MA347 – HW4

Jonathan Lam

February 4, 2021

1. Prove that for $b, g, h, m, n \in \mathbb{Z}$, $b|g$ and $b|h \Rightarrow b|mg + nh$.

   Proof. $b|g \Rightarrow g = xb$ for some $x \in \mathbb{Z}$, and $b|h \Rightarrow h = yb$ for some $y \in \mathbb{Z}$. Thus $mg + nh = m(xb) + n(yb) = (mx)b + (ny)b = (mx + ny)b \Rightarrow b|mg + nh$. □

2. For p prime and $[x]_p \neq [0]_p$, prove that there is $[y]_p \in \mathbb{Z}/p\mathbb{Z}$ such that $[x]_p[y]_p = [1]_p$. (I.e., prove that there exists a multiplicative inverse in the quotient group formed by the modulus.)

   Proof. Let $a \in [x]_p$ (i.e., $a \equiv x \bmod p$). Since the product is well-defined (i.e., $[x]_p[y]_p = [xy]_p$), we need only prove that $\exists m$ such that $am \equiv 1 \pmod p$ (i.e., that $am \in [1]_p$).

   $a \notin [0]_p \Rightarrow p \nmid a$. Since the only factors of p are 1 and p, $\gcd(a, p) = 1$. Then 1 exists in the ideal generated by a and p, i.e., $\exists m, n \in \mathbb{Z}$ such that $ma + nb = 1 \Rightarrow ma \equiv 1 \pmod p \Rightarrow ma \in [1]_p$.

   Choose $[y]_p = [m]_p$, i.e., the modular equivalence class of which m is a member. Then $[x]_p[y]_p = [a]_p[m]_p = [am]_p = [1]_p$. □