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 $k = \text{ord}_n(a)$. Then the numbers a^1, a^2, ..., a^k are pairwise incongruent modulo n.*

Proof. et a and n be natural numbers with $(a, n) = 1$ and let $k = \text{ord}_n(a)$. We will show the numbers a^1, a^2, ..., a^k are pairwise incongruent modulo n. Assume by way of contradiction that there exist two natural numbers i and j such that $1 \le i, j \le k$, $i \ne j$, and $a^i \equiv a^j \pmod{n}$. Assume without loss of generality that $i > j$. Let $m = i - j$ so $i = j + m$ and $0 < m < k$. Then $a^i = a^j a^m$ and $a^j = a^j \cdot 1$. Now substituting into our congruence, we obtain $a^j a^m \equiv a^j 1 \pmod{n}$. Therefore by theorem 4.5 $a^m \equiv 1 \pmod{n}$. However, $m < k$ and k is defined to be the smallest natural number such that a^k is congruent to 1 modulo n, so we have a contradiction. □

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

Proof. Let a and n be natural numbers with $(a, n) = 1$ and let $k = \text{ord}_n(a)$. Let m be any arbitrary natural number. We will show that a^m is congruent modulo n to one of the numbers a^1, a^2, ..., a^k. If $m \le k$, then $a^m \equiv a^m \pmod{n}$ so we're done. In the case that $m > k$, use the division algorithm to find two integers q and r such that $m = qk + r$ where $0 \le r < k$. If $r = 0$, then let $s = q - 1$ and $t = k$, otherwise let $s = q$ and $t = r$. So $m = sk + t$ and $0 < t \le k$. Now $a^{sk} = (a^k)^s$, and because $a^k \equiv 1 \pmod{n}$, we can say by theorem 1.18 that $(a^k)^s \equiv 1^s \pmod{n}$. Then by theorem 1.?? $a^{ks} a^t \equiv 1 a^t \pmod{n}$ or equivalently $a^m \equiv a^t$. Therefore since $0 < t \le k$, we have shown that a^m is congruent modulo n to one of the numbers a^1, a^2, ..., a^k. □

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. Let a and n be natural numbers with $(a, n) = 1$, let $k = \mathrm{ord}_n(a)$, and let m be a natural number. Use the division algorithm to find integers q and r such that $m = qk + r$ where $0 \leq r < k$. Then $a^{qk} = (a^k)^q$ and since $a^k \equiv 1 \pmod{n}$, by theorem 1.18 $(a^k)^q \equiv 1^q \pmod{n}$. By theorem 1.?? $a^{qk}a^r \equiv 1a^r \pmod{n}$ and $a^m \equiv a^r \pmod{n}$.

If $k \mid m$, then r will equal 0, so $a^r = 1$ and $a^m \equiv 1 \pmod{n}$.

If $k \nmid m$ then assume by way of contradiction that $a^m \equiv 1 \pmod{n}$. In this case, by theorem 1.11 $a^r \equiv 1 \pmod{n}$ and since $0 < r < k$, this contradicts the definition of k as $\mathrm{ord}_n(a)$. □

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

Proof. □