Homework 2 Solutions

MTH 310

2. (a) We observe that

$$\begin{aligned}
5^2 &= 25 = 8(3) + 1\\
7^2 &= 49 = 8(6) + 1\\
11^2 &= 121 = 8(15) + 1\\
27^2 &= 729 = 8(90) + 1.
\end{aligned}$$

   (b) We conjecture that if we divide an odd square by 8, the remainder is always 1.

   (c) Observe that by the Division Algorithm, any integer may be written as one of $4k, 4k+1, 4k+2, 4k+3$ for suitable k. Clearly $4k$ and $4k+2$ are divisible by 2, hence even, so indeed any odd integer a may be written as one of $a = 4k+1$ or $a = 4k+3$ for suitable k. Therefore, the square of an odd integer a takes one of the following two forms:

$$\begin{aligned}
a^2 &= (4k+1)^2 = 16k^2 + 8k + 1 = 8(2k^2 + k) + 1\\
a^2 &= (4k+3)^2 = 16k^2 + 24k + 9 = 8(2k^2 + 3k + 1) + 1
\end{aligned}$$

   In either case we observe that the remainder when a^2 divided by 8 is 1.

3. (a) We observe that $138 = 24(5) + 18$, so $(138, 24) = (24, 18)$. But $24 = 18(1) + 6$, so $(24, 18) = (18, 6)$. And $18 = 6(3) + 0$, so we conclude that $(18, 6) = 6$. Therefore $(138, 24) = 5$.

   (b) We observe that $231 = 143(1)+88$, so $(231, 143) = (143, 88)$. But $143 = 88(1)+55$, so $(143, 88) = (88, 55)$. And $88 = 55(1) + 33$, so $(88, 55) = (55, 33)$. And $55 = 33(1) + 22$, so $(55, 33) = (33, 22)$. Next $33 = 22(1) + 11$, so $(33, 22) = (22, 11)$. And finally $22 = 2(11)$, so $(22, 11) = 11$. We conclude that $(231, 143) = 11$.

4. (a) We notice that $n + 1 = n(1) + 1$. Therefore $(n, n + 1) = (n, 1) = 1$ for all n.

   (b) First we consider $(n, n + 2)$. We see that $n + 2 = n(1) + 2$, implying that $(n, n+2) = (n, 2)$. The possible values of $(n, 2)$ are 1 and 2 depending on whether n is odd or even (respectively).

   Next we consider $(n, n+6)$. We observe that $n+6 = n(1)+6$, so $(n, n+6) = (n, 6)$. The number $(n, 6)$ could be any positive divisor of 6, namely $1, 2, 3$ or 6.

5. Let a be an integer with digits $a_0, a_1, a_2, \ldots, a_n$, so that $a = a_0 + a_1(10) + \cdots + a_n(10^n)$. Observe that $10^i - 1$ is divisible by 3 for all $i > 0$. Then we have

$$\begin{aligned} a &= a_0 + a_1(10) + a_2(100) + \cdots + a_n(10^n) \\ &= a_0 + a_1(1+9) + a_2(1+99) + \cdots + a_n(1 + (10^n - 1)) \\ &= (a_0 + a_1 + a_2 + \cdots + a_n) + 3\left(3a_1 + 33a_2 + \cdots + \left(\frac{10^n - 1}{3}\right) a_n\right) \end{aligned}$$

We see that a is divisible by 3 if and only if the sum $a_0 + a_1 + \cdots + a_n$ is.

6. Let $d = (a, b)$ and $k = (ca, cd)$. Since d divides both a and b, we see that cd divides both ca and cb. Since cd is a common divisor of ca and cb, it divides the greatest common divisor of ca and cb. So $cd|k$. Write $k = cde$ for some $e > 0$. Then we observe that $cde|ca$ and $cde|cb$, implying that $de|a$ and $de|b$. Since $d = (a, b)$, this implies that $de|d$, and in particular that $cde|cd$. So $k|cd$. Since k and cd are positive integers such that $k|cd$ and $cd|k$, we conclude that $k = cd$.

7. First, suppose that p is not prime. Then we may write $p = ab$ such that neither a nor b is ± 1. We may additionally insist that $a > 0$. Then we see that $a|p$, so $(a, p) = a \neq 1$. Moreover $a|p$, so $0 < a \leq |p|$; indeed, since $b \neq \pm 1$, we must have $0 < a < |p|$. Hence it cannot be the case that a is divisible by p. Therefore neither $(a, p) = 1$ or $p|a$ is true.

   Conversely, suppose that p is prime. Given an integer a, if it is not the case that $(a, p) = 1$, then since p has only two positive divisors, it must be the case that $(a, p) = |p|$. But this implies that $p|a$. Hence for every integer a, either $(a, p) = 1$ or $p|a$.

8. We check the congruences of the three potential ISBN numbers.

   (a) We see $10(3)+9(5)+8(4)+7(0)+6(9)+5(0)+4(5)+3(1)+2(8)+9 = 209 = 11(19)$, so $3 - 540 - 90518 - 9$ is a valid ISBN number.

   (b) We see $10(0) + 9(0) + 8(3) + 7(1) + 6(1) + 5(0) + 4(5) + 3(5) + 2(9) + 5 = 95$ is not divisible by 11, so $0 - 031 - 10559 - 5$ is not a valid ISBN number.

   (c) We see $10(0)+9(3)+8(8)+7(5)+6(4)+5(9)+4(5)+3(9)+2(6)+10 = 264 = 11(24)$, so $0 - 385 - 49596 - X$ is a valid ISBN number.

9. (a) Observe that $5 \equiv 1 \pmod{4}$. Since congruence is preserved by taking products, we may raise both sides of the equation to the 2000th power, obtaining $5^{2000} \equiv 1^{2000} \equiv 1 \pmod{4}$. We conclude that in $\mathbb{Z}_4$, we have $[5^{2000}] = [1]$.

   (b) Observe that $4 \equiv -1 \pmod{5}$. So as previously we may compute that $4^{2001} \equiv (-1)^{2001} \equiv -1 \equiv 4 \pmod{5}$. We conclude that $[4^{2001}] = [4]$ in $\mathbb{Z}_5$.

10. (a) This is false. We observe that $(2)(3) \equiv 0 \pmod{6}$, but neither 2 nor 3 is congruent to 0 modulo 6. So $ab \equiv 0 \pmod{n}$ does not necessarily imply that one of a and b is congruent to 0 mod n.

(b) Let n be prime, and suppose $ab \equiv 0 \pmod{n}$. Then we know $n|(ab - 0)$, implying that $n|ab$. But if a prime integer divides a product, it divides at least one of the factors. Suppose $n|a$. Then $n|(a - 0)$, so $a \equiv 0 \pmod{n}$. Similarly if $n|b$, $b \equiv 0 \pmod{n}$. So if n is prime, $ab \equiv 0 \pmod{n}$ implies that at least one of $a \equiv 0 \pmod{n}$ and $b \equiv 0 \pmod{n}$ is true.