1. Mediante un sencillo procedimiento de simulación, hacer que el ordenador encuentre las parejas (a,c) que den lugar a un esquema de hashing válido (sucesión que no cicle antes de tiempo).

```cpp
#include <iostream>
#include <stdio.h>
#include <stdlib.h>

using namespace std;

static int M;

/* Comprueba si elemento se cuentra en el vector v[] */
bool pertenece(int v[], int util_v, int elemento)
{
   bool pertenece = false;

   for (int i=0; i<util_v && !pertenece; ++i)
      pertenece = (v[i] == elemento);

   return pertenece;
}

/* Comprueba si la secuencia de los d_i construida
   a partir del par (a,c) cicla antes de tiempo */
bool noCicla(int a, int c)
{
   int *v = new int[M];   /**< Vector con los d_i anteriores */
   v[0] = 0;
   int util_v = 1;

   bool no_cicla = true;
   int d_i = 0;

   for (util_v; util_v<M && no_cicla; ++util_v)
   {
      d_i = (a * d_i + c) %M;
      no_cicla = !pertenece(v,util_v,d_i);
      v[util_v] = d_i;
   }

   return no_cicla;
}

int main(int argc, char const *argv[])
{
   M = atoi(argv[1]);

   cout << " ------------ " << M << " ------------ " << endl;


   for (int c=0; c<M; ++c)
      for (int a=0; a<M; ++a)
         if(noCicla(a,c))
            cout << "| c:" << c << ", a:" << a << " | " << endl;

   cout << " ---------- FIN ---------- " << endl;

   return 0;
}
```

2. Extraer conclusiones del resultado, es decir dar posibles soluciones teóricas independientemente del tamaño M de la tabla que tengamos.

Antes de extraer las conclusiones del simulador, destacamos una propiedad de las posibles soluciones (a, c) que justifica que el simulador solo compruebe los valores para $0 < a < M$ y $0 < c < M$:

- **Si (a,c) es una combinación válida, (a',c') también lo es, con** $\begin{cases} a' = a + n_1 M & \forall n_1 \in \mathbb{N} \\ c' = c + n_2 M & \forall n_2 \in \mathbb{N} \end{cases}$

  Se cumple ya que $d_i = [ad_{i-1} + c] \,\%\, M = [a' d_{i-1} + c'] \,\%\, M$ ($\%M$ anula el sumando $n_i M$)

Una consecuencia directa de lo anterior es que existirán infinitas soluciones siempre que exista una solución particular. Por otro lado, es fácil darse cuenta que toda solución (a, c) es equivalente a una solución (a_o, c_o) comprendida en el intervalo $a_o, c_o \in [1, M-1]$.

Nuestro estudio se basa en analizar el conjunto de soluciones (a_o, c_o) comprendidas en $[1, M-1]$, pero no hay que olvidar que bajo una solución se esconde una infinidad de soluciones equivalentes entre sí módulo M. Además como $(a, c) = (1, 1)$ siempre una solución particular, para cualquier M existen infinitas soluciones (mínimo las equivalentes a (1,1)).

Principales resultados teóricos:

- **Si M es primo, las únicas soluciones son de la forma** (a, c) **con** $\begin{cases} a = 1 \\ c = 1, 2, .., M-1 \end{cases}$

  Para este caso es posible dar una justificación teórica simple. En primer lugar, una solución $(a, c) \in [1, M-1]$ es válida si los d_i son todos distintos entre sí, esto es:

$$d_i \neq d_j, \, \forall i \neq j \tag{1}$$

  Si $a = 1$ y teniendo en cuenta que $d_o = 0$, la caracterización (1) se reduce a:

$$ic \neq nM, \; i = 1, ..., M-1 \Leftrightarrow c \neq M \Leftrightarrow c = 1, 2, .., M-1 \,.$$

  Si $a > 1$, un caso particular de (1) es el siguiente:

$$d_o \neq d_{M-1} \Leftrightarrow (1 + a^{\mathbf{1}} + ... + a^{M-2}) \,\%M \neq 0 \tag{2}$$

  Teniendo en cuenta la suma parcial de una progresión aritmética de razón a es:

$$1 + a^{\mathbf{1}} + ... + a^{M-2} = \sum_{i=0}^{M-2} a^i = \frac{1 - a^{M-1}}{1 - a}$$

  Por el pequeño teorema de Fermat tenemos que si M es primo y $a > 1$, entonces:

$$a^{M-1} \,\%M = 1 \tag{3}$$

  Sustituyendo (2) en (3) tenemos finalmente:

$$(1 + a^{\mathbf{1}} + ... + a^{M-2}) \,\%M = (\frac{1 - a^{M-1}}{1 - a}) \,\%M = 0 \,.$$

  Luego si M es primo, $a = 1$.

- **Si M no es primo, las soluciones (a,c) son de la forma** $c = i$ con $\begin{cases} mcd(c,i) = 1 \\ i = 1, ..., M-1 \end{cases}$,

  Es decir, los c serán los números coprimos o primos relativos con M. Para el caso de las a es necesario un estudio mas exhaustivo.

  - *Si* $M = 2^e$*, con* $e \geq 3$*, entonces* $\begin{cases} a_i = 1 + 4i \\ i = 0, 1, 2, ... \ / \ a_i < M \end{cases}$
    - $M = 16 = 2^4$, $\begin{cases} a = 1, 5, 9, 13 \\ c = 1, 3, 5, 7, 9, 11, 13, 15 \end{cases}$
  - *Si* $M = p^f$*, con* $p \geq 3$*,* $f \geq 2$*,* p *primo, entonces* $\begin{cases} a_i = 1 + pi \\ i = 0, 1, 2, ... \ / \ a_i < M \end{cases}$
    - $M = 9 = 3^2$, $\begin{cases} a = 1, 4, 7 \\ c = 1, 2, 4, 5, 7, 8 \end{cases}$
  - Si $M = 2^e p_1^{x_1} p_2^{x_2} ... p_k^{x_k}$ con $e \geq 3$, p_j *primo, entonces* $\begin{cases} a_i = 1 + 4p_1 p_2 ... p_k i \\ i = 0, 1, 2, ... \ / \ a_i < M \end{cases}$
    - $M = 40 = 2^3 * 5$, $\begin{cases} a = 1, 21 \\ c = 1, 2, 4, 5, 7, 8 \end{cases}$
  - Si $M = q^f p_1^{x_1} p_2^{x_2} ... p_k^{x_k}$ con $f \geq 2$, $q \geq 3, p_j$ *primo, entonces* $\begin{cases} a_i = 1 + qp_1 p_2 ... p_k i \\ i = 0, 1, 2, ... \ / \ a_i < M \end{cases}$
    - $M = 45 = 3^2 * 5$, $\begin{cases} a = 1, 16, 31 \\ c = coprimos(M) \end{cases}$
    - NOTA: si aparece $p_1^{x_1} = 2^2$, entonces $a_i = 1 + q4p_2 ... p_k i$
  - Si M no está en algún caso anterior, $a = 1$.

Toda esta distinción de casos se podría haber simplificado (nótese que los primos casos son situaciones particulares de los últimos), sin embargo, hemos querido dejar las soluciones en forma explícita y recalcar la diferencia existente entre el 2 y el resto de primos. Básicamente:

- **Sea M no primo. Existe una solución** $a \neq 1$ (asociada a un caso anterior) **si:**
  1. En la descomposición de M aparece un $p \neq 2$ elevado (al menos) al cuadrado.
  2. No se cumple 1, pero aparece $p = 2$ elevado (al menos) al cubo.