Problem 0.1 (Chapter 14, problem 1b). Show that $n^7 - n$ is divisible by 42 for all integers n.

Proof. We note that $42 = 2 \cdot 3 \cdot 7$. Let n be an integer. If n is even, then n^7 is also even, and if n is odd, then n^7 is also odd. Therefore

$$n^7 \equiv n \pmod 2$$

Now let's look modulo 3. Applying Fermat's little theorem we get

$$n^3 \equiv n \pmod 3$$

Therefore

$$n^7 \equiv \cdot n \cdot n^3 \cdot n^3 \equiv n \cdot n \cdot n \equiv n \pmod 3$$

Finally let's look modulo 7. Applying Fermat's little theorem we have

$$n^7 \equiv n \pmod 7$$

We have shown that n^7 is congruent to n modulo $2, 3$, and 7. Thus, $n^7 - n$ is divisible by $2, 3$, and 7. As these numbers are all coprime, this implies $n^7 - n$ is divisible by $2 \cdot 3 \cdot 7 = 42$. Therefore $n^7 \equiv n \pmod{42}$. ☐

Problem 0.2 (Chapter 14, problem 3). Let $N = 561 = 3 \cdot 11 \cdot 17$. Prove that, for every integer a which is coprime to N, we have

$$a^{N-1} \equiv 1 \pmod N$$

Proof. Suppose that a is coprime to N. By Fermat's little theorem, we have

$$\begin{aligned} a^2 &\equiv 1 \pmod 3 \\ a^{10} &\equiv 1 \pmod{11} \\ a^{16} &\equiv 1 \pmod{17} \end{aligned}$$

We notice that $N - 1 = 560$ is divisible by $2, 10$, and 16 (the first two are pretty clear, and for the last one we have $560 = 16 \cdot 35$). It follows that

$$a^{560} \equiv (a^2)^{280} \equiv 1 \pmod 3$$

Similarly,

$$a^{560} \equiv (a^{10})^{56} \equiv 1 \pmod{11}$$

and

$$a^{560} \equiv (a^{16})^{35} \equiv 1 \pmod{17}$$

Thus $a^{560} - 1$ is divisible by $3, 11$, and 17. These are all distinct prime numbers, so $a^{560} - 1$ is divisible by $3 \cdot 11 \cdot 17 = 561$, and therefore

$$a^{560} \equiv 1 \pmod{561}$$

☐

Problem 0.3 (Chapter 14, problem 6). Calculate $(p - 1)! \pmod p$.

Proof. We will show that

$$(p - 1)! \equiv p - 1 \pmod p$$

To prove this, we expand out $(p - 1)!$ to get

$$(p - 1)! = (p - 1) \cdot (p - 2) \cdots 2 \cdot 1$$

We proved in class that every integer $0 < a < p$ has a multiplicative inverse modulo p. Thus, for each of the numbers in the above product, its multiplicative inverse also appears somewhere in the product. As long as a is not its own multiplicative inverse, we can therefore pair up a and its inverse in the above product, and they will cancel each other out. Let's work out when it is that a number is its own multiplicative inverse. Suppose that $0 < a < p$ and

$$a \cdot a \equiv a^2 \equiv 1 \pmod{p}$$

Then p divides $a^2 - 1 = (a+1)(a-1)$. This means p divides either $a+1$ or $a-1$, so either $a \equiv -1 \pmod{p}$ or $a \equiv 1 \pmod{p}$. Thus we have $a = 1$ or $a = p-1$. Going back to the product, we see that for all the numbers besides 1 and $p-1$, we can pair them with their multiplicative inverse. Thus we have

$$(p-1)! \equiv (p-1) \cdot (p-2) \cdots 2 \cdot 1 \equiv (p-1) \cdot 1 \equiv p-1 \pmod{p}$$

which is what we claimed. $\square$