Coding and Cryptography Fall 2016
Proof Practice Worksheet - Solutions

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).

   Theorem 1. *Suppose that $a_1, a_2, b_1, b_2, n \in \mathbb{Z}$, and that $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Then $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$.*

   Proof. Suppose that $a_1, a_2, b_1, b_2, n \in \mathbb{Z}$, and that

   $$\begin{aligned} a_1 &\equiv a_2 \pmod{n}, \\ b_1 &\equiv b_2 \pmod{n}. \end{aligned}$$

   Then, by definition, $n \mid (a_1 - a_2)$ and $n \mid (b_1 - b_2)$. This implies that there are some integers k and ℓ such that

   $$\begin{aligned} a_1 - a_2 &= kn, \\ b_1 - b_2 &= \ell n. \end{aligned}$$

   We wish to consider the difference

   $$\begin{aligned} (a_1 + b_1) - (a_2 + b_2) &= (a_1 - a_2) + (b_1 - b_2) \\ &= kn + \ell n \\ &= (k + \ell)n. \end{aligned}$$

   Since this difference is a multiple of n, we have shown that

   $$n \mid (a_1 + b_1) - (a_2 + b_2),$$

   or, in other words, that $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$. □

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.)

Theorem 2. *Suppose that $x \in \mathbb{Z}/n\mathbb{Z}$ has multiplicative order k. Then $k \mid \phi(n)$.*

Proof. Suppose that $x \in \mathbb{Z}/n\mathbb{Z}$ has multiplicative order k. Then, by this fact and by Euler's Theorem, we have two facts:

$$\begin{aligned} x^k &\equiv 1 \pmod{n} \\ x^{\phi(n)} &\equiv 1 \pmod{n}. \end{aligned}$$

This implies that

$$x^{ak+b\phi(n)} \equiv 1^a 1^b \equiv 1 \pmod{n}$$

for any $a, b \in \mathbb{Z}$. In particular,

$$x^{\gcd(k,\phi(n))} \equiv 1 \pmod{n}.$$

But, by definition k is the *smallest* positive integer such that $x^k \equiv 1 \pmod{n}$, so that $k \leq \gcd(k, \phi(n))$. But then (since $k \geq \gcd(k, \phi(n))$ by the definition of gcd), we conclude $k = \gcd(k, \phi(n))$. Therefore $k \mid \phi(n)$. □

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.

Theorem 3. *The group $\mathbb{Z}/n\mathbb{Z}$ has zero divisors if and only if n is composite.*

Proof. Suppose that $\mathbb{Z}/n\mathbb{Z}$ has a zero divisor. Then there exists $x, y \in \mathbb{Z}/n\mathbb{Z}$, such that $x, y \not\equiv 0 \pmod{n}$, but such that $xy \equiv 0 \pmod{n}$. Then $n \mid xy$. If n were prime, then this would imply $n \mid x$ or $n \mid y$, which is a contradiction. So n is composite.
For the converse, suppose that n is composite. Then we may write $n = ab$ for some $1 < a, b, < n$. In particular, $a, b \not\equiv 0 \pmod{n}$, but $ab \equiv 0 \pmod{n}$, i.e. we have located zero divisors in $\mathbb{Z}/n\mathbb{Z}$. □

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 $\gcd(a, \phi(n)) = 1$.

Theorem 4. *Suppose $\mathbb{Z}/n\mathbb{Z}$ has a primitive root. Consider the function*

$$f_a : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*, \quad x \mapsto x^a.$$

Then f_a is bijective if and only if $\gcd(a, \phi(n)) = 1$.

Proof. First, suppose that $\gcd(a, \phi(n)) = 1$. Then a is invertible modulo $\phi(n)$. In particular, for invertible x, we can compute, using the fact that $x^{\phi(n)} \equiv 1 \pmod{n}$, that

$$f_a \circ f_{a^{-1}}(x) \equiv x^{a^{-1}a} \equiv x \pmod{n},$$
$$f_{a^{-1}} \circ f_a(x) \equiv x^{aa^{-1}} \equiv x \pmod{n}.$$

Therefore, f_a is invertible.
For the converse, suppose that f_a is bijective, and let $g = \gcd(a, \phi(n))$. Then let $d = \phi(n)/g$. Then, $\phi(n) = dg$, so that

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

for any invertible x. But by bijectivity of f_a, this implies

$$x^d \equiv 1 \pmod{n}$$

for any invertible x. Since $d < \phi(n)$, this contradicts the existence of a primitive root. □