Math 4740: Number theory for Lemma 1.16

Lemma. *For a state x of a Markov chain, let $I_x = \{n \geq 1 : P^n(x,x) > 0\}$. If the greatest common divisor of I_x is 1 (i.e. x has period 1), then there is an integer n_0 such that for all $n \geq n_0$, $n \in I_x$.*

Proof. A subset I of $\mathbf{Z}$ is called an *ideal* if it is closed under addition and "ambient multiplication." That is, if $a, b \in I$ then $a + b \in I$, and if $a \in I$, then $ca \in I$ for all $c \in \mathbf{Z}$. Examples of ideals include $I = \{0\}$, $I = \mathbf{Z}$, and $I = \{3c : c \in \mathbf{Z}\}$. An ideal is called *principal* if it takes the form $I = \{cd : c \in \mathbf{Z}\}$ for fixed d. All three of the examples above are principal ideals: respectively we take $d = 0$, $d = 1$, and $d = 3$.

In fact, every ideal in $\mathbf{Z}$ is a principal ideal. (A number theorist would say that $\mathbf{Z}$ is a "principal ideal domain.") The proof is this. Let $I \subseteq \mathbf{Z}$ be an ideal. For any $n \in I$, I must contain all the integer multiples of n; in particular this means $-n \in I$, so I is symmetric about 0. If actually $I = \{0\}$ then it is principal. If not, I must contain at least some positive elements, so we can let d be the least positive element of I. Immediately, I contains the set $\{cd : c \in \mathbf{Z}\}$. We claim I is actually equal to this set. Suppose for contradiction that I contains an element b which is not an integer multiple of d. Using division with remainder, we can write $b = dq + r$ where $q, r \in \mathbf{Z}$ and $0 < r < d$. Now, since $b \in I$ and $-dq = (-q)d \in I$, we have $r = b - dq \in I$ by closure under addition. But since $0 < r < d$, this contradicts the definition of d as the least positive element of I. We conclude that $I = \{cd : c \in \mathbf{Z}\}$, so it is a principal ideal.

Returning now to the lemma, the set I_x is not quite an ideal. It is closed under addition and under ambient multiplication by *positive* integers c, but not negative integers. To "fix" this problem we consider the set of all finite linear combinations of elements of I_x:

$$J = \{c_1 a_1 + c_2 a_2 + \cdots + c_\ell a_\ell : \ell \geq 1, a_1, \ldots, a_\ell \in I_x, c_1, \ldots, c_\ell \in \mathbf{Z}\}.$$

You can check that J is closed under addition and ambient multiplication by $\mathbf{Z}$, hence J is an ideal. The argument above shows that J is principal, that is, $J = \{cd : c \in \mathbf{Z}\}$ for some positive integer d. In fact d is the period of x, as we will show.

Certainly $I_x \subseteq J$, so every element of I_x is divisible by d. Since $d \in J$, there exist fixed elements $a_1, \ldots, a_\ell \in I_x$ and coefficients $c_1, \ldots, c_\ell \in \mathbf{Z}$ such that

$c_1a_1 + \cdots + c_\ell a_\ell = d$. Say that md is the least element of I_x. We'll choose large positive coefficients $C_1, \ldots, C_\ell$ and consider the elements

$$\begin{aligned} k &= C_1a_1 + C_2a_2 + \cdots + C_\ell a_\ell, \\ k + d &= (C_1 + c_1)a_1 + (C_2 + c_2)a_2 + \cdots + (C_\ell + c_\ell)a_\ell, \\ k + 2d &= (C_1 + 2c_1)a_1 + (C_2 + 2c_2)a_2 + \cdots + (C_\ell + 2c_\ell)a_\ell, \\ &\vdots \\ k + md &= (C_1 + mc_1)a_1 + (C_2 + mc_2)a_2 + \cdots + (C_\ell + mc_\ell)a_\ell. \end{aligned}$$

We want to make the C_i big enough that each coefficient $C_i + jc_i$ for $0 \leq j \leq m$ is nonnegative; one way to accomplish this is to let $C_i = m|c_i|$. Given this choice of C_i, all the elements $k, k + d, \ldots, k + md$ are contained in I_x. Since also $md \in I_x$, by repeatedly adding md we conclude that I_x contains every multiple of d above k.

Already just from the statements $k \in I_x$ and $k + d \in I_x$ we can see that the period of x is d. (We knew it was at least d, and if for sake of contradiction the period were $D > d$, every pair of elements in I_x would be at least D apart.) In the special case that x has period 1, we have shown that I_x contains every integer above k, proving the lemma. □