Homework 4
Section 2.1

Jonathan Petersen
A01236750

February 1st, 2016

---

7. **If $a \in \mathbb{Z}$, prove that a^2 is not congruent to 2 modulo 4 or to 3 modulo 4.**

   By Corollorary 2.5, we see that for every $a \in \mathbb{Z}$, either $a \equiv_4 [0]_4$, $a \equiv_4 [1]_4$, $a \equiv_4 [2]_4$, or $a \equiv_4 [3]_4$. Further, by the reflexive property of congruence, $a \equiv_4 [a]_4$, which implies that $[a]_4 \in \{[0]_4, [1]_4, [2]_4, [3]_4\}$.

   Finally, we can see by Theorem 2.4 that since $a \equiv_4 a$,

$$\begin{aligned} a * a &\equiv_4 a * a \\ a^2 &\equiv_4 [a] * [a] \\ a^2 &\equiv_4 [a]^2 \end{aligned}$$

   and therefore

$$\begin{aligned} [a]^2 &\in \{[0]_4{}^2, [1]_4{}^2, [2]_4{}^2, [3]_4{}^2\} \\ [a]^2 &\in \{[0]_4, [1]_4, [4]_4, [9]_4\} \\ [a]^2 &\in \{[0]_4, [1]_4, [0]_4, [1]_4\} \\ [a]^2 &\in \{[0]_4, [1]_4\} \end{aligned}$$

   which implies that $[a]^2 \not\equiv_4 2$ and $[a]^2 \not\equiv_4 3$ ■

8. **Prove that every odd integer is congruent to 1 modulo 4 or 3 modulo 4.**

   Given any odd integer, we know that the integer may be expressed as $2i + 1$ with $i \in \mathbb{Z}$. We also know by the definition of equivalence class that

$$[2i+1]_4 = x \in \mathbb{Z} s.t. 4|x-(2i+1)$$

If we now examine the statement $4|x-(2i+1)$, we can see that since $x-(2i+1)$ must be divisible by 4, $x-(2i+1)$ must be even. Therefore, by the properties of subtraction on even and odd numbers, $x-(2i+1)$ could only be odd when x is odd.

Finally, we also know from Corollary 2.5 that

$$[x]_4 \in \{[0]_4, [1]_4, [2]_4, [3]_4\}$$

but since x must be odd we are only left with the possibilities

$$[x]_4 \in \{[1]_4, [3]_4\}$$

Substituting for x we find that

$$[2i+1]_4 \in \{[1]_4, [3]_4\} \tag{1}$$

and indeed, if $i=0$ then $2i+1$ must be in $[1]_4$, and if $i=1$ then it must be in $[3]_4$. Therefore, we know that $2i+1$ must be congruent to 1 modulo 4 or 3 modulo 4, and that both cases exist $\blacksquare$

17. **Prove that $10^n \equiv_{11} (-1)^n$ for $n>0$, $n \in \mathbb{Z}$.**

    Since $11 = 10-(-1)$, it is clear that

$$\begin{aligned} 11&|(10-(-1)) \\ 10 &\equiv_{11} -1 \end{aligned}$$

    and so by Theorem 2.2, we can see that $10^n \equiv_{11} (-1)^n$ $\blacksquare$

21. a. **Show that $10^n \equiv_9 1^n$ for $n>0$, $n \in \mathbb{Z}$.**

    Similar to the logic in problem 17, we see that:

$$\begin{aligned} 9&|(10-1) \\ 10 &\equiv_9 1 \end{aligned}$$

    So by Theorem 2.2 we find that $10^n \equiv_9 1^n \equiv_9 1$ $\blacksquare$

b. **Prove that every integer is congruent to the sum of its digits mod 9.**

It is clear that $9|10-1$. Now suppose that $9|10^n-1$. Then

$$\begin{aligned}10^{n+1}-1 &= 10(10^n)-1\\ &= (9(10^n)+10^n)-1\\ &= 9(10^n)+10^n-1\end{aligned}$$

Therefore $9|10^{n+1}-1$, and by induction it follows that $9|10^n-1$. Now consider an arbitrary integer a expressed as

$$a = 10^n d_n + 10^{n-1}d_{n-1} + ... + 10^2 d_2 + 10^1 d_1 + 10^0 d_0$$

As we showed above, each of the terms composing a are divisible by 9, which by theorem 2.2 means that they are all congruent. Furthermore, their sums are all congruent, and therefore $a \equiv_9 10^n d_n + 10^{n-1}d_{n-1} + ... + 10^2 d_2 + 10^1 d_1 + 10^0 d_0$ ■

22. a. **Give an example to show that the following statement is false: If $ab \equiv_n ac$, and $a \not\equiv_n 0$, then $b \equiv_n c$.**

Let $a = 2, b = 2, c = 4, n = 4$. Then $ab = 4$, $ac = 8$, and $ab \equiv_4 ac$. Also, $a \not\equiv_4 0$, but $b = 2 \not\equiv_4 = 4 = c$ ■

b. **Prove that the above statement is true when $gcd(a, n) = 1$.**

Given the statement $ab \equiv_n ac$, we see that this may only be true if

$$\begin{aligned}&n|ab-ac\\ &n|a(b-c)\\ &n|ak \qquad k = (b-c) \therefore k \in \mathbb{Z}\end{aligned}$$

By the properties of division, we know this may be true only if $n|a$ or $n|k$. It then follows that if the $gcd(a, n) = 1$ that n does not divide a, and therefore

$$\begin{aligned}&n|k\\ &n|b-c\\ b \equiv_n c&\end{aligned}$$

by definition ■