Geoffrey Parker - grp352
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. Let $a = 3$ and $n = 7$. So:

$$3^1 \equiv 3 \pmod 7$$

$$3^2 \equiv 2 \pmod 7$$

$$3^3 \equiv 6 \pmod 7$$

$$3^4 \equiv 4 \pmod 7$$

$$3^5 \equiv 5 \pmod 7$$

$$3^6 \equiv 1 \pmod 7$$

Conjecture: $ord_n(a) < n$. □

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

Proof. et a and n be natural numbers with $(a, n) = 1$ and let $k = \operatorname{ord}_n(a)$. We will show the numbers $a^1, a^2, \ldots, a^k$ are pairwise incongruent modulo n. Assume by way of contradiction that there exist two natural numbers i and j such that $1 \leq i, j \leq k$, $i \neq j$, 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 $k = \mathrm{ord}_n(a)$. For any natural number m, a^m is congruent modulo n to one of the numbers a^1, a^2, $\ldots$, a^k.*

Proof. Let a and n be natural numbers with $(a, n) = 1$ and let $k = \mathrm{ord}_n(a)$. 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, $\ldots$, a^k. If $m \leq k$, 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 qLet a and n be natural numbers with $(a, n) = 1$. Then $\mathrm{ord}_n(a) < n$. and r such that $m = qk + r$ where $0 \leq r < k$. If $r = 0$, then let $s = q - 1$ and $t = k$, otherwise let $s = q$ and $t = r$. So $m = sk + t$ and $0 < t \leq k$. 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 1.14 $a^{ks}a^t \equiv 1a^t \pmod{n}$ or equivalently $a^m \equiv a^t$. Therefore since $0 < t \leq k$, we have shown that a^m is congruent modulo n to one of the numbers a^1, a^2, $\ldots$, a^k. $\square$

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 1.14 $a^{qk}a^r \equiv 1a^r \pmod{n}$ 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 $\mathrm{ord}_n(a)$. $\square$

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

Proof. Let a and n be natural numbers with $(a, n) = 1$. Let $k = \text{ord}_n(a)$. Assume by way of contradiction that $k \geq n$. Let the set $S = \{a^1, a^2, \ldots, a^k\}$. Because $k \geq n$, $|S| > n - 1$. By the definition of complete residue systems, every natural number is congruent modulo n to exactly one element of the canonical complete residue system modulo n. However, because $(a, n) = 1$, there is no s element of S such that $s \equiv 0 \pmod{n}$. Therefore every element of S is congruent modulo n to exactly one element of $T = \{1, 2, \ldots n - 1\}$. Note that $|T| = n - 1$. So by the pigeon hole principle there must be some element x of T to which two different elements of S, call them a^i and a^j are congruent modulo n. So by theorem 1.11 $a^i \equiv a^j \pmod{n}$. However, since $(a, n) = 1$, theorem 4.8 states that all elements of S are pairwise incongruent modulo n. So we have a contradiction. $\square$