Lemma Let v, u be non-empty strings ($|u|, |v| \geq 1$).

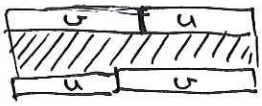
If $vu = uv$ then there exists a string r such that $v = r^i$ and $u = r^j$ for some $i, j \geq 1$.

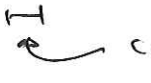
Proof: By induction on $k = |u| + |v|$.

Basis: $k = 2$. Then $|u| = |v| = 1$. So $vu = uv$ implies $v = u$, so $r = v\ (= u)$ will do.

Induction step: $k > 2$. If $|u| = |v|$, same argument as for basis (above) shows that $r = v\ (= u)$ will do. So we may assume wlog. that $|u| < |v|$

Then the situation is:





We see from the figure that $uw = v = wu$.

As $|u| + |w| = |v| < |v| + |u| = k$ and as $|u|, |w| \geq 1$, we can use the induction hypothesis. This gives the existence of a string r (and integers i, j) such that $r^i = u$ and $r^j = w$.

Hence $r^i = u$ and $r^{i+j} = r^i r^j = uw = v$ shows the lemma for this k.

□

From the lemma easily follows the

Primitivity Corollary:

If a string is primitive it cannot be equal to any (proper) cyclic shift of itself.

Proof:

A cyclic shift of a string s is any string formed by partitioning s into two parts $s = uv$ and then reversing their order.

It is proper if $|u|, |v| \geq 1$.
If these two strings are equal ($uv = vu$), the lemma above gives an r such that

$$s = uv = r^i r^j = r^{i+j} \qquad (i, j \geq 1)$$

I.e. s is a power of another string, hence it cannot be primitive.

□