Homework 8

For practice: 7.42,

...and one more: For each of the following pairs (a, n) find the multiplicative inverse of $\bar{a} \in \mathbf{Z}_n$ or explain why no such inverse exists.

- $a = 51$, $n = 38$;
- $a = 17$, $n = 1029$;
- $a = 169$, $n = 4641$.

To turn in: 7.9, 7.24, 7.32 (don't worry about showing there are exactly d solutions), 7.33, 7.35,

...and one more: Recall that in class, we discussed a nice trick for checking whether a number is divisible by 3. Find a similar trick for checking whether a number is divisible by 11. Describe this test and justify it. Finally, illustrate this test using a specific example.

Solutions to graded problems

7.9. Fermat's Little Theorem says that $2^{12} \equiv 1 \bmod 13$, so since $100 = 12 \cdot 8 + 4$, we have

$$2^{100} \equiv (2^{12})^8 \cdot 2^4 \equiv 1^8 \cdot 16 \equiv 16 \equiv 3 \bmod 13.$$

$\square$

7.24. I claim that f is injective if and only if $n = 2$.
Proof. Note that $f(1) \equiv f(-1) \equiv 1 \bmod n$. So if f is injective, we must have that $1 \equiv -1 \bmod n$. In other words, $2 = 1 - (-1)$ is a multiple of n. Of course, the only way this can happen is if $n = 2$. So if f is injective, then $n = 2$. On the other hand, $\mathbf{Z}_2 = \{\bar{0}, \bar{1}\}$ consists of only two elements. Moreover, $f(\bar{0}) = \bar{0}$ and $f(\bar{1}) = \bar{1}$, so f really is injective when $n = 2$.
$\square$

7.32 We have

$$\begin{aligned} \bar{a}\bar{x} &= \bar{b} \in \mathbf{Z}_n \quad \Leftrightarrow \\ ax &\equiv b \bmod n \quad \Leftrightarrow \\ ax - b &= kn \text{ for some } k \in \mathbf{Z} \quad \Leftrightarrow \\ ax - kn &= b. \end{aligned}$$

So in summary, $\bar{a}\bar{x} = \bar{b}$ for some $\bar{x} \in \mathbf{Z}_n$ if and only if there is an integer combination of a and n equal to b. By theorem 6.12, such a combination exists if and only if b is a multiple of $\gcd(a, n)$. $\square$

7.33. We seek an $x \in \mathbf{N}$ a little less than 1500 such that

$$\begin{aligned} x &\equiv 1 \bmod 5 \\ x &\equiv 3 \bmod 7 \\ x &\equiv 3 \bmod 11. \end{aligned}$$

The algorithm for finding such an x goes as follows. First we find integer combinations of 5 and $7 \cdot 11$, 7 and $5 \cdot 11$, and 11 and $5 \cdot 7$ that equal one. I was able to find the first two combinations by trial and error; I had to use the Euclidean algorithm to find the last combination. Anyhow, here's what I found (there are other combinations that work):

$$\begin{aligned} 1 &= 5 \cdot 31 + 77 \cdot (-2) \\ 1 &= 7 \cdot 8 + 55 \cdot (-1) \\ 1 &= 11 \cdot 16 + 35 \cdot (-5). \end{aligned}$$

Now to get one possible solution x, we take the second term in each integer combination, multiply it by the number on the right side of the corresponding congruence, and add up the results. That is,

$$x = 1 \cdot 77 \cdot (-2) + 3 \cdot 55 \cdot (-1) + 3 \cdot 35 \cdot (-5) = -844$$

is one common solution of the three given congruences. The Chinese Remainder Theorem tells us that we can find all other solutions by adding on multiples of $5 \cdot 7 \cdot 11 = 385$. For instance, the smallest non-negative solution is

$$x = -844 + 3 \cdot 385 = 311.$$

To answer the question, though, we need to find the largest solution x that is smaller than 1500. This is

$$x = -844 + 6 \cdot 385 = 1466.$$

So there were 1500 - 1466 = 34 deserters.

7.35. We seek the smallest $x \in \mathbf{N}$ such that

$$\begin{aligned} x &\equiv 3 \bmod 6 \\ x &\equiv 4 \bmod 7 \\ x &\equiv 5 \bmod 8. \end{aligned}$$

The Chinese remainder theorem does not apply directly here, because 6 and 8 are not relatively prime. However, $x \equiv 3 \bmod 6$ if and only if x is an odd multiple of 3. Moreover, if

$x \equiv 5 \bmod 8$, then x is certainly odd, so instead of asking for $x \equiv 3 \bmod 6$, it's enough to ask for $x \equiv 0 \bmod 3$. Our three congruences therefore become

$$\begin{aligned} x &\equiv 0 \bmod 3 \\ x &\equiv 4 \bmod 7 \\ x &\equiv 5 \bmod 8. \end{aligned}$$

Since the integers 3,7,8 are pairwise relatively prime, we can apply the algorithm from the Chinese remainder theorem to find x. Working as in the previous problem, we observe that

$$\begin{aligned} 1 &= 3 \cdot 19 + 56 \cdot (-1) \\ 1 &= 7 \cdot 7 + 24 \cdot (-2) \\ 1 &= 8 \cdot 8 + 21 \cdot (-3). \end{aligned}$$

From this we obtain the solution

$$x = 0 \cdot (-56) + 4 \cdot (-48) + 5 \cdot (-63) = -507.$$

And the smallest non-negative solution will then be the only one between 0 and $3 \cdot 7 \cdot 8 = 168$. This is

$$x = -507 + 4 \cdot 168 = 165.$$

Additional problem: Let $x \in \mathbf{N}$ be a number with base ten decimal expansion $a_k \dots a_0$. Then

$$x = \sum_{j=0}^{k} a_j \cdot 10^j = a_k \cdot 10^k + \dots + a_1 \cdot 10 + a_0,$$

and $11|x$ if and only if $x \equiv 0 \bmod 11$. Now $10 \equiv -1 \bmod 11$, so $10^j \equiv (-1)^j \bmod 11$. Hence

$$x \equiv \sum_{j=0}^{k} (-1)^j a_j \equiv a_0 - a_1 + a_2 - + \dots + (-1)^k a_k \bmod 11$$

This means that x is divisible by 11 if and only if sum of the even order digits minus the sum of the odd order digits is divisible by 11.

For instance, 18394728 is divisible by 11, because

$$8 - 2 + 7 - 4 + 9 - 3 + 8 - 1 = 22$$

which is certainly divisible by 11.