Is $\mathbb{Z}_n^* = \langle 10 \rangle$? and repeating decimal expansions.

When we write $\frac{1}{7} = .\overline{142857}$, what we really mean is that

$$\frac{1}{7} = \frac{142857}{10^6} + \frac{142857}{10^{12}} + \frac{142857}{10^{18}} + \cdots = \frac{142857}{10^6}\sum_{n=0}^{\infty}\left(\frac{1}{10^6}\right)^n = \frac{142857}{10^6}\cdot\frac{1}{1-10^{-6}} = \frac{142857}{10^6}\cdot\frac{10^6}{10^6-1} = \frac{142857}{10^6-1},$$

which really means that

$$7 \cdot 142857 = 10^6 - 1, \text{ i.e., } 7|10^6 - 1, \text{ i.e., } 10^6 \equiv_7 1,$$

and 6 is the smallest power of 10 which is congruent to 1 modulo 7 (since otherwise the repeating decimal for $\frac{1}{7}$ would be shorter), i.e.,

$$|10| = 6 \text{ in } \mathbb{Z}_7^*.$$

This relationship between repeating decimals and the group $\mathbb{Z}_n^*$ holds more generally (and the proof is identical to the argument above)! The length of the repeating decimal expansion of $\frac{1}{n}$, when n and 10 are relatively prime, is the order of 10 in $\mathbb{Z}_n^*$. [When n and 10 are not relatively prime, you need to first remove all factors of 2 and 5 from n (which contribute to the non-repeating initial part of the decimal expansion of $\frac{1}{n}$) before computing the order of 10; e.g., $\frac{1}{6}$ has repeating part of length 1, because $|10| = 1$ in $\mathbb{Z}_3^*$.]

As we have just seen, $\frac{1}{7}$ has repeating decimal of length 6, so $|10| = 6$ in $\mathbb{Z}_7^*$. On the other hand, in class we showed that $|10| = 16$ in $\mathbb{Z}_{17}^*$, and so we now know that the length of the repeating decimal for $\frac{1}{17}$ is 16 (and we can compute the term that repeats, as $\frac{10^{16}-1}{17}$ (!)).

Since we know that $|\mathbb{Z}_7^*| = 6$ and $|\mathbb{Z}_{17}^*| = 16$, what these order calculations also tell us is that $\mathbb{Z}_7^* = \langle 10 \rangle$ and $\mathbb{Z}_{17}^* = \langle 10 \rangle$, that is, both of these groups are cyclic, and are generated by 10.

There is a conjecture, originally due to Gauss, that there are in fact infinitely many integers n so that [$\gcd(10, n) = 1$ and] the repeating decimal for $\frac{1}{n}$ has length $n-1$; that is, $|10| = n-1$ in $\mathbb{Z}_n^*$). [Note that if n is not prime, then it is not possible for $|10|$ to equal $n-1$, since $|\mathbb{Z}_n^*| < n-1$ (the factors of n do not lie in $\mathbb{Z}_n^*$) and we know that $|10| \leq |\mathbb{Z}_n^*|$, since the elements 1, 10, 10^2, …, $10^{|10|-1}$ must be distinct.] This conjecture remains unproven to this day, however! A computation using Maple finds that the first several prime numbers p so that $\mathbb{Z}_p^* = \langle 10 \rangle$ (and so $\frac{1}{p}$ has decimal expansion of length $p-1$) are:

$p =$ 7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, 223, 229, 233, 257, 263, 269, 313, 337, 367, 379, 383, 389, 419, 433, 461, 487, 491, 499, 503, 509, 541, 571, 577, 593, 619, 647, 659, 701, 709, 727, 743, 811, 821, 823, 857, 863, 887, 937, 941, 953, 971, 977, 983, 1019, 1021, 1033, 1051, 1063, 1069, 1087, 1091, 1097, 1103, 1109, 1153, 1171, 1181, 1193, 1217, 1223, 1229, 1259, 1291, 1297, 1301, 1303, 1327, 1367, 1381, 1429, 1433, 1447, 1487, 1531, 1543, 1549, 1553, 1567, 1571, 1579, 1583, 1607, 1619, 1621, 1663, 1697, 1709, 1741, 1777, 1783, 1789, 1811, 1823, 1847, 1861, 1873, 1913, 1949, 1979, 2017, 2029, 2063, 2069, 2099

On the other hand, considerable progress has been made on the conjecture; in fact there is a stronger conjecture, due to Emil Artin, that if k is not a perfect square, then $\mathbb{Z}_p^* = \langle k \rangle$ for infinitely many primes p. [Even more, it is conjectured that the fraction of p so that $\mathbb{Z}_p^*$ is generated by k, as p goes to infinity, converges to the same constant, approximately 0.3739558 ("Artin's constant").] In 1986 David Heath-Brown proved that Artin's conjecture fails for at most two prime numbers k, but his proof is non-constructive, and to date there is not a single value of k for which the conjecture is known to be true!