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—Anonymous, unpublished correspondence (2023)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?