なお,性質2は次のように精密化した形でも述べることができる.

【定理5】
q は必ずしも素数ではないとし，a を正の整数とする.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.
このとき，$f(a,q)$ は q' によって，$f(a,q)=f(a,q')$ が成り立ち,この値は $\varphi(q')$ の約数である.特にこれは $\varphi(q)$ の約数である.

定理5の例:
$q=21$ の場合
$q=21$ と互いに素でない数として 14 がある.ここでは $14^n(mod\,21)$ を考える.
$m>n$ として，$14^m\equiv 14^n(mod\,21)$ とおくと，$14^n(14^{m-n}-1)=21l$ （ l は整数）
両辺を 7 で割ると，$2^n\cdot 7^{n-1}(14^{m-n}-1)=3l$
これより，$14^{m-n}-1=3l$ すなわち，$14^{m-n}\equiv 1(mod\,3)$
上記の循環周期の表をみると，$f(14,3)=f(14-12,3)=f(2,3)=2$ であるので，$f(14,21)=2$
すなわち，$f(14,21)=f(14,3)=2$ であり,この値は $\varphi(3)=2$ に等しい.（ $q'=3$ ）
これは $\varphi(21)=12$ の約数.

$q=6^2=36$ の場合
$q=6^2$ と互いに素でない数として 2 がある.ここでは $2^n(mod\,6^2)$ を考える.
$m>n$ として，$2^m\equiv 2^n(mod\,6^2)$ とおくと，$2^n(2^{m-n}-1)=6^2l$ （ l は整数）
両辺を 2^2 で割ると，$2^{n-2}(2^{m-n}-1)=3^2l$
これより，$2^{m-n}-1=3^2l$ すなわち，$2^{m-n}\equiv 1(mod\,3^2)$
上記の循環周期の表をみると，$f(2,3^2)=6$ であるので，$f(2,6^2)=6$.
すなわち，$f(2,6^2)=f(2,3^2)=2$ であり,この値は $\varphi(3^2)=3^2-3=6$ に等しい.（ $q'=3^2$ ）

$q=30^2$ の場合
$q=30^2$ と互いに素でない数として 2 がある.ここでは $2^n(mod\,30^2)$ を考える.
$m>n$ として，$2^m\equiv 2^n(mod\,30^2)$ とおくと，$2^n(2^{m-n}-1)=30^2l$ （ l は整数）
両辺を 2^2 で割ると，$2^{n-2}(2^{m-n}-1)=3^2\cdot 5^2l=15^2l$
これより，$2^{m-n}-1=3^2\cdot 5^2l$ すなわち，$2^{m-n}\equiv 1(mod\,3^2\cdot 5^2)$
Excel で計算すると，$f(2,3^2\cdot 5^2)=f(2,15^2)=60$ であるので，$f(2,30^2)=60$ である.
すなわち，$f(2,30^2)=f(2,3^2\cdot 5^2)=60$ であり,この値は $\varphi(3^2\cdot 5^2)=\varphi(3^2)\varphi(5^2)=6\cdot 20=120$ の約数に等しい.（ $q'=15^2$ ）
(証明)系3より，$f(a,q)=f(a,q')$ が成り立つ. $(a,q')=1$ であるから,定理4の性質2により,これは $\varphi(q')$ の約数である.特に $\varphi(q)$ の約数でもある.(終)
p を奇数素数とすると,性質1,性質2の結果は $mod\,p^k$ の場合に一般化される.その理由は原始根定理により,奇数素数のべきに対しても原始根は必ず存在することが示されているからである.証明は略す.

【性質1'】 a が奇数素数べき p^k の原始根のとき，$f(a,p^k)$ は $\{f(a,p^k):a\in N\}$ の中の最大値を与える.その値は $\varphi(p^k)=p^{k-1}(p-1)$ である.(逆も成り立つ)
【性質2'】一般に b が奇数素数べき p^k の原始根とは限らないとする. $(b,p^k)=1$ のとき,(すなわち b が p^k の単元群の元であるとき) $f(b,p^k)$ は $\varphi(p^k)=p^{k-1}(p-1)$ の約数である.

Excel の表から,次のことが予想される.

【定理6】 p,q が互いに素で,Max($f(a,p)$: $a\in N$)= $\varphi(p)$ かつ Max($f(a,q)$: $a\in N$) = $\varphi(q)$ ならば
Max($f(a,pq)$: $a\in N$)=Max($f(a,p)$: $a\in N$)× Max($f(a,q)$: $a\in N$) の約数が成り立つ.

定理6(および以下の系4)の例:
周期の最大値をみると
$p=3,q=5$ のとき, 4 =(2×4 の約数)
$p=3,q=7$ のとき, 6 =(2×6 の約数)
$p=5,q=7$ のとき, 12 =(4×6 の約数)
$p=2,q=11$ のとき, 10 =(1×10 の約数,特に一致)
$p=3,q=11$ のとき, 20 =(2×10 の約数,特に一致)
$p=2,q=17$ のとき, 16 =(1×16 の約数,特に一致)
$p=35$ までの表には載っていないが, $p=100$ までの表で確かめると
$p=7,q=13$ のとき, 12 =(6×12 の約数)

これは【定理5】を用いて,次のように容易に解決する.

(証明)定理5により,Max($f(a,pq)$: $a\in N$)は $\varphi(pq)$ の約数である.
一方,仮定より Max($f(a,p)$: $a\in N$)= $\varphi(p)$, Max($f(a,q)$: $a\in N$) = $\varphi(q)$
であるから,Max($f(a,p)$: $a\in N$)× Max($f(a,q)$: $a\in N$) = $\varphi(p)\varphi(q)=\varphi(pq)$ である.
(p,q は互いに素を用いた)したがって成り立つ.(終)

【系4】 p,q が相異なる素数ならば
Max(: $f(a,pq)$ $a\in N$)=Max($f(a,p)$: $a\in N$)× Max(: $f(a,q)$ $a\in N$) の約数が成り立つ.

(証明) p,q が相異なる素数ならば,定理6の条件を満たすので,定理4の性質1により成り立つ.(終)

【定理7】
p を素数とする.このとき $f(a,p^n)$ は $f(a,p)$ の倍数である.

これは循環周期を横に見ていったときの性質である.

定理7の例:
$p=2,3,4,5,6$ の各行で確かめることができる.

(証明)
$f(a,p^n)=L$ とおくと, $a^n\equiv 1(mod\ p^n)$ となる正の整数の最小値が L である.このとき,定理3の記号において $p'=p^n$ とできるから $a^L\equiv 1(mod\ p)$ が成り立つ.ゆえに最小性により $f(a,p)\leq L=f(a,p^n)$.
$f(a,p^n)$ を $f(a,p)$ で割った余りを r とすると, $f(a,p^n)=f(a,p)Q+r$ ($0\leq r<f(a,p)$)
と表せる(Q は整数)が,このとき
$a^{f(a,p^n)}=a^{f(a,p)Q+r}=a^{f(a,p)Q}\cdot a^r$ であるから $mod\ p$ で考えれば $a^r\equiv 1(mod\ p)$ である.
したがって $f(a,p)$ の最小性により, $r=0$ でなければならない.ゆえに成り立つ.(終)

【定理8】
(1)　n が $f(a,p)$ の約数のとき，$f(a^n,p)=\dfrac{f(a,p)}{n}$ が成り立つ.
(2)　$(a,p)=1$　$(b,f(a,p))=1$ のとき，$f(a^b,p)=f(a,p)$

(1)は循環周期の表を縦に見ていったときの性質であり、(2)は循環周期の表を縦に見ていったときにその周期が一致するところに関する定理である.

定理8の例:
(1)　$n=2,a=3$ で考えれば，$a=3$ の周期が偶数になっているような p に関しては，
$f(3^2,p)=\dfrac{f(3,p)}{2}$ が成り立つ.
例えば，$p=7$ のとき，$n=2,a=3$ で考えれば，$f(3,21)=6$ であるから，$n=2$ はその約数.
このとき，$f(3^2,7)=f(2,7)=3$ 一方，$\dfrac{f(3,7)}{2}=\dfrac{6}{2}=3$ となるので成り立つ.
また $p=17$ のとき，$n=2,a=3$ で $f(3^2,17)=f(9,17)=8$.一方，$\dfrac{f(3,17)}{2}=\dfrac{16}{2}=8$ となるので成り立つ.

(2)　$p=5,a=2$ のときは $(a,p)=1$ であり，$f(2,5)=4$.ここで b は4と互いに素であるので例えば $b=3$ とすると $f(2^3,5)=f(8,5)=f(3,5)=4$ となるので成り立つ.
$p=17,a=2$ のときは $(a,p)=1$ であり，$f(2,17)=8$.ここで b は8と互いに素であるので例えば $b=3$ とすると $f(2^3,17)=f(8,17)=8$ となるので成り立つ.

この議論は p の原始根がいくつ存在するかというときの議論とまったく同じである.

(証明)(1)循環周期の中身を考えれば，n 個飛びで循環することになるので,上の式が成り立つ.
(2)　$(b,f(a,p))=1$ であるから,ある整数 x,y が存在して $bx+f(a,p)y=1$ が成り立つ.
このとき $bx\equiv 1(mod\, f(a,p))$ となる.したがって $a^{bx}=a(mod\, p)$ が成り立つ.このことから任意の a^k $(k\in Z/\varphi(p)Z)^{\times}$ は a^b の累乗で表すことができ，$f(a^b,p)$ は $f(a,p)$ に等しいことは,循環する順番がずれるだけということからしたがう.よって成り立つ.(終)

以上の性質は,巡回群のよく知られた性質を焼き直しただけに過ぎない.

【定理9】
p,q を互いに素な2つの数とし，$(a,p)=1$ かつ $(a,q)=1$ とする.
このとき $f(a,pq)=LCM(f(a,p),f(a,q))$ が成り立つ.

これは循環周期の表を横に見ていったときに、 q が合成数の場合、その素因数分解との関係を表す.

定理9の例:
$p=3,q=5,a=2$ のとき，$f(2,15)=4,f(2,3)=2,f(2,5)=4$. $4=LCM(2,4)$ なので成り立つ.
$p=3,q=7,a=2$ のとき，$f(2,21)=6,f(2,3)=2,f(2,7)=3$. $6=LCM(2,3)$ なので成り立つ.
$p=3,q=7,a=5$ のとき，$f(5,21)=6,f(5,3)=2,f(5,7)=6$. $6=LCM(2,6)$ なので成り立つ.
(証明)
$f(a,p)=L$, $f(a,q)=K$ とおくと,系2により $a^L\equiv 1(mod\, p)$ かつ $a^K\equiv 1(mod\, q)$
である.ここで $LCM(L,K)=Ln=Km$ となるような整数 n,m を考える.
$a^{LCM(L,K)}=a^{Ln}=(a^L)^n\equiv 1^n=1(mod\, p)$, $a^{LCM(L,K)}=a^{Km}=(a^K)^m\equiv 1^m=1(mod\, q)$ であるから
$a^{LCM(L,K)}\equiv 1$ $(mod\, LCM(p,q))$ であるが，$(p,q)=1$ であるから，$LCM(p,q)=pq$

ゆえに $a^{LCM(L,K)}\equiv 1(mod\ pq)$ である.
ここで $f(a,pq)=LCM(L,K)\cdot Q+r$ （ $0\leq r<LCM(L,K)$ ）とすれば,

$$1\equiv a^{f(a,pq)}=a^{LCM(L,K)\cdot Q+r}=\left\{a^{LCM(L,K)}\right\}^{Q}\cdot a^{r}\equiv a^{r}\ \ (mod\ pq)$$

すなわち $a^{r}\equiv 1(mod\ pq)$ となる.ここでもし $r>0$ ならば, $f(a,pq)>r>0$ であるから,これは循環周期の最小性に矛盾する.よって $r=0$.
ゆえに $f(a,pq)$ は $LCM(L,K)$ の倍数.再び循環周期の最小性により $f(a,pq)=LCM(L,K)$ でなければならない.（終）

【定理10】
Max（ $f(a,q)$ ： $a\in N$ ）＝ $\varphi(q)$ が成り立つためには, q が以下のいずれかを満たすことが必要かつ十分な条件である.
（i） $q=2,4$ のとき
（ii） $q\neq 2$ が１種類の素因数からなる素因数分解をもつとき
（iii） q が2種類以上の素因数からなる素因数分解をもつとき,それに対応した巡回群への直積分解があるが,その位数について, すべての異なる2つの巡回群の位数が互いに素であるとき

これは循環周期の最大値と $\varphi(q)$ が一致するときの q の特徴づけである.
（証明）
もしMax（ $f(a,q)$ ： $a\in N$ ）＝ $\varphi(q)$ となるとすれば,既約剰余類群 $(Z/qZ)^{\times}$ が巡回群であるということになる.
したがって,既約剰余類群 $(Z/qZ)^{\times}$ が巡回群となる q についてはMax（ $f(a,q)$ ： $a\in N$ ）＝ $\varphi(q)$ が成り立つということは言える.（ q が素数や奇素数べきなど,原始根が存在するときには,この条件を満たしている.）
具体的に q の満たすべき条件については,既約剰余類群を巡回群の直積に分解して考えることで,次のように表すことができる.

$q=2^{e_0}\cdot p_1^{e_1}\cdot p_1^{e_1}\cdot p_2^{e_2}\cdots\cdots p_h^{e_h}$ （ $e_0\geq 0$, $e_1,e_2,\cdots,e_h\geq 1$ ）と表されるとき, $(Z/qZ)^{\times}$ は次のような巡回群の直積に準同型であることはよく知られている.

（1） $e_0=0,1$ のとき, $(Z/qZ)^{\times}\simeq Z(\varphi(p_1))\times Z(\varphi(p_2))\times\cdots\cdots\times Z(\varphi(p_h))$
（2） $e_0=2$ のとき, $(Z/qZ)^{\times}\simeq Z(2)\times Z(\varphi(p_1))\times Z(\varphi(p_2))\times\cdots\cdots\times Z(\varphi(p_h))$
（3） $e_0\geq 3$ のとき, $(Z/qZ)^{\times}\simeq Z(2)\times Z(2^{e_0-2})\times Z(\varphi(p_1))\times Z(\varphi(p_2))\times\cdots\cdots\times Z(\varphi(p_h))$

ただし,ここで $Z(g)$ は位数が g の巡回群を表す.

このことから,以下の場合は $(Z/qZ)^{\times}$ は巡回群となり,したがってMax（ $f(a,q)$ ： $a\in N$ ）＝ $\varphi(q)$ が成り立つ.
（i） $q=2,4$ のとき
（ii） $q\neq 2$ が１種類の素因数からなる素因数分解をもつとき（すなわち $p=q_1^{k_1}$ の形）
（iii） q が２種類以上の素因数からなる素因数分解をもつとき,上の（1）（2）（3）のように直積分解されるが,どの異なる2つの巡回群の位数の最大公約数も 1 であるとき.すなわち,異なる2つの巡回群の位数の最大公約数をすべての2つのペアについて考えたとき,それらすべてが 1 に等しいときである.その理由は、中国の剰余定理から得られる剰余環に関する環同型 $Z/(m_1m_2\cdots m_l)Z\simeq Z/m_1Z+Z/m_2Z+\cdots+X/m_lZ$ に対し、その同型写像から得られる単元群の間の自然な同型定理である.（終）

（例）上記の条件に当てはまる自然数を 100 以下のなかから抽出すれば,
2,3,4,5,6,7,9,10,11,13,14,17,18,19,22,23,25,26,27,29,31,34,37,38,41,43,46,47,49,50,53,54,58,59,61,62,67,71,73,74,79,81,82,83,86,89,94,97,98 であるが,Excel の表でMax（ $f(a,q)$ ： $a\in N$ ）＝ $\varphi(q)$ を確認することができる.（p.15 参照）

【未解決の問題について】

（問題1） q を指定したときに,循環周期 $f(a,q)$ （ $a\in N$ ）が最大値を与えるときの a の値は何か. a と q の関係.

（問題2）系4の結果を次のようにさらに精密化できるか.
p,q が相異なる素数ならば
Max（ $f(a,pq)$ ： $a\in N$ ）＝LCM（Max（ $f(a,p)$ ： $a\in N$ ）× Max（ $f(a,q)$ ： $a\in N$ ））

（問題1）について
原始根が存在する場合は a が原始根になる.原始根が存在するとは限らない場合,どのような a について最大の循環周期を与えるかは今後の課題としたい.

（問題2）について
循環周期の表を見る限りは成り立つことが予想される. p,q の原始根が共通の数で与えられる場合は成り立つことは,定理9からわかるが,常にそのようなことが成り立つのだろうか？また共通の原始根が見つからなくても最小公倍数をとった時点で一致することもある.
また異なる2つの素数に素因数分解される場合だけでなく,さらに多くの異なる素因数に素因数分解される場合も成り立ちそうである.実際 100 以下の場合について検証したところ成り立っていることがわかった.素因数が重複している場合については成り立たないことが多い.
（ 100 以下では, $4,8,9,16,18,25,27,32,36,45,48,49,50,54,64,72,75,81,90,96,98,99,100$ ）
これらについては今は未解決の問題である.

最後に課題2について考える.これについては,かなり多くのペア a,q について a,q が小さい数のときをもとにして決定することができた.（ただし,すべて調べてはいない.）

（例1） $f(2,30)$ の値
$f(2,30)=f(2,15)=f(2,3\cdot5)=LCM(f(2,3),f(2,5))=LCM(2,4)=4$

（例2） $f(3,20)$ の値
$f(3,20)=f(3,2^2\cdot5)=LCM(f(3,2^2),f(3,5))=LCM(2,4)=4$

（例3） $f(14,21)$ の値
$f(14,21)=f(14,3)=f(2,3)=2$ （ただし 2 は 3 の原始根であることはわかっているとする.）

（例4） $f(2,36)$ の値
$f(2,36)=f(2,3^2)$ これは $f(2,3)=2$ の倍数であるから $2,4,6,8,\cdots$ のいずれか.
一方, $\varphi(9)=6$ であるから, $1,2,3,6$ のいずれか.
したがって候補は $2,6$ である. $2^n(mod\,9)$ をいくつか計算して（3つで十分） $2,4,8,\cdots$ となるので明らかに循環周期は 3 以上となる.よって周期 2 はありえない.このことから $f(2,36)=6$ である.
また $f(2,9)=6=\varphi(9)$ が成り立つので,性質 1'により 2 が 9 の原始根であることもわかる.

（例5） $f(2,30^2)$ の値
$f(2,30^2)=f(2,15^2)=f(2,3^2\cdot5^2)=LCM(f(2,9),f(2,25))=LCM(6,20)=60$
これは Excel で求めたものと一致する.

（例6） $f(16,27)$ の値
$\varphi(27)=18$ であるから,この値は 18 の約数の $1,2,3,6,9,18$ のいずれかである.
$f(16,27)=f(4^2,27)$ であるが,ここで $(4,27)=1$, $(2,f(4,27))=(2,9)=1$ であるから,
定理8の（2）より, $f(16,27)=f(4^2,27)=f(4,27)=9$.

最後に,循環周期と言っても位数とそれほど変わらない面が多々あり,以上の結果は後から考えてみれば明らかなもので,研究としては稚拙なものになってしまい,大変申しわけなく感じている.
課題1については,以上とは別の性質が見つかり,その方法で循環周期を絞り込むことができるかもしれない.問題2については未解決の課題であり,私自身の力不足もあり,解答が得られていない.
また,下 k 桁で成り立った他の性質についても,一般の場合はどのように定式化できるかについても手をつけられていない.今後はこれらの課題に取り組むことで罪滅ぼしとしたい.何かご教示くだされば大変幸いです.

〈その後の発展について〉

未解決問題の（問題1）については、次の関係があることを知った。（参考文献[2]）
（解答） q を与えると単元群 $(Z/qZ)^{\times}$ が考えられるが、循環周期 $f(a,q)$ （ $a\in N$ ）が最大値を与えると a は、単元群 $(Z/qZ)^{\times}$ の元の中で位数が最大のものと言うことになる。
これは q の特殊分解を利用すれば求められる。

（例1） $q=42$
$\varphi(42)=\varphi(2)\varphi(3)\varphi(7)=1\cdot2\cdot6=2\cdot(2\cdot3)=2\cdot2\cdot3$ （標準分解）
よって、特殊分解は $\varphi(42)=(3\cdot2)\cdot2=6\cdot2$ （特殊分解）
したがって $f_1=6$ が最大位数である。これは周期の最大値と一致している。

（例2） $q=72$
$\varphi(72)=\varphi(2^3)\varphi(3^2)=(2\cdot2^1)\cdot(2\cdot3)=2\cdot2\cdot2\cdot3$ （標準分解）
よって、特殊分解は $\varphi(72)=(3\cdot2)\cdot2\cdot2=6\cdot2\cdot2$ （特殊分解）
したがって $f_1=6$ が最大位数である。これは周期の最大値と一致している。

（例3） $q=100$
$\varphi(100)=\varphi(2^2)\varphi(5^2)=2\cdot(5\cdot4)=2\cdot2^2\cdot5$ （標準分解）
よって、特殊分解は $\varphi(100)=(5\cdot2^2)\cdot2$ （特殊分解）
したがって $f_1=20$ が最大位数である。これは周期の最大値と一致している。

【参考文献】
[1] 2^n の末尾の循環周期について（東京書籍ニューサポート高校　教育実践レポート）pp.8-9　木部陽一
[2]初等整数論入門　銀林　浩