TYPE YOUR NAME HERE
HW 21: 4.7 - 4.11
M328K
April 10th, 2012

4.7 Question. *Choose some relatively prime natural numbers a and n and compute the order of a modulo n. Frame a conjecture concerning how large the order of a modulo n can be, depending on n.*

Answer. □

4.8 Theorem. *Let a and n be natural numbers with $(a, n) = 1$ and let $k = \mathrm{ord}_n(a)$. Then the numbers a^1, a^2, ..., a^k are pairwise incongruent modulo n.*

Proof. □

4.9 Theorem. *Let a and n be natural numbers with $(a, n) = 1$ and let $k = \mathrm{ord}_n(a)$. For any natural number m, a^m is congruent modulo n to one of the numbers a^1, a^2, ..., a^k.*

Proof. □

4.10 Theorem. *Let a and n be natural numbers with $(a, n) = 1$, let $k = \mathrm{ord}_n(a)$, and let m be a natural number. Then $a^m \equiv 1 \pmod{n}$ if and only if $k|m$.*

Proof. □

4.11 Theorem. *Let a and n be natural numbers with $(a, n) = 1$. Then $\mathrm{ord}_n(a) < n$.*

Proof. □