_2 - x_1$. From this we conclude there is some integer k for which

$$x_2 - x_1 = k \cdot \frac{m}{g}.$$

Rearranging for our new solution x_2, we get

$$x_2 = x_1 + k \cdot \frac{m}{g}.$$

We have therefore found another solution to our original congruence:

$$x_2 \equiv x_1 + k \cdot \frac{m}{g} \pmod{m}.$$

Since m/g is not congruent to 0 modulo m, the two solutions x_2 and x_1 will be incongruent as long as k takes one of the values $1, 2, \ldots, g-1$. We need not consider $k \geq g$ because those values of k do not yield a new solution. For example, if $k = g + 1$, we get $x_2 = x_1 + m + g/m$, which is the same solution modulo m as if we took $k = 1$.

We get all solutions to the congruence (1) by running k through the values $0, 1, 2, \ldots, g-1$; hence there are exactly g incongruent solutions.

The result of this rather arduous journey is a most exciting theorem about the solubility of linear congruences. Here is a concise summary. If a and b are integers, m is a positive integer greater than 1, and $g = \gcd(a, m)$, the congruence

$$ax \equiv b \pmod{m}$$

has exactly g incongruent solutions. To find these solutions, first solve the equation $ax - my = g$. Let the solution to this equation be $(x, y) = (u, v)$. Then all g solutions can be found by computing

$$x_k = \frac{bu}{g} + k \cdot \frac{m}{g}$$

for $k = 0, 1, 2 \ldots, g-1$.

Linear congruences are the tip of the iceberg when it comes to solving congruences. In the future we shall consider congruences of higher degree, in which there are many interesting theorems. In particular, the study of quadratic congruences has led to a theorem that Gauss considered the "golden theorem" and is no doubt one of the most beautiful theorems in all of mathematics. But more on this exciting topic at another time.

§2.4 Problems

1. I have invited 118 people to my party, but unfortunately 13 of them can't make it. Therefore at the end of my party, after everyone eats the same number of cupcakes, I would like 13 cupcakes left for them. However, each person at my party can eat a maximum of 50 cupcakes; anyone who eats more than that will become seriously ill, and that's not good. If my cupcake vendor only sells in batches of 97 cupcakes, am I able to satisfy the needs of my party?

2. Given an integer a and a modulus m, the *multiplicative inverse of a modulo m* is another integer denoted by a^{-1} such that $aa^{-1} \equiv 1 \pmod{m}$. Show that if a and m are coprime, then there always exists a multiplicative inverse of a modulo m.

3. Hence, or otherwise, prove that

   $$(p-1)! \equiv -1 \pmod{p}$$

   for any prime p. (This is known as *Wilson's Theorem.*)

4. Let a and m be coprime integers with $m > 1$. Show that if each element of the set

   $$\{0a, a, 2a, \ldots, (m-1)a\}$$

   is reduced modulo m, the resulting set is equal to the set

   $$\{0, 1, 2, \ldots, m-1\}.$$

   Hence find a second proof that the equation $ax \equiv b \pmod{m}$ is soluble when $\gcd(a, b) = 1$.

Melbourne High School
Maths Extension Group 2023
Term 1 Holiday Problems

1. Suppose you have n distinct objects, each with an equal probability of being selected. After an object is selected, it is replaced. Each selection of an object is considered a "turn." What is the expected value of turns that you need to complete before you have selected at least one of each object?

2. Your good friend Harold is about to start reading Virginia Woolf's *Between the Acts*. The book has 199 pages, which you instantly recognise as being prime.

   Since Harold is much smarter than you, he doesn't read books in the correct page order. He begins by choosing a random number between 1 and 199—call this number x. To determine the nth page that he will read, he multiplies n by x, and if the number is greater than 199, he subtracts off a multiple of 199 so that he has a page number that is actually in the book. He then reads that page before calculating the next page he will read.

   Show that not only will Harold read each page of the book, but he will also never read a page more than once.

3. Find all natural numbers n such that $2^{2^n} + 5$ is prime.

4. Let N be a regular nonagon, having O as the centre of its circumcircle, and let PQ and QR be adjacent edges of N. The midpoint of PQ is A and the midpoint of the radius perpendicular to QR is B. Determine the angle between AO and AB.

5. Let $0 < a < 1$. Solve
   $$x^{a^x} = a^{x^a}$$
   for positive numbers x.

6. Find the sum of all positive integers n for which
   $$n^2 - 19n + 99$$
   is a perfect square.

7. Prove that the fraction
   $$\frac{21n + 4}{14n + 3}$$
   cannot be reduced further for all natural number values of n.

8. Show that we can colour the elements of the set $S = \{1, 2, \ldots, 2007\}$ with 4 colours such that any subset of S with 10 elements, whose elements form an arithmetic sequence, is not all one colour.

9. Two points K and L are chosen inside triangle ABC and a point D is chosen on the side AB. Suppose that B, K, L, C are concyclic, $\angle AKD = \angle BCK$ and $\angle ALD = \angle BCL$. Prove that $AK = AL$.

10. (This is a long problem.)

    (a) Evaluate $(a + b)^2 \pmod 2$, $(a + b)^3 \pmod 3$, and $(a + b)^5 \pmod 5$.

(b) The Binomial Theorem states that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Prove that

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

for any prime p

(c) Suppose you have 6 different applied mathematics books that you would like place in 3 bins. How many ways are there to distribute the books such that the first bin has 1 book, the second 2 books, and the third 3 books?

(d) Now suppose you have n different applied mathematics books and m bins. Someone supplies you a list of numbers whose sum is n: $k_1, k_2, k_3, \ldots, k_m$. How many ways are there to distribute the books such that the ith bin receives k_i books? That is, the first bin should receive k_1 books, the second k_2 books, and so on. Note that $k_1 + k_2 + k_3 + \cdots + k_m = n$.

(e) If you have completed the last part correctly, you have just discovered *multinomial coefficients*, which, as you might be able tell by the name, generalise the venerable binomial coefficients.

Let n be a positive integer and let $k_1, k_2, k_3, \cdots k_m$ be m positive integers that sum to n. This multinomial coefficient is denoted

$$\binom{n}{k_1, k_2, \ldots, k_m}.$$

If your answer to the previous part involved binomial coefficients, make use of a telescoping product to show that

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1! k_2! \cdots k_m!}.$$

(f) Expand $(a+b+c)^3$, taking note of the coefficients and the powers of a, b, and c in each term.

(g) By first doing some more examples if necessary, come up with a conjecture about the expansion of

$$(x_1 + x_2 + x_3 + \cdots + x_m)^n$$

using multinomial coefficients.

(h) Prove your conjecture by induction (you will need the binomial theorem).

(i) If you have made it this far in the problem, well done.
Prove that

$$(x_1 + x_2 + x_3 + \cdots + x_m)^p \equiv x_1^p + x_2^p + x_3^p + \cdots x_m^p \pmod{p}$$

for any prime p. (You can induction, but you could also look at the definition of a multinomial coefficient directly.)

(j) Hence, show that

$$a^p \equiv a \pmod{p}$$

for any prime p and any positive integer a.

11. Find $(102^{73} + 55)^{37}$ modulo 111.

12. We define the Fibonacci numbers by the recurrence relation $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Earlier in the term we discovered that the generating function

$$G(x) = F_0 + F_1 x + F_2 x^2 + F_3 x^3 + \cdots$$

has the closed form expression

$$\frac{x}{1 - x - x^2}.$$

In this problem, we will use this result to derive a closed-form expression for the nth Fibonacci number.

(a) Begin by showing that the closed-form expression for $G(x)$ can be written

$$\frac{x}{(1 - \alpha x)(1 - \beta x)}$$

where

$$\alpha = \frac{1 + \sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

(b) This fraction can be split into the sum of two fractions:

$$\frac{A}{1 - \alpha x} + \frac{B}{1 - \beta x}.$$

Show that $A = 1/\sqrt{5}$ and $B = -1/\sqrt{5}$.

(c) Show that

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1 - x}.$$

(This value makes sense for $|x| < 1$.)

(d) Hence show that

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right).$$

This is known as *Binet's Formula*.

Melbourne High School
Maths Extension Group 2023
Some of Euler's Gems

Read Euler, read Euler, he is the master of us all.

—Pierre-Simon Laplace

1. (In this problem, the famous geometric series formula

$$a + ar + ar^2 + ar^3 + \cdots + ar^{n-1} = \frac{a(r^n - 1)}{r - 1}$$

may or may not be useful.)

We begin by considering the charming *perfect numbers*. A perfect number is one that is equal to the sum of its proper divisors—that is, all of its divisors including 1 but excluding itself. For example, 6 is a perfect number because its proper divisors 1, 2, and 3 sum to 6. The next perfect number is 28, which is $1 + 2 + 4 + 7 + 14$.

Euler and Euclid proved that these numbers have something to do with *Mersenne primes*. These are the primes of the form $2^n - 1$. For example, $3 = 2^2 - 1$, $7 = 2^3 - 1$, and $31 = 2^5 - 1$ are all Mersenne primes.

In terms of notation, we denote the sum of all the divisors of n (including n) as $\sigma(n)$. Therefore $\sigma(6) = 1 + 2 + 3 + 6 = 12$ and $\sigma(10) = 1 + 2 + 5 + 10 = 18$. Note that n is perfect if $\sigma(n) = 2n$. It will also be useful to have a function $d(n)$ that we use to denote the number of divisors of n. Keeping with the previous examples, we have $d(6) = d(10) = 4$.

   (a) Begin by showing that if $2^n - 1$ is prime, then n is also prime. (This might not seem particularly relevant now, but trust that it will crop up later.)

   (b) Let's find out a little more about $\sigma(n)$. As with most things in mathematics, if we know nothing about the properties of a function, we can only begin by plugging values in and seeing what the results are. In this spirit, compute the values of $\sigma(n)$ for the first twenty values of n.

   (c) In your table, you may notice that

$$\sigma(mn) = \sigma(m)\sigma(n)$$

   whenever m and n are coprime. (A function that exhibits this property is called *multiplicative*.) Out goal now is to prove this property.
   Suppose the divisors of m are

$$a_1, a_2, \ldots, a_{d(m)}$$

   and the divisors of n are

$$b_1, b_2, \ldots, b_{d(n)}.$$

   Note that this means

$$\sigma(m) = a_1 + a_2 + \cdots + a_{d(m)}$$

   and

$$\sigma(n) = b_1 + b_2 + \cdots + b_{d(n)}.$$

   By considering a concrete example if necessary, list the divisors of mn. (Remember that m and n are coprime.) Hence complete the proof that

$$\sigma(mn) = \sigma(m)\sigma(n).$$

(d) We may also wish to find a formula for $\sigma(n)$, a mysterious black box into which we can just plug in a number and magically get out the sum of its divisors. A formula does exist but for now we shall be content with proving that

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$$

where p is prime and k is an integer.

(e) Now that we have proved the multiplicative property of the function $\sigma(n)$ and found a formula for $\sigma(p^k)$, we can turn our attention back to Euclid, Euler, and perfect numbers.

The numbers connecting them are those of the form $N = 2^{p-1}(2^p - 1)$ where $2^p - 1$ is prime (a Mersenne prime). Follow in the footsteps of the great Euclid and prove that N is perfect. That is, prove

$$\sigma(N) = 2N.$$

(f) Now it is time for Euler to step in; he proved the converse. That is, if an even number is perfect, then it must be of the form $2^{p-1}(2^p - 1)$. (Interestingly, no odd perfect numbers have ever been found.)

Let N be our even perfect number. Show that $N = 2^k m$ for some $k \geq 1$ and odd integer m.

(g) Use results we have already proved to show that

$$2^{k+1}m = (2^{k+1} - 1)\sigma(m). \tag{1}$$

(h) Clearly $2^{k+1} - 1$ is odd. Since Equation (1) implies that $(2^{k+1} - 1)\sigma(m)$ is a multiple of 2^{k+1}, it follows that 2^{k+1} must divide $\sigma(m)$. Hence $\sigma(m) = 2^{k+1}c$ for some integer c. Now show that Equation (1) becomes

$$m = (2^{k+1} - 1)c.$$

(i) If we assume that $c > 1$, then m is divisible by at least 1, m, and c. Show that

$$\sigma(m) \geq 1 + 2^{k+1}c.$$

(j) Use the preceding inequality to derive a contradiction, and hence show that $c = 1$.

(k) Use the fact that $c = 1$ to prove that m must be prime.

(l) We have just shown that $m = 2^{k+1} - 1$ is prime. Use the first part of this problem to complete Euler's proof that every even perfect number is of the form $2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are prime.

2. In this problem we shall consider the fascinating infinite series

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots$$

known as the *Harmonic series*.

A few words about notation: we denote the nth partial sum of the series H_n and call it the nth harmonic number; that is,

$$H_n = \sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

(a) Our first goal is to prove that this infinite series diverges (the sum goes to infinity and doesn't converge to a finite value). Do this by considering consecutive terms in the sum of the form

$$\cdots \frac{1}{2^k+1} + \frac{1}{2^k+2} + \cdots + \frac{1}{2^{k+1}} \cdots .$$

(b) If we represent each term in the Harmonic series as the area of a rectangle with base 1 and height $1/k$, we get a series of rectangles that look like the graph of $f(x) = 1/x$, as might be expected. This is shown in Figure 1. Note how the rectangles approximate

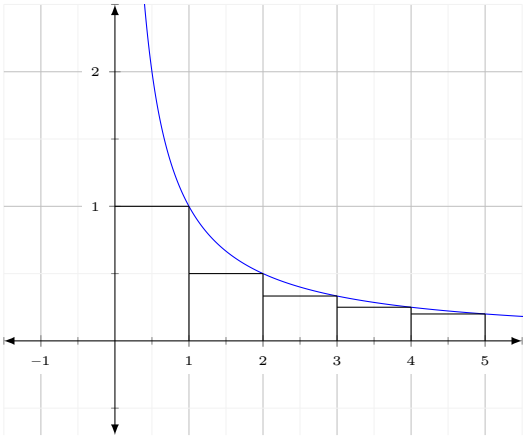


Figure 1: A lower bound for $\ln n$ in terms of H_n

the area under the graph of $1/x$ from below. If we shift the rectangles one to the right we get an overestimate for the area, as shown in Figure 2. This overestimate is what

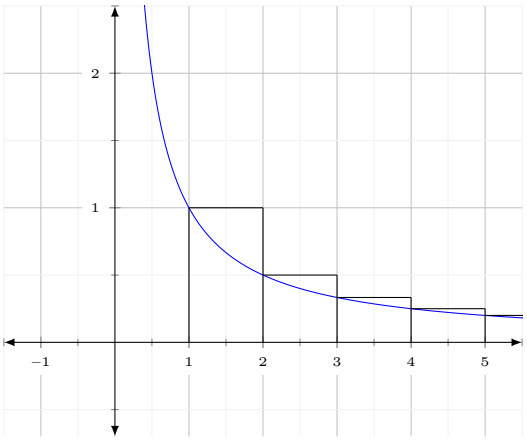


Figure 2: An upper bound for $\ln n$ in terms of H_n

we're interested in, since we also know that the area under the graph of $1/x$ starting at $x = 1$ is given by

$$\int_1^x \frac{1}{t} dt = \ln x.$$

Therefore it seems like the harmonic series approximates the natural logarithm, with, as is evident from the diagram, some degree of error.

Using the two diagrams, show that

$$\ln(n) < H_n < \ln(n) + 1.$$

(c) From Figure 2, H_n is slightly bigger than $\ln(n)$. Let's call the difference between them γ. That is,

$$H_n \approx \ln(n) + \gamma.$$

Just empirically, we can see that γ changes depending on how large n is. Figure 3 is a table showing the value of γ for different values of n (generated using Mathematica). We see that not only does the value of γ decreases as n increases, the rate of its

n	H_n	$\ln(n)$	γ
1	1	0	1
2	1.5	0.693147	0.806853
3	1.83333	1.09861	0.734721
4	2.08333	1.38629	0.697039
5	2.28333	1.79176	0.673895
6	2.45	1.79176	0.658241
7	2.59286	1.94591	0.646947
8	2.71786	2.07944	0.631744
⋮	⋮	⋮	⋮
97	5.15707	4.57471	0.583261
98	5.16728	4.58497	0.582309
99	5.17738	4.59512	0.582258
100	5.18738	4.60517	0.582207

Figure 3: Table of values of n, H_n, $\ln(n)$, and γ

decrease is also decreasing. Certainly it looks like it has a limiting value but the rate of convergence is quite slow.

Prove that as n approaches infinity,

$$H_{kn} - H_n = \ln(k)$$

for any positive integer k. Hence derive the following beautiful formulas for natural logarithms.

i.
$$\ln 2 = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \cdots.$$

ii.
$$\ln 3 = 1 + \frac{1}{2} - \frac{2}{3} + \frac{1}{4} + \frac{1}{5} - \frac{2}{6} + \frac{1}{7} + \frac{1}{8} - \frac{2}{9} + \cdots$$

iii.
$$\ln 4 = 1 + \frac{1}{2} + \frac{1}{3} - \frac{3}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} - \frac{3}{8} + \cdots$$

Now try explaining why

$$\ln n = \sum_{k=1}^{\infty} (1-n)^{1-\lceil k/n - \lfloor k/n \rfloor \rceil} \frac{1}{k}.$$

(Note that $\lfloor x \rfloor$ means the greatest integer less than or equal to x and $\lceil x \rceil$ means the smallest integer greater than or equal to x.)

(d) The preceding infinite series don't really give us a way to figure out what γ is. To do that, we need some heavier mathematical machinery, and they don't come much heavier than the Riemann Zeta Function, which is defined by

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}.$$

This sum is quite close to the harmonic series; we get it by plugging in $s = 1$. Interestingly, the zeta function converges for all $s > 1$, which might explain why H_n diverges so slowly.

For convenience, we define harmonic numbers *of order r* by

$$H_n^{(r)} = \sum_{k=1}^{n} \frac{1}{k^r}.$$

This means $H_\infty^{(r)} = \zeta(r)$.

We would like to somehow use the zeta function to calculate γ. How do we do this? We know γ is connected with the natural logarithm, so it makes sense to try to express a natural logarithm as an infinite series somewhat resembling the zeta function.

Luckily, there is one such infinite series:

$$\ln(1+x) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{x^k}{k} = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots.$$

If such an infinite series looks too good to be true, derive it for yourself by letting $\ln(1+x)$ be an infinite polynomial and determining the coefficients by comparing the higher-order derivatives of both sides at $x = 0$.

(e) We see that the series has some resemblance to the zeta function, the biggest difference being that the powers are in the numerator. By introducing an appropriate substitution, show that

$$\ln\left(\frac{t}{t-1}\right) = \sum_{k=1}^{\infty} \frac{1}{kt^k} = \frac{1}{t} + \frac{1}{2t^2} + \frac{1}{3t^3} + \cdots. \tag{2}$$

The infinite series for $\ln(1+x)$ makes sense only when $|x| \leq 1$ and $x \neq -1$. Use this to prove that Equation (2) is defined when $t > 1$.

(f) Use Equation (2) to show that

$$\ln(n) = (H_n - 1) + \frac{1}{2}(H_n^{(2)} - 1) + \frac{1}{3}(H_n^{(3)} - 1) + \cdots. \tag{3}$$

(g) Rearranging Equation (3), we get

$$H_n - \ln(n) = 1 - \frac{1}{2}(H_n^{(2)} - 1) - \frac{1}{3}(H_n^{(3)} - 1) - \cdots.$$

This is the difference γ that we are looking for.

As n approaches infinity, $H_n^{(r)}$ becomes $\zeta(r)$, so we can evaluate the limiting value of $H_n - \ln(n)$:

$$\gamma = \lim_{n\to\infty}(H_n - \ln(n)) = 1 - \frac{1}{2}(\zeta(2)-1) - \frac{1}{3}(\zeta(3)-1) - \cdots.$$

Using something like Mathematica or Python, calculate the limiting value of γ. We have just discovered *Euler's constant* (sometimes also called the Euler-Mascheroni constant). This number is very mysterious but appears in many areas of mathematics, much like the mathematical constants π and e. Unlike π and e, however, we are not sure if γ is algebraic or transcendental (whether it is the root of a polynomial with integer coefficients), or whether it is even irrational!

(h) As a bonus, here's another cool thing. Since we know that

$$H_n \approx \ln(n) + \gamma$$

we can approximate the harmonic numbers extremely well without actually adding up all the terms in the series. For example, using Mathematica I get

$$H_{1000} \approx 7.48547$$

and

$$\ln(1000) + \gamma \approx 7.48497.$$

Try this for larger values of n to see how closely the natural logarithm and γ approximate H_n.

3. In this problem we shall consider the theory of partitions, which Euler made several contributions to. This theory is so rich and interesting that we only scratch the surface and consider only one of the many amazing results.

A *partition* of a number n is a representation of it as the sum of any number of positive integers. For example, the following are all the partitions of 5.

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1+1 = 1+1+1+1+1$$

Think of partitions as the additive equivalent of factorisation. Unlike factorisation, however, there is no concept of a "prime", and partitions are certainly not unique, as is clearly shown in the above example. Note that partitions with the same numbers but different order are considered the same partition.

In terms of notation, we denote the number of partitions of a positive number n to be $p(n)$. Thus, for example, we have $p(5) = 7$.

(a) Few questions about partitions can be answered from a purely combinatorial perspective. Euler managed to find the following generating function[1] for $p(n)$:

$$F(x) = (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^3 + x^6 + \cdots)\cdots. \tag{4}$$

[1] A *generating function* is a polynomial in which the coefficients are the terms of the sequence we wish to investigate. Here a generating function for the partition function would be a polynomial in which the coefficient of the x^i term is $p(i)$.

Describe, informally, how the coefficient of x^n in the expansion of the infinite product above is $p(n)$. (If you're stuck, the partition $10 = 3 + 2 + 2 + 2 + 1$ is equivalent to the term in the expanded polynomial obtained by choosing the x^3 term in the third factor, the x^6 in the second factor, and the x term in the first factor. Likewise, the partition $5 = 1+1+1+1+1$ analogous to choosing the x^5 term from the first factor.)

(b) Find $p(n)$ for $n = 1, 2, 3, 4, 5, 6$. What seems to be the pattern? Evaluate $p(7)$ to see whether it continues.

(c) Show that

$$F(x) = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots}.$$

(d) Now we begin investigating the theorem behind this problem. Let $p_d(n)$ be the number of partitions of n that use distinct integers (that is, no number is used more than once in the partition). Find $p_d(7)$.

(e) Let $p_o(n)$ be the number of partitions of n that use only odd numbers (the same number is allowed to be used multiple times in this case). Find $p_o(7)$.

(f) Use Equation (4) to explain why the generating function for $p_d(n)$ is

$$F_d(x) = (1+x)(1+x^2)(1+x^3)\cdots.$$

(g) Use Equation (4) to explain why generating function for $p_o(n)$ is

$$F_o(x) = \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots}.$$

(h) Finally, complete Euler's marvellous proof that $p_d(n) = p_o(n)$; that is, *the number of partitions of a number into distinct numbers is equal to the number of partitions of that number into odd numbers.*

Melbourne High School
Maths Extension Group 2023
Term 2 Week 5 Handout

> *Given a diagram, insert all the angles you can. Label one angle α or some other symbol, and then work out what you can in terms of α. Continuing this process disposes of many a geometry problem.*
>
> —A. Di Pasquale, N. Do, D. Mathews, *Problem Solving Tactics* (2014)

Angle chasing problems

1. Quadrilateral $WXYZ$ is a quadrilateral with perpendicular diagonals. If $\angle WZX = 30^\circ$, $\angle XWY = 40^\circ$, and $\angle WYZ = 50^\circ$, find $\angle WZY$.

2. Two parallel lines are tangent to a circle with centre O. A third line, also tangent to the circle, meets the two parallel lines at A and B. Prove that AO is perpendicular to OB

3. Let $O = (0, 0)$, $A = (0, a)$, and $B = (0, b)$, where $0 < a < b$ are reals. Let τ be a circle with diameter AB and let P be any other point on τ. Line A meets the x-axis again at Q. Prove that $\angle BQP = \angle BOP$. BAMO 1999/2

4. Let $ABCD$ be a convex quadrilateral. Suppose there is a point P on the segment AB with $\angle APD = \angle BPC = 45^\circ$. If Q is the intersection of the line AB with the perpendicular bisector of CD, prove that $CQD = 90^\circ$. AMO 2008

5. We are given an acute triangle ABC. Let D be the point on its circumcircle such that AD is a diameter. Suppose that points K and L lie on segments AB and AC, respectively, and that DK and DL are tangent to circle AKL. Show that line KL passes through the orthocentre of triangle ABC. EGMO 2023/2

If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers.

—Euclid[1], *Elements Book VII* (c. 300 BC)

The Fundamental Theorem of Arithmetic

Prime numbers are to the natural numbers what atoms are to matter. They are the fundamental, indivisible building blocks of the universe we call number theory. As such, we might expect there is some grand theorem that explains the importance of primes in higher arithmetic, and in fact there is; this theorem is the Fundamental Theorem of Arithmetic.

Let's begin by considering the number 12. Clearly 12 is composite, because it is divisible by 2. So we write $12 = 2 \times 6$. Turning our attention to 6, we realise it too is composite because it is 2×3. The numbers 2 and 3 being prime, we cannot factorise further, leaving us with $12 = 2 \times 2 \times 3$.. This is called the prime factorisation of 12. What the Fundamental Theorem of Arithmetic asserts is that there is no other way to write 12 as a product of primes other than what we have written down. That is, it is impossible to write down a prime factorisation of 12 without using 2 exactly twice and 3 exactly once and using no other primes. Of course, 12 was just an example; we could've picked any positive integer. But no matter which number we might have picked, the Fundamental Theorem of Arithmetic guarantees that any prime factorisation we work out is unique.

Just to be clear, by 'unique' we mean unique up to reordering of the factors. So we may write $12 = 2 \times 2 \times 3$ or $12 = 2 \times 3 \times 2$, but we have still used 2 twice and 3 once. Also note how this theorem precludes 1 from being a prime, because inserting any number of 1s doesn't change the value of the product.

Mathematicians considered unique factorisation an obvious property of the integers for thousands of years. To illustrate how special this property of the natural numbers is, consider numbers of the form $4k+1$. These are the numbers beginning

$$1, 5, 9, 13, 17, 21, \ldots .$$

A "prime" in this system is a number that cannot be factorised without going outside of the set of numbers. The first non-prime in this system of numbers is $25 = 5 \times 5$. Just like with the positive integers, each number is either a prime or able to factorised as a product of primes, but this factorisation is not always unique. For example, $693 = 9 \times 77 = 21 \times 33$, and 77, 9, 21, and 13 are all primes in this number system.

Before we examine *unique* factorisation, we first need to verify that every number is actually a product of primes. Fortunately this is easy and follows at once by the definition of prime and composite numbers. The method is by strong induction; try it for yourself.

Note that there is something fishy about 1. This is why we define the empty product to be equal to 1, so that 1 is still a product of primes—it is the product of zero primes.

The real crux of the problem is showing that a prime factorisation is necessarily unique. The most common proof uses Euclid's Lemma, the proof of which we left as an exercise on a previous handout. Here is the proof for completeness.

Euclid's Lemma asserts that if a prime p divides a product ab, then p must divide at least one of a and b. To begin the proof, we assume that p does not divide a, because if it does then we have nothing to prove. Now the aim is to show that p divides b.

If p does not divide a, then $\gcd(p, a)$ must be equal to 1. This follows immediately from p having only itself and 1 as factors by definition. Since $\gcd(p, a) = 1$, there exist positive integers x and y such that

$$px - ay = 1.$$

(The proof of this was given in the same previous handout on the Euclidean algorithm.)

[1]Translated by T. L. Heath in *The thirteen books of the Elements* (1956).

Multiplying both sides by b, we obtain

$$pbx - aby = b.$$

By hypothesis, p divides ab, so p divides aby. Certainly p divides pbx, so p divides both pbx and aby. Hence p also divides their difference $pbx - aby$, which is b. This completes the proof of the lemma.

We are now able to prove prime factorisation by contradiction. Assume that there exists some positive integer n that has two distinct factorisations: let

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where all of $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are primes. Further suppose that this is the smallest number with the property. We can assume this because every subset of the natural numbers has a least element; hence the set of all natural numbers with at least two different prime factorisations also has a least element.

The property of every subset having a least element is called the *well-ordering property* of the natural numbers. It is certainly not true for real numbers. Is there a least element of the set of real numbers in the interval $(0, 1)$?

From our definition of n, we observe that p_1 divides $n = q_1 q_2 \cdots q_s$. By Euclid's lemma p_1 divides either q_1 or $q_2 q_3 \cdots q_s$. If p_1 doesn't divide q_1 then it divides $q_2 q_3 \cdots q_s$. But by reapplication of Euclid's lemma p_1 divides either q_2 or $q_3 q_4 \cdots q_s$. Eventually we find that p_1 divides at least one of the prime factors q_i for some $1 \leq i \leq s$. Assume without loss of generality that this prime is q_1.

Since p_1 and q_1 are both primes, if p_1 divides q_1, then p_1 must equal q_1. This means we can cancel out p_1 and q_1 from both sides of the equation, which yields a smaller number that can be expressed as a product of primes in two different ways. This contradicts our assumption that n is the smallest number with that property, completing the proof.

This proof, although apparently short, is not the most direct method because it relies on the development of the Euclidean algorithm and the properties of numbers and their greatest common divisors. Gauss offered a shorter proof using modular arithmetic, and there is an even more direct proof that does not require any preliminary lemmas. Both are left as exercises.

The property of prime factorisation seems neat, but why is it useful? There are many reasons why the theorem deserves its grand name; the main one is that it allows us to develop theorems about all the natural numbers by first focusing on the primes. If we can answer some question about the primes, it is likely we can answer the same question about all positive integers. Consider the following example.

We define a function $\sigma(n)$ to be the sum of the divisors of n. For example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$. Suppose our goal is to find a formula for $\sigma(n)$. By computing the first twenty or so values, we observe that the formula is unlikely to be a nice algebraic function, since $\sigma(n)$ doesn't seem to be increasing, decreasing, or exhibiting any sort of behaviour we might expect from a polynomial or exponential function. The way to get started is by looking first at the case when n is prime.

I chose 6 because it's an example of a *perfect number*, which is a number that is equal to the sum of its divisors except itself. This means a number n is perfect if $\sigma(n) = 2n$.

What is $\sigma(p)$ for any prime p? This is easy because the only divisors of p are itself and 1, so $\sigma(p) = p + 1$. The next step up is to consider powers of p. What is $\sigma(p^k)$ for any nonnegative integer k? Here is our first use of the fundamental theorem. Since the factorisation p^k is unique, no other prime can divide it. Hence the only divisors are the powers of p, namely $1, p, p^2, \ldots, p^k$. Summing these together yields

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k.$$

This sum is just a geometric series with first term 1 and common ratio p; therefore it has the following nice formula:

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

We have succeeded in the first part of our plan. Having found a formula for $\sigma(p^k)$ we can find a general formula for $\sigma(n)$. This is left as an exercise.

This idea of first examining a problem for primes and then generalising to all natural numbers is a common theme in number theory. Another example is the classical problem about which numbers are the sum of two squares, which we shall examine in the future. Fermat conjectured, and Euler proved, that every prime of the form $4k+1$ is the sum of two squares. Using this result and a multiplicative property of such numbers, Euler was able to determine a general criterion for which numbers can be expressed as the sum of two squares.

Problems

1. In this problem we complete our investigation of the function $\sigma(n)$.

   More accurate would be to 'extend' our investigation. There are still many interesting things to do with this function and, more specifically, perfect numbers. For example, no odd perfect numbers have ever been found, but a proof of this still eludes mathematicians. Have a go at proving some less general statements. For example, can a number of the form $p^a q^b$, where p and q are odd primes, be perfect?

   (a) The divisors of 5 are 1 and 5, and the divisors of 4 are 1, 2, and 4. Note that the divisors of their product, 20, are 1, 2, 4, 5, 10, and 20. By considering further examples if necessary, show that if m and n are coprime then

   $$\sigma(mn) = \sigma(m)\sigma(n).$$

   (b) By the Fundamental Theorem of Arithmetic, every positive integer can be written as

   $$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$$

   where all of $p_1, p_2, \ldots, p_r$ are distinct primes. Find a general formula for $\sigma(n)$.

2. (a) From our present view, knowing the Fundamental Theorem, it is obvious that if two numbers are both less than a prime p, then their product is not divisible by p, because p cannot possibly occur in the factorisation of either of the two numbers. Prove this without relying on unique factorisation.

   The following proof was given in Gauss' magnum opus, *Disquisitiones Arithmeticae* (1801).

   (b) Hence show that if $a \not\equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p}$ then $ab \not\equiv 0 \pmod{p}$.

   This is equivalent to Euclid's lemma (it's the contrapositive). Therefore by completing this question you have also proved the Fundamental Theorem of Arithmetic in a different way.

3. (a) Suppose that a number n has two different prime factorisations and it is the smallest number with the property. This means all of $1, 2, \ldots, n-1$ can be uniquely factorised. Let

   $$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

   where all of $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are primes. Note that none of the p's equal any of the q's, because otherwise they could be cancelled to yield a smaller number with two different factorisation, which contradicts our definition of n.

   Show that there exist numbers i and j such that $n - p_i q_j > 0$.

   (b) Let $N = n - p_i q_j$. Clearly, N is less than n, and so can be factorised in only one way by hypothesis. Show that the product $p_i q_j$ must divide n.

   (c) Hence complete the proof of the Fundamental Theorem of Arithmetic.

   This proof is direct and requires no other results. Which do you prefer?

Melbourne High School
Maths Extension Group 2023
Term 2 Week 6 Handout

I love geometry.

—Anonymous, unpublished correspondence (2023)

More interesting geometry problems

1. What is the measure of an angle, in degrees, if its supplement is six times its complement?

2. The point O is the center of the circle circumscribed about $\triangle ABC$, with $\angle BOC = 120^\circ$ and $\angle AOB = 140^\circ$. What is the degree measure of $\angle ABC$?

3. Prove that if $\angle ACB$ is inscribed in a circle, then it subtends an arc with measure $2\angle ACB$. — Inscribed angle theorem

4. Points E and F are on side $\overline{BC}$ of convex quadrilateral $ABCD$ (with E closer to B). It is known that $\angle BAE = \angle CDF$ and $\angle EAF = \angle FDE$. Prove that $\angle FAC = \angle EDB$ — Russia 1996

5. Points A, B, C, D, E lie on a circle ω and point P lies outside the circle. The given points are such that (i) lines PB and PD are tangent to ω, (ii) P, A, C are collinear, and (iii) $\overline{DE} \parallel \overline{AC}$. Prove that $\overline{BE}$ bisects $\overline{AC}$. — USAJMO 2011/5

Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

—P. de Fermat, letter to F. de Bessy (October 18, 1640)

Fermat's Little Theorem

Do not confuse Fermat's Little Theorem with his *last theorem*. While Fermat's Little Theorem is fairly easy to prove and was first proved hundreds of years ago, Fermat's Last Theorem was an unsolved mystery for centuries.

Modular arithmetic is an incredibly powerful tool in part because it allows us to reduce an infinite set of numbers (the integers) into a finite set with comparatively few elements, and yet (most of) the usual laws of arithmetic hold. It is unlikely we would be able to calculate the value of 2^{100} in a normal equation, but what about that expression in a congruence modulo 101? The answer is that we can easily evaluate it; in fact, 2^{100} is congruent to a very nice number modulo 101. For this marvel we have Fermat's Little Theorem to thank.

We being by examining only prime moduli, as is customary in number theory. Take any prime p and any integer a not divisible by p and consider the powers of a

$$a^0, a^1, a^2, a^3, ...$$

modulo p. Our first observation is that eventually the numbers must repeat because there are only p possible residues. Since the sequence starts with $a^0 \equiv 1$, we know for sure that 1 will appear again; that is, there exists some $l > 0$ such that

$$a^l \equiv 1 \pmod{p}.$$

For example, consider the powers of 3 modulo 7 shown in Figure 1. It

n	1	2	3	4	5	6
3^n	3	9	27	81	243	729
$3^n \pmod 7$	3	2	6	4	5	1

Figure 1: The powers of 3 modulo 7

is plain that the first power of 3 that is congruent to 1 modulo 7 is 3^6. Having reached 1, the powers of 3 will then cycle, since

$$3^7 = 3^6 \times 3 \equiv 1 \times 3 \equiv 3 \pmod{7}.$$

So if we continue finding the powers of 3 modulo 7 we get $3^7 \equiv 3$, $3^8 \equiv 2$, $3^9 \equiv 6$, and so on. More generally, if $a^l \equiv 1 \pmod{p}$, then $a^{l+k} \equiv a^k$ for any positive integer k.

We define the smallest integer $l > 0$ such that $a^l \equiv 1 \pmod{p}$ to be the *order of a to the modulus p*. In the above example, the order of 3 to the modulus 7 is 6, because 6 is the smallest positive integer satisfying $3^n \equiv 1 \pmod{7}$. If we replace the modulus by 11, we find that the order of 3 to this new modulus is 5.

If you have time, list powers of numbers to various prime moduli and try to spot some patterns.

Combining our observation that the powers of a number modulo a prime number are periodic and the definition of the order of a number, we find that if $a^n \equiv 1 \pmod{p}$ then n must be a multiple of the order of a. Conversely, if n is a multiple of the order of a then $a^n \equiv 1 \pmod{p}$. The former proposition follows immediately from the cyclic nature of the powers of a. If we let l be the order of a, then the powers of a modulo p repeat every l terms, so $a^n \equiv 1$ only if n can be obtained from l by adding a multiple of l. Consequently n must be a multiple of l.

This latter statement is also easy to prove. If again l is the order of a and $n = lk$ for some integer k, then $a^{lk} = (a^l)^k$. By definition $a^l \equiv 1 \pmod{p}$ so a^{lk} is congruent to 1^k, which is just 1.

Fermat's Little Theorem (yes, we are finally getting to it) states that for any prime p and an integer a coprime with p, the order of a is a divisor of $p-1$. Equivalently, we may state the theorem as the congruence

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Sometimes the theorem is expressed as

$$a^p \equiv a \pmod{p}. \tag{2}$$

This equation holds for any a, not just those coprime with p. We can obtain Equation (1) just by dividing both sides of Equation (2) by a—but recall that this is only allowed if a is coprime with p, and hence we derive the condition on a for the first formulation of the theorem.

There are several proofs of Fermat's Little Theorem. The proof we present here was discovered by British Mathematician James Ivory in 1806. Interestingly, there are a range of combinatorial proofs, which suggest there is a deeper connection with combinatorics that might be apparent at first glance.

If you're interested, look up 'Fermat's Little Theorem necklace proof.'

We shall prove the formulation of the theorem as described in Equation (1). Remember that in this case a is coprime with p.

To begin the proof, we consider the numbers

$$1a, 2a, 3a, \ldots, (p-1)a.$$

None of these numbers are divisible by p, so each is congruent to one of the numbers

$$1, 2, 3, \ldots, p-1$$

modulo p. In fact, each of the numbers in the first list is congruent to a different number in the second list. Why is this the case? Take two numbers in the first list, say ja and ka for $1 \leq j, k \leq p-1$. If $ja \equiv ka$ then by the cancellation law $j \equiv k$, and since both j and k are less than p, the two must be equal. Note that this is where we use the assumption that a is coprime with p, for otherwise the cancellation of a from both sides is invalid.

Hence we have shown that each of the numbers in the first list is congruent to exactly one number in the second, because if any two numbers in the first list are congruent then they are actually the same number. As a result the product of the two sets must be congruent to each other. That is, we have

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \pmod{p}.$$

On both sides we discover a $(p-1)!$ term and on the LHS we have $p-1$ copies of a, so the congruence becomes

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

We observe that $(p-1)!$ consists only of factors less than p and is therefore not divisible by p, by the Fundamental Theorem of Arithmetic. Therefore, on cancelling $(p-1)!$ from both sides, we obtain

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's Little Theorem holds an interesting place in the theory of primality testing, the area of mathematics dedicated to finding ways of telling whether a number is prime or not. Rather frustratingly, the converse of Fermat's Little Theorem is not true. If $a^{p-1} \equiv 1 \pmod{p}$,

It's very easy to multiply large prime numbers together, but given a large number it is *very difficult* to determine if it is prime. This simple idea is the basis of many ideas in cryptography.

then p need not be prime. In fact, there are numbers that look very much like they are primes based on Fermat's Little Theorem, but are in fact composite; these are called *Carmichael numbers*. A Carmichael number is a composite number n that satisfies

$$a^n \equiv a \pmod{n}$$

for all integers a. Thus from the perspective of Fermat's Little Theorem Carmichael numbers look very much like they are prime, but they are actually composite. The smallest Carmichael number is 561.

Carmichael numbers are named after Robert Carmichael, an American mathematician who was an early pioneer in this area of primality testing.

Problems

1. Prove that Equation (2) holds for all positive integers a by induction.

2. Let $\phi(m)$ denote the number of numbers less than m that are coprime with m, and let the numbers

   $$k_1, k_2, \ldots, k_{\phi(m)}$$

   be those numbers. Using a method similar to Ivory's proof of Fermat's Little Theorem, show that if a is coprime with m, then

   $$a^{\phi(m)} \equiv 1 \pmod{m}.$$

This function $\phi(m)$ is called *Euler's Totient Function*.

Can you see how this is a generalisation of Fermat's Little Theorem?

Melbourne High School
Maths Extension Group 2023
Term 2 Week 7 Handout

> *Angling may be said to be so like the mathematics that it can never be fully learnt.*
>
> —Izaak Walton, *The Complete Angler* (1653)

The Art of Angling

1. In $\triangle ABC$, $AB = AC$ and $\angle A = 40^\circ$. The bisector from $\angle B$ intersects AC at point D. What is $\angle BDC$?

2. Let $ABCD$ be a square with side length 24. Let P be a point on side AB with $AP = 8$, and let AC and DP intersect at Q. Determine the area of triangle CQD — AIMO 2019/3

3. Let ABC be a triangle and D be a point on $\overline{BC}$ so that $\overline{AD}$ is the internal angle bisector of $\angle BAC$. Show that — Angle Bisector theorem

$$\frac{AB}{AC} = \frac{DB}{DC}.$$

4. In $\triangle ABC$ let I be the center of the inscribed circle, and let the bisector of $\angle ACB$ intersect AB at L. The line through C and L intersects the circumscribed circle of $\triangle ABC$ at the two points C and D. If $LI = 2$ and $LD = 3$, then find IC. — AIME 2016/6

5. Let ABC be an acute triangle inscribed in circle Ω. Let X be the midpoint of the arc $\widehat{BC}$ not containing A and define Y, Z similarly. Show that the orthocenter of XYZ is the incenter I of ABC.

The great masters of modern analysis are Lagrange, Laplace, and Gauss…

—W. W. R. Ball, *A Short Account of the History of Mathematics* (1888)

Lagrange's Theorem

Linear congruences share many properties with linear equations; what about polynomials in general?

Consider the polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where all of $a_0, a_1, \ldots, a_n$ are integers. The Fundamental Theorem of Algebra asserts that f has exactly n complex roots (as long as the polynomial is not constant, of course). But if we consider the congruence

$$f(x) \equiv 0 \pmod{m}$$

for some modulus m, does the same theorem hold? That is, does f have n incongruent roots modulo m?

It is n complex roots counted with multiplicities, which means repeated roots are counted separately. For example, the polynomial $(x-1)^2$ has only one distinct root, but two roots counted with multiplicities.

Simple experimeintation precludes the idea. For example, it is easy to show that the congruence

$$x^4 - 2 \equiv 0 \pmod{16}$$

has no solution. Run x through a complete set of residues, say $0, 1, \ldots, 15$, and if there are any solutions this finite process would find it. In fact, the same brute-force method works for finding solutions to any polynomial congruence; and therein lies one of the beauties of modular arithmetic. A second example: by running x through the values $0, 1, \ldots, 7$ we find that the congruence

$$x^2 - 1 \equiv 0 \pmod{8}$$

has four solutions, namely $x \equiv 1, 3, 5, 7$. In this case the number of solutions is greater than the degree of the congruence, but in the first example the number of solutions is less than the degree of the congruence. Clearly something different is at play here.

Mathematicians are not easily discouraged, and we are no exception. Instead of considering all moduli, consider congruences to prime moduli only; we hope that this heuristic, a familiar one in number theory, leads to progress. And indeed it does—after similar experimentations to the ones we did above, we notice that sometimes the number of roots is less than the degree of the congruence, sometimes it is equal to the degree, but it is never greater than the degree. This apparently weaker analogue of the Fundamental Theorem of Algebra is known as *Lagrange's Theorem*.

Guess who was the first to prove the Fundamental Theorem of Algebra?

More concretely, Lagrange's Theorem states that the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most $\deg f$ incongruent solutions. From here on, we make one further restriction on the coefficients of f; we have already stated they must be integers, but when considering f to a prime modulus, the leading coefficient must not be a multiple of p, or else it would vanish. Such an inconvenience does not exist in normal polynomial equations.

Our proof consists of two parts; first we show that if f has a root, then f can be factorised into a linear factor and a polynomial of degree

$\deg f - 1$. The second part is to show that repeating this process leads us to either exactly $\deg f$ or fewer roots; in either case the number roots does not exceed the degree. To ease the notation, let $d = \deg f$.

We begin by assuming that f has a root, for otherwise our proof is already complete; 0 is definitely less than or equal to d. Let this root be $x \equiv r$. Hence

$$f(r) \equiv 0 \pmod{p}$$

and so

$$f(x) \equiv f(x) - f(r) \pmod{p}.$$

Expanding the RHS, we have

$$f(x) - f(r) = \sum_{k=0}^{d} a_k x^k - \sum_{k=0}^{d} a_k r^k.$$

These summation signs look scary, but they really aren't. They are just a compact way of expressing the general form of polynomials, which is written in expanded form on the previous page.

The only difference between $f(x)$ and $f(r)$ is that x is replaced by r; the coefficients remain the same. Therefore we can group the terms with the same power together and factorise out the coefficients, leaving us with

$$f(x) - f(r) = \sum_{k=0}^{d} a_k (x^k - r^k).$$

More explicity, we can write the expression as

$$f(x) - f(r) = a_d(x^d - r^d) + a_{d-1}(x^{d-1} - r^{d-1}) + \cdots + a_1(x - r). \quad (1)$$

(The constant terms simply vanish.) From here, we note that $(x - r)$ is a factor of the polynomial $x^k - r^k$ for $k > 0$. So we pull out a factor of $(x - r)$ from each of the terms in the above expansion of $f(x) - f(r)$ to obtain

$$f(x) - f(r) = (x - r)(b_{d-1}x^{d-1} + b_{d-2}x^{d-2} + \cdots + b_1 x + b_0)$$

where all of $b_0, b_1, \ldots, b_{d-1}$ are integers that depend on $a_0, a_1, \ldots, a_d$. It doesn't matter what the coefficients of the factored polynomial actually are; the only thing that matters is that it must have degree of $d - 1$, because when we pulled out a factor of $(x - r)$ from each of the terms of Equation (1) the highest power of x that remained was x^{d-1}.

Therefore, we have shown that

$$f(x) - f(r) = (x - r)g(x),$$

where g is a polynomial of degree $d - 1$. But recall that $f(x) \equiv f(x) - f(r)$, and so we actually have

$$f(x) \equiv (x - r)g(x) \pmod{p}.$$

The first part of our plan is complete. Now the game is just to repeat the process, because any root of g is also a root of f. If $g(x)$ has no roots modulo p, we are done; otherwise we apply exactly the same reasoning to factor $g(x)$ as a product of a linear factor and another polynomial with degree of $\deg g - 1$. The degree of the original polynomial f is d, and so we can play the game a maximum of d times. If we encounter a polynomial that has no roots before we completely factorise f as a product of linear factors, then f itself has fewer than d roots. If f can be factorised all the way, it has exactly d roots. In either case the number of roots cannot exceed d. This completes the proof of Lagrange's Theorem.

A more succint way of saying it is that each time we find a root of f modulo p, we can pull out another linear factor. But we can only pull out a linear factor a maximum of d times; hence there cannot be more than d roots modulo p.

The discerning reader notices a glaring hole in our proof: we have not used the assumption that p is prime! In fact, we have, but in a subtle way that is easy to overlook. Exactly where we have implicitly relied on the primality of p is left as the object of the first exercise.

Problems

1. In the above proof, where did we use the assumption that p is prime?

2. Prove Lagrange's Theorem by contradiction. Assume that a polynomial f with degree d has $d+1$ roots

   $$r_1, r_2, \ldots, r_{d+1}$$

   modulo some prime p. Further assume that this is the polynomial with smallest degree with this property. Show that this leads to a contradiction.

   Hint: use the same method as the proof shown above.

3. In this problem consider the congruence

   $$x^d - 1 \equiv 0 \pmod{p}$$

   where d is a factor of $p-1$.

   (a) Let $p - 1 = dd'$ and $y = x^d$. Show that

   $$x^{p-1} - 1 \equiv (y-1)(y^{d'-1} + y^{d'-2} + \cdots + 1) \pmod{p}.$$

   (b) What is the degree of the polynomial

   $$y^{d'-1} + y^{d'-2} + \cdots + 1$$

   in terms of p and d?

   (c) Fermat's Little Theorem tells us that the congruence

   $$x^{p-1} - 1 \equiv 0 \pmod{p}$$

   has exactly $p-1$ solutions, as any value of x except 0 is a solution. Use this to show that the congruence

   $$x^d - 1 \equiv 0 \pmod{p}$$

   has exactly d solutions.

   Don't forget to use Lagrange's Theorem too!

Melbourne High School
Maths Extension Group 2023
Term 2 Holiday Handout

If all the year were playing holidays,
To sport would be as tedious as to work.

—W. Shakespeare, *King Henry IV, Part 1* (1596)

Term 2 Holiday Problems

1. Our friend Harold is back and is now reading Franz Kafka's *The Trial*, which has 167 pages. Taking the title literally, he decides to read it in a new way. First he picks a random number between 1 and 166 inclusive, say x. To find the nth page that he reads, where $n = 1, 2, ...$, he multiplies x by n^2, and, if the resulting page number is greater than 167, subtracts off a multiple of 167 to get a page that is actually in the book. He continues reading until he hits a page that he has already read before.

   For what values of x will Harold be able to read the entire book this way? If there are no such values of x, how many pages will he read before he stops? Note that 167 is a prime number.

   It turns out that 167 is the smallest prime that is not the sum of 7 or fewer cubes.

   Reading below on primitive roots won't hurt in solving this problem, although it is not necessary.

2. Find all integer solutions to the equation

   $$y^k = x^2 + x$$

   where k is a natural number greater than 1.

   Tournament of Towns Junior 1981/1

3. Write $\left(1 + \frac{1}{3}\right)\left(1 + \frac{1}{3^2}\right)\left(1 + \frac{1}{3^{2^2}}\right) ... \left(1 + \frac{1}{3^{2^{100}}}\right)$ in the form $a(1 - b^c)$, where a, b and c are constants.

4. Find the number of ways to colour each square of a 2007×2007 square grid black or white such that each row and each column has an even number of black squares.

5. Let ABC be an acute triangle. Let BE and CF be altitudes of $\triangle ABC$, and denote by M the midpoint of BC. Prove that ME, MF, and the line through A parallel to BC are all tangents to circle AEF.

6. If g is a primitive root modulo p, show that

   $$g^{(p-1)/2} \equiv -1 \pmod{p}.$$

   For this problem and the next, see below for a description of what primitive roots are.

7. Use primitive roots to prove Wilson's theorem for odd primes p:

   $$(p-1)! \equiv -1 \pmod{p}.$$

Primitive Roots

In exploring Fermat's Little Theorem, we have seen what the order of some number a to a prime modulus p is; it is the smallest number $l > 0$ such that

$$a^l \equiv 1 \pmod{p}.$$

Furthermore, we discovered that Fermat's Little Theorem is equivalent to saying that the order of a number not divisible by p is always a divisor of $p-1$. Now we shall look at particular numbers that have orders exactly equal to $p-1$; these are called *primitive roots*.

More explicitly, a primitive root of a prime p is a number g with the property that the smallest power of it that is equal to unity is $p-1$. This means that all of the numbers

$$g, g^2, g^3, \ldots, g^{p-1}$$

are all distinct and form the complete set of positive residues

$$1, 2, \ldots, p-1.$$

Before we examine why this is useful, we shall prove that every prime number has at least one primitive root.

Euler was the first to state this theorem, but his proof was incorrect; the first correct proof belongs to Legendre. The initial result we establish is the following: if two numbers a and b have order l and k respectively and l and k are coprime then the number ab has order lk. The proof of this preliminary result falls into two parts; first we prove that ab raised to the power of lk is indeed 1, and then that lk is the smallest number with this property. The first part is easy, for

Adrien-Marie Legendre (1752–1833) was a French mathematician who, besides making great contributions to number theory, has only one known portrait. Funnily enough, this portrait is a caricature.

$$(ab)^{lk} \equiv (a^l)^k (b^k)^l \equiv 1^k 1^l \equiv 1 \pmod{p}.$$

The second part is more difficult. Suppose that the order of ab is $l_1 k_1$ and let l_2 and k_2 be the numbers satisfying $l = l_1 l_2$ and $k = k_1 k_2$. Then by definition, we have

$$(ab)^{l_1 k_1} \equiv 1 \equiv a^{l_1 k_1} b^{l_1 k_1} \pmod{p}.$$

Raising both sides of this congruence to l_2, the power of a vanishes because $l_1 l_2 = l$ and $a^l \equiv 1$; therefore it leaves

$$b^{l k_1} \equiv 1 \pmod{p}.$$

The order of b is k, so k divides lk_1. Since k and l are relatively prime, k must divide k_1. But k_1 also divides k, so the only way this is possible is if $k = k_1$. Similarly, if we had raised both sides of the above congruence to k_2, we would find that l must divide l_1. Again, this implies that $l_1 = l$, and therefore the order of ab is $l_1 k_1 = lk$, as required.

The preceding simple result is the core of our proof that every prime has a primitive root. Next: factorise $p-1$ as a product of primes in *canonical form*, as follows.

$$p - 1 = q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}$$

where all of $q_1, q_2, \ldots, q_r$ are distinct primes and $a_1, a_2, \ldots, a_r$ are positive integers. From this it follows that all of $q_1^{a_1}, q_2^{a_2}, \ldots, q_r^{a_r}$ are coprime. Hence if we can show that there exists some number that has order $q_i^{a_i}$, for $1 \leq i \leq r$, then by repeated application of the preceding result there must be a number that has order $p-1$, which is the primitive root we are looking for.

Luckily, we have a previous result from Lagrange's Theorem on our side. Let q^a be one of the prime powers that is in the prime factorisation of $p-1$. In the previous handout we showed that the congruence

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions. From this we deduce that there are exactly q^a solutions to the congruence

$$x^{q^a} \equiv 1 \pmod{p} \tag{1}$$

but only q^{a-1} to the congruence

$$x^{q^{a-1}} \equiv 1 \pmod{p}. \tag{2}$$

Let b be some number that satisfies Equation (1). Then the order of b divides q^a. If the order of b is not q^a exactly, it must be one of the proper divisors of q^a, namely one of the numbers

$$q, q^2, \ldots, q^{a-1}.$$

If the order of b is one of these numbers, then b also satisfies (2). Therefore b has order q^a if and only if it satisfies Equation (1) but not Equation (2). There are $q^a - q^{a-1}$ of such numbers, and hence there exists at least one number whose order is q^a. With this we conclude the proof that every prime number has a primitive root.

The result was actually left as an exercise on the last handout, so if you didn't do it you must take it for granted for now.

Why are primitive roots useful? One reason is that they provide a way to simplify multiplication modulo a prime number using a device known as the *discrete logarithm*. Firstly, if g is a primitive root of a prime p, then we have already seen that the numbers

$$g, g^2, g^3, \ldots, g^{p-1}$$

reduced modulo p are the numbers

$$1, 2, \ldots, p-1$$

in some order. For example, if $p = 5$ and $g = 2$, then the numbers $2, 2^2, 2^3, 2^4$ reduced modulo 5 are

$$2, 4, 3, 1,$$

which form a complete set of positive residues.

You may notice that this proof provides a way to actually a construct a primitive root using an algorithm. Try it!

In other words, for each number a between 1 and $p-1$, there exists some number α also between 1 and $p-1$ such that

$$g^\alpha \equiv a \pmod{p}.$$

This number α is called the *index* of a to the modulus p for the given primitive root g and may be denoted $I(a)$. This function $I(a)$ is called the discrete logarithm because of its analogous behaviour to the normal logarithm.

Try proving some properties of the discrete logarithm, such as $I(ab) \equiv I(a) + I(b)$.

One application of indices is in performing calculations with large numbers modulo p. Suppose that we wish to evaluate ab modulo p, and that α and β are the indices of a and b respectively. Then

$$ab \equiv g^\alpha g^\beta \equiv g^{\alpha+\beta} \pmod{p}.$$

In other words, to get the product ab, simply add the indices of a and b, and the number corresponding to the desired index is the product we are looking for. For course, $\alpha+\beta$ may be greater than $p-1$, but since the powers of a primitive root repeat every $p-1$ terms, reducing $\alpha+\beta$

modulo $p-1$ doesn't change which number the index corresponds to. As a result primitive roots and indices have changed a difficult problem of multiplying two large numbers into a simple matter of adding two indices and reducing modulo $p-1$.

The crucial question is: how do we know which number corresponds to a given index? The answer is that we can make a table of indices relatively easily. Given a primitive root g, we make a table of its powers modulo p, where each successive power is obtained just by multiplying the previous one by g and reducing modulo p. For example, given $g = 3$ and $p = 7$, the table would look like Figure 1. If necessary, we

n	1	2	3	4	5	6
$3^n \pmod p$	3	2	6	4	5	1

Figure 1: An example where 3 is a primitive root of 7

can just reverse the table to be able to look up the index of a particular number instead of looking up which number corresponds to a particular index. Of course the example above is simple, but it illustrates that when given much larger primes, it is comparatively easier to make a table of values and use indices in computations than doing large multiplications by brute-force. In fact, a table of indices is similar to how logarithm tables were used before there were calculators. Tables of indices have been compiled by number theorists in the past, including Jacobi's *Canon Arithmeticus*, which contained tables for primes up to 1000.

Carl Jacobi (1804–1851) was a German mathematician who made many great contributions to many fields of mathematics, including in the field of differential equations.

Primitive roots have other applications beyond being a simple 'trick' to perform calculations. They play a role in the elementary theory of higher-degree congruences; these higher-degree congruences include quadratic congruences, behind which lies one of the most beautiful theorems in all of number theory.

Melbourne High School
Maths Extension Group 2023
Term 3 Week 4 Handout

> *If we arrive at an equation containing on each side the same term but with different coefficients, we must take equals from equals until we get one term equal to another term. But, if there are on one or on both sides negative terms, the deficiencies must be added on both bides until all the terms on both sides are positive. Then we must take equals from equals until one term is left on each side.*
>
> —Diophantus,[1] *Arithmetica* (c. 250 AD)

Problems in factorisation and Diphantine equations

1. Find integers (x, y) such that $x^2 = 12 + y^2$.

2. Find all paris of integers (b, c) such that

$$2b + 3c = bc.$$

3. Determine all non negative integral pairs (x, y) for which INMO

$$(xy - 7)^2 = x^2 + y^2.$$

4. The integer n is positive. There are exactly 2005 ordered pairs (x, y) of positive integers satisfying BMO Round 3 2015

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}.$$

   Prove that n is a perfect square.

5. Determine all pairs (x, y) of integers such that IMO 2006/4

$$1 + 2^x + 2^{2x+1} = y^2.$$

[1] As quoted by Thomas Little Heath in *Diophantus of Alexandria* (1885)

The mathematician's patterns, like the painter's or the poet's, must be beautiful*; the ideas, like the colours or the words, must fit together in a harmonious way. Beuaty is the first test: there is no permanent place in the world for ugly mathematics.*

—G. H. Hardy, *A Mathematician's Apology* (1940)

Quadratic Residues

Be aware that we are now entering a most beautiful area of number theory; prepare yourself.

Having conquered linear congruences, let's turn to quadratic congruences. The central question in this area of number theory is:

When is the congruence $x^2 \equiv a \pmod{m}$ solvable?

Note that we are primarily interested in *when* the congruence has a solution, not what the solutions are (if there are any).

As should be familiar by now, we start by considering when m is prime. Therefore our main goal is to determine when

$$x^2 \equiv a \pmod{p}$$

is solvable. Let's begin with the congruence

$$x^2 \equiv 3 \pmod{7},$$

Is there a solution? Since the modulus is small it is easy to run through all the possibilities, like so:

$$\begin{aligned} 1^2 &\equiv 1 \pmod{7} \\ 2^2 &\equiv 4 \pmod{7} \\ 3^2 &\equiv 2 \pmod{7} \\ 4^2 &\equiv 2 \pmod{7} \\ 5^2 &\equiv 4 \pmod{7} \\ 6^2 &\equiv 1 \pmod{7} \end{aligned}$$

It looks like our equation is not solvable, as when numbers are squared modulo 7, the only possible residues are 1, 2, and 4. We note that $3^2 \equiv 4^2$, $2^2 \equiv 5^2$, $1^2 \equiv 6^2$, but after some thought this is hardly surprising, as $1 \equiv= 6$, $2 \equiv -5$, and $3 \equiv -4$ modulo 7.

Let's try another example, this time with the congruence

$$x^2 \equiv 10 \pmod{7}.$$

If we run through the possible values of x again, we find that the squares are congruent to $1, 4, 9, 5, 3$ only. Therefore our congruence is not solvable.

The numbers that are congruent to squares modulo a particular prime—$1, 2, 4$ in the case of modulo 7 and $1, 4, 9, 5, 3$ in the case of modulo 11—have a special name; they are called *quadratic residues*. Numbers that are not quadratic residues are called *quadratic nonresidues*. In other words if a is a quadratic residue modulo p, the congruence

$$x^2 \equiv a \pmod{p}$$

is solvable; if a is a quadratic nonresidue, then the congruence is not solvable. We always exclude 0 has a quadratic residue, not only because it is trivial, but also because it simplifies many of our arguments, as will be seen shortly. Additionally, in general we consider only odd

primes, leaving 2 for special cases because modulo 2 every number is a quadratic residue.

All the quadratic residues of a given prime can be found by running x through a set of positive residues, like we did above. As one further example, let's find the quadratic residues modulo 13: $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 3$, $5^2 \equiv 12$, and $6^2 \equiv 10$. As you might have realised already, we do not need to go further than 6, for the residues repeat. Therefore the quadratic residues modulo 13 are $1, 4, 9, 3, 12, 10$.

That is, $7^2 \equiv 10$, $8^2 \equiv 12$, and so on, as you can verify.

Let's turn to the general case. The first question, which you may have already answered, is: How many quadratic residues are there modulo an odd prime p? (Remember that we exclude 2 from all of these investigations.) From the examples above, it seems that the numbers

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

are all incongruent and therefore form quadratic residues, and all the numbers greater than $(p-1)/2$ and less than p form the same set of quadratic residues but in reverse order. A consequence of this is that there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues, which is consistent with the above examples.

How do we prove this hypothesis? An easy way is using primitive roots. If $a \equiv x^2$ is a quadratic residue and α is the index of x, then

Another way is to show that if a and b are both less than $p/2$, then $a^2 \not\equiv b^2$.

$$a \equiv g^{2\alpha} \pmod{p}.$$

The index of a is 2α reduced modulo $p-1$, and since $p-1$ is even, the index of a is even. Hence if a is a quadratic residue then its index is even. The contrapositive: if the index of a is odd, then a is a quadratic nonresidue. Combining these two statements, it follows that the quadratic residues modulo p are precisely those numbers with even indices, and the quadratic nonresidues are precisely those numbers with odd indices. Indices range from 1 to $p-1$, and as there are $(p-1)/2$ even numbers and $(p-1)/2$ odd numbers in that range, there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues.

You may verify this by constructing a table of indices for 11 using 2 as the primitive root; you will see that the indices of the quadratic residues 1, 4, 9, 5, and 3 are the even numbers 10, 2, 6, 4, and 8 respectively.

The connection between primitive roots and quadratic residues allows us to formulate a simple multiplicative property. Recall that multiplying numbers modulo p is equivalent to adding their indices and reducing that index modulo $p-1$ if necessary. If two quadratic residues are multiplied, the sum of their indices, which are both even, is also even, and so the product is another quadratic residue. If a quadratic residue is multiplied by a quadratic nonresidue, an even index and an odd index are added together; the resulting index is odd and so the product is a quadratic nonresidue. Finally, if two quadratic nonresidues are multiplied, the resulting index is even because the sum of two odd numbers is even. It follows that the product of two quadratic nonresidues is a quadratic residue.

These multiplicative rules bear a strange resemblance to the rules governing the multiplication of positive and negative numbers. Indeed, if we take a quadratic residue to be represented by the number 1 and a quadratic nonresidue to be represented by the number -1, the multiplicative properties hold, for

$$\begin{aligned} 1 \times 1 &= 1, \\ 1 \times -1 &= -1, \\ -1 \times -1 &= 1. \end{aligned}$$

These multiplicative properties led Legendre to come up with a convenient symbol, called the *Legendre symbol*, to represent whether a

certain number a is a quadratic residue modulo some prime p. It is defined as follows.

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

For ease of display, when the Legendre symbol is to be used inline, it will be denoted (a|p).

Problems

1. Is the congruence
$$x^2 \equiv -1 \pmod{17}$$
solvable?

2. Prove the following two properties of the Legendre symbol:
   (a) $(ab|p) = (a|p)(b|p)$.
   (b) If $a \equiv b \pmod{p}$ then $(a|p) = (b|p)$.

3. Wilson's Theorem states that
$$(p-1)! \equiv -1 \pmod{p}.$$
Use Wilson's Theorem and the results about quadratic residues developed above to find for which primes -1 is a quadratic residue and for which primes -1 is a quadratic nonresidue.

This result is a very famous one and forms the first supplement to the *Law of Quadratic Reciprocity*.

Melbourne High School
Maths Extension Group 2023
Term 3 Week 5 Handout

> *Greek algebra before Diophantus was essentially rhetorical.*
>
> —T. Dantzig, *Number: The Language of Science* (1954)

More factorisation and Diophantine equation problems

1. Show that for every integer $n > 1$ it is possible to write $\frac{1}{n}$ as a sum of two reciprocals of distinct positive integers.

2. Find $3x^2y^2$ if x and y are integers such that $y^2 + 3x^2y^2 = 30x^2 + 517$. AIME 1987/5

3. Find all integer solutions to the equation
$$(x-y)^2 = x + y.$$

4. Tyler has a large number of square tiles, all the same size. He has four times as many blue tiles as red tiles. He builds a large rectangle using all the tiles, with the red tiles forming a boundary 1 tile wide around the blue tiles. He then breaks up this rectangle and uses the tiles to make two smaller rectangles. Like the large rectangle, each of the smaller rectangles has four times as many blue tiles as red tiles, and the red tiles form a boundary 1 tile wide around the blue tiles. How many blue tiles does Tyler have? AMC Intermediate 2021/30

5. Factor $a^4 + 4b^4$. Sophie Germain's Identity

…knowledge of every truth is a worthy matter in itself…

—L. Euler[1], *Theorems on Divisors of Numbers* (1748)

Euler's Criterion

Refer to the previous handout for particulars.

Let's recap what has been covered so far in the story of quadratic residues. A quadratic residue modulo some odd prime p is a nonzero number a such that the congruence

$$x^2 \equiv a \pmod{p}$$

is solvable. A number that is not a quadratic residue is a quadratic nonresidue, or just nonresidue for short if there is no chance of ambiguity. Among the numbers $1, 2, \ldots, p-1$ there are the same number of quadratic residues as nonresidues; there are $(p-1)/2$ of each. A consequence of this fact is that quadratic residues and nonresidues satisfy the same multiplicative property as 1 and -1. That is, the product of a residue and a nonresidue is a nonresidue, and the product of two residues or two nonresidues is a residue. This can be summarised using the Legendre symbol:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

where

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

To continue our investigations, we look for a new goal. The most obvious one is to find a way to tell whether a given number is a quadratic residue of a prime. In other words, is there an easy way to evaluate $(a|p)$?

As a sneak peek for things to come, this problem can be broken down into three stages. First we need a way to evaluate $(-1|p)$, then $(2|p)$, and finally $(q|p)$ for any odd prime q. Since $(ab|p) = (a|p)(a|p)$ solving those three cases suffices to let us find $(a|p)$ for any a.

Of course, the brute force approach of enumerating the quadratic residues is guaranteed to give the right answer, but clearly the mathematician has no interest in this method. It is tedious, inelegant, and given the hints of beauty in the theory already developed, it is likely that there is a better way—some connection or theorem we have yet to discover.

Let's go back to Fermat's Little Theorem. It states that

$$a^{p-1} \equiv 1 \pmod{p}$$

for all $a \not\equiv 0$. Since p is an odd prime, $p-1$ is even, and therefore if we set $P = (p-1)/2$, the left-hand side can be factorised to give

$$(a^P - 1)(a^P + 1) \equiv 1 \pmod{p}.$$

Since the modulus is prime, either

$$a^P \equiv 1 \pmod{p}$$

or

$$a^P \equiv -1 \pmod{p}.$$

What is the distinction between these two cases? Clearly some numerical data would be useful. Suppose that $p = 7$. Let's run a through the values $1, \ldots, 6$ and compute a^P.

[1] Translated by David Zhao from Latin, in which the title was *Theoremata Circa Divisores Numerorum.*

a	1	2	3	4	5	6
$a^3 \pmod 7$	1	1	-1	1	-1	-1

One example may not be enough to establish the pattern, so here is another. This time $p = 11$.

a	1	2	3	4	5	6	7	8	9	10
$a^5 \pmod{11}$	1	-1	1	1	1	-1	-1	-1	1	-1

The first thing we notice about the two examples is that -1 and 1 appear the same number of times; there are $(p-1)/2$ of each. This alone is enough to suggest that there is some connection with quadratic residues. This connection is obvious if we look a little closer. Each 1 appears whenever a is a quadratic residue and each -1 appears whenever a is a quadratic nonresidue.

Verify this by finding the quadratic residues by hand. Then try a few more values of p to convince yourself that the pattern does indeed continue.

A few more examples would be enough to allow us to make a conjecture. We conjecture that $a^P \equiv 1$ if a is a quadratic residue and $a^P \equiv -1$ if a is a quadratic nonresidue. But 1 and -1 are exactly the possibilities of the Legendre symbol (excluding 0 because right from the beginning in using Fermat's Little Theorem we have taken $a \not\equiv 0$), so our conjecture can be expressed as

$$a^P \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$$

for $a \not\equiv 0$. In fact the conjecture is also true, albeit trivially so, when $a \equiv 0$.

The result we have just discovered is known as *Euler's Criterion*. At this point we have some intuition as to why it is true, but a proper proof is needed. Here is that proper proof.

If a is a quadratic residue, then

$$a \equiv x^2 \pmod p.$$

Hence

$$a^P \equiv a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$$

by Fermat's Little Theorem. The first part of the proof is complete.

Now consider the general congruence

$$x^{(p-1)/2} - 1 \equiv 0 \pmod p.$$

From Lagrange's Theorem there are at most $(p-1)/2$ solutions, and we have just shown that if a is a quadratic residue, then it is a solution to that equation. Since there are exactly $(p-1)/2$ quadratic residues, it follows that every quadratic residue is a solution to the above equation, and every solution to the above equation is a quadratic residue. The two statements are thus equivalent.

Recall that Lagrange's Theorem guarantees that a polynomial congruence of degree d modulo a prime has at most d incongruent roots.

For the second part of the proof, the case where a is a quadratic nonresidue, we have to go back to the equation

$$(a^P - 1)(a^P + 1) \equiv 0 \pmod p.$$

We know that either $a^P - 1 \equiv 0$ or $a^P + 1 \equiv 0$; but the former cannot be true because we have just proved that if that were the case, then a would be a quadratic residue. Thus the latter is true and

$$a^P \equiv a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p,$$

completing the proof of the theorem.

How does this help us evaluate the Legendre symbol? The answer is that it doesn't, at least not directly, because it is often inconvenient

to calculate $a^{(p-1)/2}$. The only value of a for which it gives us a direct solution to the problem is $a = -1$, for substituting this in gives

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Since both sides are equal to either -1 or 1, we may do away with the congruence and write it as an equation:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

(We don't have this liberty for other values of a.) From this equation it is clear that $(a|p)$ is equal to 1 or -1 depending on whether $(p-1)/2$ is even or odd, and $(p-1)/2$ is even if $p \equiv 1 \pmod 4$ and odd if $p \equiv 3 \pmod 4$. Thus -1 is a quadratic residue of all primes of the form $4k+1$ and a nonresidue of all those of the form $4k+3$.

This is the result proved in the last exercise to last week's handout; the difference is that there it was proved using primitive roots. Euler's Criterion gives an immediate proof.

Although Euler's Criterion gives us a direct way to evaluate $(-1|p)$ only, it will be needed to prove *Gauss's Lemma*. And Gauss's Lemma is central to this entire theory and is used to prove the ultimate, beautiful, golden theorem.

Problems

1. Show that if $p \equiv 1 \pmod 4$, then the quadratic character of a (whether it is a residue or nonresidue) is the same as that of $p-a$, and if $p \equiv 3 \pmod 4$, then the quadratic character of a is opposite that of $p-a$.

2. Prove Euler's Criterion using primitive roots and indices. (Hint: If g is a primitive root and $g^l \equiv 1$, then l must be a multiple of $p-1$.)

3. Use Wilson's Theorem to come up with a construction for the solutions to the equation

   $$x^2 + 1 \equiv 0 \pmod{p}$$

   when $p \equiv 1 \pmod 4$.

This is a hard problem.

Melbourne High School
Maths Extension Group 2023
Term 3 Week 6 Handout

```
out[8]=
```

$$\left\{\left\{x \to -\frac{2i\pi c_1 + \ln 2 - \ln 3}{\ln 2 + \ln 3} \text{ if } c_1 \in \mathbb{Z}\right\},\right.$$
$$\left.\left\{x \to -1 - \frac{2i\pi c_1}{-\ln 2 + \ln 3} \text{ if } c_1 \in \mathbb{Z}\right\}\right\}$$

—Mathematica (2023)

Problems in solving equations

1. Find all x such that $-4 < \frac{1}{x} < 3$.

2. Solve the following system of equations

$$xy = 12\sqrt{6}$$
$$yz = 54\sqrt{2}$$
$$zx = 48\sqrt{3}.$$

3. Find all real numbers x for which

$$\frac{8^x + 27^x}{12^x + 18^x} = \frac{7}{6}.$$

4. Mr Fat is going to pick three non-zero real numbers and Mr Taf is going to arrange the three numbers as coefficients of a quadratic equation USSR 1990

$$\_\_\_\_x^2 + \_\_\_\_x + \_\_\_\_ = 0$$

Mr Fat wins the game if and only if the resulting equation has two distinct rational solutions. Who has the winning strategy?

5. Find a triple of rational numbers (a, b, c) such that ARML 1997

$$\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{a} + \sqrt[3]{b} + \sqrt[3]{c}.$$

! Missing delimiter (. inserted).

—`lualatex` (2023)

Gauss's Lemma

We have seen that Euler's Criterion doesn't provide a good way to evaluate $(a|p)$ except when $a = -1$. When $a \neq -1$, how do we attack the problem?

The answer is that Euler's Criterion can be used to prove something called *Gauss's Lemma*, which, in theory although not in practice, would allow us to evaluate $(a|p)$ for any a. In other words, using Gauss's Lemma we can find all the primes for which $2, 3, 5, 7, 11, ...$ are quadratic residues.

The lemma and its proof are hard to motivate despite their simplicity. In fact, the proof is very similar to Ivory's proof of Fermat's Little Theorem. But how anyone could have come up with the lemma in the first place is somewhat mystifying.

The fact that Gauss was one of the greatest mathematicians of all time might have had something to do with it.

The lemma is as follows. Given a number a and an odd prime p, let $P = (p-1)/2$ and form the set of numbers

$$A = a, 2a, ..., Pa.$$

The set of integers in the range $(-p/2, p/2)$ form a complete set of residues, so every number in the above list can be reduced to a number in that range. The rule for this reduction is simple; if ja reduced modulo p is greater than $p/2$, then reduce it further into the range $(-p/2, 0)$; otherwise, leave it because it's already in the range $(0, p/2)$. Let B be the set of numbers in A that are reduced in this manner. The numbers in B are all in the range $(-p/2, p/2)$.

In the set B clearly there are some numbers that are positive and some that are negative. If we count the number of negative numbers in the set and call that number v, then

$$\left(\frac{a}{p}\right) = (-1)^v.$$

This is Gauss's Lemma.

Let's make things a little clearer with a numerical example. Suppose $a = 3$ and $p = 7$. We would like to know if 3 is a quadratic residue modulo 7. Following the above procedure, we set $P = (7-1)/2 = 3$ and form the numbers $a, 2a, ..., Pa$. Thus we have

Numerical examples, although no substitute for proper proofs, are key in number theory because they allow us to formulate conjectures or verify the truth of a general case that would otherwise be impossible to guess. It is said that based on numerical evidence Gauss guessed the Prime Number Theorem, although the proof was not discovered until some years after his death.

$$A = \{3, 6, 9\}.$$

Reducing this set into the range $(-p/2, p/2) = (-7/2, 7/2)$ to get B, we have

$$B = \{3, -1, 2\}.$$

The number of negative numbers is 1, so

$$\left(\frac{3}{7}\right) = (-1)^1 = -1$$

and thus 3 is not a quadratic residue modulo 7.

Check this by enumerating the quadratic residues modulo 7 as shown in previous handouts.

Here is another example before we begin the proof. This time let $p = 11$ and $a = 5$. We would like to know whether 5 is a quadratic residue modulo 11.

As before, set $P = (11-1)/2 = 5$. Then form the set

$$A = \{5, 10, 15, 20, 25\}.$$

Reduce each element of that set into the range $(-11/2, 11/2)$ and we get

$$B = \{5, -1, 4, -2, 3\}.$$

The number of negative numbers is B is 2, and therefore

$$\left(\frac{5}{11}\right) = (-1)^2 = 1.$$

Verify this by noting that $4^2 \equiv 5 \pmod{11}$.

Now we begin the proof. Take the sets A and B to be the formed as described above. Two things are immediately clear to us about the numbers in B. No two numbers of the set are equal; if $ia \equiv ja \pmod{p}$ then $i \equiv j$ because $a \not\equiv 0$, and since $i, j < P$ we have $i = j$. On the other hand, it is also not possible for $ia \equiv -ja \pmod{p}$ (that is, if we take the absolute value of all the numbers in B, we won't get two duplicates); for if that is the case then $ia + ja \equiv 0 \pmod{p}$ and since $a \not\equiv 0$ we must have $i + j \equiv 0$. This is clearly impossible because $i, j \leq P$ and so $i + j \leq 2P = p - 1$.

Therefore the numbers $1, 2, \ldots, P$ appear exactly once in B with either a positive or negative sign, but not both, and each number in B is congruent to one and only one number in A. Thus the products of the two sets are congruent. If we let v be the number of negative signs in B, we have

$$a \times 2a \times \cdots \times Pa \equiv (-1)^v 1 \times 2 \times \cdots \times P \pmod{p}.$$

Condensing the products yields

$$a^P P! \equiv (-1)^v P! \pmod{p}.$$

Clearly $P! \not\equiv 0 \pmod{p}$, so

$$a^P \equiv (-1)^v \pmod{p}.$$

This is where Euler's Criterion comes into play. Recall that it states

$$a^P \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Consequently we have

$$\left(\frac{a}{p}\right) \equiv (-1)^v \pmod{p}$$

which is the result we're trying to prove; the quadratic character of a is dependent only on the number of negative numbers in the set B, which is denoted here by v.

As stated previously, Gauss's Lemma allows us to determine $(a|p)$ for any $a \not\equiv 0$, but it can do much more than that. In fact we can go the other way and ask for which primes p is $(a|p) = 1$ for given values of a. For example, for which primes p is $(2|p) = 1$? That is, for which primes is 2 a quadratic residue? Yet another way of phrasing the question is to ask for which primes p the equation

$$x^2 - 2 \equiv 0 \pmod{p}$$

is solvable.

Note how the theory of quadratic residues is actually connected with *solving quadratic congruences*. Linear congruences were simple enough, but it seems quadratic ones are a different thing altogether.

The most natural way to proceed, perhaps the only way, is to blindly follow the steps of Gauss's Lemma and see how far the general case can lead us. So let $P = (p - 1)/2$ and form the set

$$A = \{2, 4, \ldots, 2P\}.$$

Note that $2P = p - 1$. This means that every member of A is in the range $(0, p-1)$. Now the question is: if we reduce each member of A into the range $(-p/2, p/2)$ to make B, how many numbers in B are negative?

Since every member of A is already less than p, the number of negative numbers in B is the same as the number of numbers in A that are greater than $p/2$. Let u be the number in the range $(1, P)$ satisfying

$$2u < p/2$$

and

$$2(u+1) > p/2.$$

Thus u is the number of numbers in A that are *less than* $p/2$; therefore the number of numbers in A that are greater than $p/2$ is

$$v = P - u = (p-1)/2 - u.$$

Now we just need to determine the parity of v based on some condition regarding p, because we know that

$$\left(\frac{2}{p}\right) = (-1)^v.$$

But this information seems to depend on both p and u, so we cannot just plug in $p = 4k+1$ or $p = 4k+3$ like we did for the case $a = -1$. What do we do instead?

There's nothing quite like a good cliffhanger.

Problems

1. Use Gauss's Lemma to find $(5|19)$.
2. Determine whether 2 is a quadratic residue for as many primes as you can, starting $3, 5, 7, 11, \ldots$. Do you see any patterns that might give us a clue as to how to finish the above proof of the quadratic character of 2?
3. (Continuation of the above proof of the quadratic character of 2)
   (a) If
   $$a < u < b$$
   find a and b in terms of p.
   (b) If we are optimistic, perhaps $(2|p)$ has something to do with whether $p \equiv 1$ or $p \equiv -1$ modulo 4, as for the case $a = -1$. Let $p = 4k+1$ and $p = 4k+3$ and show in both cases that $u = k$.
   (c) Is the preceding information enough to pin down the parity of v and hence solve the problem?
   (d) If not, try other congruence classes for p. If you get the right one, you will have solved the problem of evaluating $(2|p)$.

This problem is much easier if you did question 2.

Melbourne High School
Maths Extension Group 2023
Term 3 Week 8 Handout

Boiling water will soften a potato but harden an egg.

—J. Clear, *Atomic Habits* (2018)

Don't ask how this is related to functional equations.

Problems: functions and functional equations

1. The function $f(x) = x^2$ is not invertible. However, if we let $g(x) = \sqrt{x}$ then $f(g(x)) = (\sqrt{x})^2 = x$. So, why isn't f invertible?

2. Let $f(x)$ be a function such that $f(x + y) = x + f(y)$ for any two real numbers x and y, and $f(0) = 2$. What is the value of $f(1998)$? AHSME 1998/17

3. An involution is a function whose inverse is itself ($f(f(x) = x$ for all x in the domain of f). Show that an involution must be bijective.

4. Find all solutions to the equation

$$f(x + y) + f(x - y) = 2x^2 - 2y^2.$$

5. Find all functions $f : \mathbb{R} \to \mathbb{R}$ for which

$$f(x + y) - 2f(x - y) + f(x) - 2f(y) = y - 2$$

for all $x, y \in \mathbb{R}$.

As a six-year-old lad I could easier understand a mathematical proof than I could understand why I should take my cap off in the parlour, or why I should use a knife to cut a slice of meat rather than tearing it apart with a fork.

Soon Mr. Eisenstein is to play an important role in our story.

—G. Eisenstein[1], *Curriculum Vitae* (c. 1843)

Cliffhanger

Let's begin by revisiting the problem of finding $(2|p)$ for odd primes p. We shall not leave ourselves on a cliffhanger this time, but our method of solving the problem will be different. The method employed here will make our transition to the most general case ($(p|q)$ for odd primes p and q) easier and perhaps more enlightening.

The basis of our proof, like before, is Gauss's Lemma. Such a venerable lemma is easy to forget, so here it is again: given an odd prime p and some number a coprime with p,

$$\left(\frac{a}{p}\right) = (-1)^v$$

where v is the number of numbers in the set

$$\left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\} \tag{1}$$

that have least positive residues greater than $p/2$. An equivalent definition of v is the number of negative numbers in the set formed by taking each element of (1) and reducing it to be between $-p/2$ and $p/2$, for if $ka > p/2$ then reducing it in this manner will make it negative.

Armed with this weapon, let's introduce another. This one is called the *floor function*; it is denoted by $\lfloor x \rfloor$. This symbol means the largest integer less than or equal to x. So if x is a positive number, $\lfloor x \rfloor$ is the integer part of x. For example, $\lfloor \pi \rfloor = 3$, $\lfloor e \rfloor = 2$, $\lfloor 28/5 \rfloor = 5$. Using this notation we can write any number x as

What happens when x is negative?

$$x = \lfloor x \rfloor + y$$

where $0 \leq y < 1$.

Now we can turn back to the original problem. For our specific case where $a = 2$, we have to find how many numbers in the set

$$\{2, 4, \ldots, p-1\}$$

are greater than $p/2$. Let u be the number of numbers in the set that are less than $p/2$ and v be the number of numbers in the set that are greater than $p/2$. In other words, u satisfies

Clearly only strict inequality signs are needed because $p/2$ is not an integer.

$$2u < \frac{p}{2}$$

and

$$2(u+1) > \frac{p}{2}.$$

Rearranging these two inequalities yields

$$u < \frac{p}{4}$$

and

$$u > \frac{p}{4} - 1,$$

[1]Translated from the German by M. Schmitz in *Res. Lett. Inf. Math. Set.,* 2004, Vol. 6, pp 1–13.

which is more succinctly written as

$$\frac{p}{4} - 1 < u < \frac{p}{4}.$$

A little thought convinces us that between $p/4$ and $p/4 - 1$ there is one and only one integer, and that integer is $\lfloor p/4 \rfloor$. Thus $u = \lfloor p/4 \rfloor$.

By definition, $u + v = (p-1)/2$, so $v = (p-1)/2 - \lfloor p/4 \rfloor$. To get rid of the floor function so that we can collect like terms, consider two cases: when $p \equiv 1 \pmod 4$ and when $p \equiv 3 \pmod 4$. If $p = 4k+1$, then $\lfloor p/4 \rfloor = \lfloor k + 1/4 \rfloor = k$; substituting this into the above equation for v we get $v = k$. But $k = (p-1)/4$, so we have

$$v = \frac{p-1}{4}.$$

Similarly, if $p = 4k+3$, then $\lfloor p/4 \rfloor = k$ and $v = k+1$. In this case $k = (p-3)/4$ so

$$v = \frac{p+1}{4}.$$

Here is the final hurdle. As shown above, when $p = 4k+1$ we have $v = (p-1)/4$. If $p-1$ is divisible by 4, then $p - 1 + 2 = p + 1$ is not divisible by 4, but has the same quotient. That is,

$$\frac{p-1}{4} = \left\lfloor \frac{p+1}{4} \right\rfloor$$

when $p = 4k+1$. If $p = 4k+3$, we have $v = (p+1)/4$ anyway, and clearly $(p+1)/4 = \lfloor (p+1)/4 \rfloor$. Therefore we have shown that

$$v = \left\lfloor \frac{p+1}{4} \right\rfloor$$

regardless of whether p is 1 or 3 more than a multiple of 4.

From Gauss's Lemma

$$\left(\frac{2}{p}\right) = (-1)^v;$$

substituting in the value of v just found gives

$$\left(\frac{2}{p}\right) = (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor}. \tag{2}$$

Here is where we need numerical evidence to help us continue; we would be lost without a rough idea of what we're trying to prove because it is not clear how to proceed. In this case the best way is to evaluate $(2|p)$ for the first hundred primes to see if a pattern is apparent. If we do this, we find that $(2|p) = 1$ for

$$p = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97$$

and $(2|p) = -1$ for

$$p = 3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83.$$

What is the difference between the two lists? If we look closely, we observe that all the numbers in the first list are congruent to ± 1 modulo 8 while the ones in the second are congruent to ± 3 modulo 8. Our conjecture, therefore, is that $(2|p) = 1$ if $p \equiv \pm 1 \pmod 8$ and $(2|p) = -1$ if $p \equiv \pm 3 \pmod 8$.

To prove the conjecture, first put $p = 8k+1$ into Equation (2). We get

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor 2k + 1/2 \rfloor} = (-1)^{2k} = 1.$$

In the following section some of the calculations have been omitted for brevity; carry them out yourself if necessary to understand the logic.

If you successfully solved last week's problems you will know what comes next.

In this case the pattern is so overwhelming as to make the conjecture obvious once it is noticed, but in other cases, such as the one at the end of this handout, many different guesses might have to made before the correct one is landed upon and successfully proved.

Similarly if $p = 8k - 1$ then $\lfloor (p+1)/4 \rfloor = 2k$, which implies $(2|p) = (-1)^{2k} = 1$ again.

Now for the other case. If $p = 8k + 3$ then

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor 2k+1 \rfloor} = (-1)^{2k+1} = -1.$$

Putting $p = 8k - 3$ instead yields

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor 2k-1/2 \rfloor} = (-1)^{2k-1} = -1.$$

This proves our conjecture! Indeed it is true that the quadratic character of 2 modulo p depends on the the residue class of p modulo 8.

Let's summarise what we have discovered so far in the quest to evaluate the Legendre symbol. We have solved two cases: $a = -1$ and $a = 2$. In the former case $(-1|p) = -1$ if $p \equiv 1 \pmod 4$ and $(-1|p) = -1$ if $p \equiv -1 \pmod 4$; in the latter case $(2|p) = 1$ if $p \equiv \pm 1 \pmod 8$ and $(2|p) = -1$ if $p \equiv \pm 3 \pmod 8$.

Although it may not seem like it, we are in fact two thirds of the way towards evaluating any Legendre symbol. Suppose we want to find $(a|p)$. Using the multiplicative property $(ab|p) = (a|p)(b|p)$, if we write $a = q_1 q_2 \cdots q_r$, where all the q's are primes, then

Ok, maybe two thirds is an exaggeration, because the part left for us to discover (and prove) is much more difficult than what we have just done. But it's still good to be optimistic.

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_r}{p}\right).$$

If $a < 0$ then stick at $(-1|p)$ at the front—we know how to evaluate that. So the only goal now is to evaluate $(q|p)$ when q is an odd prime.

This question is much more difficult to answer than the two we have already tackled. To get started, here is a table values of p, q, and $(p|q)$.

p \ q	3	5	7	11	13	17	19	23	29	31	37
3	0	−1	1	−1	1	−1	1	−1	−1	1	1
5	−1	0	−1	1	−1	−1	1	−1	1	1	−1
7	−1	−1	0	1	−1	−1	−1	1	1	−1	1
11	1	1	−1	0	−1	−1	−1	1	−1	1	1
13	1	−1	−1	−1	0	1	−1	1	1	−1	−1
17	−1	−1	−1	−1	1	0	1	−1	−1	−1	−1
19	−1	1	1	1	−1	1	0	1	−1	−1	−1
23	1	−1	−1	−1	1	−1	−1	0	1	1	−1
29	−1	1	1	−1	1	−1	−1	1	0	−1	−1
31	−1	1	1	−1	−1	−1	1	−1	−1	0	−1
37	1	−1	1	1	−1	−1	−1	−1	−1	−1	0

In the table there exists a pattern that is at the heart of what may be the most beautiful theorem in number theory. But for now, the story remains to be continued.

Admittedly I am biased.

Problem

Spot as many patterns as possible in the above table.

Melbourne High School
Maths Extension Group 2023
Term 3 Week 9 Handout

Stupors however do not last for ever, and Farmer Oak recovered from his.

—T. Hardy, *Far From the Madding Crowd* (1874)

Keep this in mind if you ever fall into a stupor because you're stuck on a problem (or have lost all of your sheep).

AIMO Problems

1. Gaston and Jordan are two budding chefs who unfortunately always misread the cooking time required for a recipe. For example, if the required cooking time is written 1:32 meaning 1 hour and 32 minutes, Jordan reads it as 132 minutes while Gaston reads it as 1:32 hours. For one particular recipe, the difference between Jordan's and Gaston's misread time is exactly 90 minutes. What is the actually cooking time in minutes? AIMO 2019/1

2. Let x and y be positive integers that simultaneously satisfy the equations $xy = 2048$ and $\frac{x}{y} - \frac{y}{x} = 7.875$. Find x. AIMO 2014/3

3. There are 5 lily pads on a pond, arranged in a circle. A frog can only jump from each lily pad to an adjacent lily pad on either side. How many ways are there for the frog to start on one of these lily pads, make 11 jumps, and end up where it started. AIMO 2022/5

4. A triangle PQR is to be constructed so that the perpendicular of PQ cuts the side QR at N and the line PN splits the angle QPR into two angles, not necessarily of integer degrees, in the ratio 1:22. If $\angle QPR = p$ degrees, where p is an integer, find the maximum value of p. AIMO 2019/7

5. Prove that 38 is the largest even integer that is *not* the sum of two positive odd composite numbers. AIMO 2018/9

If we compared the Bernoullis to the Bach family, then Leonhard Euler is unquestionably the Mozart of mathematics…

—E. Maor, *e: The Story of a Number* (1994)

A Golden Conjecture

Here's the table of values of p, q, and $(p|q)$ from last time:

p \ q	3	5	7	11	13	17	19	23	29	31	37
3	0	−1	1	−1	1	−1	1	−1	−1	1	1
5	−1	0	−1	1	−1	−1	1	−1	1	1	−1
7	−1	−1	0	1	−1	−1	−1	1	1	−1	1
11	1	1	−1	0	−1	−1	−1	1	−1	1	1
13	1	−1	−1	−1	0	1	−1	1	1	−1	−1
17	−1	−1	−1	−1	1	0	1	−1	−1	−1	−1
19	−1	1	1	1	−1	1	0	1	−1	−1	−1
23	1	−1	−1	−1	1	−1	−1	0	1	1	−1
29	−1	1	1	−1	1	−1	−1	1	0	−1	−1
31	−1	1	1	−1	−1	−1	1	−1	−1	0	−1
37	1	−1	1	1	−1	−1	−1	−1	−1	−1	0

It contains a pattern central to the problem of evaluating $(q|p)$ for any odd prime q. For now, however, let's leave it, and instead try to gain more numerical evidence.

Have faith that this detour is not an unwise one.

So far, we have proved that $(-1|p) = 1$ for primes of the form $4k+1$ and $(-1|p) = -1$ for primes of the form $4k-1$. Using Gauss's Lemma we have also shown that $(2|p) = 1$ for primes of the form $8k \pm 1$ and $(2|p) = -1$ for primes of the form $8k \pm 3$. Recall that since

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_r}{p}\right)$$

the remaining step is to evaluate $(q|p)$ for an odd prime q.

Here 'evaluate' means to find the conditions on p and q that determine whether $(q|p) = 1$ or $(q|p) = -1$.

The natural way forward, given our route thus far, is to evaluate $(3|p)$, $(5|p)$, and so on. Perhaps if we solve enough special cases a pattern will appear. Let's tackle $(3|p)$.

As before, the weapon to use is Gauss's Lemma. The question: how many numbers in the set

$$\left\{3, 6, 9, \ldots, \frac{3(p-1)}{2}\right\}$$

are negative when reduced into the range $(-p/2, p/2)$?

Divide the numbers in the above set into the three intervals

$$\left(0, \frac{p}{2}\right), \left(\frac{p}{2}, p\right), \left(p, \frac{3p}{2}\right).$$

The numbers in the first interval are positive and less than $p/2$; hence they remain unchanged when reduced to be in the interval $(-p/2, p/2)$. All the numbers in the second interval will become negative because they are greater than $p/2$ but less than p. The numbers in the third interval, being greater than p but less than $3p/2$, will be reduced to be between 0 and $p/2$ and therefore remain positive. Hence the number of negative signs is the number of numbers in the second interval, $(p/2, p)$.

So there is some condition on p, most likely to do with its residue class modulo some number, that determines whether the number of

numbers in the interval $(p/2, p)$ is even or odd, and that is the same condition that determines whether $(3|p) = 1$ or $(3|p) = -1$.

Now is the time for the numerical evidence. By simply evaluating $(3|p)$ for many values of p, we find that $(3|p) = 1$ for

$$p = 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107$$

and $(3|p) = -1$ for

$$p = 5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101.$$

If we continue trying out values of p, we notice that the numbers in the first list are of the form $12k \pm 1$ while the numbers in the second are of the form $12k \pm 5$. So we conjecture that $(3|p) = 1$ for $p = 12k \pm 1$ and $(3|p) = -1$ for $p = 12k \pm 5$.

To prove the conjecture, let $p = 12k + r$, where $r = \pm 1, \pm 5$. We wish to know how many numbers a satisfy

Note that these values of r are the only values for which p could be prime. We leave out $p = 2$ because $(3|2) = (1|2)$, which is trivial.

$$\frac{p}{2} < 3a < p,$$

or

$$\frac{12k + r}{2} < 3a < 12k + r.$$

Dividing through by 3 and splitting the fraction yield

$$2k + \frac{r}{6} < a < 4k + \frac{r}{3}.$$

When $r = 1$, the inequality becomes

$$2k + \frac{1}{6} < a < 4k + \frac{1}{3}.$$

If $a > 2k + 1/6$, then $a \geq 2k + 1$ because a is an integer. Similarly if $a < 4k + 1/3$, then $a \leq 4k$. Therefore the inequality is equivalent to

$$2k + 1 \leq a \leq 4k.$$

The number of numbers in this interval is $4k - (2k + 1) + 1 = 2k$, which is even, and hence $(3|p) = 1$. Similarly, when $r = -1$ the interval becomes

How many numbers are between 5 and 9 inclusive of both? Answer: $5, 6, 7, 8, 9$, so 5, or $9 - 5 + 1$.

$$2k - \frac{1}{6} < a < 4k - \frac{1}{3}.$$

Using the same reasoning as before, the number of numbers in this interval is $4k - 1 - 2k + 1 = 2k$; therefore $(3|p) = 1$ when $r = -1$ too.

The second case is much the same as the first. When $r = 5$ the inequality becomes

$$2k + \frac{5}{6} < a < 4k + \frac{5}{3}$$

and when $r = -5$ the inequality becomes

$$2k - \frac{5}{6} < a < 4k - \frac{5}{3}.$$

In the former the number of values of a that satisfy the inequality is $4k+1-(2k+1)+1 = 2k+1$; in the latter case it is $4k-2-(2k)+1 = 2k-1$. In both cases the number is odd and hence $(3|p) = -1$.

We have successfully solved another special case of the Legendre symbol: the case $a = 3$. Is there a pattern we can spot? With only two cases completed, $a = 2$ and $a = 3$, it might seem hard to find a pattern. However two things are plain. Firstly, in the case $a = 2$ the condition on p is its residue class modulo 8; for $a = 3$ it is its residue class modulo 12. Secondly, $(2|p)$ is the same for $p = 8k + r$ and $8k - r$

The case $a = -1$ is special because -1 is not prime; we need it so evaluate $(a|p)$ when $a < 0$.

for $r = 1, 3$, just as $(3|p)$ is the same for $p = 12k + r$ and $12k - r$ for $r = 1, 5$. From these two observations, we may guess, perhaps tentatively, that $(a|p)$ is dependent on the modulo class of p modulo $4a$, and that the quadratic character of a modulo $p = 4a - r$ is the same as that of $p = 4a + r$.

Let's try another case: $a = 5$. Using a computer, the first few values of p for which $(5|p) = 1$ are

$$p = 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, 151$$

and those for which $(5|p) = -1$ are

$$p = 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 103, 107, 113, 127, 137.$$

From experience, it is likely that the pattern has something to do with the residue class of p modulo a multiple of 4; it was 8 for $a = 2$ and 12 for $a = 3$. Naturally we try 20 for $a = 5$. And, indeed, if we examine the values of p closely, it seems that $(5|p) = 1$ for $p = 20k \pm 1$ or $p = 20k \pm 11$ and $(5|p) = -1$ for $p = 20k \pm 3$ or $p = 20k \pm 13$. The proof of this is far less exciting than the observation because of the number of different cases, but it is left as an exercise for the devoted.

Note also how this preceding observation is consistent with our earlier conjecture about the quadratic character of a being the same for $p = 4ak+r$ as it is for $p = 4ak-r$. When new numerical data agrees with previous conjectures, it is more evidence that those conjectures have a grain of truth to them.

From our guesswork for the case $a = 5$ something else jumps out as being a possible pattern: if $p = 4ak + r$ the same values of r seem to yield the same values for the Legendre symbol. That is, all of $(2|p)$, $(3|p)$, and $(5|p)$ equal 1 when $r = \pm 1$, and $(2|p)$ and $(5|p)$ both equal -1 when $r = \pm 3$. Of course there is not enough data here, but, perhaps, there is an inkling of gold just beneath the surface.

Problems

1. If no patterns are apparent in the table on page 2, try again.
2. Prove our conjecture about $(5|p)$.
3. Tackle the case $a = 7$. Do our two hypotheses hold?
4. Let This is a hard problem.

$$S(q, p) = \sum_{s=1}^{(p-1)/2} \left\lfloor \frac{sq}{p} \right\rfloor.$$

Prove that

$$S(q, p) + S(p, q) = \frac{(p-1)(q-1)}{4}.$$

Melbourne High School
Maths Extension Group 2023
MEG 2023 Term 3 Holiday Handout

For too much rest itself becomes a pain.

—Homer, *Odyssey* (c. 8th or 7th century BC)

Problems

1. The number x is 111 when written in base b, but it is 212 when written in base $b-2$. What is x in base 10? AIMO 2017/1

2. Find the number of permutations x_1, x_2, x_3, x_4, x_5 of numbers $1, 2, 3, 4, 5$ such that the sum of five products AIME II 2021/3

$$x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2$$

is divisible by 3

3. Let ABC be a triangle and P be any point on the circumcircle of ABC. Let X, Y, Z be the feet of the perpendiculars from P onto lines BC, CA and AB. Prove that points X, Y, Z are collinear. Simson Line

4. Find all functions $f : \mathbb{R}\backslash\{-1, 1\} \to \mathbb{R}$ for which

$$f\left(\frac{x-3}{x+1}\right) + f\left(\frac{3+x}{1-x}\right) = x$$

for all $x, y \in \mathbb{R}\backslash\{-1, 1\}$.

5. Prove that a convex pentagon with integer side lengths and an odd perimeter can have two right angles, but cannot have more than two right angles. AMO 2022/1

6. Having conquered *The Trial*, Harold is now reading *Gulliver's Travels*, a 319 page picture book. Eager as he is to dive into the travels of Gulliver, he also has a brilliant idea as to how he is going to read the book. He tells you that he is going to form the set of ordered pairs

$$\{(1,1), (1,2), \dots, (1,11), (2,1), (2,2), \dots, (2,11),$$
$$(3,1), (3,2), \dots, (29,1), \dots, (29,11)\}.$$

As he is a genius (and a good friend too), you don't doubt him.

As if that was not distressing enough, he then says that he will randomly arrange those ordered pairs by giving each a number. So if the above set was the arrangement, the pair $(1,1)$ would be 1, $(1,2)$ would be 2, and so on. To find the nth page that he reads, he takes the nth ordered pair (x_n, y_n) and forms the number $11x_n + 29y_n$; if this number is too big he subtracts off a multiple of 319 until he gets a page in the book. He then reads that page.

Show that regardless of how Harold arranges the ordered pairs, he will be able to read the entire book without reading the same page twice.

The king, although he be as learned a person as any in his dominions, had been educated in the study of philosophy, and particularly mathematics; yet when he observed my shape exactly, and saw me walk erect, before I began to speak, conceived I might be a piece of clock-work (which is in that country arrived to a very great perfection) contrived by some ingenious artist.

—J. Swift, *Gulliver's Travels* (1726)

A Golden Conjecture: Part 2

Easily summarised is the story so far. We first discovered that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv -1 \pmod 4 \end{cases}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8; \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Recall that the rule for $(-1|p)$ is more succinctly written as

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

As a side note, $(2|p)$ has a succinct rule too, namely

Verifying this by enumerating p shreds any incredulity.

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)(p+1)/8}.$$

We then took a slight detour to gather more numerical evidence; the following two conjectures resulted:

- The value of $(a|p)$ depends only on the residue class of p modulo $4a$, or, equivalently, the value of r when p is written as $p = 4ak + r$. In other words, if $p \equiv q \pmod{4a}$ then
$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$
- The value of $(a|p)$ is the same for $p = 4ak + r$ as it is for $p = 4ak - r$. In other words, if $p \equiv -q \pmod{4a}$ then
$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Note this conjecture holds regardless of whether r is positive or negative or whether r is between $-p/2$ and $p/2$. For $(2|p)$ it was prudent to split the residue classes modulo 8 into ± 1 and ± 3; but we could have chosen ± 7 and ± 5 instead, because $7 \equiv -1$, $-7 \equiv 1$, and similarly for ± 5.

These two conjectures found firm ground in two special cases that were proved using Gauss's Lemma. They are

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}; \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}, \end{cases}$$

and

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \text{ or } p \equiv \pm 11 \pmod{20}; \\ -1 & \text{if } p \equiv \pm 3 \text{ or } p \equiv \pm 13 \pmod{20}. \end{cases}$$

Euler was the first to make the two conjectures that we have also made; therefore from here they will be referred to as Euler's Conjectures. He was, however, unable to supply a proof. The problem of Gauss's

It's fairly rare to find a conjecture that eluded Euler, but this is one of them.

Lemma not being discovered yet might have had something to do with it.

We begin the proof of Euler's conjectures by applying Gauss's Lemma in full generality. Form the set

$$\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\};$$

how many of those multiples of a become negative when reduced to be in the range $(-p/2, p/2)$? Answer: all those that have least positive residues in the range $(p/2, p)$. This means we need to determine the parity of all the multiples of a in all the intervals

$$\left(\frac{p}{2}, p\right), \left(\frac{3p}{2}, 2p\right), \left(\frac{5p}{2}, 3p\right), \ldots. \tag{1}$$

Since we are assuming that a is not a multiple of p (because if it were the Legendre symbol, by definition, is equal to 0), none of the endpoints of any of the intervals can be multiplies of a. Therefore we don't have to worry about whether we need to count them or not.

Let's take one of these intervals, say the interval

$$\left(\frac{(2t-1)p}{2}, tp\right) \tag{2}$$

for some positive integer t. Now the question becomes how many numbers x satisfy the inequality

$$\frac{(2t-1)p}{2} < ax < tp.$$

Let this number be μ.

Dividing through by a yields

$$\frac{(2t-1)p}{2a} < x < \frac{tp}{a}. \tag{3}$$

Before continuing, let's take a step back and think about what we want to prove. Our conjecture is that $(a|p)$ depends only on the residue of p modulo $3a$. So let's write $p = 4ak + r$ for a positive integer value of r. Substitute this into our interval above, and, after a cumbersome expansion and simplification, we get

$$4tk + \frac{tr}{a} - 2k - \frac{r}{2a} < x < 4tk + \frac{tr}{a}.$$

Since we are interested only in the number of values of x (actually we are interested in the *parity* of that number) that satisfy the inequality, and not what those values actually are, we can manipulate the inequality by adding the same value to both endpoints, and the number of values of x that satisfy it will not change. For example, two values of x satisfy $3 < x < 6$ (4 and 5), but two values of x also satisfy $5 < x < 8$ or $1 < x < 4$.

Recall that we are interested only in the parity because of Gauss's Lemma, which tells us that $(a|p) = (-1)^v$ where v is the number of numbers in all the intervals in (1).

Therefore, we can get rid of all the terms involving t in the inequality, which means we are looking for the number of values of x that satisfy

$$-2k - \frac{r}{2a} < x < 0.$$

It is easier to work with positive numbers, so add $2k$ and r/a to both sides to obtain the inequality

$$\frac{r}{2a} < x < 2k + \frac{r}{a}.$$

The smallest integer greater than $r/2a$ is $\lceil r/2a \rceil$ and the largest integer less than $2k + r/a$ is $2k + \lfloor r/a \rfloor$. Therefore the number of numbers in the sequence

$$\lceil r/2a \rceil, \lceil r/2a \rceil + 1, \ldots, 2k + \lfloor r/a \rfloor$$

Note that the $\lceil x \rceil$ is the *ceiling function*; it is the smallest integer greater than or equal to x.

Is the use of floor and ceiling functions here dependent on r being positive?

is μ, the magic number we are looking for. Calculating μ is very simple because

$$\mu = 2k + \lfloor r/a \rfloor - \lceil r/2a \rceil + 1.$$

If this is baffling, remember the example from last time. How many numbers x satisfy $5 \leq x \leq 9$? The answer is $9 - 5 + 1 = 5$.

Since we are only interested in the parity of μ, we note that

$$2k + \lfloor r/a \rfloor - \lceil r/2a \rceil + 1 \equiv \lfloor r/a \rfloor - \lceil r/2a \rceil + 1 \pmod 2$$

and hence $\mu \equiv \mu' \pmod 2$ if μ' is the number of integers in the interval

$$\left(\frac{r}{2a}, \frac{r}{a}\right).$$

Take a breath. What have we shown? Answer: regardless of which interval in (1) we choose, the parity of the number of numbers in that interval is equal to the parity of the number of numbers in the interval $(r/2a, r/a)$.

Now consider what happens if, instead of writing $p = 4ak + r$, we write $p = r$ instead. That is, substitute $p = r$ into (3). Expand and we get

$$\frac{tr}{a} - \frac{r}{2a} < x < \frac{tr}{a}.$$

Again we can manipulate the interval like we did before; getting rid of the tr/a term and adding r/a to both sides yields

$$\frac{r}{2a} < x < \frac{r}{a}.$$

Bingo! This is the interval we ended up getting when we put $p = 4ak + r$. This means that for each interval in (1), the parity of the number of numbers in that interval is the same when $p = 4ak + r$ and when $p = r$; therefore the parity of the total number of numbers in all the intervals is the same in both cases. Thus, the glorious conclusion, after much work, is that $(a|p)$ does not depend on k if $p = 4ak + r$, but only on r, the residue class of p modulo $4a$. We have proved the first part of Euler's Conjecture.

The second part of Euler's Conjecture is, quite thankfully, a little easier to prove. We need to show that replacing r by $-r$ does not change the parity of the number of numbers in the intervals in (1).

We have shown that the parity of the number of numbers in each of the intervals in (1) is the same as the parity of the number of numbers in the interval

$$\left(\frac{r}{2a}, \frac{r}{a}\right).$$

If we replace r by $-r$, we get the interval

$$\left(\frac{-r}{a}, \frac{-r}{2a}\right);$$

note the reversal of the endpoints because $-r$ is negative. Now just add $3r/2a$ to both sides and we get the interval $(r/2a, r/a)$, which shows that replacing r by $-r$ has no effect on the parity of the numbers in the intervals in (1). Hence the second part of the conjecture is also true.

What we have proved can be thus summarised: if $p \equiv r \pmod{4a}$ and $q \equiv r \pmod{4a}$, or if $p \equiv r \pmod{4a}$ and $q \equiv -r \pmod{4a}$, then

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

More succinctly: if $p \equiv \pm q \pmod{4a}$ then

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Where does this leave us? It leaves us on the precipice of the most famous theorem in this area of number theory.

Melbourne High School
Maths Extension Group 2023
First Meeting Problems Solutions

1. Solve to get the solution $t = 9$.

2. The square has side length $2a$; hence its area is $4a^2$. The circle has area πa^2, so the probability a randomly chosen point in the square is also in the circle is $\pi a^2/4a^2 = \pi/4$.

3. Solving $x + 5 = 5x$ yields $x = 5/4$.

4. Compute the first few partial sums to spot a pattern, viz.

$$\begin{aligned}\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3} &= \frac{3+1}{6} = \frac{2}{3}\\ \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4} &= \frac{2}{3}+\frac{1}{12} = \frac{3}{4}\\ \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{4\cdot 5} &= \frac{3}{4}+\frac{1}{20} = \frac{4}{5}\end{aligned}$$

If this pattern continues, the desired result is 99/100. (Extension: for those who have learnt proof, try proving that

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$$

by induction.)

5. The number must be divisible by both 5 and 3, and so the last digit must be a 0. To be divisible by 3, the sum of the digits must be divisible by 3; we need three 2s. Hence the smallest number that is gobbus is 2220.

6. All triples that have a product of 36 are: $(1, 1, 36)$, $(2, 1, 18)$, $(2, 2, 9)$, $(3, 3, 4)$, $(4, 9, 1)$, $(6, 6, 1)$. If knowing the sum of the three numbers is not enough information, then it must be either $(2, 2, 9)$ or $(6, 6, 1)$, as both sum to 13. Since there is a jar with the most cookies in it, the answer is $(2, 2, 9)$.

7. First rearrange to find that $a+b = 1/4$. Square both sides and we get $a^2+b^2+2ab = 1/16$. Substitute in $a^2 + b^2 = 16$ and the equation becomes $2ab = -255/16$; hence $ab = -255/32$. Note that $1/a + 1/b = (a + b)/ab$, so we have

$$\begin{aligned}\frac{1}{a}+\frac{1}{b} &= \frac{1/4}{-255/32}\\ &= \frac{-8}{255}.\end{aligned}$$

8. $2, 5, 13, 17, 29, ...$, i.e., all the primes in the form $4k + 1$ (except for 2).

9. Rearrange and factorise to get $(5x-y)(3x-2y) = 100$. Now we just need to enumerate the factors of 100 and solve for x and y.

It is wise to consider that since x and y are positive integers, $5x - y > 3x - 2y$, so we only need to consider half the pairs of factors of 100. Beginning with $5x - y = 100$ and

$3x-2y=1$, we see that this means $7x=199$, which has no solution in positive integers. Then we move on to $5x-y=50$ and $3x-2y=2$. Solving these two simultaneous equations yields $7x=98$, or $x=14$, which implies $y=20$.

Continuing in this fashion, we find one other solution, when $5x-y=20$ and $3x-2y=5$. In this case $x=5$ and $y=5$. So all the solutions in positive integers to our original equation are $(5,5)$ and $(14,20)$.

10. Reduce modulo 10 to get the final digit of $2^3=8$.

If not familiar with modular arithmetic, consider the last digit of the first few powers of 2: $2,4,8,16,32,64,128,256,512,\ldots$. Note how the the last digits go $2,4,8,6,2,4,8,6,2,\ldots$. That is, the last digits repeat every fourth term in the sequence. Since 2023 is 3 more than a multiple of 4, its last digit is the third number in the repeated sequence $2,4,8,6$. Hence the last digit of 2^{2023} is 8.

11. Without loss of generality, assume $a\geq b\geq c$. This will be needed for an application of the rearrangement inequality.

Square both sides of the equation $a+b+c=1$ to get

$$a^2+b^2+c^2+2(ab+bc+ac)=1.$$

Substituting this into $a^2+b^2+c^2+1$ yields

$$\begin{aligned} a^2+b^2+c^2+1 &= a^2+b^2+c^2+(a^2+b^2+c^2+2(ab+bc+ac)) \\ &= 2(a^2+b^2+c^2)+2(ab+bc+ac). \end{aligned}$$

By the rearrangement inequality, $a^2+b^2+c^2\geq ab+bc+ac$, so we have

$$\begin{aligned} 2(a^2+b^2+c^2)+2(ab+bc+ac) &\geq 2(ab+bc+ac)+2(ab+bc+ac) \\ &= 4(ab+bc+ac). \end{aligned}$$

Hence $a^2+b^2+c^2+1\geq 4(ab+bc+ac)$.

12. Consider a set $S_n=\{1,2,3,\ldots,n\}$. Let $a_1,a_2,a_3,\ldots,a_{2^n}$ be the alternating sums of its 2^n subsets, and let A_n equal the sum of all alternating sums of all the subsets of S_n. By these definitions we have

$$\begin{aligned} S_n &= \sum_{i=0}^{n} a_i \\ &= a_1+a_2+a_3+\cdots+a_{2^n}. \end{aligned}$$

Now consider the set $S_{n+1}=\{1,2,3,\ldots,n,n+1\}$. Note that 2^n of its subsets are the same as those of S_n; the other 2^n subsets can be formed by taking each subset of S_n and adding $n+1$ to it. Now let $b_1,b_2,b_3,\ldots,b_{2^n}$ be the alternating sums of the 2^n subsets that are not subsets of S_n. In other words, these are the alternating sums of all the subsets of S_n with $n+1$ added to them. Since $n+1$ is the biggest element in each of these sets, each alternating sum begins with $n+1$, followed by the rest of the numbers in the set.

We see that $b_i=(n+1)-a_i$ for $1\leq i\leq 2^n$. To see why this is true consider the set $\{1,2,3,4\}$; its alternating sum is $4-3+2-1=2$. If we add 5 to the set, the alternating sum becomes $5-4+3-2+1=5-(4-3+2-1)$.

So we have

$$\begin{aligned} b_1 &= (n+1) - a_1 \\ b_2 &= (n+1) - a_2 \\ b_3 &= (n+1) - a_3 \\ &\vdots \\ b_{2^n} &= (n+1) - a_{2^n}. \end{aligned}$$

Adding these together we get

$$\begin{aligned} b_1 + b_2 + b_3 + \cdots + b_{2^n} &= (n+1) \cdot 2^n - (a_1 + a_2 + a_3 + \cdots + a_{2^n}) \\ &= (n+1) \cdot 2^n - S_n \end{aligned}$$

The sum of the alternating sums of all subsets of S_{n+1} is the sum of the alternating sums of all subsets of S_n plus all of $b_1, b_2, b_3, \cdots, b_{2^n}$. Hence

$$\begin{aligned} A_{n+1} &= S_n + b_1 + b_2 + b_3 + \cdots + b_{2^n} \\ &= S_n + (n+1) \cdot 2^n - S_n \\ &= (n+1) \cdot 2^n. \end{aligned}$$

Thus we have found a closed-form expression for A_{n+1}. We can just plug in $n = 9$ to get $A_{10} = 10 \cdot 2^9$.

13. This can be done with just a scientific calculator. First we calculate the 5 raised to powers of 2 modulo 397. This is doable because we get the next power by squaring the previous residue and reducing modulo 397. Since our residues are guaranteed to be less than 397, our calculators do not blow up, as they would do if we tried computing 5^{261}.

$$\begin{aligned} 5^1 &\equiv 5 \pmod{397} \\ 5^2 &\equiv 25 \pmod{397} \\ 5^4 &\equiv 228 \pmod{397} \\ 5^8 &\equiv 374 \pmod{397} \\ 5^{16} &\equiv 132 \pmod{397} \\ 5^{32} &\equiv 353 \pmod{397} \\ 5^{64} &\equiv 348 \pmod{397} \\ 5^{128} &\equiv 19 \pmod{397} \\ 5^{256} &\equiv 361 \pmod{397} \end{aligned}$$

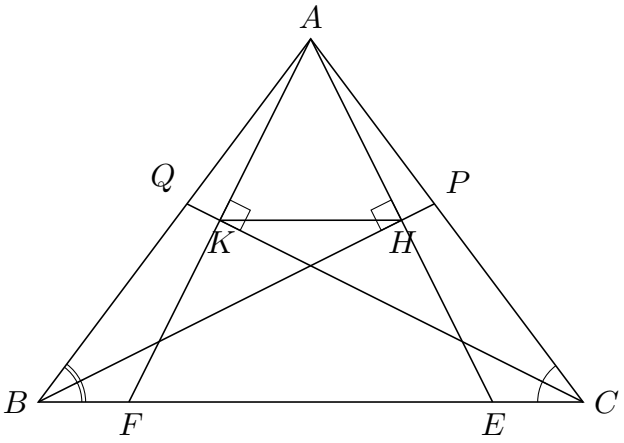
Since $261 = 256 + 4 + 1$, we get

$$\begin{aligned} 5^{261} &\equiv 5^{256} \cdot 5^4 \cdot 5^1 \\ &\equiv 361(228)(5) \pmod{397} \\ &\equiv 248 \pmod{397}. \end{aligned}$$

Here's an example of how to evaluate one of those powers of 5 modulo 397 on a simple calculator. Let's say we wanted to compute $5^{16} \pmod{397}$. We see that $5^8 \equiv 374 \pmod{397}$, so we evaluate $374^2/397$ on our calculator. We get something like $352.332\ldots$. Round down and take away that multiple of 397 from 374^2 to get $5^{16} \pmod{397}$. In

other words, now we evaluate $374^2 - 352 \cdot 397$ to get 132; this number is $5^{16} \pmod{397}$. Think about this a few times to understand why it works.

14.



Since $\angle BHE$ is also a right angle, $\angle HBE = \angle HBA$ by definition, and HB is a common side, $\triangle AHB$ is congruent to $\triangle BHE$ by ASA. This means $AH = HE$, as they are corresponding sides of the two triangles. Similarly, $\triangle AKC$ is congruent to $\triangle KFC$, again by ASA. This implies $AK = KF$.

Since $AK = KF$ and $AH = HE$, $\triangle AFE$ is similar to $\triangle AKH$ by SAS; from this we conclude that $\angle AKH = \angle AFE$ and $\angle AHK = \angle AEF$. Thus HK is parallel to FE, and because FE lies on BC, HK is also parallel to BC, as required.

15. Firstly, since $F_0 = 0$ we can get rid of the the F_0 term. Our power series becomes

$$G(x) = F_1 x + F_2 x^2 + F_3 x^3 + \cdots.$$

Replace each coefficient, except for the first, with its recursive definition:

$$G(x) = F_1 x + (F_0 + F_1)x^2 + (F_1 + F_2)x^3 + (F_2 + F_3)x^4 + \cdots.$$

Now rearrange and group the first terms of each set of parentheses together. Do likewise with the second term of each set of parentheses.

$$G(x) = F_1 x + (F_0 x^2 + F_1 x^3 + F_2 x^4 + \cdots) + (F_1 x^2 + F_2 x^3 + F_3 x^4 + \cdots).$$

Notice that by factoring out each set of parentheses we get $G(x)$ again.

$$\begin{aligned} G(x) &= F_1 x + (F_0 + F_1 x + F_2 x^2 + F_3 x^3 + \cdots)x^2 + (F_1 x + F_2 x^2 + F_3 x^3 + \cdots)x \\ &= x + x^2 G(x) + xG(x) \end{aligned}$$

Rearranging yields

$$G(x) = \frac{x}{1 - x - x^2}.$$

Melbourne High School
Maths Extension Group 2023
Term 1 Week 7 Handout

Section B

1. Substituting $a = st$ and $b = (s^2 - t^2)/2$ into the LHS of $a^2 + b^2 = c^2$ yields

$$\begin{aligned} s^2t^2 + \frac{s^4 - 2s^2t^2 + t^4}{4} &= \frac{4s^2t^2 + s^4 - 2s^2t^2 + t^4}{4} \\ &= \frac{s^4 + 2s^2t^2 + t^4}{4} \\ &= \left(\frac{s^2 + t^2}{2}\right)^2 \end{aligned}$$

The second part of the proof is to show that the three numbers do indeed share no common factors. Note that this proof requires knowledge of the Euclid's lemma, which asserts that if a prime divides a product of two numbers, it must divide at least one of the two numbers. This will be covered in future handouts.

Using Euclid's lemma, We note that if any pair of a, b, and c shared a common prime factor, the third would share that same common factor. This is because if a prime divides $n^2 = n \cdot n$, it divides either n or n; hence it must divide n.

Now suppose that p is a common prime divisor of $a = st$, $b = (s^2 - t^2)/2$, and $c = (s^2 + t^2)/2$. From Euclid's lemma p divides either s or t, but not both, because s and t share no common factors; for now, let's assume that it divides s. Then we can write $s = pu$ for some integer u. Substituting this into b and we get $b = (p^2u^2 - t^2)/2$. Since, by assumption, p divides b, we have $b = pv$ for some integer v. Combining these two statements yields

$$p^2u^2 - t^2 = 2pv.$$

Rearrange for t^2 and we get $t^2 = p^2u^2 - 2pv$. The RHS is clearly divisible by p; hence t^2 must be divisible by p, which implies t is divisible by p. This is a contradiction, because s and t share no common factors.

Now we turn to the case when p divides t instead of s. As before, we can write $t = pu$ for some integer u, and $b = pv$ for some integer v. Again using these statements, we find that

$$s^2 - p^2u^2 = pv.$$

Rearrange for s^2 and deduce that s is divisible by p, once again contradicting the assumption that s and t share no common factors.

Thus a and b cannot share any common factors; this completes the proof that the triple $(st, (s^2 - t^2)/2, (s^2 + t^2)/2)$ for coprime odd integers s and t, where $s > t$, always generates a primitive Pythagorean triple.

2. Since s and t are odd, let $s = 2m + 1$ and $t = 2n + 1$ for integers m and n. We have chosen a

to be odd and b even, and so substituting s and t into $b = (s^2 - t^2)/2$, we get

$$\begin{aligned} b &= \frac{(2m+1)^2 - (2n+1)^2}{2} \\ &= \frac{4m^2 + 4m + 1 - 4n^2 - 4n - 1}{2} \\ &= 2m^2 + 2m - 2n^2 - 2n \\ &= 2m(m+1) - 2n(n+1) \end{aligned}$$

Note that $m(m+1)$ and $n(n+1)$ must be even; hence 4 divides both $2m(m+1)$ and $2n(n+1)$. This completes the proof that b is divisible by 4.

3. We first note that a square can only leave a remainder of 0 or 1 when divided by 3. We can see this just by calculating the squares of the numbers 0, 1, and 2:

$$\begin{aligned} 0^2 &\equiv 0 \pmod 3 \\ 1^2 &\equiv 1 \pmod 3 \\ 2^2 &\equiv 1 \pmod 3 \end{aligned}$$

Assume that neither a or b is divisible by 3. Then both a^2 and b^2 must be congruent to 1 mod 3. Then $c^2 \equiv a^2 + b^2 \equiv 2 \pmod 3$. We have just shown that this is impossible; a square cannot leave a remainder of 2 when divided 3. Hence either a or b must be divisible by 3.

If not familiar with modular arithmetic or its notation, this can also be proven by expanding expression such as $(3m+1)^2$ to determine that the square of a number 1 more than a multiple of 3 is also 1 more than a multiple of 3.

4. We begin, as before, by nothing that the only squares modulo 5 are 0, 1, and 4.

Assume that none of a, b, or c is divisible by 5. Then a^2 and b^2 are both congruent to either 1 or 4. Enumerating all the possibilities we get one of the following possibilities for c^2:

$$\begin{aligned} c^2 &\equiv 1 + 1 \equiv 2 \pmod 5 \\ c^2 &\equiv 1 + 4 \equiv 0 \pmod 5 \end{aligned}$$

We know the first possibility is impossible, so $c^2 \equiv 0 \pmod 5$, which contradicts our initial assumption.

Hence one of a, b, or c must be divisible by 5.

We have shown that each 3, 4, and 5 will always divide one of the numbers in a Pythagorean triple. So every the product of Pythagorean triple must be divisible by $3 \cdot 4 \cdot 5 = 60$. However, the highest common factor of the product of all Pythagorean triples must also be a factor of the product of the Pythagorean triple $(3, 4, 5)$; hence the HCF we are looking for is 60.

5. The equation of the live is $y = m(x+1)$. Substituting this into the equation of the circle, we get

$$\begin{aligned} x^2 + m^2(x^2 + 2x + 1) &= 1 \\ (1 + m^2)x^2 + m^2 2x + m^2 - 1 &= 0 \end{aligned}$$

From here, the quadratic formula could be used, but the better way is to recognise that $x = -1$ is a solution to the above equation; therefore we can use polynomial division to determine the other factor. So dividing the quadratic by $(x+1)$, we get

$$\frac{(1 + m^2)x^2 + m^2 2x + m^2 - 1}{x + 1} = (1 + m^2)x + (m^2 - 1)$$

Solving this equation for x gives $x = (1 - m^2)/(1 + m^2)$. Substitute this value of x into the equation $y = m(x + 1)$ to find

$$\begin{aligned} y &= m\left(\frac{1 - m^2 + 1 + m^2}{1 + m^2}\right) \\ &= m\left(\frac{2}{1 + m^2}\right) \\ &= \frac{2m}{1 + m^2}. \end{aligned}$$

Now we know that the other point of intersection is given by

$$(x, y) = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2}\right)$$

Since this point is on the circle given by the equation $x^2 + y^2 = 1$, we have

$$\left(\frac{1 - m^2}{1 + m^2}\right)^2 + \left(\frac{2m}{1 + m^2}\right)^2 = 1.$$

Multiplying both sides by $(1 + m^2)^2$,

$$(1 - m^2)^2 + 4m^2 = (1 + m^2)^2.$$

Since m is a rational number, let $m = v/u$, where u and v are integers. The above equation becomes

$$\begin{aligned} \left(1 - \frac{v^2}{u^2}\right)^2 + \frac{4v^2}{u^2} &= \left(1 + \frac{v^2}{u^2}\right)^2 \\ \left(\frac{u^2 - v^2}{u^2}\right)^2 + \frac{4v^2}{u^2} &= \left(\frac{u^2 + v^2}{u^2}\right)^2. \end{aligned}$$

Finally, multiply both sides by u^4 and we get

$$(u^2 - v^2)^2 + 4v^2u^2 = (u^2 + v^2)^2.$$

This Pythagorean triple generating formula $(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$ doesn't always generate primitive triples. As an extension, come up with conditions on u and v under which the triple generated is primitive.

6. Assume an arithmetic progression of three squares with a common difference that is also a square exists. If we let a^2, b^2, and c^2 be the terms of the sequence and d^2 be the common difference, we have

$$a^2 + d^2 = b^2$$

and

$$b^2 + d^2 = c^2.$$

This implies that

$$\begin{aligned} b^4 &= (a^2 + d^2)(c^2 - d^2) \\ &= a^2c^2 - d^2(a^2 - c^2) - d^4 \end{aligned} \tag{1}$$

Since $a^2 = b^2 - d^2$ and $c^2 = b^2 + d^2$, we have $a^2 - c^2 = b^2 - d^2 - b^2 - d^2 = -2d^2$. Substituting this into (1) yields

$$\begin{aligned} b^4 &= a^2c^2 + 2d^4 - d^4 \\ &= a^2c^2 + d^4 \end{aligned}$$

Let $X = b$, $Y = d$ and $Z = ac$ and rearrange to get the equation

$$X^4 - Y^4 = Z^2.$$

Since this equation has no nonzero integer solutions (and you can try proving this if you are interested), there cannot exist three squares in a arithmetic progression that have a common difference of a square.

7. We could use the formula for primitive triples derived earlier, but it is easier to use Euclid's formula as it was originally written down:

$$(a, b, c) = (2uv, u^2 - v^2, u^2 + v^2)$$

where u and v are coprime integers of different parity. The area of this triangle is $(1/2)ab = uv(u^2 - v^2)$. Assume that this value is a square. The factors of the right-hand side are u, v, $u + v$, and $u - v$; since u and v are coprime, each of those factors are coprime too. Thus we conclude that each of the four factors must be squares themselves, since their product is a square.

Let $u + v = x^2$, $u - v = y^2$, $u = r^2$, and $v = s^2$. Then

$$s^2 + y^2 = r^2$$

and

$$r^2 + s^2 = x^2.$$

Hence y^2, r^2, and x^2 form an arithmetic progression with common difference s^2. From the previous problem we know this is impossible; hence a right-angled triangle with integer length sides cannot have a square area.

You may notice that the question asked for *rational* length sides. Try to determine how the above proof is also (or is not) a proof that a right-angled triangle with rational length sides cannot have a square area.

Melbourne High School
Maths Extension Group 2023
Term 1 Week 8 Handout solutions

1. The octagon is made of 8 congruent triangles each with two side lengths of 1 unit and angle 45° between them. Therefore the area of the octagon is $8 \times (1/2)(\sqrt{2}/2) = 2\sqrt{2}$. Similarly, the square is made up of four triangles, each with two side lengths of 1 unit. Therefore its area is $4 \times (1/2) = 2$. The ratio between the area of the square and the octagon is $1/\sqrt{2}$.

2. The circumference of the circle is 9π, so the angle subtended at the centre by arc BC is 120°. This is double the angle subtended by the same arc at the circumference, so $\angle BAC = 60°$ and $\angle ABC = 30°$. Use the sine ratio to find that $AC = 9/2$, and then use the formula for the area of a triangle to find that the area is $(81\sqrt{3})/8$.

3. The idea is to express π as a continued fraction. Begin by considering the fractional part of π, which is approximately 0.14159. This is approximately equal to $1/7$, so $\pi \approx 3 + (1/7) = 22/7$. This does not give the required number of decimal places yet so we repeat the process; $0.14159... \approx 7 + 0.625133...$ and $0.625133^{-1} \approx 16$. So

$$\pi \approx 3 + \frac{1}{7 + \frac{1}{16}} \approx \frac{355}{113}.$$

   This fraction does approximate π to six decimal places.

4. (a) We see that

$$1 + \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{3}\cdot\frac{1}{3} + \frac{1}{4}\cdot\frac{1}{4} + \cdots < 1 + \frac{1}{1}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{3} + \frac{1}{3}\cdot\frac{1}{4} + \cdots.$$

   The RHS can be expressed as a telescoping that gets closer and closer to 2. Therefore the LHS, the sum we're interested in, converges to a finite value less than 2.

   (b) The solution is given in the question.

   (c) Plugging in $x = 0$ to the RHS gives us

$$1 = a(-\pi^2)(-4\pi^2)(-9\pi^2)(-16\pi^2)\cdots.$$

   Rearranging for a, we get

$$a = \frac{1}{(-\pi^2)(-4\pi^2)(-9\pi^2)(-16\pi^2)\cdots}.$$

   Putting this back into the original equation and distributing each factor in the denominator to the corresponding bracket we get

$$\begin{aligned}\frac{\sin x}{x} &= \frac{1}{-\pi^2}(x^2 - \pi^2)\frac{1}{-4\pi^2}(x^2 - 4\pi^2)\frac{1}{-9\pi^2}(x^2 - 9\pi^2)\cdots \\ &= \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\left(1 - \frac{x^2}{9\pi^2}\right)\cdots.\end{aligned}$$

   (d) The coefficient of x^2 is

$$-\left(\frac{1}{\pi^2} + \frac{1}{4\pi^2} + \frac{1}{9\pi^2} + \cdots\right).$$

   (e) The coefficient of the x^2 term in the original expansion was $-1/6$, so we have

$$\frac{1}{\pi^2} + \frac{1}{4\pi^2} + \frac{1}{9\pi^2} + \cdots = \frac{1}{6}.$$

   Multiplying both sides by π^2 yields the desired result.

5. (a) Note that

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \cdots$$

and so

$$\zeta(s) - \frac{1}{2^s}\zeta(s) = \left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots.$$

Now apply the same process again:

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \cdots$$

and therefore

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \cdots.$$

If we repeat the process over all primes p, we are left with only 1 on the RHS, and therefore

$$\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{7^s}\right)\cdots\zeta(s) = 1.$$

(b) Rearranging for $\zeta(s)$, we have

$$\zeta(s) = \frac{1}{\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{7^s}\right)\cdots}.$$

Plugging in $s = 2$ gives us the desired result.

(c) Two numbers are coprime if they share no common prime factors. The probability that two randomly chosen are not both divisible by a prime p is $1 - 1/p^2$. Multiplying the product over all primes p gives us the a probability of

$$\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{7^s}\right)\cdots.$$

This is just the reciprocal of $\zeta(s)$, so the required probability is $6/\pi^2$.

(d) This is the same as before except that $s = 4$, so the probability is the reciprocal of $\zeta(4) = \pi^4/90$. Therefore the probability is $90/\pi^4$.

Melbourne High School
Maths Extension Group 2023
Term 1 Week 9 Handout Solutions

§1. More combinatorics problems

§2. Euclid's Algorithm

1. Let $g = \gcd(a, b)$. First solve
$$ax - by = g$$
and then multiply the solution by n/g, for if (x', y') satisfies $ax' - by' = g$ then $(x'n/g, y'n/g)$ satisfies
$$\frac{ax'n}{g} - \frac{by'n}{g} = n.$$

2. $(x, y) = (5, 16)$.

3. We get a solution, but the solution is not in positive integers: $(x, y) = (-10, -23)$. To get the solution in positive integers, we argue generally. Suppose $x = x'$ and $y = y'$ are the solutions we have found that are both not positive integers. To make them positive integers, we need to add a number to both without changing the equality sign. We note that
$$7200(x' + M) - 3132(y' + N) = 36$$
if and only if $7200M = 3132N$. Cancelling 36 from both sides we get $200M = 87N$. Therefore we can take $M = 87$ and $N = 200$ (this is the 'smallest' solution because 200 and 87 are coprime).

   Our original solution was $x' = -10$ and $y' = -23$, so our positive integer solution is $(x, y) = (77, 177)$.

4. Let $u = u'$ and $v = v'$ be the integers satisfying the equation
$$ux + vy = \gcd(x, y).$$
Therefore we have
$$a^{\gcd(x,y)} \equiv a^{u'x+v'y} \equiv (a^x)^u (a^y)^v \equiv 1 \cdot 1 \equiv 1 \pmod{n}.$$

5. We want to show that the equations
$$N = am$$
and
$$N + k = bn$$
for integers m and n are soluble. Putting the first into the second we get
$$am + k = bn$$
which implies
$$am - bn = k.$$
This equation is always soluble because a and b are coprime.

6. Suppose that p does not divide a (if it did we have nothing to prove), Our goal now is to show that it divides b.

   If p does not divide a, then it must be coprime with a. Hence there exist positive integers x and y such that

   $$px - ay = 1.$$

   Multiplying both sides by b yields

   $$pbx - aby = b.$$

   Clearly p divides pbx, and by assumption p divides ab, so it must divide aby too. But if p divides both pbx and aby, it must divide their difference, which is b.

Melbourne High School
Maths Extension Group 2023
Term 1 Week 10 Handout Solutions

§1. Problems relating to combinatorial games

§2. Modular arithmetic and congruences

§2.1 Theory and notation

§2.2 Exercises

1. If $a \equiv b \pmod{m}$ then $a-b = km$ for some integer k. Then $b-a = -km$, and hence $b \equiv a$.
   If $b \equiv c$ then let $b-c = mt$ for some integer t. Then $a-c = a-(b-mt) = km+mt = m(k+t)$. Hence $a \equiv c$.

2. A number n in decimal with digits $a_0, a_1, \ldots, a_n$ can be written as
   $$n = a_0 + a_1 10 + \cdots + a_n 10^n.$$
   Since $10 \equiv 1$ modulo 3 and 9,
   $$n \equiv a_0 + a_1 + \cdots + a_n$$
   and hence $n \equiv 0$ if and only if its digit sum is also congruent to 0 modulo 3 or 9.

3. This proof is much the same as the preceding one except that we have
   $$10^n \equiv \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases} \pmod{11}$$
   Therefore
   $$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n.$$
   That is, a number is divisible by 11 if the difference between the sum of all the digits in the even places and the digits in the odd places is divisible by 11. (This is the same thing as saying that divisibility depends on the alternating sum of the digits.)

4. Let $a - b = 2tm$ for some integer t. Then
   $$a^2 = b^2 + 4btm + 4t^2m^2$$
   which implies
   $$a^2 - b^2 = 4m(bt + t^2m).$$
   Therefore $a^2 \equiv b^2 \pmod{4m}$.

   The more general result requires the binomial theorem. Again let $a = tkm + b$ for some integer t. Then by the binomial theorem
   $$\begin{aligned} a^k &= \sum_{i=0}^{k} b^{k-i}(tkm)^i. \\ &= b^k + \binom{k}{1} b^{k-1}(tkm) + \binom{k}{2} b^{k-2}(tkm)^2 + \cdots + (tkm)^k. \\ &= b^k + b^{k-1}(tk^2m) + \binom{k}{2} b^{k-2}(tkm)^2 + \cdots + (tkm)^k. \end{aligned}$$

Hence

$$a^k - b^k = b^{k-1}(tk^2m) + \binom{k}{2} b^{k-2}(tkm)^2 + \cdots + (tkm)^k.$$

Each term on the RHS is clearly divisible by k^2m. This completes the proof.

§2.3 Linear congruences

§2.4 Problems

1. If the cupcake vendor only sells in batches of 97, I need to order $97x$ cupcakes, for some positive integer x. There are only 105 people at my party, and the remainder after everyone eats the same amount needs to be 13. Therefore the linear congruence to solve is

   $$97x \equiv 13 \pmod{105}.$$

   We find that the solution is $x \equiv 64$, which is greater than 50. Therefore I cannot satisfy the needs of my party.

2. Finding the multiplicative inverse a^{-1} is really the same as solving the congruence

   $$ax \equiv 1 \pmod{m},$$

   which has 1 solution when a and m are coprime.

3. From the preceding problem, every number in the list

   $$1, 2, 3, ..., (p-1)$$

   has exactly one multiplicative inverse in the same list. It is clear that apart from 1 and $(p-1)$, each number will not be paired with itself. Hence taking the product of $2, 3, \ldots, (p-2)$ is the same as taking the product of pairs that all are congruent to 1 modulo p; hence

   $$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod{p}.$$

   Multiplying both sides by $p-1$ yields the desired result.

4. Both sets have m numbers, so we only need to show that none of the numbers in the first set are congruent. If $ia \equiv ja \pmod{m}$ for $0 \leq i, j < m$, by the cancellation law we have $i \equiv j \pmod{m}$. But since $0 \leq i, j < m$, we must have $i = j$, and therefore no two numbers in the first set are congruent. This completes the proof.

   Now for the linear congruence. We may assume that b is already a least residue; that is, $0 \leq b < m - 1$. We have already shown that the numbers

   $$0, a, 2a, \ldots, (m-1)a$$

   run through a complete set of least residues, which must include b. Therefore one of those numbers is congruent to b, say $ka \equiv b \pmod{m}$, and this number k is the solution we are looking for.

Melbourne High School
Maths Extension Group 2023
Term 1 Holiday Problems Solutions

1. On the first turn, it is guaranteed that we get an object we haven't selected before, so the expected number of turns needed to get the first distinct object is just 1. After this there are only $n-1$ objects left that we haven't gotten yet, so the probability of getting a new object on the next turn is $(n-1)/n$. Therefore the expected number of turns needed to get that second new object is $n/(n-1)$. Continuing in this way we find that the total expected value is

$$1+\frac{n}{n-1}+\frac{n}{n-2}+\cdots+n=n\left(\frac{1}{n}+\frac{1}{n-1}+\frac{1}{n-2}+\cdots+1\right).$$

2. Since 199 is prime, the number Harold chooses to guaranteed to be coprime with 199. The pages that Harold reads are the numbers

$$x, 2x, 3x, \ldots, 199x$$

reduced modulo 199. Since x is coprime with 199, those numbers have a one-to-one correspondence with the numbers

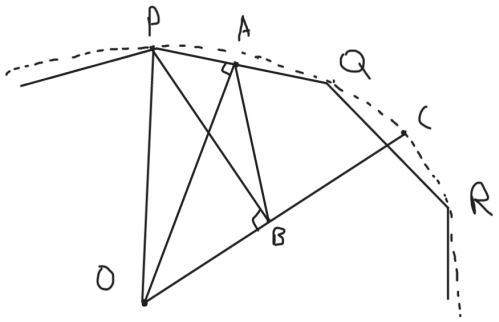
$$1, 2, 3, \ldots, 199$$

because if $jx \equiv kx \pmod{199}$ then $j \equiv k$ by the cancellation law. Therefore Harold is able read every page of the book without reading the same page twice.

3. Since $2^{2^n}+5>3$ and is also 0 mod 3, it is never prime.

4. Since $\angle POQ = \angle QOR = \frac{360^\circ}{9} = 40^\circ$, and C is halfway in between on the circumcircle, so $\angle POC = 60^\circ$ and hence $\triangle OPC$ is equilateral.

   Quadrilateral PABO is cyclic since $\angle PAO = \angle PBO = 90^\circ$. Then $\angle OPB$ and $\angle OAB$ are subtended by the same arc so $\angle OAB = \angle OPB = \frac{60^\circ}{2} = 30^\circ$.



5. Taking $\log_a$ on both sides gives us $a^x \log_a x = x^a$. Since $f(x) = a^x$ and $g(x) = \log_a x$ are decreasing and $h(x) = x^a$ is increasing for $0 < a < 1$, they have one unique solution.

   It follows that $x = a$ is the only solution.

6. Let $n^2-19n+99 = k^2$ for some integer k. If there are solutions to this quadratic in integers, the discriminant must be a perfect square. Rearranging gets us $n^2 - 19n + (99 - k^2) = 0$. Solve using the quadratic formula:

$$n = \frac{19 \pm \sqrt{4k^2 - 35}}{2}.$$

Set $4k^2 - 35 = t^2$ and rearrange to get $(2k - t)(2k + t) = 35$. Checking the factors of 35, we find that $(2k - t, 2k + t) = (1, 35)$ or $(2k - t, 2k + t) = (5, 7)$. These give us $k = 9$ or $k = 3$. Substituting this into the quadratic formula we get the solutions $n = 1, 9, 10, 18$, the sum of which is 38.

7. By the division algorithm we have $\gcd(21n+4, 14n+3) = \gcd(14n+3, 7n+1) = \gcd(7n+1, 1) = 1$. Therefore the fraction is irreducible because the numerator and the denominator share no common factors.

8. Since arithmetic sequences are of the form $a, a + d, \ldots, a + 9d$, we can find the number of 10 element arithmetic sequences by counting the pairs (a, d) such that $a + 9d \leq 2007$. This is equivalent to

$$d \leq \frac{2007 - a}{9}$$

If $1 \leq a \leq 9$, then $d \leq 222$, if $10 \leq a \leq 18$, then $d \leq 221$. Similarly every time a increases by 9, d has one less possible value since the expression $2007 - a$ is being divided by 9.

Continuing until $1990 \leq a \leq 1998$, then $d \leq 1$, we have $9(222+221+\cdots+1) = 9(\frac{222(1+222)}{2}) = 222777$ total 10 element arithmetic sequences.

Now the probability of a subset of 10 random elements in a random colouring being one colour is $1 \times (\frac{1}{4})^9 = \frac{1}{262144}$. Meaning the expected number of monochromatic arithmetic sequences of length 10 is $\frac{222777}{262144}$. Since the expected number of monochromatic arithmetic sequences of length 10 is less than 1, there must be at least 1 sequence that is not all one colour.

9. Extend the segment AK to the circumcircle of BKLC and call the intersection K'; define L' similarly.

Since $\angle AL'B = \angle ACB = \angle ALD$ and $\angle AK'B = \angle BCK = \angle AKD$, we have $\triangle ALD \sim \triangle AL'B(AA)$ and $\triangle ADK \sim ABK'(AA)$.

Now considering the ratio $AK : AL$, we have

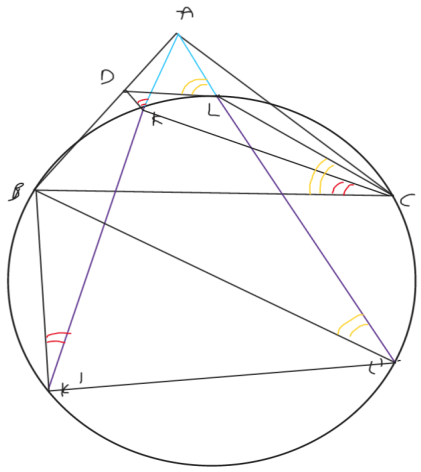
$$(AK : AD) : (AL : AD)$$

$$= (KK' : DB) : (LL' : DB)$$

$$= KK' : LL'$$

Since $KLL'L$ is a trapezium (KL is parallel to $K'L'$ by similar triangles), and is cyclic, it

is isosceles and hence $KK' = LL'$. So $AK : Al = KK' : LL' = 1$ and thus $AK = AL$.



10. (a) Expanding out, we get $(a+b)^2 \equiv a^2 + b^2$, $(a+b)^3 \equiv a^3 + b^3$, and $(a+b)^5 \equiv a^5 + b^5$ to their respective moduli.

    (b) The binomial coefficient

    $$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

    is divisible by p for any prime p when both k and $p-k$ are less than p. This is because in that case the denominator consists only of factors less than p, so the obvious factor of p in the numerator is not cancelled out. Therefore all the terms in the expansion vanish except for the first and last term with binomial coefficients $\binom{p}{0}$ and $\binom{p}{p}$ when computed modulo p.

    (c) In the first bin, we have $\binom{6}{1}$ choices. After the second bin we only have 5 books left, and we need to choose 2, so there are $\binom{5}{2}$ ways. Finally, all remaining 3 books must go into the third bin, so there is $\binom{3}{3} = 1$ way. Multiplying these choices together, we have

    $$\binom{6}{1}\binom{5}{2} = 6 \times 10 = 60$$

    ways of placing the books into the bins.

    (d) Generalising what we did in the previous part the number of ways is

    $$\binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-k_1-k_2}{k_3}\cdot\ldots\cdot\binom{n-k_1-k_2-\cdots-k_{m-2}}{k_{m-1}}\binom{k_m}{k_m}.$$

    (e) Expanding the binomial coefficients we obtained in the previous part gives

    $$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{(n-k_1)!k_1!}\cdot\frac{(n-k_1)!}{(n-k_1-k_2)!k_2!}\cdot\frac{(n-k_1-k_2)!}{(n-k_1-k_2-k_3)!k_3!}\cdot\ldots \cdot\frac{(n-k_1-k_2-\cdots-k_{m-1})!}{0!k_m!}$$

One of the factors of the denominator of each fraction, except for the last, cancels with the numerator of the next (this is the telescoping product), so we are left with

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1!k_2!k_3!\cdots k_m!}.$$

(f)

$$(a+b+c)^3 = a^3 + 3a^2b + 3a^2c + 3ab^2 + 6abc + 3ac^2 + b^3 + 3b^2c + 3bc^2 + c^3$$

The thing to note here is that all possible ways of adding up three numbers to the number 3 are enumerated—this corresponds to all the possible ways of distributing the books among the bins. For example, the $6abc$ term corresponds to putting 1 book in each bin, with the 6 out the front being the multinomial coefficient $\binom{6}{1,1,1}$. The powers of a, b, and c correspond to the 1's.

(g) Generalising the previous example, we see that the sum is taken over all possible ways of adding m numbers $k_1, k_2, \ldots, k_m$ to get the number n, and each term is the corresponding multinomial coefficient multiplied by the terms raised to the corresponding k value. Putting this all together we get the multinomial theorem:

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{k_1+k_2+\cdots+k_m=n} \binom{n}{k_1, k_2, \ldots, k_m} x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}.$$

(h) This might be a bit of a nightmare in notation, so hopefully it is understandable.

We wish to prove the multinomial theorem by induction. The first step, of course, is to show that the base case is true. The case when $m = 1$ is trivial, and when $m = 2$ we have the Binomial Theorem. Therefore we can move onto the inductive step. Suppose that the theorem is true for $m = p$ for some positive integer p. In other words, we have a valid expansion of the sum of p terms all raised to the power of n. Now the trouble is to prove that the theorem is true for $m = p + 1$.

We can rewrite the $m = p + 1$ case in terms of the $m = p$ case, which we know how to handle by the inductive hypothesis. That is, write

$$(x_1 + x_2 + \cdots + x_p + x_{p+1})^n = (x_1 + x_2 + \cdots + (x_p + x_{p+1}))^n.$$

To make what comes next a little easier, let $X_1 = x_1$, $X_2 = x_2$, all the way up to $X_{p-1} = x_{p-1}$. Let $X_p = (x_p + x_{p+1})$. Thus the $m = p + 1$ case becomes $(X_1 + X_2 + \cdots + X_p)^n$. By the inductive hypothesis we can expand this expression as

$$\sum_{K_1+K_2+\cdots+K_p=n} \binom{n}{K_1, K_2, \ldots, K_p} X_1^{K_1} X_2^{K_2} \cdots X_{p-1}^{K_{p-1}} X_p^{K_p}.$$

But $X_p^{K_p} = (x_p + x_{p+1})^{K_p}$, so we can expand the last term using the Binomial Theorem. But we can do better than this. We can actually expand it as the case $m = 2$ of the Multinomial Theorem, which gives us

$$(x_p + x_{p+1})^{K_p} = \sum_{k_p+k_{p+1}=K_p} \binom{K_p}{k_p, k_{p+1}} x_p^{k_p} x_{p+1}^{k_{p+1}}.$$

Putting this into the previous equation gives us

$$\sum_{K_1+K_2+\cdots+K_p=n} \binom{n}{K_1, K_2, \ldots, K_p} X_1^{K_1} X_2^{K_2} \cdots X_{p-1}^{K_{p-1}} \sum_{k_p+k_{p+1}=K_p} \binom{K_p}{k_p, k_{p+1}} x_p^{k_p} x_{p+1}^{k_{p+1}}.$$

Our final leap involves realising that

$$\frac{n!}{K_1!K_2!\cdots K_p!} \cdot \frac{K_p!}{k_p!k_{p+1}!} = \frac{n!}{K_1!K_2!\cdots k_p!k_{p+1}!} = \binom{n}{K_1, K_2, \ldots, k_p, k_{p+1}}.$$

Combining this with the merging of the two summation signs using $K_p = k_p + k_{p+1}$ we get

$$\sum_{K_1+K_2+\cdots+k_p+k_{p+1}=n} \binom{n}{K_1, K_2, \ldots, k_p, k_{p+1}} x_1^{K_1} x_2^{K_2} \cdots x_p^{k_p} x_{p+1}^{k_{p+1}}.$$

The numbers $K_1, K_2, \ldots, k_p, k_{p+1}$ don't have anything special about them except that they sum to n, so we may as well make everything lowercase to be a little nicer in terms of notation. Therefore replacing K_i with k_i we finally reach the end of this glorious induction proof:

$$(x_1+x_2+\cdots+x_p+x_{p+1})^n = \sum_{k_1+k_2+\cdots+k_p+k_{p+1}=n} \binom{n}{k_1, k_2, \ldots, k_p, k_{p+1}} x_1^{k_1} x_2^{k_2} \cdots x_p^{k_p} x_{p+1}^{k_{p+1}}.$$

(i) Proving that all but the first and last multinomial coefficients are divisible by p works too. The proof by induction is in, in some ways, nicer, and uses the same idea as the preceding proof of the multinomial theorem. The base case is done, for we know that $(x_1 + x_2)^2 \equiv x_1^2 + x_2^2 \pmod{p}$ by the Binomial Theorem. Supposing the proposition is true for $m = k$, we find that

$$\begin{aligned}(x_1 + x_2 + \cdots + x_k + x_{k+1})^p &\equiv x_1^p + x_2^p + \cdots + x_{k-1}^p + (x_k + x_{k+1})^p \pmod{p} \\ &= x_1^p + x_2^p + \cdots + x_{k-1}^p + x_k^p + x_{k+1}^p \pmod{p}\end{aligned}$$

Hence the proposition is true for $m = k + 1$, completing the induction.

(j) This theorem is known as *Fermat's Little Theorem*.

$$\begin{aligned}a^p &\equiv (\underbrace{1 + 1 + \cdots + 1}_{a \text{ times}})^p \\ &\equiv \underbrace{1^p + 1^p + \cdots + 1^p}_{a \text{ times}} \pmod{p} \\ &= a \pmod{p}.\end{aligned}$$

11. The way to solve this problem is to consider the expression to the modulus 3 and the modulus 37 first, since $111 = 3 \times 37$. Let $A = (102^{73} + 55)^{37}$. We find that

$$A \equiv 1 \pmod{3}$$

and

$$A \equiv 9 \pmod{37}.$$

Now we need to find some number x such that

$$A \equiv x \pmod 3 \tag{1}$$

and

$$A \equiv x \pmod{37}, \tag{2}$$

for that would mean $A \equiv x \pmod{111}$. (Try proving this yourself—remember that this only works because 3 and 37 are coprime.)

Equation (1) implies that $x = 1 + 3k$ for some integer k. Substitute this into Equation (2) and rearrange to get the linear congruence

$$3k \equiv 8 \pmod{37}.$$

Solving this equation yields $k = 15$. From this we obtain $x = 1+45 = 46$. Therefore $A \equiv 46 \pmod{111}$.

12. (a) Let $P(x) = 1 - x - x^2$. Use the quadratic formula to find that the roots are

$$x_1 = \frac{-1 + \sqrt{5}}{2}$$

and

$$x_2 = \frac{-1 - \sqrt{5}}{2}.$$

If $P(x_1) = 0$ and $P(x_2) = 0$, then $P(1/\alpha) = 0$ and $P(1/\beta) = 0$ if $\alpha = 1/x_1$ and $\beta = 1/x_2$. Therefore $1/\alpha$ and $1/\beta$ are also roots; this implies $P(x)$ can be factorised as $(1 - \alpha x)(1 - \beta x)$. Computing α and β, we find

$$\begin{aligned}\alpha &= \frac{2}{-1 + \sqrt{5}} \\ &= \frac{-2 - 2\sqrt{5}}{1 - 5} \\ &= \frac{1 + \sqrt{5}}{2}\end{aligned}$$

and

$$\begin{aligned}\beta &= \frac{2}{-1 - \sqrt{5}} \\ &= \frac{-2 + 2\sqrt{5}}{1 - 5} \\ &= \frac{1 - \sqrt{5}}{2}.\end{aligned}$$

(b) Multiplying the fraction out and comparing numerators yields

$$A(1 - \beta x) + B(1 - \alpha x) = x.$$

Comparing coefficients, we have $A+B = 0$ and $-A\beta-B\alpha = 1$. Solve the two equations simultaneously to get the desired result.

(c) If

$$H(x) = 1 + x + x^2 + x^3 + \cdots$$

then

$$xH(x) = x + x^2 + x^3 + \cdots = H(x) - 1.$$

Rearrange for $H(x)$ to find that

$$H(x) = \frac{1}{1-x}.$$

(d) At this point we know that

$$G(x) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\right).$$

The fractions in parentheses can be expanded using the formula just derived to get

$$\frac{1}{1-\alpha x} = 1 + \alpha x + (\alpha x)^2 + (\alpha x)^3 + \cdots$$

and

$$\frac{1}{1-\beta x} = 1 + \beta x + (\beta x)^2 + (\beta x)^3 + \cdots.$$

Thus we have

$$\begin{aligned} G(x) &= \frac{1}{\sqrt{5}}\left(\{1 + \alpha x + \alpha^2 x^2 + \alpha^3 x^3 + \cdots\} - \{1 + \beta x + \beta^2 x^2 + \beta^3 x^3 + \cdots\}\right) \\ &= \frac{1}{\sqrt{5}}\left((\alpha^0 - \beta^0) + (\alpha^1 - \beta^1)x + (\alpha^2 - \beta^2)x^2 + (\alpha^3 - \beta^3)x^3 + (\alpha^4 - \beta^4)x^4 + \cdots\right) \\ &= \frac{1}{\sqrt{5}}(\alpha^0 - \beta^0) + \frac{1}{\sqrt{5}}(\alpha^1 - \beta^1)x + \frac{1}{\sqrt{5}}(\alpha^2 - \beta^2)x^2 + \frac{1}{\sqrt{5}}(\alpha^3 - \beta^3)x^3 + \cdots \end{aligned}$$

Comparing coefficients from our original definition of $G(x)$ and substituting in the values for α and β, we derive the formula

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Melbourne High School
Maths Extension Group 2023
Some of Euler's Gems: Solutions

1. (a) Suppose that n is composite and write $n = mp$ for some prime p and integer m. From the formula for the sum of a geometric series, the fraction

$$\frac{2^{pm}-1}{2^m-1}$$

is the sum of the first p terms of a geometric series with first term 1 and common ratio 2^m. That is,

$$\frac{2^{pm}-1}{2^m-1} = 1 + 2^m + 2^{2m} + \cdots + 2^{(p-1)m}.$$

Hence $2^n - 1$ is divisible by $2^m - 1$ and therefore can only be prime if $m = 1$ and $n = p$.

(b)

n	$\sigma(n)$
1	1
2	3
3	4
4	7
5	6
6	12
7	8
8	15
9	13
10	18
11	12
12	28
13	14
14	24
15	24
16	31
17	18
18	39
19	20
20	42

(c) Since m and n are coprime, the divisors of mn are exactly

$$a_1b_1, a_1b_2, \ldots, a_1b_{d(n)}, a_2b_1, \ldots, a_2b_{d(n)}, \ldots, a_{d(m)}b_1, \ldots, a_{d(m)}b_{d(n)}.$$

Hence

$$\begin{aligned}\sigma(mn) &= a_1(b_1 + b_2 + \cdots + b_{d(n)}) + a_2(b_1 + b_2 + \cdots + b_{d(n)}) + \cdots + a_{d(m)}(b_1 + b_2 + \cdots + b_{d(n)}) \\ &= (a_1 + a_2 + \cdots + a_{d(m)})(b_1 + b_2 + \cdots + b_{d(n)}) \\ &= \sigma(m)\sigma(n)\end{aligned}$$

(d) The divisors of p_k are exactly

$$1, p, p^2, \ldots, p^k.$$

Therefore

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

(e) We know that $\sigma(N) = \sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1)$, so we can do each separately. From the preceding exercise we have

$$\sigma(2^{p-1}) = \frac{2^p - 1}{2 - 1} = 2^p - 1.$$

Since $2^p - 1$ is prime, its only divisors are $2^p - 1$ and 1, so

$$\sigma(2^p - 1) = 2^p - 1 + 1 = 2^p.$$

Therefore

$$\sigma(N) = \sigma(2^{p-1}(2^p - 1)) = (2^p - 1)2^p = 2(2^{p-1}(2^p - 1)) = 2N.$$

Therefore $2^{p-1}(2^p - 1)$ is perfect.

(f) If N is even, it divides some power of 2. Let 2^k be the highest power of 2 that divides N; this means $k \geq 1$. Hence $N/2^k$ must be odd; otherwise 2^k would not be the highest power of 2 that divides N. Therefore $N = 2^k m$ for $k \geq 1$ and odd m.

(g) We have

$$\sigma(N) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m).$$

But $\sigma(N) = 2N$ because N is a perfect number, so we have

$$2N = (2^{k+1} - 1)\sigma(m).$$

Clearly $2N = 2^{k+1}m$. Substituting this in yields

$$2^{k+1}m = (2^{k+1} - 1)\sigma(m)$$

as required.

(h) Substituting in $\sigma(m) = 2^{k+1}c$, we get

$$2^{k+1}m = (2^{k+1} - 1)2^{k+1}c.$$

Cancelling 2^{k+1} from both sides we have

$$m = (2^{k+1} - 1)c.$$

(i) If $c > 1$, then m is at least divisible by 1, m, and c. (We note that $m \neq c$ because $k \geq 1$.) Then

$$\sigma(m) \geq 1 + m + c = 1 + (2^{k+1} - 1)c + c = 1 + 2^{k+1}c.$$

(j) But $\sigma(m) = 2^{k+1}c$, so the preceding inequality implies

$$2^{k+1}c \geq 1 + 2^{k+1}c$$

which implies $0 \geq 1$. Clearly this is a contradiction, so $c = 1$.

(k) If $c = 1$ then $\sigma(m) = 2^{k+1} = m + 1$. The number m is at least divisible by itself and 1, so the sum of its divisors is at least $m + 1$, but if $\sigma(m)$ actually equals $m + 1$ then no other number can divide it except for 1 and m; hence m must be prime.

(l) From $m = 2^{k+1} - 1$ we have

$$N = 2^k(2^{k+1} - 1).$$

We know that $2^{k+1} - 1$ is prime, so $k + 1$ must also be prime. If $k + 1$ is prime, then k is one less than a prime, say p. So if we put $k = p - 1$, then we get

$$N = 2^{p-1}(2^p - 1).$$

This completes the proof.

2. (a) Starting from the 1/3 term, we note that $1/3+1/4 > 1/4+1/4 = 1/2$, since $1/3 > 1/4$. Similarly, $1/5 + 1/6 + 1/7 + 1/8 > 1/8 + 1/8 + 1/8 + 1/8 = 1/2$. This can be repeated to infinity to show that

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots > 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots.$$

Clearly the RHS goes to infinity, and therefore the LHS must diverge too.

(b) In the first graph, where the rectangles are underneath the graph, the first rectangle is excluded because $\ln(x)$ is the area under the graph of $1/x$ from 1 to x. So we get $H_n - 1 < \ln(n)$. From the second graph, $H_n > \ln(n)$. Putting these two inequalities together yields

$$\ln(n) < H_n < \ln(n) + 1.$$

(c) We have

$$H_{kn} \approx \ln(kn) + \gamma_1$$

and

$$H_n \approx \ln(n) + \gamma_2.$$

As n approaches infinity, γ_1 and γ_2 will approach the same value, so we have

$$H_{kn} - H_n = \ln(kn) - \ln(n) = \ln(k).$$

i. From the preceding formula, $\ln 2 = H_{2n} - H_n$ as n goes to infinity. At first, it's not obvious how to subtract these two values because the first n terms will disappear. The trick is the same as that of recognising that the even numbers and all the numbers are both still countable infinities even though the even numbers seems to be an infinity that is half as small, in a sense. Countable infinity means that there is a one-to-one correspondence with the positive integers, which the even numbers have. We associate 1 with 2, 2 with 4, 3 with 6 and so on. The same principle applies here. Instead of subtracting in order, we change the order of the series slightly (we're allowed to this because the series is convergent) and subtract a term of H_n from every second term of H_{2n}; in this way an infinite number of terms can be subtracted without losing an infinite number of terms at the beginning. Hopefully this is clear:

$$\begin{aligned}\ln 2 &= 1 + \left(\frac{1}{2} - 1\right) + \frac{1}{3} + \left(\frac{1}{4} - \frac{1}{2}\right) + \frac{1}{5} + \left(\frac{1}{6} - \frac{1}{3}\right) + \cdots \\ &= 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \cdots\end{aligned}$$

ii. Apply the same method as for $\ln 2$.

iii. Apply the same method as for $\ln 2$.

The formula is simply a compact form of the algorithm we use to subtract the two infinite series. From the preceding examples we note that the algorithm consists of doing the subtraction every nth term (if we're calculating $\ln n$). This subtraction is equivalent to multiplying the fraction by $1 - n$. The combination of the floor and ceiling functions evaluate to either 0 or 1 depending on whether k is a multiple of n and therefore determine which fractions to multiply by $1 - n$.

(d) Let

$$\ln(1 + x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots.$$

Putting in $x = 0$ we get $a_0 = 0$. Differentiating both sides yields

$$\frac{1}{(1 + x)} = a_1 + 2a_2 x + 3a_3 x^2 + \cdots.$$

Again putting in $x = 0$, we find that $a_1 = 1$. We continue this process to find the other coefficients. Differentiating again we have

$$\frac{-1}{(1 + x)^2} = 2a_2 + 6a_3 x + \cdots.$$

Putting in $x = 0$ results in $-1 = 2a_2$; hence $a_2 = -1/2$. Eventually we find that $a_3 = 1/3$, $a_4 = -1/4$, and so on, leaving us with

$$\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots.$$

(e) Put $x = -1/t$ and substitute it in to get

$$\ln\left(\frac{t-1}{t}\right) = -\frac{1}{t} - \frac{1}{2t^2} - \frac{1}{3t^3} - \cdots.$$

Flip the fraction in the logarithm on the LHS to get rid of all the minus signs:

$$\ln\left(\frac{t}{t-1}\right) = \frac{1}{t} + \frac{1}{2t^2} + \frac{1}{3t^3} + \cdots.$$

Since the series only makes sense for $|x| < 1$, the restriction on t is that $|-1/t| < 1$. From this $t < -1$ or $t > 1$.

(f)

$$\sum_{k=2}^{n} \ln\left(\frac{k}{k-1}\right) = \sum_{k=2}^{n} \left(\frac{1}{k} + \frac{1}{2k^2} + \frac{1}{3k^3} + \cdots\right)$$

By adding the logarithms on the LHS, we get a telescoping product (or sum if we break the logarithms into the difference of two logarithms) that leaves us with $\ln(n) - \ln(1) = \ln(n)$. By expanding the sum on the RHS, we get

$$\ln(n) = \left(\frac{1}{2} + \frac{1}{2 \cdot 4} + \frac{1}{3 \cdot 8} + \cdots +\right) + \left(\frac{1}{3} + \frac{1}{2 \cdot 9} + \frac{1}{3 \cdot 27} + \cdots\right) + \cdots + \left(\frac{1}{n} + \frac{1}{2n^2} + \frac{1}{3n^3} + \cdots\right).$$

If we take the first term of each bracket, we get the sum

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

which is just $H_n - 1$. Similarly, if we take the second term of each bracket, we get

$$\frac{1}{2 \cdot 4} + \frac{1}{2 \cdot 9} + \frac{1}{2 \cdot 16} + \cdots + \frac{1}{2n^2} = \frac{1}{2}(H_n^{(2)} - 1).$$

The third term of each bracket gives us

$$\frac{1}{3}(H_n^{(3)} - 1).$$

Continuing this rearrangement of the terms, we find that

$$\ln(n) = H_n - 1 + \frac{1}{2}(H_n^{(2)} - 1) + \frac{1}{3}(H_n^{(3)} - 1) + \frac{1}{4}(H_n^{(4)} - 1) + \cdots.$$

(g) The limit of the sum should a number around 0.577216.

3. (a) Each partition of n contributes a unit to the coefficient of x^n. Each infinite sum represents the number of times a particular number appears in the partition—the first bracket represents the number of 1s, the second the number of 2s, the third the number of 3s, and so on. A partition of n is really just selecting a term from each bracket such that the indices add to n when the terms are multiplied. Multiplying out the brackets results in an enumeration of all the possible ways of choosing different terms from each bracket, and therefore each coefficient will be all the ways to partition that number.

(b) The first 6 values of $p(n)$ seem to yield the prime numbers. However, this would-be glorious theorem is destroyed when we find that $p(7) = 15$.

(c) Using the formula

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1 - x}$$

the result follows immediately.

(d) $p_d(7) = 5$.

(e) $p_o(7) = 5$.

(f) From each bracket now we can only choose x^i or 1; this is equivalent to either including i in the partition or not. Whereas before we could choose x^{2i}, x^{3i}, and so on to include more than one of i in the partition, only being able to choose x^i means only one of i ends up in the final partition, and therefore the coefficients of the expanded product are the number of partitions that use only unique numbers.

This generating function is equivalent to finding how many subsets of a set $\{1, 2, 3, \ldots, n\}$ sum to a particular number, since a partition with distinct elements is the same as choosing elements of that set that sum to that particular number.

(g) This generating function can be written as

$$(1 + x + x^2 + x^3 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots)(1 + x^5 + x^{10} + x^{15} + \cdots)\cdots.$$

This is the same as the original generating function except that the brackets determining which even numbers ended up in the partition are missing. Therefore by expanding the brackets only partitions that use odd numbers will be counted in the coefficient of each term.

(h) This problem shows the power of generating functions. If we can manipulate our generating functions so that they are equal, we have completed the proof.

Euler's proof involves transforming each factor in $F_d(x)$ into a fraction using the difference of two squares, as follows.

$$\begin{aligned} F_d(x) &= \frac{(1+x)(1-x)}{1-x} \cdot \frac{(1+x^2)(1-x^2)}{1-x^2} \cdot \frac{(1+x^3)(1-x^3)}{1-x^3} \cdots \\ &= \frac{(1-x^2)(1-x^4)(1-x^6)\cdots}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)\cdots} \\ &= \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots} \\ &= F_o(x) \end{aligned}$$

Melbourne High School
Maths Extension Group 2023
Term 2 Week 5 Handout Solutions

The Fundamental Theorem of Arithmetic

1. (a) If the divisors of m are

$$a_1, a_2, \dots, a_r$$

and the divisors of n are

$$b_1, b_2, \dots, b_s$$

the divisors of mn are exactly all the products of all pairs of a's and b's. Therefore

$$\begin{aligned}\sigma(mn) &= a_1 \sum_{k=1}^{s} b_k + a_2 \sum_{k=1}^{s} b_k + \cdots + a_r \sum_{k=1}^{s} b_k \\ &= \sum_{k=1}^{r} a_k \cdot \sum_{k=1}^{s} b_k \\ &= \sigma(m)\sigma(n).\end{aligned}$$

(b) Since

$$\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$$

the formula for $\sigma(n)$ is just the product of these terms for all powers of primes that divide n. Therefore if

$$n = \prod_{k=1}^{r} p_k^{a_k}$$

then

$$\sigma(n) = \prod_{k=1}^{r} \frac{p_k^{a_k+1}-1}{p_k-1}.$$

2. (a) Let p be a prime and a be a number less than p. Suppose that the proposition is false and that there exist numbers $x \equiv b, b', b'', \dots$ all less than p such that

$$ax \equiv 0 \pmod{p}.$$

Let b be the smallest of these.

Since $b < p$, it must be that p lies between two successive multiples of b; that is, there exists some m such that

$$bm < p < b(m+1).$$

From $bm < p$ it follows that $p - bm > 0$, and from $p < bm + b$ it follows that $p - bm < b$. Put $c = p - bm$. Then we have $0 < c < b$. But

$$ac \equiv a(p - bm) \equiv ap - abm \equiv 0 \pmod{p}$$

because clearly $ap \equiv 0$, and by hypothesis $ab \equiv 0$ too. Therefore $ac \equiv 0$, which contradicts the minimality of b because $c < b$. This contradiction completes the proof.

(b) If $a \not\equiv 0$ and $b \not\equiv 0$, their least positive residues, say α and β, are also not congruent to 0. If

$$ab \equiv 0 \pmod{p}$$

then

$$\alpha\beta \equiv 0 \pmod{p},$$

but this contradicts the previous result as $0 < \alpha, \beta < p$.

3. (a) Let the two sets of prime factors be arranged in ascending order, so that

$$p_1 < p_2 < \cdots < p_r$$

and

$$q_1 < q_2 < \cdots < q_s.$$

None of the p's can be a q because otherwise it could be cancelled out, and we know the resulting number cannot have two different factorisations because it is smaller than n. Therefore either $p_1 < q_1$ or $q_1 < p_1$. Since $p_1^2 \leq n$ and $q_1^2 \leq n$, we have $p_1 q_1 < n$, which implies $n - p_1 q_1 > 0$.

(b) Since both p_1 and q_1 divide n, they also divide $N = n - p_1 q_1$. Rearranging for n, we get $n = N + p_1 q_1$, and so $p_1 q_1$ divides n.

(c) If $p_1 q_1$ divides n, then q_1 divides $p_2 \ldots p_r$. This is impossible because n/p_1, being less than n, has a unique factorisation consisting of exactly those primes p_2 up to p_r, and since no q is a p, it cannot be that q_1 occurs in the factorisation. This contradiction completes the proof.

Melbourne High School
Maths Extension Group 2023
Term 2 Week 6 Handout Solutions

Fermat's Little Theorem

1. We aim to show that the congruence

$$a^p \equiv a \pmod{p}$$

holds for all a. Clearly $0^p \equiv 0$ and $1^p \equiv 1$. Assume that the congruence holds for $a = k$.

We need to know how to expand $(k+1)^p$ for the inductive step. By the Binomial Theorem

$$(k+1)^p = \sum_{i=0}^{p} \binom{p}{i} k^i.$$

The Binomial coefficient

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}$$

is divisible by p for $0 < n < p$, because $n!$ and $(p-n)!$ are both coprime with p, and so after simplifying the fraction, a factor of p in the $p!$ term remains. Consequently, when considering the expression $(k+1)^p$ modulo p, all the middle terms of the expansion vanish, leaving us with

$$(k+1)^p \equiv k^p + 1^p \pmod{p}.$$

Applying the induction hypothesis, which is that $k^p \equiv k$, we get

$$(k+1)^p \equiv k + 1 \pmod{p}$$

which completes the induction.

2. Since a and m are coprime, the numbers

$$ak_1, ak_2, \ldots, ak_{\phi(m)}$$

reduced modulo m are the numbers

$$k_1, k_2, \ldots, k_{\phi(m)}$$

in some order. The argument is the same as that of Ivory's proof of Fermat's Little Theorem. All the numbers in the first set are clearly coprime with m, and no two are congruent, for if $ak_i \equiv ak_j$ then $k_i \equiv k_j$. Therefore both sets are $\phi(m)$ numbers that are coprime with m, meaning that when both are reduced modulo m, they must be the same sets.

From this we conclude that

$$ak_1 \cdot ak_2 \cdots ak_{\phi(m)} \equiv k_1 \cdot k_2 \cdots k_{\phi(m)} \pmod{m}.$$

On the LHS we have $\phi(m)$ copies of a; hence

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} k_i \equiv \prod_{i=1}^{\phi(m)} k_i \pmod{p}.$$

The product of the k's may be cancelled from both sides as it is clearly coprime with m, and therefore

$$a^{\phi(m)} \equiv 1 \pmod{p}.$$

Melbourne High School
Maths Extension Group 2023
Term 2 Week 7 Handout Solutioins

Lagrange's Theorem

1. In the proof, we reasoned that this factorisation process eventually results in all the roots; this reasoning assumes that if

$$f(x) \equiv g(x)h(x) \pmod{p}$$

and $f(r) \equiv 0$ then $g(r) \equiv 0$ or $h(r) \equiv 0$. This is only true when the modulus is prime; the idea is the same as that of Euclid's Lemma. Recall that Euclid's Lemma states if a prime divides a product of two numbers, the prime must divide at least one of the two numbers. In the notation of modular arithmetic, it states that if $ab \equiv 0 \pmod{p}$ then $a \equiv 0$ or $b \equiv 0$. Note that this is not true when the modulus is composite. A simple example: 6 divides $12 = 3 \times 4$, but it divides neither 3 nor 4. So if the modulus was not prime in our proof of Lagrange's Theorem, at the point where we have

$$f(x) \equiv (x - r)g(x) \pmod{p},$$

if p was a composite number, there might be a root of f that is neither a root of $x - r$ or $g(x)$, which means we have failed to count it.

When the modulus is prime, it is guaranteed that any further root of f that is not r is a root of g, and hence the factorisation argument correctly leads to a maximum of d roots.

2. Since $x \equiv r_1$ is a root, write

$$f(x) \equiv (x - r_1)g(x) \pmod{p}$$

where $g(x)$ is some polynomial of degree $d - 1$. Since all of the roots $r_1, r_2, \ldots, r_{d+1}$ are distinct, all of $r_2, \ldots, r_{d+1}$ must be roots of g (here is where we use the assumption that p is prime). This is a contradiction because it means that g) has d roots but its degree is $d - 1$, and we have assumed that f is the polynomial with smallest degree that has more roots that its degree. This contradiction completes the proof.

3. (a) Since $p - 1 = dd'$ we have

$$x^{p-1} - 1 = x^{dd'} - 1 = y^{d'} - 1.$$

It is handy to know that a polynomial of this form, $y^{d'} - 1$, can be factorised as

$$y^{d'} - 1 = (y - 1)(y^{d'-1} + y^{d'-2} + \cdots + 1).$$

The factorisation follows at once from the geometric series formula

$$1 + a + a^2 + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}$$

by multiplying both sides by $a - 1$.

(b) The degree of $y - 1 = x^d - 1$ is d, and the degree of $x^{p-1} - 1$ is $p - 1$, so the degree we're looking for is $p - 1 - d$.

(c) Let

$$f(x) = y^{d'-1} + y^{d'-2} + \cdots + 1.$$

By Lagrange's Theorem, $x^d - 1 \equiv 0$ has at most d solutions while f has at most $p - 1 - d$ solutions. Since $x^{p-1} - 1 \equiv 0$ has exactly $p - 1$ solutions, $x^d - 1$ must have at least $p - 1 - (p - 1 - d) = d$ solutions. Hence

$$x^d - 1 \equiv 0 \pmod{p}$$

must have exactly d solutions.

Melbourne High School
Maths Extension Group 2023
Term 3 Week 4 Handout Solutions

Quadratic Residues

1. Enumerating the squares modulo 17, the squares are $1, 4, 9, 16, 8, 2, 15, 13$. Since $16 \equiv -1$ the congruence is solvable.

2. (a) If a and b are both nonresidues, then $(a|p) = -1$ and $(b|p) = -1$. But ab is a residue, so $(ab|p) = 1 = (a|p)(b|p)$. If both a and b are residues, then $(a|p) = 1$, $(b|p) = 1$, and $(ab|p) = 1$; and again $(ab|p) = (a|p)(b|p)$. For the last case, we may assume with loss of generality that $(a|p) = -1$ and $(b|p) = 1$; then $(ab|p) = -1 = (a|p)(b|p)$ and the proof is complete.

   (b) If $(a|p) = 1$ and $a \equiv x^2 \pmod{p}$, then it follows that $b \equiv x^2$ also if $a \equiv b$. Thus $(a|p) = (b|p)$. If $(a|p) = -1$, suppose that there exists some x such that $b \equiv x^2 \pmod{p}$. But since $b \equiv a$ that would mean $a \equiv x^2$, which is a contradiction. Hence no such x exists, and so $(a|p) = -1 = (b|p)$.

3. From a property of the Legendre symbol we have

$$\left(\frac{-1}{p}\right) = \left(\frac{(p-1)!}{p}\right).$$

   The number $(p-1)!$ consists of the product of all the numbers from 1 to $p-1$. We know that amongst those numbers exactly $(p-1)/2$ of them are quadratic residues and exactly $(p-1)/2$ of them are quadratic nonresidues. The product of the quadratic residues will give a quadratic residue, so whether $(p-1)!$ is a residue or nonresidue depends only on whether the product of the $(p-1)/2$ nonresidues gives a residue or nonresidue. Recall that the product of two nonresidues gives a residue; hence if the number of nonresidues is even, the resulting product will be a residue, and if the number of nonresidues is odd, then the resulting product will be a nonresidue. When is $(p-1)/2$ even and when is it odd? If it is to be even, then $p-1$ must be a multiple of 4, and hence $p \equiv 1 \pmod{4}$. If it is to be odd, then $p-1$ must an odd multiple of 2, so that that $(p-1)/2$ is not further divisible by 2. Hence $p - 1 = 2(2k+1)$ from which it follows that $p = 4k+3$, or $p \equiv 3 \pmod{4}$. Hence

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}; \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

   Observe that since $(-1|p)$ depends on whether the number of nonresidues $(p-1)/2$ is even or odd, the result can be also be written more succinctly as

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Melbourne High School
Maths Extension Group 2023
Term 3 Week 5 Handout Solutions

Euler's Criterion

1. We observe that

$$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$$

since $p - a \equiv -a \pmod{p}$. If $p \equiv 1 \pmod{4}$ then $(-1|p) = 1$, and so

$$\left(\frac{p-a}{p}\right) = \left(\frac{a}{p}\right).$$

If $p \equiv 3 \pmod{4}$ then $(-1|p) = -1$, and so

$$\left(\frac{p-a}{p}\right) = -\left(\frac{a}{p}\right).$$

This completes the proof.

2. Let $P = (p-1)/2$ and α be the index of a for some primitive root of p that we shall call g. From Fermat's Little Theorem we know that either

$$a^P \equiv 1 \pmod{p}$$

or

$$a^P \equiv -1 \pmod{p};$$

the goal here is to prove that the distinction between the two cases is exactly the distinction between $(a|p) = 1$ and $(a|p) = -1$.

First consider the case where $(a|p) = 1$. Then $a^P \equiv g^{\alpha P} \pmod{p}$. Since $(a|p) = 1$, it follows that α is even and therefore that αP is a multiple of $p - 1$. We know that g raised to any multiple of $p - 1$ is unity, so

$$a^P \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

If $(a|p) = -1$, then α is odd, and so αP cannot be a multiple of $p - 1$. Since g is a primitive root, the only powers of g that are congruent to unity are the multiples of $p - 1$, and so $g^{\alpha P} \not\equiv 1$; hence

$$a^P \equiv g^{\alpha P} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

This completes the proof of Euler's Criterion.

3. Since $p = 4k + 1$, we have $p - 1 = 4k$. By Wilson's Theorem

$$(p-1)! \equiv (4k)! \equiv -1 \pmod{p}.$$

Notice that $4k \equiv -1$, $4k - 1 \equiv -2$, $4k - 2 \equiv -3$, and so on, all the way down to $2k + 1 \equiv -2k$, so we actually have

$$1 \times (-1) \times 2 \times (-2) \times \cdots \times 2k \times (-2k) \equiv -1 \pmod{p}$$

which becomes

$$(2k)!^2 \equiv -1 \pmod{p}.$$

The solution to the congruence is therefore $x \equiv \pm(2k)! \pmod{p}$.

Part II

SEHS Maths Games Day

Mixed School Problem Solving Questions

1. Define the "reverse" of a number to be the same digits written backwards. For example, the reverse of 135 is 531, and the reverse of 4630 is 0364.

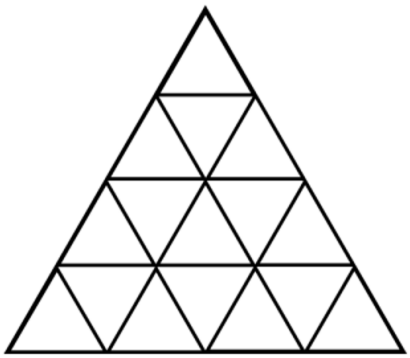
   Prove that the sum of any four-digit number and its reverse is divisible by 11.

   Hint: Represent the 4-digit number as $ABCD$.

2. (a) Suppose you have an analogue clock with an hour hand and a minute hand. If it is currently midnight, at what time will the two hands form a right angle? Give your answer to the nearest second, in the form HH:MM:SS.

   (b) How many times will the hour and minute hand form a right-angle over the course of 24 hours?

3. How many triangles are there in the image below?



4. (a) Find the smallest integer x such that $480x$ is a perfect square.

   (b) What is the general strategy to find the smallest integer x such that $N \times x$ is a perfect square for positive integer N?

5. (a) Prove that there is no smallest positive number.

   (b) Explain why there is no biggest number.

6. (a) Must a quadratic pass through the x axis? Why or why not?

   (b) Must a cubic pass through the x axis? Why or why not?

7. The scales at Jasper's house only work if two people weigh themselves at the same time. He has four people in his house who weigh themselves in pairs obtaining 89kg, 105kg, 112kg, 113kg, 120kg and 136kg. What is the difference between the weights of the heaviest and lightest people in the house?

Year 9

1. (2 points) Three consecutive numbers sum to 141. What are the numbers?

   Total for Question 1: 2

2. (3 points) There are twelve lockers, numbered from 110 to 121. The keys to these twelve lockers are numbered 1 to 12. Each locker number is divisible by the number on its key.

   Determine the key number for each locker.

   Total for Question 2: 3

3. In an AFL game, a goal is worth 6 points and a behind is worth 1 point.
   (a) (1 point) How many points does a team have if they score 4 goals and 8 behinds?
   (b) (2 points) How many different ways are there to score some number of goals and some number of behinds such that the score is the product of the number of goals and the number of behinds?
   (c) (2 points) By considering a graph, show that you have found all the ways that this could occur.

   Total for Question 3: 5

4. (a) (2 points) What is the area of the largest square that can fit inside a unit circle?
   (b) (2 points) What is the area of the largest circle that can fit inside a unit square?
   (c) (3 points) A triangle is placed inside a unit square so that of its vertices either lie on the square's edges or inside the square. What areas are possible for this triangle?
   (d) (2 points) What is the side length of the largest square that can fit inside an equilateral triangle that has side length 1 unit?

   Total for Question 4: 9

5. (3 points) What is the volume of a regular tetrahedron with side length 1 unit?

   Total for Question 5: 3

6. (a) (1 point) How many positive integer solutions are there to the equation $2x + 3y = 25$?
   (b) (2 points) How many integer solutions are there to the equation $2x + 3y = 25$?
   (c) (2 points) How many integer solutions are there to the equation $51x+24y = 17$?
   (d) (1 point) Consider the expression $9x + 15y$. Put in as many integer values of x and y as you can. Which number are all the resulting numbers multiples of?
   (e) (2 points) When does the equation $ax + by = c$ always have integer solutions?

   Total for Question 6: 8

7. (a) (2 points) When is the sum of 2 consecutive numbers divisible by 2?
   (b) (2 points) When is the sum of 3 consecutive numbers divisible by 3?

(c) (2 points) When is the sum of 4 consecutive numbers divisible by 4?

(d) (2 points) When is the sum of 5 consecutive numbers divisible by 5?

(e) (2 points) When is the sum of n consecutive numbers divisible by n?

Total for Question 7: 10

8. (a) (1 point) Two lines can divide the plane into at most how many regions?

   (b) (1 point) Three lines can divide the plane into at most how many regions?

   (c) (1 point) If we add a fourth line, what is the maximum number of intersection points that line can make with the existing lines?

   (d) (1 point) Four lines can divide the plane into at most how many regions?

   (e) (3 points) What is the maximum number of regions that n lines can divide the plane into?

Total for Question 8: 7

9. (3 points) Prove it is possible to pair up the numbers $0, 1, 2, 3, \ldots, 61$ in such a way that when we sum each pair, the product of the 31 numbers we get is a perfect fifth power.

Total for Question 9: 3

Total: 50

Year 10

1. (3 points) There are twelve lockers, numbered from 110 to 121. The keys to these twelve lockers are numbered 1 to 12. Each locker number is divisible by the number on its key.

   Determine the key number for each locker. Total for Question 1: 3

2. (2 points) Three consecutive numbers sum to 141. What are the numbers?

   Total for Question 2: 2

3. (a) (2 points) When is the sum of 2 consecutive numbers divisible by 2?
   (b) (2 points) When is the sum of 3 consecutive numbers divisible by 3?
   (c) (2 points) When is the sum of 4 consecutive numbers divisible by 4?
   (d) (2 points) When is the sum of 5 consecutive numbers divisible by 5?
   (e) (2 points) When is the sum of n consecutive numbers divisible by n?

   Total for Question 3: 10

4. (3 points) Prove it is possible to pair up the numbers $0, 1, 2, 3, \ldots, 61$ in such a way that when we sum each pair, the product of the 31 numbers we get is a perfect fifth power. Total for Question 4: 3

5. (a) (1 point) Two lines can divide the plane into at most how many regions?
   (b) (1 point) Three lines can divide the plane into at most how many regions?
   (c) (1 point) If we add a fourth line, what is the maximum number of intersection points that line can make with the existing lines?
   (d) (1 point) Four lines can divide the plane into at most how many regions?
   (e) (3 points) What is the maximum number of regions that n lines can divide the plane into?

   Total for Question 5: 7

6. (a) (2 points) Is the sum or difference of two rational numbers always rational? Why or why not?
   (b) (2 points) Is the product or quotient of two rational numbers always rational? Why or why not?
   (c) (2 points) When one rational number is raised to another is the result guaranteed to be rational?
   (d) (3 points) It is known that $\sqrt{2}$ is irrational, but it is not known whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational. Do there exist two irrational numbers such that when one is raised to the other the result is rational? Prove your conjecture.

   Total for Question 6: 9

7. (a) (2 points) Prove that $x^2 + y^2 \geq 2xy$ for real numbers x, y.
   (b) (2 points) Prove that $2a^2 + b^2 + c^2 \geq 2(ab + ac)$ for real numbers a, b, c.

(c) (2 points) Prove that $3(a^2 + b^2 + c^2 + d^2) \geq 2(ab + ac + ad + bc + bd + cd)$ for real numbers a, b, c, d.

(d) (3 points) Real numbers a, b, c, d, e are linked by the two equations:

$$e = 40 - a - b - c - d$$

$$e^2 = 400 - a^2 - b^2 - c^2 - d^2$$

Determine the largest value for e.

Total for Question 7: 9

8. (a) (1 point) How many ways are there to create a two-element subset from the set $\{1, 2, 3, 4\}$?

(b) (2 points) How many ways are there to split the set $\{1, 2, 3, 4\}$ into two disjoint nonempty sets? (Disjoint means the two sets share no elements.) For example, if we had the set $\{1, 2, 3\}$ a valid splitting would be $\{1, 2\}$ and $\{3\}$.

(c) (2 points) How many ways are there to split the set $\{1, 2, 3, 4, 5\}$ into two disjoint nonempty sets?

(d) (2 points) Denote by $S(n, k)$ the number of ways to split a set of n elements into k disjoint nonempty sets. Suppose we know what $S(n - 1, 2)$ is. What happens when we add another element to the set? What happens to each of the $S(n - 1, 2)$ ways to do the partitioning?

(e) (2 points) What is $S(n, 2)$?

(f) (3 points (bonus)) If there are $S(n - 1, k - 1)$ ways to partition a set of $n - 1$ elements into $k-1$ nonempty disjoint sets, what is $S(n, k)$ in terms of $S(n-1, k)$ and $S(n - 1, k - 1)$?

Total for Question 8: 9

Total: 52

Year 11/12

1. (3 points) There are twelve lockers, numbered from 110 to 121. The keys to these twelve lockers are numbered 1 to 12. Each locker number is divisible by the number on its key.

   Determine the key number for each locker.

   Total for Question 1: 3

2. (a) (1 point) Two lines can divide the plane into at most how many regions?
   (b) (1 point) Three lines can divide the plane into at most how many regions?
   (c) (1 point) If we add a fourth line, what is the maximum number of intersection points that line can make with the existing lines?
   (d) (1 point) Four lines can divide the plane into at most how many regions?
   (e) (3 points) What is the maximum number of regions that n lines can divide the plane into?

   Total for Question 2: 7

3. (a) (1 point) How many ways are there to create a two-element subset from the set $\{1, 2, 3, 4\}$?
   (b) (2 points) How many ways are there to split the set $\{1, 2, 3, 4\}$ into two disjoint nonempty sets? (Disjoint means the two sets share no elements.) For example, if we had the set $\{1, 2, 3\}$ a valid splitting would be $\{1, 2\}$ and $\{3\}$.
   (c) (2 points) How many ways are there to split the set $\{1, 2, 3, 4, 5\}$ into two disjoint nonempty sets?
   (d) (2 points) Denote by $S(n, k)$ the number of ways to split a set of n elements into k disjoint nonempty sets. Suppose we know what $S(n-1, 2)$ is. What happens when we add another element to the set? What happens to each of the $S(n-1, 2)$ ways to do the partitioning?
   (e) (2 points) What is $S(n, 2)$?
   (f) (3 points (bonus)) If there are $S(n-1, k-1)$ ways to partition a set of $n-1$ elements into $k-1$ nonempty disjoint sets, what is $S(n, k)$ in terms of $S(n-1, k)$ and $S(n-1, k-1)$?

   Total for Question 3: 9

4. (a) (2 points) Is the sum or difference of two rational numbers always rational? Why or why not?
   (b) (2 points) Is the product or quotient of two rational numbers always rational? Why or why not?
   (c) (2 points) When one rational number is raised to another is the result guaranteed to be rational?
   (d) (3 points) It is known that $\sqrt{2}$ is irrational, but it is not known whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational. Do there exist two irrational numbers such that when one is raised to the other the result is rational? Prove your conjecture.

   Total for Question 4: 9

5. (a) (1 point) If two normal six-sided dice are rolled, what is the probability that the sum of the two numbers is 2?

   (b) (1 point) If two normal six-sided dice are rolled, what is the probability that the sum of the two numbers is 7?

   (c) (2 points) Consider a biased six-sided die in which the probability of rolling n is p_n. This die is rigged so that when two of them are rolled, every possible sum of the two numbers is equally likely. What is p_2 in terms of p_1?

   (d) (1 point) What is p_3 in terms of p_1?

   (e) (2 points) What is p_4 in terms of p_1? Do you notice a pattern?

   (f) (2 points) Let $p_i = a_{i-1}p_1$. So $a_0 = 1$, $p_2 = a_1p_1$, $p_3 = a_2p_1$, $p_4 = a_3p_1$ and so on. What are $a_0a_1 + a_1a_0$, $a_0a_2 + a_1a_1 + a_2a_0$, $a_0a_3 + a_1a_2 + a_2a_1 + a_3a_0$, etc. all equal to?

   (g) (1 point) Since we have a six-sided die,

$$p_1 + p_2 + \cdots + p_6 = 1.$$

   What is p_1 in terms of $a_0, a_1, a_2, \ldots, a_5$?

   (h) (2 points) Let $s_i = a_0 + a_1 + \cdots + a_i$. What are s_0, s_1, s_2? What is s_5?

   (i) (3 points) Is such a six-sided die possible?

Total for Question 5: 15

6. (a) (1 point) What is $1 + 2 + 3 + \cdots + 200$?

   (b) (2 points) Find a formula for $1 + 2 + \cdots + n$ and prove it.

   (c) (1 point) Define

$$F_k(n) = 1^k + 2^k + \cdots + n^k.$$

   (So in the previous part you found a formula for $F_1(n)$.) More compactly it may be written as

$$F_k(n) = \sum_{i=1}^{n} i^k.$$

   What is

$$1^3 + (2^3 - 1^3) + (3^3 - 2^3) + \cdots + (100^3 - 99^3)?$$

   (d) (2 points) By considering

$$1^3 + \sum_{i=1}^{n}((i+1)^3 - i^3)$$

   find a formula for $F_2(n)$.

   (e) (2 points) Find a formula for $F_3(n)$.

   (f) (1 point) The Binomial Theorem states that

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

If

$$(i+1)^k - i^k = \sum_{j=0}^{x} \binom{k}{j} i^j$$

what is x in terms of k?

(g) (3 points) By considering the general telescoping sum

$$1^k + \sum_{i=1}^{n} ((i+1)^k - i^k) = (n+1)^k$$

show that

$$F_{k-1}(n) = \frac{(n+1)^k - 1}{k} + \frac{1}{k} \sum_{i=0}^{k-2} \binom{k}{i} F_i(n).$$

Total for Question 6: 12

Total: 55

Mixed School Problem Solving Questions

1. Express the four digit number as $ABCD$, then

$$1000A + 100B + 10C + D + 1000D + 100C + 10B + A = 11(91A + 10B + 10C + 91D).$$

2. Solve $6x - 0.5x = 90$
3. Counting gives 27.
4. a) $x = 30$
5. a) Let $\frac{p}{q}$ be the smallest element, then $\frac{p}{2q} < \frac{p}{q}$ and we have a contradiction.
b) If n is the biggest number then $n + 1$ is bigger.
6. a) no b) yes
7. Let the weights be $a \leq b \leq c \leq d$. Then $a + b = 89$ since it is the smallest sum, $b + d = 120$ since it is the second largest sum. Hence $d - a = b + d - (a + b) = 120 - 89 = 31kg$. (The possible weights are 41, 48, 64, 72 or 40.5, 48.5, 64.5, 71.5.)

Year 9

1. (2 points) Three consecutive numbers sum to 141. What are the numbers?

   Solution: $46, 47, 48$

2. (3 points) There are twelve lockers, numbered from 110 to 121. The keys to these twelve lockers are numbered 1 to 12. Each locker number is divisible by the number on its key.

   Determine the key number for each locker.

   Solution:

110	111	112	113	114	115	116	117	118	119	120	121
10	3	8	1	6	5	4	9	2	7	12	11

3. In an AFL game, a goal is worth 6 points and a behind is worth 1 point.

   (a) (1 point) How many points does a team have if they score 4 goals and 8 behinds?

   Solution: 32

   (b) (2 points) How many different ways are there to score some number of goals and some number of behinds such that the score is the product of the number of goals and the number of behinds?

   Solution: The problem boils down to finding solutions to the equation $6x + y = xy$. There are 5 solutions for nonnegative integers x and y but accept if trivial solution $(0, 0)$ is not given.

   (c) (2 points) By considering a graph, show that you have found all the ways that this could occur.

   Solution: Rearrange the equation to get

   $$y = \frac{6x}{x-1}.$$

   Via s simple algebraic manipulation we get

   $$y = 6 + \frac{6}{x-1}.$$

   The 4 solutions obtained through enumeration are $(2, 12)$, $(3, 9)$, $(4, 8)$, $(7, 7)$. For $x > 7$ the denominator of the fraction becomes greater than 6 and therfore y cannot be an integer. Hence there are no solutions for $x > 7$ and thus we have found all the solutions.

4. (a) (2 points) What is the area of the largest square that can fit inside a unit circle?

Solution: The diagonal of the square is the diameter of the circle, which is 2. Therefore the side length of the square is $\sqrt{2}$ units, meaning the area is 2 square units.

(b) (2 points) What is the area of the largest circle that can fit inside a unit square?

Solution: The radius of the circle is half the side length of the square, so the radius is 1/2. The area of the circle is therefore $\pi(1/2)^2 = \pi/4$.

(c) (3 points) A triangle is placed inside a unit square so that of its vertices either lie on the square's edges or inside the square. What areas are possible for this triangle?

Solution: It is possible for the triangle to have an area of 1/2, as that occurs when all three vertices are three vertices of the square. Therefore it can plainly have any area between 0 and 1/2. Can it have an area that is greater than 1/2? The answer is no.

(d) (2 points) What is the side length of the largest square that can fit inside an equilateral triangle that has side length 1 unit?

Solution: Let x be the sidelength of the square. By similar triangles we can deduce that

$$\frac{2x}{1-x} = \sqrt{3}.$$

Solving this equation gives $x = 2\sqrt{3} - 3$.

5. (3 points) What is the volume of a regular tetrahedron with side length 1 unit?

Solution: The volume of a pyramid is 1/3 multiplied by the area of its base times its height. Using Pythagoras' Theorem we can deduce that the height of a unit tetrahedron is $\sqrt{2/3}$. The area of the base of the tetrahedron is the area of an equilateral triangle with sidelength 1, which is $(1/2)(\sqrt{3}/2) = \sqrt{3}/4$. Therefore the area of the unit regular tetrahedron is $(1/3) \times (\sqrt{3}/4) \times \sqrt{2/3} = \sqrt{2}/12$.

6. (a) (1 point) How many positive integer solutions are there to the equation $2x + 3y = 25$?

Solution: Enumerating the cases and counting gives 4 solutions.

(b) (2 points) How many integer solutions are there to the equation $2x + 3y = 25$?

Solution: There are infinitely many integer solutions.

(c) (2 points) How many integer solutions are there to the equation $51x + 24y = 17$?

Solution: There are no integer solutions because every number of the form $51x + 24y$ is a multiple of the greatest common divisor of 51 and 24, which is 3.

(d) (1 point) Consider the expression $9x + 15y$. Put in as many integer values of x and y as you can. Which number are all the resulting numbers multiples of?

Solution: The resulting numbers are multiples of 3.

(e) (2 points) When does the equation $ax + by = c$ always have integer solutions?

Solution: The equation has integer solutions only when c is a multiple of the greatest common divisor of a and b.

7. (a) (2 points) When is the sum of 2 consecutive numbers divisible by 2?

Solution: Never, because $n + (n + 1) = 2n + 1$ is odd.

(b) (2 points) When is the sum of 3 consecutive numbers divisible by 3?

Solution: Always, as $n + (n + 1) + (n + 2) = 3n + 3$.

(c) (2 points) When is the sum of 4 consecutive numbers divisible by 4?

Solution: Never, as $n + (n + 1) + (n + 2) + (n + 3) = 4n + 10 \equiv 2 \pmod 4$.

(d) (2 points) When is the sum of 5 consecutive numbers divisible by 5?

Solution: Always, as $n + (n + 1) + (n + 2) + (n + 3) + (n + 4) = 5n + 10$.

(e) (2 points) When is the sum of n consecutive numbers divisible by n?

Solution: The sum of n consecutive numbers starting from k is kn plus the $n - 1$th triangular number, so it is

$$n\left(k + \frac{n-1}{2}\right).$$

The resulting number is divisible by n if $(n - 1)/2$ is an integer, and that is when n is odd.

8. (a) (1 point) Two lines can divide the plane into at most how many regions?

Solution: 4

(b) (1 point) Three lines can divide the plane into at most how many regions?

Solution: 7 (If you try it on paper, you will see that the third line can only intersect the existing 2 lines in at most 2 places, resulting in 3 new regions. Therefore the number of regions is $4 + 3 = 7$.)

(c) (1 point) If we add a fourth line, what is the maximum number of intersection points that line can make with the existing lines?

Solution: 3

(d) (1 point) Four lines can divide the plane into at most how many regions?

Solution: 11

(e) (3 points) What is the maximum number of regions that n lines can divide the plane into?

Solution: $1 + n(n+1)/2$

9. (3 points) Prove it possible to pair up the numbers $0, 1, 2, 3, \ldots, 61$ in such a way that when we sum each pair, the product of the 31 numbers we get is a perfect fifth power.

Solution: Pair 0 with 1, and k with $63 - k$ for all $2 \leq k \leq 31$. This would result in a product equal to $1 \times 63^{30} = (63^6)^5$ which is a perfect 5^{th} power.

Total: 50

Year 10

1. (3 points) There are twelve lockers, numbered from 110 to 121. The keys to these twelve lockers are numbered 1 to 12. Each locker number is divisible by the number on its key.

   Determine the key number for each locker.

Solution:

110	111	112	113	114	115	116	117	118	119	120	121
10	3	8	1	6	5	4	9	2	7	12	11

2. (2 points) Three consecutive numbers sum to 141. What are the numbers?

Solution: $46, 47, 48$

3. (a) (2 points) When is the sum of 2 consecutive numbers divisible by 2?

   Solution: Never, because $n + (n+1) = 2n + 1$ is odd.

   (b) (2 points) When is the sum of 3 consecutive numbers divisible by 3?

   Solution: Always, as $n + (n+1) + (n+2) = 3n + 3$.

   (c) (2 points) When is the sum of 4 consecutive numbers divisible by 4?

   Solution: Never, as $n + (n+1) + (n+2) + (n+3) = 4n + 10 \equiv 2 \pmod 4$.

   (d) (2 points) When is the sum of 5 consecutive numbers divisible by 5?

   Solution: Always, as $n + (n+1) + (n+2) + (n+3) + (n+4) = 5n + 10$.

   (e) (2 points) When is the sum of n consecutive numbers divisible by n?

   Solution: The sum of n consecutive numbers starting from k is kn plus the $n-1$th triangular number, so it is

   $$n\left(k + \frac{n-1}{2}\right).$$

   The resulting number is divisible by n if $(n-1)/2$ is an integer, and that is when n is odd.

4. (3 points) Prove it possible to pair up the numbers $0, 1, 2, 3, \ldots, 61$ in such a way that when we sum each pair, the product of the 31 numbers we get is a perfect fifth power.

Solution: Pair 0 with 1, and k with $63 - k$ for all $2 \leq k \leq 31$. This would result in a product equal to $1 \times 63^{30} = (63^6)^5$ which is a perfect 5^{th} power.

5. (a) (1 point) Two lines can divide the plane into at most how many regions?

Solution: 4

(b) (1 point) Three lines can divide the plane into at most how many regions?

Solution: 7 (If you try it on paper, you will see that the third line can only intersect the existing 2 lines in at most 2 places, resulting in 3 new regions. Therefore the number of regions is $4 + 3 = 7$.)

(c) (1 point) If we add a fourth line, what is the maximum number of intersection points that line can make with the existing lines?

Solution: 3

(d) (1 point) Four lines can divide the plane into at most how many regions?

Solution: 11

(e) (3 points) What is the maximum number of regions that n lines can divide the plane into?

Solution: $1 + n(n+1)/2$

6. (a) (2 points) Is the sum or difference of two rational numbers always rational? Why or why not?

Solution: Yes, because $a/b + c/d = (ad + bc)/bd$ and both $ad + bc$ and bd are integers.

(b) (2 points) Is the product or quotient of two rational numbers always rational? Why or why not?

Solution: Yes, because $(a/b)(c/d) = ac/bd$ and both ac and bd are integers.

(c) (2 points) When one rational number is raised to another is the result guaranteed to be rational?

Solution: No; an example is $2^{1/2}$.

(d) (3 points) It is known that $\sqrt{2}$ is irrational, but it is not known whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational. Do there exist two irrational numbers such that when one is raised to the other the result is rational? Prove your conjecture.

Solution: The answer is yes. Let $A = \sqrt{2}^{\sqrt{2}}$. We don't know if A is rational or irrational, but it doesn't matter. If A is rational, then it is an example of a rational number that is an irrational number raised to another irrational number. If A is irrational, then $A^{\sqrt{2}} = \sqrt{2}^{2} = 2$ and this number is the desired example.

7. (a) (2 points) Prove that $x^2 + y^2 \geq 2xy$ for real numbers x, y.

Solution: Moving $2xy$ to the left we get $(x - y)^2 \geq 0$. Which is true.

(b) (2 points) Prove that $2a^2 + b^2 + c^2 \geq 2(ab + ac)$ for real numbers a, b, c.

Solution: Using the result from a), we add the two following inequalities

$$a^2 + b^2 \geq 2ab$$

$$a^2 + c^2 \geq 2ac$$

to get

$$2a^2 + b^2 + c^2 \geq 2(ab + ac).$$

(c) (2 points) Prove that $3(a^2 + b^2 + c^2 + d^2) \geq 2(ab + ac + ad + bc + bd + cd)$ for real numbers a, b, c, d.

Solution: Same deal as part b), just with more inequalities. We add up

$$a^2 + b^2 \geq 2ab$$

$$a^2 + c^2 \geq 2ac$$

$$a^2 + d^2 \geq 2ad$$

$$b^2 + c^2 \geq 2bc$$

$$b^2 + d^2 \geq 2bd$$

$$c^2 + d^2 \geq 2cd$$

to get

$$3(a^2 + b^2 + c^2 + d^2) \geq 2(ab + ac + ad + bc + bd + cd).$$

(d) (3 points) Real numbers a, b, c, d, e are linked by the two equations:

$$e = 40 - a - b - c - d$$

$$e^2 = 400 - a^2 - b^2 - c^2 - d^2$$

Determine the largest value for e.

Solution: From the first equation we have

$$(40-e)^2 = (a+b+c+d)^2 = a^2+b^2+c^2+d^2+2(ab+ac+ad+bc+bd+cd)$$

Using the result from part c), we get that

$$(40-e)^2 \leq 4(a^2+b^2+c^2+d^2)$$

Using the second equation we get

$$(40-e)^2 \leq 4(400-e^2)$$

After expanding the brackets and simplifying, it follows that

$$e(80-5e) \geq 0$$

Implying that $0 \leq e \leq 16$. Thus the largest value for e that satisfies the given equations is 16. This value of e is attainable when $a = b = c = d = 6$.

8. (a) (1 point) How many ways are there to create a two-element subset from the set $\{1, 2, 3, 4\}$?

Solution: There are $\binom{4}{2} = 6$ ways.

(b) (2 points) How many ways are there to split the set $\{1, 2, 3, 4\}$ into two disjoint nonempty sets? (Disjoint means the two sets share no elements.) For example, if we had the set $\{1, 2, 3\}$ a valid splitting would be $\{1, 2\}$ and $\{3\}$.

Solution: The valid ways are: $\{1\}$ and $[\{2, 3, 4\}$, $\{2\}$ and $\{1, 3, 4\}$, $\{3\}$ and $\{1, 2, 4\}$, $\{4\}$ and $\{1, 2, 3\}$, $\{1, 2\}$ and $\{3, 4\}$, $\{1, 3\}$ and $\{2, 4\}$, and $\{1, 4\}$ and $\{2, 3\}$. So 7 ways.

(c) (2 points) How many ways are there to split the set $\{1, 2, 3, 4, 5\}$ into two disjoint nonempty sets?

Solution: By listing all the ways again, we find that there are 15 ways.

(d) (2 points) Denote by $S(n, k)$ the number of ways to split a set of n elements into k disjoint nonempty sets. Suppose we know what $S(n-1, 2)$ is. What happens when we add another element to the set? What happens to each of the $S(n-1, 2)$ ways to do the partitioning?

Solution: For each way to do the partitioning, we may add the new number n to either set to obtain a new partitioning. There is also one new partition that is not obtained by adding n to existing one, and that is the splitting into $\{n\}$ and $\{1, 2, \ldots, n-1\}$. Therefore we have

$$S(n, 2) = 2S(n-1, 2) + 1.$$

(e) (2 points) What is $S(n, 2)$?

Solution: We have $S(1, 2) = 0$, $S(2, 2) = 1$, $S(3, 2) = 3$, $S(4, 2) = 7$, and $S(5, 2) = 15$. From this pattern and the recursive formula found above it is easy to prove by induction that $S(n, 2) = 2^{n-1} - 1$.

(f) (3 points (bonus)) If there are $S(n-1, k-1)$ ways to partition a set of $n-1$ elements into $k-1$ nonempty disjoint sets, what is $S(n, k)$ in terms of $S(n-1, k)$ and $S(n-1, k-1)$?

Solution: We need to think about what happens when we add the nth element. Clearly we may put this object into a separate set by itself and partition the other $n-1$ objects into $k-1$ nonempty disjoint subsets, because all up there would be k sets. There are $S(n-1, k-1)$ ways to do this. We may also take the $n-1$ objects and partition them into k sets and add the nth element to any one of them to get another valid partitioning. How many ways are there to do this? In each of the $S(n-1, k)$ ways to partition $n-1$ objects into k nonempty sets, there are k different subsets we can put the nth object into. Therefore in this case there are $kS(n-1, k)$ ways. In total then we have

$$S(n, k) = S(n-1, k-1) + kS(n-1, k).$$

Total: 52

Year 11/12

1. (3 points) There are twelve lockers, numbered from 110 to 121. The keys to these twelve lockers are numbered 1 to 12. Each locker number is divisible by the number on its key.

   Determine the key number for each locker.

   Solution:

110	111	112	113	114	115	116	117	118	119	120	121
10	3	8	1	6	5	4	9	2	7	12	11

2. (a) (1 point) Two lines can divide the plane into at most how many regions?

   Solution: 4

   (b) (1 point) Three lines can divide the plane into at most how many regions?

   Solution: 7 (If you try it on paper, you will see that the third line can only intersect the existing 2 lines in at most 2 places, resulting in 3 new regions. Therefore the number of regions is $4 + 3 = 7$.)

   (c) (1 point) If we add a fourth line, what is the maximum number of intersection points that line can make with the existing lines?

   Solution: 3

   (d) (1 point) Four lines can divide the plane into at most how many regions?

   Solution: 11

   (e) (3 points) What is the maximum number of regions that n lines can divide the plane into?

   Solution: $1 + n(n+1)/2$

3. (a) (1 point) How many ways are there to create a two-element subset from the set $\{1, 2, 3, 4\}$?

   Solution: There are $\binom{4}{2} = 6$ ways.

   (b) (2 points) How many ways are there to split the set $\{1, 2, 3, 4\}$ into two disjoint nonempty sets? (Disjoint means the two sets share no elements.) For example, if we had the set $\{1, 2, 3\}$ a valid splitting would be $\{1, 2\}$ and $\{3\}$.

Solution: The valid ways are: $\{1\}$ and $[\{2,3,4\}$, $\{2\}$ and $\{1,3,4\}$, $\{3\}$ and $\{1,2,4\}$, $\{4\}$ and $\{1,2,3\}$, $\{1,2\}$ and $\{3,4\}$, $\{1,3\}$ and $\{2,4\}$, and $\{1,4\}$ and $\{2,3\}$. So 7 ways.

(c) (2 points) How many ways are there to split the set $\{1,2,3,4,5\}$ into two disjoint nonempty sets?

Solution: By listing all the ways again, we find that there are 15 ways.

(d) (2 points) Denote by $S(n,k)$ the number of ways to split a set of n elements into k disjoint nonempty sets. Suppose we know what $S(n-1,2)$ is. What happens when we add another element to the set? What happens to each of the $S(n-1,2)$ ways to do the partitioning?

Solution: For each way to do the partitioning, we may add the new number n to either set to obtain a new partitioning. There is also one new partition that is not obtained by adding n to existing one, and that is the splitting into $\{n\}$ and $\{1,2,\ldots,n-1\}$. Therefore we have

$$S(n,2) = 2S(n-1,2) + 1.$$

(e) (2 points) What is $S(n,2)$?

Solution: We have $S(1,2) = 0$, $S(2,2) = 1$, $S(3,2) = 3$, $S(4,2) = 7$, and $S(5,2) = 15$. From this pattern and the recursive formula found above it is easy to prove by induction that $S(n,2) = 2^{n-1} - 1$.

(f) (3 points (bonus)) If there are $S(n-1,k-1)$ ways to partition a set of $n-1$ elements into $k-1$ nonempty disjoint sets, what is $S(n,k)$ in terms of $S(n-1,k)$ and $S(n-1,k-1)$?

Solution: We need to think about what happens when we add the nth element. Clearly we may put this object into a separate set by itself and partition the other $n-1$ objects into $k-1$ nonempty disjoint subsets, because all up there would be k sets. There are $S(n-1,k-1)$ ways to do this. We may also take the $n-1$ objects and partition them into k sets and add the nth element to any one of them to get another valid partitioning. How many ways are there to do this? In each of the $S(n-1,k)$ ways to partition $n-1$ objects into k nonempty sets, there are k different subsets we can put the nth object into. Therefore in this case there are $kS(n-1,k)$ ways. In total then we have

$$S(n,k) = S(n-1,k-1) + kS(n-1,k).$$

4. (a) (2 points) Is the sum or difference of two rational numbers always rational? Why or why not?

Solution: Yes, because $a/b + c/d = (ad + bc)/bd$ and both $ad + bc$ and bd are integers.

(b) (2 points) Is the product or quotient of two rational numbers always rational? Why or why not?

Solution: Yes, because $(a/b)(c/d) = ac/bd$ and both ac and bd are integers.

(c) (2 points) When one rational number is raised to another is the result guaranteed to be rational?

Solution: No; an example is $2^{1/2}$.

(d) (3 points) It is known that $\sqrt{2}$ is irrational, but it is not known whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational. Do there exist two irrational numbers such that when one is raised to the other the result is rational? Prove your conjecture.

Solution: The answer is yes. Let $A = \sqrt{2}^{\sqrt{2}}$. We don't know if A is rational or irrational, but it doesn't matter. If A is rational, then it is an example of a rational number that is an irrational number raised to another irrational number. If A is irrational, then $A^{\sqrt{2}} = \sqrt{2}^{2} = 2$ and this number is the desired example.

5. (a) (1 point) If two normal six-sided dice are rolled, what is the probability that the sum of the two numbers is 2?

Solution: Out of the 36 possible pairs the only one that has a sum of 2 is $(1, 1)$, so the probability is $1/36$.

(b) (1 point) If two normal six-sided dice are rolled, what is the probability that the sum of the two numbers is 7?

Solution: There are 6 ways to get a 7: $(1, 6)$, $(2, 5$, $(3, 4)$, $(4, 3)$, $(5, 2)$, and $(6, 1)$. Therefore the probability is $1/6$.

(c) (2 points) Consider a biased six-sided die in which the probability of rolling n is p_n. This die is rigged so that when two of them are rolled, every possible sum of the two numbers is equally likely. What is p_2 in terms of p_1?

Solution: The probability of getting a 3 is $p_2p_1 + p_1p_2$, which by hypothesis is equal to the probability of getting a 2, or p_1^2. Therefore $2p_2 = p_1$, which implies that $p_2 = p_1/2$.

(d) (1 point) What is p_3 in terms of p_1?

Solution: Following the previous procedure we find that $p_3 = 3p_1/8$.

(e) (2 points) What is p_4 in terms of p_1? Do you notice a pattern?

Solution: $p_4 = 5p_1/16$. The pattern is $1/2$, $(1/2)(3/4)$, $(1/2)(3/4)(5/6)$, and so on.

(f) (2 points) Let $p_i = a_{i-1}p_1$. So $a_0 = 1$, $p_2 = a_1p_1$, $p_3 = a_2p_1$, $p_4 = a_3p_1$ and so on. What are $a_0a_1 + a_1a_0$, $a_0a_2 + a_1a_1 + a_2a_0$, $a_0a_3 + a_1a_2 + a_2a_1 + a_3a_0$, etc. all equal to?

Solution: If $p_1p_2 + p_2p_1 = p_1^2$ then

$$a_0p_1a_1p_1 + a_0p_1a_1p_1 = p_1^2$$

which implies

$$(a_0a_1 + a_1a_0)p_1^2 = p_1^2.$$

Therefore $a_0a_1 + a_1a_0 = 1$. Similarly the other combinations of a's can be found to be 1 too.

(g) (1 point) Since we have a six-sided die,

$$p_1 + p_2 + \cdots + p_6 = 1.$$

What is p_1 in terms of $a_0, a_1, a_2, \ldots, a_5$?

Solution: Since the die is six-sided, we have $p_1 + p_2 + \cdots + p_6 = 1$. We can express this in terms of p_1:

$$a_0p_1 + a_1p_1 + a_2p_1 + \cdots + a_5p_1 = 1$$

and hence

$$p_1 = \frac{1}{a_0 + a_1 + \cdots + a_5}.$$

(h) (2 points) Let $s_i = a_0 + a_1 + \cdots + a_i$. What are s_0, s_1, s_2? What is s_5?

Solution: $s_0 = a_0 = 1$, $s_1 = a_0 + a_1 = 3/2$, $s_2 = 1 + 1/2 + 3/8 = 15/8$. Note that $s_2 = (3/2)(5/4)$, $s_3 = (3/2)(5/4)(7/6)$, $s_4 = (3/2)(5/4)(7/6)(9/8)$ and so on. Therefore

$$s_5 = \frac{3 \cdot 5 \cdot 7 \cdot 9 \cdot 11}{2 \cdot 4 \cdot 6 \cdot 8 \cdot 10} = \frac{693}{256}.$$

(i) (3 points) Is such a six-sided die possible?

Solution: From the previous part we find that $p_1 = 256/693$. This means that the probability of rolling two of these dice and getting a sum of $2, 3, \ldots, 12$ must all be $p_1^2 = 65536/480249$. But this is impossible because there are 11 possible sums and if they are equally likely each must have a probability of $1/11$. Therefore such a die is not possible.

6. (a) (1 point) What is $1 + 2 + 3 + \cdots + 200$?

Solution: 10100

(b) (2 points) Find a formula for $1 + 2 + \cdots + n$ and prove it.

Solution: The formula is

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

It is easily proved by induction. When $n = 1$ we have $1 = 1(1+1)/2$ so the base case is done. Now assume that

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

for some natural number k. Add $k + 1$ to both sides:

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

and the induction is complete.

(c) (1 point) Define

$$F_k(n) = 1^k + 2^k + \cdots + n^k.$$

(So in the previous part you found a formula for $F_1(n)$.) More compactly it may be written as

$$F_k(n) = \sum_{i=1}^{n} i^k.$$

What is

$$1^3 + (2^3 - 1^3) + (3^3 - 2^3) + \cdots + (100^3 - 99^3)?$$

Solution: This sum is an example of a telescoping sum. All the terms vanish except for the 100^3 term in the last set of parentheses, so the answer is 100^3.

(d) (2 points) By considering

$$1^3 + \sum_{i=1}^{n} ((i+1)^3 - i^3)$$

find a formula for $F_2(n)$.

Solution: We know that

$$1^3 + \sum_{i=1}^{n}((i+1)^3 - i^3) = (n+1)^3.$$

Expanding both sides using the Binomial Theorem we get

$$1^3 + \sum_{i=1}^{n}(3i^2 + 3i + 1) = n^3 + 3n^2 + 3n + 1.$$

After removing the 1 from both sides, on the LHS we can break up the sum and pull out the constant factors, like so:

$$3\sum_{i=1}^{n} i^2 + 3\sum_{i=1}^{n} i + \sum_{i=1}^{n} 1 = n^3 + 3n^2 + 3n.$$

But note that $\sum_{i=1}^{n} i^2 = F_2(n)$ and $\sum_{i=1}^{n} i = F_1(n)$, so we have

$$3F_2(n) + 3F_1(n) + n = n^3 + 3n^2 + 3n.$$

Then we just need to rearrange for $F_2(n)$ after substituting in $F_1(n) = n(n+1)/2$ to find that

$$F_2(n) = \frac{2n^3 + 3n^2 + n}{6}.$$

(e) (2 points) Find a formula for $F_3(n)$.

Solution: Using the same method as above, we find that

$$F_3(n) = \frac{n^4 + 2n^3 + n^2}{4}.$$

(f) (1 point) The Binomial Theorem states that

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

If

$$(i+1)^k - i^k = \sum_{j=0}^{x} \binom{k}{j} i^j$$

what is x in terms of k?

Solution: The leading term vanishes, so instead of going from 0 to k the loop only goes up to $k-1$. Therefore $x = k-1$.

(g) (3 points) By considering the general telescoping sum

$$1^k + \sum_{i=1}^{n}((i+1)^k - i^k) = (n+1)^k$$

show that

$$F_{k-1}(n) = \frac{(n+1)^k - 1}{k} + \frac{1}{k}\sum_{i=0}^{k-2}\binom{k}{i}F_i(n).$$

Solution: Expand the $(n+1)^k$ term using the Binomial Theorem, applying the previous part:

$$(n+1)^i = 1^k + \sum_{i=1}^{k}\sum_{j=0}^{k-1}\binom{k}{j}i^j.$$

Now expand the inner sigma notation:

$$(n+1)^k = 1^k + \sum_{i=1}^{k}\left(\binom{k}{0}i^0 + \binom{k}{1}i^1 + \binom{k}{2}i^2 + \cdots + \binom{k}{k-1}i^{k-1}\right).$$

We may take out the binomial coefficients, as they are independent of the sum variable i, so we have

$$(n+1)^k = 1^k + \binom{i}{0}\sum_{i=1}^{k}i^0 + \binom{k}{1}\sum_{i=1}^{k}i^1 + \binom{k}{2}\sum_{i=1}^{k}i^2 + \cdots + \binom{k}{k-1}\sum_{i=1}^{k}i^{k-1}.$$

We're interested in $F_{k-1}(n)$, so we notice that the binomial coefficient $\binom{k}{k-1} = k$ and isolate that term. The other sums are $F_0(n)$, $F_1(n)$, $F_2(n)$ and so on. Therefore we get

$$(n+1)^k = 1^k + \binom{k}{0}F_0(n) + \binom{k}{1}F_1(n) + \binom{k}{2}F_2(n) + \cdots + \binom{k}{k-2}F_{k-2}(n) + kF_{k-1}(n)$$

or more compactly,

$$(n+1)^k = 1 + \sum_{i=0}^{k-2}\binom{k}{i}F_i(n) + kF_{k-1}(n).$$

Rearranging for $F_{k-1}(n)$ we get the desired result.

Total: 55

Year 9

1. Find the number whose double is 60 more than its half.

2. The internal angles of a heptagon sum to $900°$. Find the sum of the internal angles of a heptadecagon.

3. Given that
$$6^{2x+y} = 36^7$$
and
$$6^{x+4y} = 216^7$$
find xy.

4. Two vertices of an equilateral triangle are $(1, 1)$ and $(7, 1)$. Find the coordinates of the third vertex.

5. What is the thousandth digit after the decimal place of $1/7$?

6. Evaluate
$$3 + 6 + 9 + \cdots + 300.$$

7. How many four-digit numbers can be formed using the digits $3, 1, 4, 1$?

8. A right-angled triangle has vertices $(0, 0)$, (a, b), $(a, 0)$ with hypotenuse $(a+b)/(a-b)$. The point (a, b) lies on a circle of radius 4. Find ab.

9. In a set of 50 numbers, the average of the first 20 is 30 while the average of the other 30 is 20. What is the average of all 50 numbers?

10. Find the first date in this millennium to have 8 unique digits when written in the form DD/MM/YYYY.

11. Find the probability that a randomly chosen number between 2 and 100 inclusive is prime.

12. A family consists of a mother, a father, and a number of children. The average age of the family is 20. The average age of just the mother and the children is 16. If the father's age is 48, how many children are there in the family?

13. An equilateral triangle with area 1 is inscribed inside a circle. This circle is itself inscribed inside a larger equilateral triangle. What is the area of the larger triangle?

14. What is the smallest positive integer that leaves a remainder of 1 when divided by each of the numbers $2, 3, \ldots, 10$?

15. At exactly midnight the hour hand of a clock begins to move twice its normal speed while the minute hand begins to move at half its normal speed. What is the correct time the next time the two hands meet?

16. A regular decagon has an area of 100 square units. What is the length of one of its sides to three decimal places?

17. If
$$A = 1^{-3} + 2^{-3} + 3^{-3} + \cdots$$
find
$$1^{-3} + 3^{-3} + 5^{-3} + \cdots$$
in terms of A.

18. Today, the 18th of July, 2023 is a Tuesday. What was the day of the week on the 18th of July 1823?

19. The numbers $1, 2, \ldots, 1000$ are written on the whiteboard. On each turn, two numbers x and y erased from the board and replaced by $xy - x - y + 2$. This continues until only one number remains. What is this number?

20. Two real numbers x and y, where $x > y$ have the property that they are equal to 1 plus their reciprocal and $x > y$. What is
$$\frac{x^2 - y^2}{\sqrt{5}}?$$

1. 40
2. 2700°
3. 20
4. $(4, 1 + 3\sqrt{3})$
5. 8
6. 15150
7. 12
8. 24/5
9. 24
10. 17/06/2345
11. 25/99
12. 6
13. 4
14. 2521
15. 3 am
16. 3.605
17. $(1 - 2^{-3})A$
18. Friday
19. 1
20. 1

Year 10

1. The Fibonacci sequence is the sequence

$$1, 1, 2, 3, 5, 8 \ldots .$$

   Find the sum of the first 10 terms.

2. The sum of the first n odd numbers is 841. Find n.

3. Today (Tuesday) I start taking lectures on potions. If these lectures happen every second day, which lecture will be the first to fall on a Sunday?

4. If the sum of two positive real numbers is 4 times their product, what is the sum of the reciprocals of the two numbers?

5. What is the area of the equilateral triangle circumscribed by a circle of radius 1?

6. My car averages 40 kilometres per litre of petrol, while my friend's car averages 10 kilometres per litre of petrol. If we both drive the same distance, what is the combined rate of kilometres per litre of petrol?

7. If the side lengths of a rectangle are in the ratio $4 : 3$ and d is the length of the diagonal, it can be shown that the area of the rectangle is given by kd^2. Find k.

8. The vertices of an isosceles triangle lie on the graph of $y = x^2$. If the area of the triangle is 64, what is the length of the shortest side?

9. A palindromic number is one that is the same read forwards and backwards. For example, 292 is palindromic. How many three-digit palindromic numbers are there less than 1000?

10. Three of a rectangular prism's faces have areas of 12, 28, and 21. What is the volume of the rectangular prism?

11. What is the last digit of 9^{2023}?

12. Two hoses can be used to fill a swimming pool. Hose B takes twice as long as Hose A to fill the pool. If Hose A takes 6 minutes to fill the pool, how long will it take for both hoses together to fill the pool?

13. A normal coin is flipped 3 times. Given that at least one coin landed tails, what is the probability that there are two consecutive heads?

14. There is a tennis tournament with 1025 players. Each round, every player is paired with another, and if there are an odd number of players one player sits out. A loss immediately knocks out a player from the tournament. The tournament continues until only one player remains. How many matches are played in total?

15. For how many integers n, where $1 \leq n \leq 100$, is n^n a square number?

16. What is the smallest positive integer n such that

$$(2^2-1)(3^2-1)(4^2-1)\cdots(n^2-1)$$

is a square number?

17. In the nine digit number

$$347*47*64$$

two digits are missing, as indicated by the asterisks. If two digits are randomly chosen for the two missing spots, what is the probability that the number is divisible by 36?

18. Given an arithmetic sequence $a_1, a_2, \ldots, a_n$ where $a_{k+1}-a_k = d$ for $k = 0, 1, \ldots, n-1$, the sum is given by

$$a_1 + a_2 + \cdots + a_n = \frac{n}{2}\left(2a + (n-1)d\right).$$

Find

$$1 - 4 + 9 - 16 + \cdots + 99^2 - 100^2.$$

19. The two digits in Jack's age are the same as the digits in Bill's age, but in reverse order. In five years Jack will be twice as old as Bill will be then. What is the difference in their current ages?

20. In $\triangle ABC$, $\angle C$ is a right angle and $AB = 12$. Squares $ACWZ$ and $ABXY$ are constructed so that points X, Y, W, and Z lie outside the triangle. If those four points also lie on a circle, what is the perimeter of the triangle?

1. 143
2. 29
3. 7th lecture
4. 4
5. $3\sqrt{3}/4$
6. 16 kilometres per litre
7. 12/25
8. 8
9. 90
10. 84
11. 9
12. 4 minutes
13. 2/7
14. 1024
15. 55
16. 8
17. 11/100
18. -5050
19. 18
20. $12 + 12\sqrt{2}$

Year 11/12

1. Find the next number in the sequence

$$1, 5, 12, 22, 35, \ldots$$

2. Twenty percent less than 60 is one-third more than what number?

3. What is the lowest common multiple of 18 and 35?

4. Find the cube root of 3^{3^3}. Note that $a^{b^c} = a^{(b^c)}$.

5. A triangle is inscribed in a circle of radius 3. Find the area of the triangle if its sides are in the ratio $3 : 4 : 5$.

6. In the plane, a lattice point is a point where both the x and y coordinates are whole numbers. The line $y = 55x/12$ is sketched for $0 < x < 12$. How many lattice points are there on the line?

7. Which number is the first number greater than 1 that is the cube of the sum of its digits?

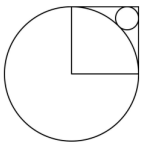
8. Evaluate

$$\sqrt{(2023 + 2023) + (2023 - 2023) + (2023 \times 2023) + (2023 \div 2023)}.$$

9. How many digits does $(2^22)^5 \times (5^55)^2$ have?

10. In how many ways can 10 objects be put into 3 bins such that one of the bins gets 5 objects, another gets 3 objects, and the third bin gets 2 objects?

11. In the diagram below the side length of the square is 1. What is the radius of the smaller circle?



12. Josh writes the numbers $1, 2, 3, \ldots, 99, 100$. He marks out 1, skips the next number (2), marks out 3, and continues skipping and marking out the next number to the end of the list. Then he goes back to the start of his list, marks out the first remaining number (2), skips the next number (4), marks out 6, skips 8, marks out 10, and so on to the end. Josh continues in this manner until only one number remains. What is that number?

13. Solve the equation

$$7\sqrt{x} - 22 = \frac{24\sqrt{x}}{x}.$$

14. Five points are randomly placed in a square with side length 2. The distance between every pair of points is measured, and the smallest distance between a pair of points is called the *minimum* distance. What is the largest possible minimum distance?

15. For how many integer values of n (positive or negative) is the value of

$$4000 \cdot \left(\frac{2}{5}\right)^n$$

an integer?

16. If $\sin a + \sin b = \sqrt{5/3}$ and $\cos a + \cos b = 1$ what is $\cos(a - b)$?

17. How many ways are there to write 6 as the sum of any number of positive integers?

18. The number

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

is the root of a quadratic with rational coefficients. Find the sum of the roots of this quadratic.

19. We have 5 disks of distinct sizes, and 3 pegs in a line. Let the left peg be A and the right-most peg be B. The disks start off on A in descending order of size; the largest disk is at the bottom. What is the minimum number of moves required to transfer the entire stack of disks from A to B if a larger disk is not allowed to be placed on top of a smaller disk and *direct transfers from A to B are not allowed?* This means every move must be made to or from the middle peg.

20. Find

$$1^3 + 2^3 + 3^3 + \cdots + 50^3$$

given the following four equations.

$$1 = 0 + 1$$

$$2 + 3 + 4 = 1 + 8$$

$$5 + 6 + 7 + 8 + 9 = 8 + 27$$

$$10 + 11 + 12 + 13 + 14 + 15 + 16 = 27 + 64$$

1. 51
2. 36
3. 3^{3^2}
4. 630
5. 8.64
6. 0
7. 512
8. 2024
9. 111
10. 2520
11. $(\sqrt{2}-1)^2$
12. 64
13. 16
14. $\sqrt{2}$
15. 9
16. 1/3
17. 11
18. 0
19. 242
20. 1625625