Cracking a Linear Congruential Generator

Let the first few numbers be X0, X1, X2, X3, X4, X5, X6, …

The 4 numbers X0, X1, X2, X3 form a 3x3 determinant D0:

X0 X1 1

X1 X2 1

X2 X3 1

The 4 numbers X1, X2, X3, X4 form a 3x3 determinant D1:

X1 X2 1

X2 X3 1

X3 X4 1.

The 4 numbers X2, X3, X4, X5 form a 3x3 determinant D2:

X2 X3 1

X3 X4 1

X4 X5 1, and so on.

A little algebraic manipulation performed on the linear congruences shows that Dk ≡ 0 (mod M) for every k. Hence M divides every Dk, so M divides h = gcd(D0, D1, D2, D3, …). This is fortunate, because the gcd will be somewhat smaller than the individual Dk.

The different Dk are unrelated to each other, so there is a good chance that h = M. Another possibility is that h = aM, where a is a small number, such as 2 or 3. Use trial-and-error to finish up.