HOMEWORK #1 – MATH 5405
SPRING 2016

DUE: THURSDAY, 1/21/2016

(1) Use the Euclidean algorithm to compute the multiplicative inverse of 131 modulo 1979. Then solve $131x \equiv 11(\text{mod} 1979)$.

(2) Write down a multiplication table for $\mathbb{Z}/15\mathbb{Z}$ and identify the invertible elements. Consider the group of invertible elements under multiplication mod 15. Does this group have a generator/a primitive root?[1]

(3) Suppose that $a, b > 0$ are integers. Suppose that d is the smallest positive integer of the form $d = ax + by$ where $x, y \in \mathbb{Z}$. We want to show that $d = \gcd(a, b)$. We do this in several steps.
   (a) Suppose $e = as + bt > 0$ is another integer where $s, t \in \mathbb{Z}$. Prove that d divides e.
   Hint: If d does not divide e, find the remainder of the division and contradict the minimality of d.
   (b) Use (a) to show that d divides both a and b.
   (c) Suppose that c is another divisor of both a and b, show that c divides d.
   Hint: Indeed, show that c divides everything of the form $au + bv$.
   (d) Use parts (b) and (c) to conclude that $d = \gcd(a, b)$.

(4) Suppose that F is a finite field with p^c elements where p is some prime. Let $F^\times$ denote the group of units under multiplication. Let's give a quick proof that $F^\times$ is cyclic (ie, it has a generator or primitive root).
   (a) Suppose that $x \in F^\times$ is an element of largest order, say $m = |x|$. If $m < p^c - 1 = |F^\times|$, show that there there is an element y with $y^m \neq 1$ and hence that $|y|$ does not divide m.
   (b) Let $n = |y|$. Show there is a prime power q^v where $q^v | n$ but q^v does not divide m. Show that $s = y^{n/q^v}$ has order q^v.
   (c) Let q^u be the largest power of q which divides m. Show that $t = x^{q^u}$ has order m/q^u.
   (d) Prove the following lemma. If a, b are elements of an Abelian group with relatively prime orders, then $|ab| = |a| \cdot |b|$.
   Hint: Notice than a a and a^{-1} have the same order.
   (e) Apply the lemma from (d), to the elements s and t and contradict the maximality of the choice of x.

(5) Consider the ring $\mathbb{Z}/2\mathbb{Z}[x]/(x^2 = x + 1)$. This is the polynomial ring where we declare $x^2 = x + 1$. Hence every polynomial in the ring can be rewritten as a linear polynomial by repeatedly applying this relation.
   (a) Write down all the elements in this ring.
   (b) Write down the multiplication table for this ring and verify that the ring is a field.

[1] An element whose order is equal to the size of the group. A group with a generator is called *cyclic*.