Math 445 Homework 3

Due Wednesday, September 22

11. [NZM p.83, # 13] When applying the Pollard ρ method, starting from a_1, suppose we find that $a_1, \ldots, a_{17}$ are all distinct, mod n, but then $a_{18} \equiv a_{11}$. What is the smallest k for which $a_{2k} \equiv a_k$?

12. [The RSA algorithm works even if $(A, n) > 1$.]

    Show that if $n = pq$ is a product of distinct primes and $de \equiv 1 \pmod{(p-1)(q-1)}$, then $A^{de} \equiv A \pmod{n}$.

    (Hint: show that it works mod p and q, first.)

13. [NZM p. 86, # 5] Show that if $p^2 | n$ for some $p \geq 2$, then there are $a \not\equiv b \pmod{n}$ for which $a^k \equiv b^k \pmod{n}$ for every $k \geq 2$.

14. Show that if $n | m$, and $(10, m) = 1$, then the period of the decimal expansion of $1/n$ divides the period of the decimal expansion of $1/m$.

15. Show that for every $n \geq 2$, $\mathrm{ord}_{3^n}(10) = 3^{n-2}$.

    (Hint: induction! Show first that $\mathrm{ord}_{3^n}(10) | 3^{n-2}$, and then that it can't be *smaller*.) [Consequently, the period of $1/3^n$ is 3^{n-2} .]