Coding and Cryptography Fall 2016
Mission #4 Template
Euler's Theorem

Katherine E. Stange

September 16, 2016

Rules: You **may** use any written resources for help and information, but **you may not copy**. Specifically, when you are writing, you **must** have all resources (books, webpages) closed. Do not switch back and forth with any frequency. Instead, learn (not memorize) what you need to understand, and then **write a complete proof in a vacuum, using only your brain**.

Instructions (erase these instructions): The goal is to fill out this document into a proper, respectable, chapter of a textbook describing Euler's Theorem. Replace each of the instructions with the appropriate, nicely written, definition, proof, example, etc.

1 Euler's Phi Function

Definition 1 (Euler's Phi Function)**.** *Provide a carefully written definition (in terms of counting invertible elements) of Euler's ϕ function here.*

Example 2. *Here, give several small examples* **of your own creation**, *from first principles. That means, count the invertible elements by actually listing them (and justifying the list; for example, give actual inverses).*

Proposition 3. *If p is a prime, then $\phi(p) = p - 1$.*

This proposition requires lemmata.

Lemma 4. *Let n and x be coprime integers. Then x is invertible modulo n.*

Proof. Provide a proof. You may use the Theorem at the top of page 68 of the text (refer to it Bézout's Lemma, also available on Wikipedia under this name). The proof is short when you base it on that theorem (in other words, it is a corollary of that theorem). □

Lemma 5. *Suppose x and n are integers such that x is invertible modulo n. Then n and x are coprime.*

Proof. Provide a proof. Hint: invertibility allows one to write a linear combination of n and x that is 1. Why does that imply coprimality? □

These two lemmata combine to give the following statement:

Lemma 6. *Let x and n be integers. Then x is invertible modulo n if and only if n and x are coprime.*

Proof of Proposition 3. Provide a proof of Proposition 3 here. Use the lemma just stated, and the definition of Euler's ϕ. □

Proposition 7. *Let $n = p^k$, where p is a prime, $k \geq 1$. Then $\phi(n) =$ $???fillintheanswer???$.*

Proof. Provide a proof. You might like to count the non-coprime residues instead of the coprime ones. □

Proposition 8. *Let n and m be coprime. Then $\phi(nm) = \phi(n)\phi(m)$.*

This one needs a lemma again.

Lemma 9. *Let n and m be coprime. Then x is invertible modulo nm if and only if it is invertible modulo n and modulo m.*

Proof. Provide a proof. One direction of the "if and only if" uses the Chinese Remainder Theorem, which you may call upon without proving. The other direction is immediate. □

Proof of Proposition 8. Provide a proof of Proposition 8 using the lemma. □

Example 10. *Demonstrate how to compute $\phi(3 \cdot 7^2 \cdot 11^3)$ using the three propositions of this section. Cite each proposition as you use it.*

2 Euler's Theorem

Theorem 11 (Euler's Theorem)**.** *State Euler's Theorem here. It's on page 81 of your text, but as with everything else, learn what it is and then generate the statement without copying, please.*

Before proving this, we will provide an example.

Example 12. *Give an example demonstrating the theorem.*

We need a lemma, which we proved in class, so you can use without proof. Here is its statement.

Lemma 13. *Let a be invertible modulo n. Then the function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $f(x) = ax$ is bijective.*

Proof of Theorem 11. Provide a proof of Euler's Theorem. Remember, the key idea is to form two lists and compare their products. You can remind yourself by looking at course notes or the proof of Fermat's Little Theorem on page 80 of your text. However, as I've emphasized before, you must internalize the argument, and then close all resources and write it, start to finish, without aids. □