Prop. If n is an integer, then $3 \mid (n^3 - n)$.

Proof. By the Division Algorithm n is congruent to one of 0, 1 or 2 $\mod 3$. There are three cases to consider.

1. If $n \equiv 0 \mod 3$, then $n^3 - n \equiv 0 - 0 \equiv 0 \mod 3$.
2. If $n \equiv 1 \mod 3$, then $n^3 - n \equiv 1 - 1 \equiv 0 \mod 3$.
3. If $n \equiv 2 \mod 3$, then $n^3 - n \equiv 8 - 2 \equiv 6 \equiv 0 \mod 3$.

In all three cases $n^3 - n \equiv 0 \mod 3$, and so $3 \mid (n^3 - n)$. □

Prop. If n is an integer, then $5 \mid (n^5 - n)$.

Proof. By the Division Algorithm n is congruent to one of $0, 1, \ldots 4 \mod 5$. There are five cases to consider.

1. If $n \equiv 0 \mod 5$, then $n^5 - n \equiv 0 - 0 \equiv 0 \mod 5$.
2. If $n \equiv 1 \mod 5$ or if $n \equiv 4 \equiv -1 \mod 5$, then $n^5 - n \equiv (\pm 1)^5 - (\pm 1) \equiv \pm(1 - 1) \equiv 0 \mod 5$.
3. If $n \equiv 2 \mod 5$ or $n \equiv 3 \equiv -2 \mod 5$, then $n^5 - n \equiv (\pm 2)^5 - (\pm 2) \equiv \pm(2^5 - 2) \equiv 0 \mod 5$.

In all five cases $n^5 - n \equiv 0 \mod 5$, and so $5 \mid (n^5 - n)$. □

Prop. If n is an integer, then $7 \mid (n^7 - n)$.

Proof. By the Division Algorithm n is congruent to one of $0, 1, \ldots, 6 \mod 7$. There are seven cases to consider.

1. If $n \equiv 0 \mod 7$, then $n^7 - n \equiv 0 - 0 \equiv 0 \mod 7$.
2. If $n \equiv 1 \mod 7$ or if $n \equiv 6 \equiv -1 \mod 7$, then $n^7 - n \equiv (\pm 1)^7 - (\pm 1) \equiv \pm(1 - 1) \equiv 0 \mod 7$.
3. If $n \equiv 2 \mod 7$ or if $n \equiv 5 \equiv -2 \mod 7$, then $n^7 - n \equiv (\pm 2)^7 - (\pm 2) \equiv \pm(2^7 - 2) \equiv 0 \mod 7$.
4. If $n \equiv 3 \mod 7$ or if $n \equiv 4 \equiv -3 \mod 7$, then $n^7 - n \equiv (\pm 3)^7 - (\pm 3) \equiv \pm(3^7 - 3) \equiv 0 \mod 7$.

In all seven cases $n^7 - n \equiv 0 \mod 7$, and so $7 \mid (n^7 - n)$. □

Remark. The case of $11 \mid (n^{11} - n)$ is similar. We will see a uniform proof that $p \mid (n^p - n)$ for all natural numbers n in the case p is a prime. It will be a corollary of Fermat's Little Theorem.

Q. Does 4 divide $n^4 - n$ for every integer n?

Answer. No. By the Division Algorithm n is congruent to one of $0, 1, 2, 3 \mod 4$. There are 4 cases to consider.

1. If $n \equiv 0 \mod 4$, then $n^4 - n \equiv 0 - 0 \equiv 0 \mod 4$.
2. If $n \equiv 1 \mod 4$, then $n^4 - n \equiv 1 - 1 \equiv 0 \mod 4$.
3. If $n \equiv 2 \mod 4$, then $n^4 - n \equiv 16 - 2 \equiv 2 \mod 4$.
4. If $n \equiv 3 \mod 4$, then $n^4 - n \equiv 81 - 3 \equiv 2 \mod 4$.

Thus, $4 \mid (n^4 - n)$ in the cases $n \equiv 0, 1 \mod 4$, and $4 \nmid (n^4 - n)$ in the cases $n \equiv 2, 3 \mod 4$.

Remark. The questions of whether $a \mid (n^a - n)$ for $a = 6, 8, 9, 10$ are handled similarly to this one.

Remark. You may be tempted to conjecture the following. *If p is a prime number, then $p \mid (n^p - n)$ for all integers n.* This would be correct, and a uniform proof (for all primes p) follows from Fermat's Little Theorem.

Remark. You may be tempted to conjecture the following. *If a is not a prime number, then $a \nmid (n^a - n)$ for some integers n.*

You could check this conjecture for all composite numbers up to 500, and find that it is true. However, there are composite numbers a for which $a \mid (n^a - n)$ for all integers n. Such numbers are called Carmichael numbers. The smallest Carmichael number is $a = 561 = (3)(11)(17)$.

To see that $561 \mid (n^{561} - n)$ for all integers n, we break the problem into more manageable pieces.

- Show that $3 \mid (n^{561} - n)$ for all integers n.
- Show that $11 \mid (n^{561} - n)$ for all integers n.
- Show that $17 \mid (n^{561} - n)$ for all integers n.
- Since 3, 11, and 17 are all relatively prime, conclude that $561 \mid (n^{561} - n)$ for all integers n.

The first 3 statements above can be verified by hand. Computing big powers is not so bad, since we are working modulo relatively small numbers (3, 11, and 17).

However, Fermat's Little Theorem will greatly speed things up. We prove the middle statement as an example. Fermat's Little Theorem tells us that

$$n^{10} \equiv 1 \mod 11$$

This implies that

$$n^{560} \equiv (n^{10})^{56} \equiv 1^{56} \equiv 1 \mod 11$$

Now multiplying across by n gives

$$n^{561} \equiv n \mod 11$$

or in other words $11 \mid (n^{561} - n)$.