Coding and Cryptography Fall 2016
Worksheet on Fermat and Euler

Katherine E. Stange

September 12, 2016

Modular multiplication

1. On the website, you'll find a tool ('Modular Multiplication' under 'Topics'), which will draw an arrow diagram of the function

$$x \mapsto ax, \quad \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

   i.e. the function which multiplies by a modulo n. Please choose n only from small primes $(2, 3, 5, 7, 11, 13, 17)$ for now, and take a look at the outputs.
2. For a fixed n, which different values of a do you have to consider? Why? Hint: there are only finitely many different functions.

3. Please take care in writing proofs, I will collect these and give feedback as if this were a quiz (no effect on your class grade).
   (a) Does the function appear to be injective always, sometimes or never? State and prove a precise statement for prime n.

   (b) Does the function appear to be surjective always, sometimes or never? State and prove a precise statement for prime n.

(c) Do you observe any other patterns?

Modular exponentiation

1. On the website, you'll find a tool ('Modular Multiplication' under 'Topics'), which will draw an arrow diagram of the function

$$x \mapsto x^a, \quad \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

   i.e. the function which exponentiates by a modulo n. Please choose n only from small primes $(2, 3, 5, 7, 11, 13, 17)$ for now, and take a look at the outputs.
2. For a fixed n, which different values of a do you have to consider? Why? Hint: there are only finitely many different functions.

3. Verify your answer above by trying various a values modulo 5. Copy down here the functions for $a = 0, 1, 2, \ldots$. How many different ones are there? When and how do they begin to repeat? Was your answer to the last section right?

4. Fill in this statement to make a precise conjecture:

   Conjecture 1. *Let p be a prime. Let a_1 and a_2 be integers. Then the maps $f_1, f_2 : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined by $f_1(x) = x^{a_1}$ and $f_2(x) = x^{a_2}$ are identical if and only if*

5. Now make some other conjectures:
   (a) Does the function appear to be injective always, sometimes or never? State a precise statement.

   (b) Does the function appear to be surjective always, sometimes or never? State a precise statement.

   (c) Do you observe any other patterns?

Order of elements modulo n

Definition 1. *Let $x \in \mathbb{Z}/n\mathbb{Z}$ be invertible. Then if a is the smallest positive integer such that $x^a \equiv 1 \pmod{n}$, then we say a is the* order *of n.*

Informally, it is the exponent to which you must raise x to get 1.

1. Read the definition above. By inspecting a multiplication table modulo 5 (tool on website!), determine the orders of each invertible element.

2. Now try the 'Orders of elements modulo n' tool on the website. Try other prime values of n (stick to primes). Record your observations here:

3. Now make a conjecture about the orders of elements modulo a prime p.

Fermat's Theorem

Theorem 1. *Let p be a prime. Suppose that p does not divide a. Then* $a^{p-1} \equiv 1 \pmod{p}$.

1. Read the theorem above, and compare with the data. Illustrate the theorem using the online tools.
2. Consider the map $f(x) = ax$ (where p does not divide a). Review that from the first section, this map is bijective. Illustrate this fact using the online tools.
3. Consider these two products:

   $$1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$$

   and

   $$f(1) \cdot f(2) \cdot f(3) \cdot \cdots \cdot f(p-1)$$

   Choosing $p = 5$ work out both products modulo p (by hand or using Sage).

4. How are the products related? Use the bijectivity if f.

5. Can you use the definition of f to simplify the second product? How does the simplified result relate to the first product?

6. Produce a proof of Fermat's Theorem.

Euler's Theorem

Open-ended:

1. What happens when the modulus is not prime?
2. What are the possible orders of elements modulo n? (There's a Sage tool for experimentation online.)