

Lehmer Generator: $L(a, m)$

X_0 is the seed

$$X_{n+1} = (a * X_n) \% m$$

Output a double $[0, 1)$: X_{n+1}/m

$L(28, 1013) * 10$

987193627389057014635836139773216911052664444984878773864748
429311477005350290951361900441173632252967979528572913476518
969204372097223971843427438796013293762506420249931533181521
507359703560365422188496162922762154247617789566111003035345
336041305127705498939950919737719810665373449406504195394417
214696207149125480544304631314402350786241356488615840002683
272794798438148287926915573300767514547568040577553186667698
393921923690628875448910213109816143547126876934300119688170
821017446071659571075812980128063726109429853641638602267830
88947335550151212261352515706885229946497090486380995588263
677470320204714270865234810307956279027760281565725612039867
062374935797500684668184784926402964396345778115038370772378
457523822104338889969646546639586948722945010600490802622801
893346265505934958046055827853037928508745194556953686855976
492137586435113841599973167272052015618517120730844266992324
854524319594224468133323016060780763093711245510897868901838
564528731230656998803118291789825539283404289241870198719362
738905701463583613977321691105266444498487877386474842931147
700535029095136190044117363225296797952857291347651896920437
209722397184342743879601329376250642024993153318152150735970

Linear Congruential Generator

$$X_{n+1} = (a * X_n + c) \% m$$

Java's Random class:

- $m = 2^{48}$
- $a = 25214903917$
- $c = 11$

- Output bits: 47..16