已知$X_{n+1} = aX_n (\mathrm{mod}\ 2^k)$，求{ X_n }最大周期与对应的 a 值。

说明:对问题中 k 仅考虑 k≥3 的情形；当 k=0,1,2 时，可通过枚举，略。

解：

引理 1：欧拉定理；

引理 2:模 m 有原根的必要条件时 $m = 1, 2, 4, p^{\propto}$或$2p^{\propto}$,其中 p 是奇素数,$\propto \geq 1$;

(1) 设对于某一 a 值，{ X_n }最大周期为 T(a)，则

$$X_{T(a)+1} \equiv a^{T(a)} X_1 \equiv X_1 (\mathrm{mod}\ 2^k)$$

即

$$a^{T(a)} \equiv 1 (\mathrm{mod}\ 2^k)$$

由引理 1：欧拉定理可知$\varphi(2^k) = 2^{k-1}$，则

$$T(a) | 2^{k-1}$$

由引理 2 知，模 2^k 没有原根，则

$$T(a) \neq \varphi(2^k)，即 T(a) \neq 2^{k-1}$$

所以

$$T(a) | 2^{k-2} 且\ T(a) \leq 2^{k-2}$$

(2) 考虑 a 的取值时，显然 a 应为奇数，可以分为 a=8t±1 与 a=8t±3 两种情形。

a) 当$a = 8t \pm 3\ (t \in N)$时，可由数学归纳法证明如下结论

$$T(a) \nmid 2^{k-3},$$

I. 当$k = 3$时，

$$a^{2^{k-3}} = (8t \pm 3)^{2^{k-3}} = (8t \pm 3)^{2^0} \neq 1 (\mathrm{mod}\ 2^3)$$

II. 假设$k = r$时，存在

$$a^{2^{r-3}} \neq 1 (\mathrm{mod}\ 2^r)$$

当$k = r + 1$时，

$$a^{2^{r-2}} - 1 = \left(a^{2^{r-3}} - 1\right)\left(a^{2^{r-3}} + 1\right)$$

由于$a^{2^{r-3}} \neq 1(\mathrm{mod}\ 2^r)$

所以$a^{2^{r-3}} - 1 = 2^b \cdot Q_1$，其中$b < r$，$Q_1$为奇数

又因为

$$a^{2^{r-3}} + 1 \equiv (8t \pm 3)^{2^{r-3}} + 1 \equiv (\pm 3)^{2^{r-3}} + 1 \equiv 2(\mathrm{mod}\ 4)$$

所以$a^{2^{r-3}} + 1 = 2 \cdot Q_2$，其中$Q_2$为奇数

因此

$$a^{2^{r-2}} - 1 = 2^{b+1} \cdot Q_1 Q_2$$

又$b + 1 < r + 1$，即$a^{2^{r-2}} \neq 1(\mathrm{mod}\ 2^{r+1})$，所以归纳法得证！

则$T(a) \nmid 2^{k-3}$得证，即存在$T(a) > 2^{k-3}$

再结合(1)中结论可知，在$a = 8t \pm 3\ (t \in N)$时，$T(a) = 2^{k-2}$。

b) 当$a = 8t \pm 1\ (t \in N)$时，由相同方法可知. $T(a) \leq 2^{k-3}$。

综上所述，当$a = 8t \pm 3\ (t \in N)$时，有最大周期2^{k-2}。