SIGNATURES OF ITERATED TORUS KNOTS

R. A. Litherland†
Department of Pure Mathematics
and Mathematical Statistics
16 Mill Lane
Cambridge CB2 1SB

By an iterated torus knot I mean a knot obtained by starting with a torus knot, taking a cable about it, then a cable about the result, and so on. One reason why this class of knots is interesting is that it contains the class $\underline{\underline{A}}$ of all one-component links of isolated singularities of complex algebraic plane curves (i.e. all algebraic knots). Recently, Lee Rudolph has asked [Ru] whether $\underline{\underline{A}}$ is an independent set in the knot cobordism group. Independence may be interpreted in any sense you desire; in particular Rudolph asks whether

$$[K] = \sum_{i=1}^{n} [K_i] \qquad K, K_i \in \underline{\underline{A}}$$

implies $n = 1$, $K_1 = K$; this is of course weaker than the usual notion of linear independence in a $\mathbb{Z}$-module.

We shall give an affirmative answer to this question. We shall also prove that the ordinary torus knots are linearly independent. This generalises the result of Tristram [Tr] that the $(2,k)$ torus knots are independent. Tristram proved that result using the signatures which he introduced, and for which I shall use the following notation. Let L be a link, V a Seifert matrix for L and ζ a complex number of modulus 1. Denote by $\sigma_\zeta(L)$ the signature of the Hermitian matrix $(1 - \zeta)V + (1 - \bar{\zeta})V^T$. (In fact, Tristram considered the cases ζ a p'th root of unity, p a prime picking one such root for each p and denoting the corresponding signature by $\sigma_p(L)$.)

We will need a re-interpretation of these signatures in terms of branched covering spaces, due to Viro [Vi] and also (for $\zeta = -1$) to Kauffman and Taylor [KT]. It will also be important to look at all the signatures available

---

† Research supported by a grant from the SRC.

so a word of caution is in order here. It is not true that $\sigma_\zeta(L)$ is a cobordism invariant for every ζ; however, if L_1 and L_2 are cobordant, then $\sigma_\zeta(L_1) = \sigma_\zeta(L_2)$ for all but finitely many $\zeta \in S^1$. In particular, if we define $f_L : R \to \mathbb{Z}$ by

$$f_L(x) \quad = \quad \tfrac{1}{2}(\text{jump in} \quad \sigma_\zeta(L) \quad \text{at} \quad \zeta = e^{2\pi i x})$$

then f_L is a cobordism invariant.

The re-interpretation of the signatures referred to above goes as follows. Let L be a link, and suppose N is a 4-manifold with $\partial N = S^3$, $H_1(N) = 0$. Suppose further that F is a properly embedded surface in N with $\partial F = L$, and such that $[F,\partial F] = 0 \in H_2(N,\partial N)$. Then we can form, for any positive integer m, the m-fold branched cyclic cover $\tilde{N}$ of N, branched over F, with canonical covering transformation τ (given by the orientations of N and F: all manifolds are to be oriented and maps orientation-preserving).

The vector space $H\,(\tilde{N};\mathbb{C})$ splits as a direct sum of eigenspaces of the automorphism τ_* :

$$H_2(\tilde{N};C) \quad = \quad \bigoplus_{\zeta^m=1} \operatorname{Ker}(\tau_* - \zeta) \quad = \quad \bigoplus_{\zeta^m=1} H_\zeta, \quad \text{say.}$$

Consider the (sesquilinear) intersection form restricted to each H_ζ ; we denote its signature by $\sigma_\zeta(\tilde{N}, \tau)$. These signatures are closely related to the Atiyah-Singer g-signatures of the $\mathbb{Z}_m$-manifold $\tilde{N}$: in fact they are linear combinations thereof (see Rohlin [Ro;§4]). Under the above conditions, Viro [Vi;§4.8] shows that

$$\sigma_\zeta(L) \quad = \quad \sigma_\zeta(\tilde{N}, \tau) - \sigma(N) \qquad \text{for} \quad \zeta^m = 1 .$$

(See also Kauffman and Taylor [KT; Theorem 3.1].) Note that the right-hand side is an invariant of L by Novitov additivity and (a very special case of) the G-signature theorem.

Now, for integers p, q, $r > 1$, the Pham-Brieskorn manifold

$$V_\delta \quad = \quad \left\{ (z_1,z_2,z_3) \in \mathbb{C}^3 \mid z_1^p + z_2^q + z_3^r \quad = \quad \delta \right\} \cap D^6$$

is, for sufficiently small δ , an r-fold cyclic cover of the 4-ball branched over some surface spanning a $(p.q)$ torus knot (or link, if p,q are not coprime); the covering transformation is given by multiplication of the z_3 factor by $e^{2\pi i/r}$. For clearly V_δ is an r-fold cyclic branched cover of $\{z_1^p + z_2^q + z_3 = \delta\} \cap D^6$ with the covering transformation stated; since $z_1^p + z_2^q + z_3 = 0$ has no singular points, this manifold is a 4-ball. It is not hard to check that the branch set meets the boundary in a (p,q) torus knot, as required. Brieskorn [Br] has calculated the signature of V_δ to be $\sigma_+ - \sigma_-$, where

$$\sigma_+ \ = \ \text{number of triples } (i,j,k) \text{ of integers, } 0 < i < p,$$
$$0 < j < q, \quad 0 < k < r \quad \text{such that} \quad 0 < \frac{i}{p} + \frac{j}{q} + \frac{k}{r} < 1 \mod 2$$
$$\sigma_- \ = \ \text{number of triples such that} \quad -1 < \frac{i}{p} + \frac{j}{q} + \frac{k}{r} < 0 \quad \mod 2\ .$$

Inspecting Brieskorn's proof (and allowing for his use of the $\mathbb{C}$-bilinear, rather than sesquilinear, form) one sees that this formula arises from a basis of eigenvectors; those of eigenvalue $2^{2\pi is/r}$ correspond to triples (i,j,s). This gives the following result. (cf. Lemma 2 of Goldsmith [Go]).

<u>*Proposition 1*</u>. *If* K *is a* (p,q) *torus knot and* $\zeta = e^{2\pi ix}$, x *rational,* $0 < x < 1$, *then* $\sigma_\zeta(K) = \sigma_{\zeta+} - \sigma_{\zeta-}$, *where*

$$\sigma_{\zeta+} \ = \ \textit{number of pairs } (i,j) \textit{ of integers, } 0 < i < p,$$
$$0 < j < q, \quad \textit{such that} \quad x-1 < \frac{i}{p} + \frac{j}{q} < x \quad \textit{mod } 2$$
$$\sigma_{\zeta-} \ = \ \textit{number of pairs such that} \quad x < \frac{i}{p} + \frac{j}{q} < x+1 \quad \textit{mod } 2\ . \ \square$$

As it stands this formula is rather unmanageable; to get it into a useful shape we look at the associated jump function f_K , which we shall denote by $f_{p,q}$. Prop.1 tells you to count, with the indicated signs, the lattice points $(\frac{i}{p}, \frac{j}{q})$ in the interiors of the regions of the unit square shown in Figure 1.

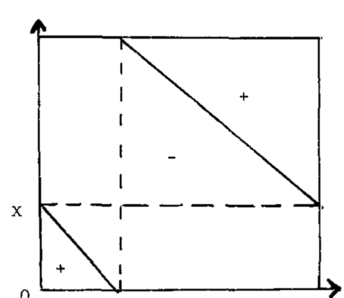

Figure 1

From this picture it is transparent that

$$f_{p,q}(x) \;=\; \text{number of lattice points on lower diagonal line} - (\text{number of lattice points on upper diagonal line}).$$

If $f_{p,q}(x) \neq 0$, so that some lattice point $(\frac{i}{p}, \frac{j}{q})$ lies on one of these lines, we have $\frac{i}{p} + \frac{j}{q} = x$ or $1+x$; it follows that $pqx \in \mathbb{Z}$ but $px, qx \notin \mathbb{Z}$. (Note that this is as it should be; σ_ζ can be discontinuous only at roots of the Alexander polynomial, which correspond to precisely these x.) Moreover there can be at most one lattice point on the union of these lines; for given two we have $(i_1 - i_2)/p + (j_1 - j_2)/q \in Z$, whence $i_1 = i_2$, $j_1 = j_2$. Finally, if $pqx \in Z$, $px, qx \notin Z$ such a lattice point does exist. We can write $pqx = ap + bq$ for some integers a, b with $0 < a < q$. There are two cases.

(1) $0 < b < p$. Then $(\frac{b}{p}, \frac{a}{q})$ is a lattice point on the lower line.

(2) $-p < b < 0$. Then $(\frac{b+p}{p}, \frac{a}{q})$ is a lattice point on the upper line.

Noticing that $f_{p,q}(x) = +1$ or -1 according as we are in case (1) or (2), we see that $f_{p,q}$ can be described as follows. For any integer $n = ap + bq$, let

$$h_{p,q}(n) \;=\; (-1)^{[a/q]+[b/p]+[n/pq]}$$

where $[..]$ denotes integer part; this is clearly well-defined and of period pq. Then

$$(*) \qquad f_{p,q}(x) = \begin{cases} h_{p,q}(pqx) & \text{if } pqx \in \mathbb{Z}, \quad px, qx \notin \mathbb{Z} \\ 0 & \text{otherwise} \end{cases} .$$

Lemma 1. *The functions* $f_{p,q} : R \to \mathbb{Z}$ *are linearly independent.*

Proof.

Suppose given some dependence relation amongst the $f_{p,q}$'s. Let K be the maximum of the product pq over those $f_{p,q}$ appearing in the relation, and enumerate the distinct factorisations of K into two coprime numbers as

$$\{p_1,q_1\}, \ldots, \{p_n,q_n\}, \quad \text{with}$$

$$1 < p_1 + q_1 < \ldots < p_n + q_n .$$

By $(*)$, $f_{p,q}(\frac{1}{K}) = f_{p,q}(\frac{p_i+q_i}{K}) = 0$ for $pq < K$; it follows that the (n+1 tuples

$$(\substack{*\\*}) \qquad (f_{p_i,q_i}(\tfrac{1}{K}), f_{p_i,q_i}(\tfrac{p_1+q_1}{K}), \ldots, f_{p_i,q_i}(\tfrac{p_n+q_n}{K})), \quad i = 1,\ldots,n$$

are linearly dependent. But by $(*)$ $f_{p,q}(x) \le 0$ for $0 \le x < \frac{p+q}{pq}$, while $f_{p,q}(\frac{p+q}{pq}) = +1$. Hence the $n \times (n+1)$ matrix with rows $(\substack{*\\*})$ is

$$\left\|\begin{matrix} -1 & 1 & & & & \\ -1 & -1 & 1 & & ? & \\ -1 & -1 & -1 & 1 & & \\ \cdot & \cdot & \cdot\cdot & \cdot & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & -1 & -1 & \ldots & -1 & 1 \end{matrix}\right\|$$

which has rank n. □

Since f_K is an additive cobordism invariant of K, this proves:

Theorem 1. The torus knots are linearly independent in the knot cobordism group (in the usual sense). □

We will now show how the signatures of a satellite knot are determined by those of its constituent parts. Putting this together with the preceding calculation will give a formula for the signatures of iterated torus knots.

We suppose given an unknotted solid torus $V \subset S^3$ and a knot k contained with (algebraic) winding number q in the interior of V. From this "pattern" and any knot K we construct a satellite knot K^* by taking a faithful embedding $f: V \to S^3$ with f (core of V) $= K$, and setting $K^* = f(k)$.

Theorem 2. If ζ is a root of unity,

$$\sigma_\zeta(K^*) = \sigma_{\zeta^q}(K) + \sigma_\zeta(k) .$$

Remarks

(1) Shinohara [Sh] has proved the case $\zeta = -1$ (the ordinary signature) by considering a Seifert surface of K^*.

(2) If k is a link, the same result holds with the same proof. If K is an n-component link, we can replace each component K_i using a pattern (V_i, k_i) of winding number q and an embedding f_i of V_i onto a neighbourhood of K_i ; if p_i is a parallel curve of V_i we require $Lk(f_i(p_i), K) = 0$. Then the corresponding result holds provided $\zeta^q \neq 1$, while if $\zeta^q = 1$ it only holds to within $\pm 2(n-1)$. The proof is similar.

Lemma 2. *If K is a knot, there is a 4-manifold N with $\partial N = S^3$, $H_1(N) = 0$ and a 2-disc D in N with $\partial D = K$ and $[D,\partial D] = 0 \in H_2(N,\partial N)$.*

Proof.

We can obtain K by starting with an unknot $\bar{K}$ and performing surgery on unknotted curves $J_1, \ldots, J_m$ in $S^3 - \bar{K}$ with framings $\varepsilon_i = \pm 1$ (to change some undercrossings to overcrossings); we can assume $Lk(J_i, \bar{K}) = 0 = Lk(J_i, J_j)$ $(i \neq j)$.

Let $N = D^4 + h_1^2 + \ldots + h_m^2$, where the 2-handle h_i^2 is attached along J_i with framing ε_i , and let D be a 2-disc in D^4 with boundary $\bar{K}$. □

Proof of Theorem 2.

Take N and D as provided by the lemma, and take a neighbourhood $D \times B^2$ of D in N with $\partial D \times B^2 = f(V)$. Let G be a surface properly embedded in $D \times B^2$ with $\partial G = f(k)$. Then $[G,\partial G] = 0 \in H_2(N,\partial N)$, so we can form the m-fold cyclic cover $(\tilde{N}, \tau)$ of N branched over G, and for $\zeta^m = 1$

$$\sigma_\zeta(\tilde{N}, \tau) = \sigma_\zeta(K^*) + \sigma(N). \qquad (1)$$

Also, since $f : V \to \partial N$ is faithful and $[D,\partial D] = 0$, f is faithful as an embedding $V \to \partial(D \times B^2)$, and so extends to a homeomorphism $S^3 \to \partial(D \times B^2)$. Hence if $\widetilde{D \times B^2} = \pi^{-1}(D \times B^2)$, where $\pi : \tilde{N} \to N$ is the projection, then

$$\sigma_\zeta(\widetilde{D \times B^2}, \tau) = \sigma_\zeta(k) . \qquad (2)$$

Now let $X = cl(N - (D \times B^2))$. Then $\pi^{-1}(X)$ is the unbranched m-fold cover of X corresponding to the homomorphism $H_1(X) \to Z_m$ given by linking number with G. But this is just q times linking number with D, so $\pi^{-1}(X)$ depends on q but not otherwise on k and G. To emphasize this we write $\pi^{-1}(X) = \widetilde{X}_q$, and also write τ_q for the restriction of τ to $\widetilde{X}_q$. We assert that the following two formulae hold.

$$\sigma_\zeta(\widetilde{X}_q, \tau_q) = \sigma_{\zeta q}(\widetilde{X}_1, \tau_1) \tag{3}$$

$$\sigma_\zeta(\widetilde{N}, \tau) = \sigma_\zeta(\widetilde{D \times B^2}, \tau) + \sigma_\zeta(\widetilde{X}_q, \tau_q) . \tag{4}$$

Now (1) - (4) give

$$\sigma_\zeta(K^*) + \sigma(N) = \sigma_\zeta(k) + \sigma_{\zeta q}(\widetilde{X}_1, \tau_1) . \tag{5}$$

Taking k to be a core of V in (5) gives

$$\sigma_\zeta(K) + \sigma(N) = \sigma_\zeta(\widetilde{X}_1, \tau_1)$$

and substituting in (5) from this gives the desired result. Notice that (3) is immediate if q is coprime to m, because then $\widetilde{X}_q \cong \widetilde{X}_1$ in such a way that τ_1 corresponds to τ_q^q. The general case follows from this by considering suitable t-fold covers of X, where $t = m/\mathrm{hcf}(m,q)$.

For (4), consider the Mayer-Vietoris sequence

$$\begin{aligned} H_2(\widetilde{X}_q \cap \widetilde{D \times B^2}) \to H_2(\widetilde{X}_q) \oplus H_2(\widetilde{D \times B^2}) \to H_2(\widetilde{N}) \to \\ \to H_1(\widetilde{X}_q \cap \widetilde{D \times B^2}) \xrightarrow{\phi} \dots \end{aligned} \tag{6}$$

Now $X \cap D \times B^2 = D \times \partial B^2$ (Fig.2), so $\widetilde{X}_q \cap D \times B^2 = \widetilde{D \times \partial B^2}$ is a disjoint union of solid tori; in particular $H_2(\widetilde{X}_q \cap \widetilde{D \times B^2}) = 0$.

Let $X \to S^1$ be a map inducing $Lk(-, D)$ on H_1; we have the diagram

$$\begin{tikzcd} D \times \partial B^2 \arrow[r] \arrow[rr, bend right, "\sim"'] & X \arrow[r] & S^1 \arrow[r, "q"] & S^1 \end{tikzcd}$$

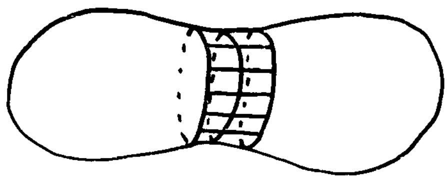

Figure 2

Pulling back the standard m-fold cover $S^1 \xrightarrow{m} S^1$ gives a diagram

$$\begin{tikzcd}
\widetilde{D \times \partial B^2} \arrow[r] \arrow[d] \arrow[rr, bend left, "\simeq"] & \tilde{X}_q \arrow[r] \arrow[d] & \tilde{S}^1 \arrow[r] \arrow[d] & S^1 \arrow[d, "m"] \\
D \times \partial B^2 \arrow[r] \arrow[rr, bend right, "\simeq"'] & X \arrow[r] & S^1 \arrow[r, "q"] & S^1
\end{tikzcd}$$

Hence $H_1(\widetilde{D \times \partial B^2}) \to H_1(\tilde{X}_q)$ is mono, so the homomorphism ϕ of (6) is mono and $H_2(\tilde{X}_q) \oplus H_2(\widetilde{D \times B^2}) \to H_2(\tilde{N})$ is an isomorphism. Since this preserves the intersection form and commutes with τ_*, (4) follows. $\square$

Now let

$$K = \{p_1, q_1; \ldots; p_n, q_n\}$$

be a (p_1,q_1) cable about a (p_2,q_2) cable about ... about a (p_n,q_n) torus knot. (A (p,q) cable goes p times meridianally and q times longitudinally about its companion.) We will only consider $p_i, q_i > 0$; without loss of generality we may assume $q_i > 1$, $p_n > q_n$. Set $r_i = q_1 q_2 \ldots q_{i-1}$. Then by induction

$$f_K = \sum_{i=1}^{n} f_{p_i, q_i; r_i},$$

where

$$f_{p,q;r}(x) = f_{p,q}(rx) .$$

Note that the signatures will certainly not suffice to give linear independence of $\underline{\underline{A}}$ in the usual sense, as a sum of $f_{p,q;r}$'s can often be reassembled into a sum of f_K's in more than one way. Also, the functions $f_{p,q;r}$ are not linearly independent. In fact

$$f_{2,3;5} = f_{6,5} - f_{2,3} - f_{2,5} - f_{3,5} .$$

(Hence, for instance, $\{2,5;3,2\} \# \{3,2\} \# \{5,3\}$ has the same signatures as $\{6,5\}$; but $\{2,5;3,2\} \notin A$.) However, the class $\underline{\underline{A}}$ is sufficiently restricted that the following rather weak result is enough.

Lemma 3. *If $pq = p'q'r = K$ with $p,q,p',q',r > 1$ and (p,q), (p',q') coprime pairs, then there exists k coprime to K with*

$$f_{p,q}\left(\frac{k}{K}\right) \neq f_{p',q';r}\left(\frac{k}{K}\right)$$

unless $\{p,q\} = \{6,5\}$, $\{p',q'\} = \{3,2\}$.

The proof of this is rather long and tedious, and is relegated to an appendix.

Let $\underline{\underline{B}}$ be the class of those $\{p_1,q_1;p_2,q_2; \dots :p_n,q_n\}$ with $p_i > p_{i+1}q_{i+1}$ $(i = 1,\dots,n-1)$. It follows from Lê [LDT;§1] that $\underline{\underline{A}} \subset \underline{\underline{B}}$, so the following result includes the answer to Rudolph's question.

Theorem 3. *$\underline{\underline{B}}$ is independent in the cobordism group, in the sense that*

$$[K] = \sum_{i=1}^{n} [K_i] \qquad K,K_i \in \underline{\underline{B}}$$

implies that $n = 1$, $K_1 = K$.

Observe that $p_i > p_{i+1}q_{i+1}$ is equivalent to $p_iq_ir_i > p_{i+1}q_{i+1}r_{i+1}$; it is then not difficult to deduce Theorem 3 from the lemma. A small amount of care is needed to ensure that the exception to the lemma causes no trouble.

REFERENCES

[Br] E. Brieskorn, Beispiele zur Differentialtopologie von Singularitaten, Invent.Math.2 (1966) 1-14.

[Go] Deborah L. Goldsmith, Symmetric fibred links, *in* Knots, groups and 3-manifolds, Ann. of Math. Studies 84, ed. L.P. Neuwirth (Princeton 1975).

[Hi] F. Hirzebruch, Singularities and exotic spheres, Sem.Bourbaki 314 (1966/7).

[KT] Louis H. Kauffman and Laurence R. Taylor, Signature of links, Trans. Amer.Math.Soc. 216 (1976) 351-365.

[LDT] Lê Dũng Tráng, Sur les noeuds algêbriques, Comp.Math. 25 (1972) 281-321.

[Ro] V.A. Rohlin, Two-dimensional submanifolds of four-dimensional manifolds, Func.Anal.Appl. 5 (1971) 39-48.

[Ru] Lee Rudolph, Notices Amer.Math.Soc. 23 (1976) 410.

[Sh] Y. Shinohara, On the signature of knots and links, Trans.Amer.Math.Soc. 156 (1971) 273-285

[Tr] A.G. Tristram, Some cobordism invariants for links, Proc.Camb.Phil.Soc. 66 (1969) 251-264.

[Vi] O.Ja. Viro, Branched coverings of manifolds with boundary and link invariants I, Math.USSR Izvestija 7 (1973) 1239-1255.

APPENDIX :

Proof of Lemma 3.

In this appendix, all variables denote integers. We denote the h.c.f. of a and b by $\langle a,b \rangle$. We start with two lemmas.

Lemma A1 *Let* $a,b > 1$, *and suppose there is no integer coprime to* a *in the interval* $[\frac{a}{b}, a(1-\frac{1}{b})]$. *Then one of the following holds:*

(i) $b = 2$;

(ii) $a = 4$, $b = 3$;

(iii) $a = 6$, $b \leq 5$;

(iv) $a = 10$, $b = 3$.

<u>*Proof.*</u> We consider three cases.

(1) $a = 2n+1$, $n > 0$. We have $\langle n,a \rangle = 1$ and $n < \frac{a}{2}$, so by assumption $n < \frac{a}{b}$. Thus $b < 2 + \frac{1}{n}$, so $b = 2$.

(2) $a = 2(2n+1)$, $n \geqq 0$. If $n = 0$, $a = 2$ and so $\frac{a}{b} \leqq 1 \leqq a(1 - \frac{1}{b})$. But 1 is coprime to a, so we have a contradiction.

If $n > 0$, $\langle 2n-1, a \rangle = 1$ and $2n-1 < \frac{a}{2}$, so $2n-1 < \frac{a}{b}$. Thus $b < 2 + \frac{4}{2n-1}$. Hence either $b = 2$ or $2n-1 < 4$. In the latter case $n \leq 2$; if $n = 1$ then $a = 6$ and $b < 6$, while if $n = 2$, $a = 10$ and $b \leq 3$.

(3) $a = 4n$, $n > 0$. We have $\langle 2n-1,a \rangle = 1$ and $2n-1 < \frac{a}{2}$, so $2n-1 < \frac{a}{b}$. Thus $b < 2 + \frac{2}{2n-1}$. Hence either $b = 2$ or $n = 1$. In the latter case $a = 4$ and $b < 4$.

<u>*Lemma A2*</u> *Suppose that $a > 2$, γ_1 and γ_2 are coprime to a with $\gamma_2 < \gamma_1$, and that there is no δ coprime to a with $\gamma_2 < \delta < \gamma_1$. Suppose further that $\gamma_1 - \gamma_2 > \frac{a}{2}$. Then either*

(i) $a = 3$ and $\gamma_1 \equiv 1 \mod 3$; or

(ii) $a = 6$ and $\gamma_1 \equiv 5 \mod 6$.

<u>*Proof.*</u> We may assume $0 < \gamma_2 < a$. There are two cases.

(1) $\gamma_2 = a-1$. Then $\gamma_1 = a+1$, so $2 > \frac{a}{2}$. Hence $a = 3$ and $\gamma_1 \equiv 1 \mod 3$.

(2) $\gamma_2 \neq a-1$. Then $\gamma_1 < a$. We must have $\gamma_2 < \frac{a}{2} < \gamma_1$, from which it follows that $\gamma_1 = a-\gamma_2$. Hence $\frac{a}{2} < a-2\gamma_2$, or $\gamma_2 < \frac{a}{4}$. Thus there is no integer coprime to a in the interval $\left[\frac{a}{4}, \frac{3a}{4}\right]$. Applying Lemma A1 with $b = 4$ we find $a = 6$, and hence $\gamma_1 \equiv 5 \mod 6$. □

From now on we consider the situation of Lemma 3. That is, $p,q,p',q' \geqq 2$, $\langle p,q \rangle = \langle p',q' \rangle = 1$, $r \geqq 2$ and $pq = p'q'r = K$. We further assume that $f_{p,q}(\frac{k}{K}) = f_{p',q';r}(\frac{k}{K})$ whenever $\langle k,K \rangle = 1$. Our aim is to prove that $\{p,q\} = \{6,5\}$ and $\{p',q'\} = \{2,3\}$. The basic idea is to use the fact that $f_{p',q';r}$ has period $\frac{1}{r}$, and try to prove that $f_{p,q}$ does not. This becomes obscured in the consideration of several special cases, but it is the basis of Lemma A3 below.

Let $p = stu$, where $s = \langle p, p'q' \rangle$, every prime factor of t divides s, and $\langle u, s \rangle = 1$.

<u>*Lemma A3.*</u> *Suppose* $0 < \beta_1 < \beta_2 < p$, $\langle \beta_i, p \rangle = 1$ *and* $\beta_1 \equiv \beta_2 \mod s$. *If* $\langle \alpha, q \rangle = 1$ *then* $\alpha \notin \left[\frac{\beta_1 q}{p}, \frac{\beta_2 q}{p}\right]$.

<u>*Proof.*</u> Set $k_i = (q-\alpha)p + \beta_i q$; then $\langle k_i, K \rangle = 1$. Suppose $\frac{\beta_1 q}{p} < \alpha < \frac{\beta_2 q}{p}$. Then $\left[\frac{\beta_1}{p}\right] = \left[\frac{q-\alpha}{q}\right] = \left[\frac{\beta_2}{p}\right] = 0$, and $0 < k_1 < pq < k_2 < 2pq$. Hence

$$f_{p,q}\left(\frac{k_i}{K}\right) = (-1)^{\left[\frac{q-\alpha}{p}\right] + \left[\frac{\beta_i}{p}\right] + \left[\frac{k_i}{pq}\right]}$$

$$= (-1)^{i-1}.$$

But $\beta_1 \equiv \beta_2 \mod s$ implies that $k_1 \equiv k_2 \mod p'q'$, and hence that $f_{p',q';r}\left(\frac{k_1}{K}\right) = f_{p',q';r}\left(\frac{k_2}{K}\right)$, a contradiction. Since $\alpha \neq \frac{\beta_i q}{p}$, we are done. □

We now distinguish four cases.

(1) $t > 1$

(2) $t = 1$, $u \geqq 3$, $(u,s) \neq (3,4)$

(3) $t = 1$, $u = 3$, $s = 4$

(4) $t = 1$, $u \leqq 2$.

In cases (1) and (2) we shall prove

(*) *If* $\langle \alpha, q \rangle = 1$, *then* $\alpha \notin \left[\frac{q}{p}, \frac{q}{2}\right]$.

From (*) it follows that $\alpha \notin \left[\frac{q}{p}, q(1 - \frac{1}{p})\right]$; since in these cases $p > 2$ (in case (1) note that $t > 1 \Longrightarrow s > 1$) and since $\langle p, q \rangle = 1$, Lemma A1 then gives $(p,q) = (3,4)$, $(5,6)$ or $(3,10)$. There are only finitely many possibilities for p', q' and r in each case, and direct calculation will exclude all combinations except $(p,q) = (5,6)$, $\{p',q'\} = \{2,3\}$.

(1) $\underline{t > 1}$. Lemma A3 with $\beta_1 = 1$, $\beta_2 = 1 + s(t-1)u$ gives (*).

(2) $\underline{t = 1,\ u \geqq 3,\ (u,s) \neq (3,4)}$. If $s = 1$, apply Lemma A3 with $\beta_1 = 1$, $\beta_2 = p-1$. If $s > 1$, choose γ_1 so that $1 = \gamma_1 s + \delta u$ for some δ; then $\langle \gamma_1, u \rangle = 1$. Let γ_2 be the greatest integer coprime to u and less than γ_1. Then $\gamma_2 > \gamma_1 - u$, so setting $\beta = (u + \gamma_2)s + \delta u$, β is coprime to p and $1 < \beta$. Also $\beta < (u + \gamma_1)s + \delta u = su + 1 = p + 1$, and so $\beta < p$. Since $\beta \equiv 1 \bmod s$, Lemma A3 shows that $\alpha \notin \left[\frac{q}{p}, \frac{\beta q}{p}\right]$. If $\frac{\beta}{p} \geqq \frac{1}{2}$, (*) is proved. If not, $\beta - 1 < \frac{p}{2}$; i.e. $(u + \gamma_2 - \gamma_1)s < \frac{su}{2}$, and so $\gamma_1 - \gamma_2 > \frac{u}{2}$. By Lemma A2, there are two possibilities.

(2.1) $\underline{u = 3,\ \gamma_1 \equiv 1 \bmod 3}$. Then $s \equiv 1 \bmod 3$. Since $s = 4$ is case (3), we have $s \geqq 7$. Apply Lemma A3 to the pairs $(\beta_1, \beta_2) = (1, s+1)$ and $(s-3, 2s-3)$ to prove (*).

(2.2) $\underline{u = 6,\ \gamma_1 \equiv 5 \bmod 6}$. Then $s \equiv 5 \bmod 6$. Apply Lemma A3 with $(\beta_1, \beta_2) = (1, 2s+1)$ and $(s+2, 3s+2)$ to prove (*).

The proof in cases (1) and (2) is now complete.

(3) $\underline{t = 1,\ u = 3,\ s = 4}$. In this case $p = 12$. Apply Lemma A3 with $\beta_1 = 1$, $\beta_2 = 5$; we find that if $\langle \alpha, q \rangle = 1$ then $\alpha \notin \left[\frac{q}{12}, \frac{5q}{12}\right]$. Lemma A1 no longer applies but we can obtain a contradiction by similar arguments. There are two subcases.

(3.1) $\underline{q = 3n+1,\ n \geq 1}$. Take $\alpha = n$. Then either $n < \frac{3n+1}{12}$ or $n > \frac{5(3n+1)}{12}$. These are both absurd.

(3.2) $\underline{q = 3n+2,\ n \geq 1}$. Since q is coprime to $p = 12$, n must be odd. Hence we can take $\alpha = n$ and again obtain a contradiction.

Since $\langle q, 12 \rangle = 1$, this exhausts case (3).

(4) $\underline{t = 1,\ u \leq 2}$. Let $q = \sigma\tau\nu$, where $\sigma = \langle q, p'q' \rangle$, every prime factor of τ divides σ, and $\langle \nu, \sigma \rangle = 1$. By symmetry in p and q we may assume that $\tau = 1$ and $\nu \leqq 2$. Now if $u = \nu = 1$

then $r = 1$, contrary to hypothesis. Also, u and ν cannot both be 2, so $r = 2$ and $p'q'$ is odd. Assume (without loss of generality) that $p' < q'$, and notice that $2p' + q' < p' + 2q' < p'q'$. Now, $p+q$ can be characterised as the least positive k such that $\langle k,K \rangle = 1$ and $f_{p,q}(\frac{k}{K}) = +1$; similarly $2p' + q'$ is the least positive k with $\langle k,K \rangle = 1$ and $f_{p',q';r}(\frac{k}{K}) = +1$ (since $\langle p' + q',K \rangle \neq 1$). Hence $p+q = 2p' + q'$; since also $pq = K = (2p')q'$, we have $\{p,q\} = \{2p',q'\}$

Now consider $k = p' + 2q'$. We have $0 < k < p'q' < K$ and $\langle k,K \rangle = 1$. So

$$f_{p',q';r}(\frac{k}{K}) = (-1)^{[1/q']+[2/p']+[k/p'q']} = +1 .$$

But also $k = \frac{1+q'}{2}\, 2p' + (2-p')q'$, so

$$f_{p,q}(\frac{k}{K}) = f_{2p',q'}(\frac{k}{K}) = (-1)^{[(1+q')/2q']+[(2-p')/2p']+[k/K]} = -$$

This contradiction disposes of case (4) and completes the proof of Lemma 3.