まず,上において10進法で表記したときの末尾を考えることは,言い換えれば　$mod\,10^k$　で考えていることに等しい.そこでこれを一般化し　$mod\,q$　で考えることにする.(　q　は正の整数)

下図は　a^n　を　$mod\,q$　で考えたときの循環周期の表である.(　q　は素数とは限らない)
横線のところは循環部分が0,0,0,・・・となるところである.この場合は自明な循環の場合である.

	a^nの循環周期	mod を考える値q																																			
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
底a	2	---	2	---	4	2	3	---	6	4	10	2	12	3	4	---	8	6	18	4	6	10	11	2	20	12	18	3	28	4	5	---	10	8	12	6
	3		---	2	4	1	6	2	---	4	5	2	3	6	4	4	16	1	18	4	6	5	11	2	20	3	---	6	28	4	30	8	5	16	12	2
	4			---	2	1	3	---	3	2	5	1	6	3	2	---	4	3	9	2	3	5	11	1	10	6	9	3	14	2	5	---	5	4	6	3
	5				---	2	6	2	6	1	5	2	4	6	2	4	16	6	9	1	6	5	22	2	---	4	18	6	14	2	3	8	10	16	6	6
	6					---	2	---	---	1	10	---	12	2	1	---	16	---	9	1	2	10	11	---	5	12	---	2	14	1	6	---	10	16	2	---
	7						---	2	3	4	10	2	12	1	4	2	16	3	3	4	1	10	22	2	4	12	9	2	7	4	15	4	10	16	4	6
	8							---	2	4	10	2	4	1	4	---	8	2	6	4	2	10	11	2	20	4	6	1	28	4	5	---	10	8	4	2
	9								---	2	5	1	3	3	2	2	8	1	9	2	3	5	11	1	10	3	---	3	14	2	15	4	5	8	6	1
	10									---	2	1	6	6	1	---	16	1	18	---	6	2	22	1	---	6	3	6	28	1	15	---	2	16	6	1
	11										---	2	12	3	2	4	16	6	3	2	6	1	22	2	5	12	18	6	28	2	30	8	2	16	3	6
	12											---	2	6	4	---	16	---	6	4	6	1	11	---	20	2	---	6	4	4	30	---	1	16	12	---
	13												---	2	4	4	4	3	18	4	2	10	11	2	20	1	9	2	14	4	30	8	10	4	4	3
	14													---	2	---	16	6	18	2	2	5	22	2	10	1	18	---	28	2	15	---	10	16	2	6
	15														---	2	8	1	18	2	1	5	22	2	---	12	---	2	28	1	10	2	5	8	1	2
	16															---	2	3	9	1	3	5	11	1	5	3	9	3	7	1	5	---	5	2	3	3
	17																---	2	9	4	6	10	22	2	20	6	6	6	4	4	30	2	10	1	12	2
	18																	---	2	4	3	10	11	---	4	4	---	3	28	4	15	---	10	1	12	---
	19																		---	2	6	10	22	2	10	12	3	6	28	2	15	8	10	8	6	2
	20																			---	2	5	22	2	---	12	18	2	7	2	15	---	10	16	2	6
	21																				---	2	22	2	5	4	---	1	28	1	30	8	2	4	1	1
	22																					---	2	1	20	3	9	1	14	4	30	---	1	16	4	3
	23																						---	2	20	6	18	6	7	4	10	4	2	16	12	6
	24																							---	2	12	---	6	7	2	30	---	10	16	6	---
	25																								---	2	9	3	7	1	3	4	5	8	3	3
	26																									---	2	6	28	2	6	---	10	8	6	2
	27																										---	2	28	4	10	8	5	16	4	2
	28																											---	2	4	15	---	10	16	4	1
	29																												---	2	10	8	10	16	2	6
	30																													---	2	---	10	4	3	---
	31																														---	2	5	16	6	6
	32																															---	2	8	12	6
	33																																---	2	12	1
	34																																	---	2	3
	35																																		---	2
	周期の最大値	1	2	2	4	2	6	2	6	4	10	2	12	6	4	4	16	6	18	4	6	10	22	2	20	12	18	6	28	4	30	8	10	16	12	6
	φ(q)	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8	12	10	22	8	20	12	18	6	28	8	30	16	20	16	24	12

まず,どのような　a　と　q　のときに循環するかということと,自明でない循環(0,0,0,・・・でない循環)が現れるのはどのようなときかについて整理しておく.
表を観察すると,任意の　a,q　に対して　$a^n(mod\,p)$　は循環している.また　q　が素数のときに限れば,
　$a\neq q$　ならば自明でない循環をもっていると推測される.
実は　q　が合成数のときも含めて次が成り立つ.

【定理3】　q　を必ずしも素数ではないとし,　a　を正の整数とする.
　このとき任意の　a,q　に対して　$a^n(mod\,q)$　は循環する.
　自明な循環かそうでないかは次のようにして判定される.

　十分大なる数　m　に対して,　q　と　a^m　の共通因数で　q　を除したものを　q'　とする.
　$q'=1$　ならば　$a^n(mod\,q)$　は自明な循環であり,
　$q'\neq 1$　ならば　$a^n(mod\,q)$　は自明でない循環である.

(証明)　$(a,q')=1$　であるから,オイラーの定理より　$a^{\varphi(q')}\equiv 1(mod\,q')$　が成り立つ.
したがって,　L　を法　q'　に関する　a　の位数とすれば,　$a^L\equiv 1(mod\,q')$　が成り立つ.・・・①

次に　$a^{l+L}\equiv a^l(mod\,q)$　が成り立つと仮定する.ただし　$l\geq 1$　とする.
これより　$a^{l+L}-a^l=q\times N$　(Nは整数)とおける.
変形して,　$a^l(a^L-1)=q\times N$

仮定より q が q' になるまで,両辺を a の素因数で割れるだけ割れば
$c \cdot a^g(a^L-1)=q' \times N$ の形になる.ここで c は a の約数のいくつかの積である.
除し方より $(a,q')=1$ であり,仮定から $(c,q')=1$ である.
このように循環があると仮定すると,上記の数 c を得る.この c を用いて,① 式を以下のように変形する.

①より $a^L \equiv 1(mod\, q')$ が成り立っていたから, $a^L-1=q' \times N$
両辺に c を掛けて, $c(a^L-1)=q' \times N$ （なぜなら $(c,q')=1$ ）
両辺に $\dfrac{q}{q'}$ を掛けて, $a^h(a^L-1)=q \times N$ （ $h \geq 1$ ）
ゆえに $a^{h+L} \equiv a^h(mod\, q)$ となる.このことから $a^n(mod\, q)$ は自明な循環も含めて循環することが示された.
a^h は循環の始まりを表す.
ここで $q'=1$ であれば,上の計算から $a^n(mod\, q)$ はある自然数 n 以上において,法 q に関して0に合同であることを意味する.したがってこれは自明な循環を表し, $q' \neq 1$ であれば,自明でない循環の場合となる.（終）

【定義】
ある $l \geq 1$ が存在して $a^{l+M} \equiv a^l(mod\, q)$ （ $M \geq 1$ ）が成り立つような M の最小値を $a^n(mod\, q)(n=1,2,3,\cdots)$ の循環周期といい,記号で $f(a,q)$ で表す.

$f(a,q)=f(a+q,q)$ が成り立つことは二項定理より明らかである.

定理3の証明中より次が成り立つ.

【系1】 q' を定理3で定めたものとすると, $f(a,q')$ は法 q' に関する a の位数に等しい.

【系2】 $(a,q)=1$ ならば $a^{f(a,q)} \equiv 1(mod\, q)$ が成り立つ.

【系3】 q を必ずしも素数ではない数とし, a を正の整数とする. q' を定理3で定めたものとする.
このときで $f(a,q)=f(a,q')$ あり,これは法 q' に関する a の位数に L に等しい.

（例） $f(12,34)=f(12,17)$
$f(18,33)=f(18,11)=f(7,11)=10$
$f(6,30)=f(6,5)=f(1,5)=1$

（証明）系1について:
L を法 q' に関する a の位数とする.
$f(a,q')$ の定義より, $a^{l+f(a,q')} \equiv a^l(mod\, q')$ であるから,変形して
$a^l(a^{f(a,q')}-1)=q' \times N$ （ N :整数）. $(a,q')=1$ であるから $a^{f(a,q')} \equiv 1(mod\, q')$
ゆえに, $L \leq f(a,q')$
定理3の証明中より $a^L \equiv 1(mod\, q')$.ゆえに $a^L-1=q' \times N$ （ N :整数）.
したがってある自然数 l に対して $a^{l+L} \equiv a^l(mod\, q')$.ゆえに $f(a,q') \leq L$.
以上により, $L=f(a,q')$ （終）
系2について:
$(a,q)=1$ であるから $q=q'$ である.したがって系1より $f(a,q)$ は法 q に関する a の位数に等しい.ゆえに成り立つ.（終）

系3について:
定理3の証明中の $a^{h+L}\equiv a^h(mod\,q)$ と系1より $a^{h+f(a,q')}\equiv a^h(mod\,q)$.したがって最小性より
$f(a,q')\geq f(a,q)$ である.
一方,循環周期の定義より, $a^{l+f(a,q)}\equiv a^l(mod\,q)$ であるが,定理3と同じように変形して,
$c\cdot a^g(a^{f(a,q)}-1)=q'\times N$ となり, $a^{f(a,q)}\equiv 1(mod\,q')$ が成り立つ.
よって循環周期の最小性より $f(a,q)\geq f(a,q')$ が成り立つ.
以上の2式より $f(a,q)=f(a,q')$ が成り立つ.(終)

以下では,この表から一般的な性質を抽出し,それらの性質を使ってこれらの表に現れた数をできる限り復元するという課題を設定し挑戦した.また同時に循環周期の表にひそむ性質についてもできる限り考えていくことにした.

(課題1)循環周期の表にひそむ一般的な性質を求める.
(課題2)簡単な数の場合の循環周期の値を使って,複雑な数の場合の循環周期を求める方法の追求.

まず,表を観察すると,次の性質が成り立つことが予想される.

【定理4】
p を素数とする.次の性質が成り立つ.
(性質1) a が p の原始根のとき, $f(a,p)$ は $\{f(a,p):a\in N\}$ の中の最大値を与える.
その値は $\varphi(p)=p-1$ である.(逆も成り立つ)
(性質2) q は素数とは限らない整数とし, $(b,q)=1$ とする.このとき, $f(b,p)$ は
$\varphi(q)$ の約数である.(これは b が q の原始根でなくても成立する.)
(性質3) $f(1,a)=1$, $f(a-1,a)=2$ が成り立つ.

性質2の例:
$q=27$ の場合
$27=3^3$ であるので $\varphi(3^3)=3^{3-1}(3-1)=9\times 2=18$
一方,最大周期は原始根が 2 であることから最大周期は表より 18 である.このことから,この結果は最良の結果と言える.

$q=6$ の場合
$q=6$ と互いに素な数は 1,5,・・・などであり,Excel の計算からわかるように,循環部分に 1 が現れている.このときの周期は 1 または 2 である.具体的には
周期が 1 のものは $a=1,7,13,19$,・・・
周期が 2 のものは $a=5,11,17,23$,・・・
確かに周期は $\varphi(6)=2$ の約数となっている.

$q=15$ の場合
$q=15$ と互いに素な数は 1,2,4,7,8,11,13,14,16,17,・・・などであり,Excel の計算からわかるように,循環部分に 1 が現れている.このときの周期は 1,2,4 である.
具体的には
周期が 1 のものは $a=1,16$,・・・
周期が 2 のものは $a=4,11,14$,・・・
周期が 4 のものは $a=2,7,8,13,17$,・・・
確かに周期は $\varphi(15)=8$ の約数となっている.

性質3はよく知られた性質である.
これらの性質を証明する.準備として次の定理が成り立つことを確認しておく.いずれもよく知られた事実であるので証明は略す.

【定義】(原始根)
(1)　p を素数とする. a $(0 \leq a \leq p-1)$ が p の原始根である
　$\Leftrightarrow$ a を $p-1$ 乗すると初めて 1 と $mod\, p$ で合同になる.

p は必ずしも素数でなくともよいが,その場合は次のようになる.

(2)　a $(0 \leq a \leq p-1)$ が p の原始根である
　$\Leftrightarrow$ a を $\varphi(p)$ 乗すると初めて 1 と $mod\, p$ で合同になる.

【定理】(原始根定理)
　p を素数とする.任意の素数 p に対して原始根 a が存在する.また奇数素数べきの原始根も存在する.
(原始根の性質)
(1)　p を素数とする.原始根の定義より, $mod\, p$ で考えると
$\{a, a^2, a^3, \cdots, a^{p-1}\} = \{1, 2, 3, \cdots, p-1\}$ であり,これは巡回群である.(巡回群の生成元は原始根)

(2)一般に p が素数とは限らない場合に,もし p の原始根が存在すれば, a を生成元とする巡回群 $\langle a \rangle$ は p の既約剰余類群(単元群)になっている.(既約剰余類群とは 1 以上 p より小さい整数で, p と互いに素であるものなす群のこと)これを原始根の定義とするものもある.

(定理4の証明)以下, p は素数であるとする.したがって p の原始根は存在する.
〈性質1の証明〉
　$mod\, p$ の値の周期について
　p の原始根の1つを a とすれば mod p で考えて $\{a, a^2, a^3, \cdots, a^{p-1}\} = \{1, 2, 3, \cdots, p-1\}$ であることより a^n の周期は $p-1$ となる.すなわち周期が $p-1$ であるものが必ず存在する.
　a が原始根のときに周期が最大になることは,一般の b に対して,フェルマーの小定理により
　$b^{p-1} \equiv 1 (mod\, p)$ が成り立つので,少なくとも b の周期は $p-1$ 以下となる.したがって, a が原始根の場合に周期が $p-1$ となることがわかっているので, a が p の原始根であるときに循環周期が最大となる.(終)

〈性質2の証明〉
定理3より $b, b^2, b^3, \cdots$ は循環するので,ある正の整数 m が存在して, $b^m \equiv b$ $(mod\, q)$ である.ここで仮定より $(b, q) = 1$ であるから $b^{m-1} \equiv 1 (mod\, q)$ である.したがって周期の中に現れる元の集合は巡回群をなす. $(b, q) = 1$ の仮定から $b \in (Z/qZ)^{\times}$ であるから,この巡回群は q に関する既約剰余類群(単元群) $(Z/qZ)^{\times}$ の部分群である.ゆえに $f(b, q)$ は $\left|(Z/qZ)^{\times}\right| = \varphi(q)$ の約数である.(終)

〈性質3の証明〉
　$f(1, a) = 1$ については $1^n \equiv 1$ $(mod\, a)$ となるので成り立つ.
　$f(a-1, a) = 2$ については,二項定理より $(a-1)^n \equiv (-1)^n$ $(mod\, a)$ であるから, n が奇数の時 -1 , n が偶数のとき 1 に合同になるので周期は 2 となる.よって成り立つ.(終)

性質1については,逆にあたる次の性質も成り立つ.

【定理4】
　p を素数とする.次の性質が成り立つ.
(性質4)　$f(a, p) = \varphi(p)$ ならば, a は p の原始根である.

(証明)
　$(a, p) = 1$ であるから,定理3の記号において $p = p'$.ゆえに系1により法 p' に関する a の位数は $f(a, p) = \varphi(p) = p-1$ に等しい.したがって $a^{p-1} \equiv 1 (mod\, p)$.ゆえに定義により a は p の原始根である.(終)