**Example 1.** The following is an example of the MASH hash function in Sage. MASH is a function based on the use of modular arithmetic. It involves use of an RSA-like modulus M, whose bitlength affects the security. M should be difficult to factor, and for M of unknown factorization, the security is based in part on the difficulty of extracting modular roots. M also determines the block size for processing messages. In essence, MASH is defined as:

*Hi* = ((*xi* + *Hi*–1) 2 OR *Hi*–1) (mod *M*)

Where

*H*-1 = The largest prime less than

*xi* = the *i*th digit of the base *M* expansion of input *n*. So:

*n = x*0 + *x*1*M* + *x*2*M*2 + …