Mathematics GU4041
Introduction to Modern Algebra

Assignment #4

Due October 3, 2016

As stated in class, we define $\langle n \rangle = \{i \in \mathbf{N} \mid 0 < i \leq n\}$. That is, $\langle n \rangle = \{1, \ldots, n\}$ if $n > 0$, while $\langle n \rangle = \varnothing$ if $n = 0$.

If S is a finite set, let $\#S$ be the number of elements in the set, that is, the number $n \in \mathbf{N}$ for which S is bijective to $\langle n \rangle$. For example, $\#\varnothing = 0$. You may use without proof the following facts: (a) $\#S$ is well-defined, that is, if $\langle m \rangle$ is bijective to $\langle n \rangle$, then $m = n$; (b) if $T \subset S$, then $\#(S \setminus T) = \#S - \#T$. You may prove these things for extra credit if you like; submit them directly to me.

Also, for $n \in \mathbf{Z}$, define the *absolute value* $|n|$ to be n if $n \geq 0$ and $-n$ if $n \leq 0$. You may use without proof that for all $a, b \in \mathbf{Z}$, we have $|ab| = |a|\,|b|$. (Again, it would be a good optional exercise to prove this.)

1. Prove that for all $n \in \mathbf{Z}$, $n > 0$ implies $n - 1 \geq 0$.

2. (Exercise 3 from class) Let $m, n \in \mathbf{Z}$. Prove that $m \mid n$ and $n \neq 0$ imply $m \leq |n|$.
Hint: trichotomy.

3. (Exercise 4 from class) Let $d, a, b \in \mathbf{Z}$. Prove that $d \mid a$ and $d \mid b$ imply that for all $x, y \in \mathbf{Z}$, $d \mid (ax + by)$.

4. Let $n \in \mathbf{Z}$, $n > 1$. An element $[a] \in \mathbf{Z}_n$ is said to have a *reciprocal* $[b] \in \mathbf{Z}_n$ if $[a][b] = [1] \in \mathbf{Z}_n$.

(a) Prove that if $(a, n) \neq 1$, then there exists $[c] \in \mathbf{Z}_n$ with $[c] \neq [0] \in \mathbf{Z}_n$ but $[a][c] = [0] \in \mathbf{Z}_n$.

(b) Prove that if $(a, n) \neq 1$, then $[a]$ has no reciprocal in $\mathbf{Z}_n$.

(c) On the other hand, prove that if $(a, n) = 1$, then $[a]$ has a reciprocal in $\mathbf{Z}_n$.

5. For $n \in \mathbf{N}$, define the *Euler totient function* $\phi(n)$ to be the number of integers $a \in \langle n \rangle$ such that the greatest common divisor $(a, n) = 1$.

(a) Determine $\phi(n)$ for $n = 7, 8, 9, 10, 11$, showing (a little of!) your work.

(b) If p is prime and $m \in \mathbf{N}$, prove that $\phi(p^m) = p^m - p^{m-1}$.

6. (a) Prove that the number of elements of $\mathbf{Z}_n$ having a reciprocal is $\phi(n)$.

(b) If $[a]$ and $[b] \in \mathbf{Z}_n$ have reciprocals, prove that $[a][b]$ does too.