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.

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

   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.

   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

   Tournament of Towns Junior 1981/1

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

   where k is a natural number greater than 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

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

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

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

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

are all distinct and form the complete set of positive residues

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

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

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

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.

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 $q_1, q_2, \dots, q_r$ are distinct primes and $a_1, a_2, \dots, a_r$ are positive integers. From this it follows that all of $q_1^{a_1}, q_2^{a_2}, \dots, q_r^{a_r}$ are coprime. Hence if we can show that there exists some number that has order $q_i^{a_i}$, for $1 \le i \le r$, 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

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

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.

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

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

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.

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

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

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

reduced modulo p are the numbers

$$1, 2, \dots, p-1$$

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.

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 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.

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

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.