Coding and Cryptography Fall 2016
Proof Practice Worksheet

Katherine E. Stange

October 7, 2016

Practice makes perfect! Here are some basic items to practice proving, based on our course. Writing is half of what makes a proof a proof, so write well.

1. Prove that if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ (this is a fact we've been using all along).
2. Let x be an element of $\mathbb{Z}/n\mathbb{Z}$. Suppose that x has multiplicative order k. Prove that k divides $\phi(n)$. (Hint: this is actually a more general group theory statement: if an element of a group has order k, then k divides the order of the group.)
3. An element x of $\mathbb{Z}/n\mathbb{Z}$ which is non-zero but satisfies $xy \equiv 0 \pmod{n}$ for some non-zero y is called a *zero divisor*. Prove that $\mathbb{Z}/n\mathbb{Z}$ has zero divisors if and only if n is composite.
4. Suppose $\mathbb{Z}/n\mathbb{Z}$ has a primitive root. A primitive root is an element which has multiplicative order $\phi(n)$ modulo n. Show that the function $x \mapsto x^a$ on the invertible elements of $\mathbb{Z}/n\mathbb{Z}$ is bijective if and only if $\gcd(a, \phi(n)) = 1$.