Homework 3 Solutions

MTH 310

2. Suppose for the sake of contradiction that there are finitely many primes $p_1, \dots, p_k$. Consider the number $a = p_1 p_2 \dots p_k + 1$. Since $(n, n+1) = 1$ for all n, we perceive that $(p_1 \dots p_k, p_1 \dots p_k + 1) = 1$, implying that a is not divisible by any of the primes $p_1, \dots, p_k$. Since every integer has a prime factorization, this is impossible. So there must be infinitely many prime numbers.

3. Suppose that a and b are integers such that $a \equiv b(\mod p)$ for every positive prime p. This implies that the difference $a - b$ is divisible by p for every prime p. But there is only one number divisible by every prime, namely 0.

4. Suppose that $[a] = [1]$ in $\mathbb{Z}_n$. Then $a - 1 = nk$ for some $k \in \mathbb{Z}$. In particular we have $a + n(-k) = 1$, so 1 may be written as a linear combination of a and n. We saw on the quiz that this implies that $(a, n) = 1$. However, conversely, observe that $(5, 6) = 1$ but $[5] \neq [1]$ in $\mathbb{Z}_6$.

5. (a) We see that $10^n = 1 + 9(1 + 10 + \dots + 10^{n-1})$. Ergo $10^n \equiv 1(\mod 9)$.

   (b) Let $a = a_0 + a_1(10) + a_2(100) + \dots + a_n(10^n)$. Then by part (a), we see that

   $$a = a_0 + a_1(10) + a_2(100) + \dots + a_n(10^n) \equiv a_1 + a_2(1) + \dots + a_n,$$

   as desired.

6. The solutions to $[x]^2 \oplus 3 \otimes [x] \oplus [2] = [0]$ in $\mathbb{Z}_6$ are [1],[2], [4], and [5] (as one can see from writing out the compuations).

7. (a) In $\mathbb{Z}_7$ we perceive that $[3]^1 = [3]$, $[3]^2 = [2]$, $[3]^3 = [6]$, $[3]^4 = [4]$, $[3]^5 = [5]$, $[3]^6 = [1]$.

   (b) In $\mathbb{Z}_5$ we perceive that $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [3]$, $[2]^4 = [1]$.

   (c) In $\mathbb{Z}_6$ this is impossible, as we see that
      - $[2]^1 = [2], [2]^2 = [4], [2]^3 = [2], \dots$
      - $[3]^1 = [3]$, $[3]^2 = [3], \dots$
      - $[4]^1 = [4]$, $[4]^2 = [4], \dots$
      - $[5]^1 = [5]$, $[5]^2 = [5], \dots$

   (d) i. We may compute directly that the solutions to $x^2 + x = [0]$ in $\mathbb{Z}_5$ are [0] and [4].

      ii. We may compute directly that the solutions to $x^2 + x = [0]$ in $\mathbb{Z}_6$ are $[0], [2], [3], [5]$.

iii. Let p be prime, and let $[a]$ be a solution to $x^2 + x = [0]$ in $\mathbb{F}_p$, chosen so that $0 \leq a < p$. Then we observe that $a^2 + a = kp$ for some integer k. So we have $p|a(a+1)$. Since p is a prime, this implies that $p|a$ or $p|a+1$. If $p|a$, we see that $a = 0$. If $p|a+1$, we see that $a + 1 = p$, so $a = p - 1$. So the solutions to $x^2 + x = [0]$ are exactly $[0]$ and $[p-1]$.

8. We observe that in $\mathbb{Z}_n$, it is always the case that $n \odot [x] = [nx] = [0]$ for all $[x]$.

   In $\mathbb{Z}_2$, we have $([a] \oplus [b])^2 = [a]^2 \oplus (2 \odot [x]) + [b]^2 = [a]^2 \oplus [b]^2$.

   In $\mathbb{Z}_3$, we have $([a] \oplus [b])^3 = [a]^3 \oplus (3 \odot [a]^2 \odot [b]) + (3 \odot [a] \odot [b]^2) \oplus [b]^3 = [a]^2 \oplus [b]^3$.

   In $\mathbb{Z}_5$, we have

$$
\begin{aligned}
([a] \oplus [b])^5 = [a]^5 + (5 \odot [a]^4 \odot [b]) \oplus (20 \odot [a]^3 \odot [b]^2) \oplus (20 \odot [a]^2 \odot [b]^3) \oplus (5 \odot [a] \odot [b]^4) \oplus [a]^5 \\
= [a]^5 \oplus [b]^5.
\end{aligned}
$$

   We conclude that probably in $\mathbb{Z}_7$ we have $([a] + [b])^7 = [a]^7 \oplus [b]^7$.