本日の課題

ハッシュから少々離れて，単なる乱数を生成するアルゴリズムについて考える．乱数を生成するアルゴリズムとして，線形合同法がある．この方法では以下の漸化式によって乱数を生成する．

$$X_{n+1} = (AX_n + B) \bmod M \qquad X_0\text{: 初期値}$$

ただし，A, B, M は適当な正の整数であるとする．このとき，X_0, X_1,...,X_{9999}を求めて，ここからこの配列の下pビットの周期を求めるプログラムを`kadai(A, B, M, p, X0)` をつくれ．ただし，この場合の下pビットの配列の周期とは，すべての要素のインデックス i （0から9999 - l 番目まで要素）について，

$$X_{\ell+i} \bmod 2^p = X_i \bmod 2^p$$

が成り立つ最小のl のことである．