

20. FERMAT AND EULER

Secure communication in the world today is based on Euler's formula and its generalizations. Euler's formula is in turn based on a formula of Fermat.

20.1. Fermat.

Theorem 20.1 (Fermat's little theorem). *If p is prime and a is relatively prime to p (p does not divide a) then*

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

The proof is based on Lagrange's Theorem which you need to know for the quiz. So, let's review that. Lagrange said that, if H is a subgroup of a finite group G , then the order of H divides the order of G . A corollary is that the order of any element of G divides the order of G since $o(g) = |\langle g \rangle|$. (The order of g is equal to the order of the subgroup of G generated by g .) This gave us the following formula which will be used to prove Fermat and Euler's formula.

Lemma 20.2. *If G is a group of order $|G| = n$ then*

$$g^n = e$$

for all $g \in G$.

This is Corollary 10.7 in these notes. Do you remember the proof?

Proof of Fermat's little theorem. This congruence equation is the same as the actual equation

$$a^{p-1} = 1$$

for all $a \neq 0$ in \mathbb{Z}_p . But \mathbb{Z}_p is a field. So,

$$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid a \neq 0\}$$

is a group of order $p-1$. So, the lemma above implies Fermat's formula. \square

Corollary 20.3. *If p is prime then*

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

for all integers a .

Proof. If p divides a then both sides are congruent to 0 modulo p . If p doesn't divide a then this follows from Fermat. \square

Application: We use this equation to test if a number is prime. There are very fast algorithms to compute a^n modulo p even if all three numbers have several hundred digits. The test is not foolproof but we do know that if

$$a^{n-1} \not\equiv 1 \pmod{n}$$

for some a then n is not prime.

20.2. Euler. Euler found a way to generalize Fermat's formula to all positive integers. He just needed the formula for the order of the group of units of \mathbb{Z}_n .

Lemma 20.4. *If R is any ring then the set of units of R is closed under multiplication and inverse and therefore forms a multiplicative group denoted $U(R)$.*

Theorem 20.5. *a is a unit in \mathbb{Z}_n if and only if a is relatively prime to n .*

Proof. This follows from the Euclidean Algorithm. (Do you remember that?) We used it to prove that the greatest common divisor d of two numbers a, b is an integer linear combination:

$$d = xa + yb$$

In this case, a and n are relatively prime so, $d = 1$ and we get:

$$1 = xa + yn$$

But then $xa \equiv 1 \pmod{n}$ or $xa = 1 \in \mathbb{Z}_n$. So, a is unit in \mathbb{Z}_n .

The converse is obvious. □

Definition 20.6. *The Euler ϕ function is defined to be*

$$\phi(n) = |U(\mathbb{Z}_n)|$$

By the Lemma above which follows from Lagrange we have:

Corollary 20.7.

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

for all integers a which are relatively prime to n .

Theorem 20.8. *If $n = \prod p_i^{k_i}$ then*

$$\phi(n) = \prod (p_i^{k_i} - p_i^{k_i-1}) = n \prod \frac{p_i - 1}{p_i}$$

For example, take $n = 561 = 3 \cdot 11 \cdot 17$. Then

$$\phi(561) = 2 \cdot 10 \cdot 16 = 240$$

Next: We need to prove the theorem and show that 561 is a *pseudo-prime*.