Épreuve de section européenne

Random number generators

While some sequences generated by natural phenomena produce truly random numbers, many applications require that we be able to create random numbers efficiently inside a computer. This may sound impossible : computers simply execute a set of instructions whose output is determined by the input. Since we supply the computer with the instructions and the input, the output is determined by our choices. How can such a number be random ? The answer is that it's not. [...]

John von Neumann proposed using the following method as one of the first random number generators. Suppose we want to create eight-digit numbers. Begin with an eight-digit number X_0, which we call the seed, and define the next integer as the middle eight digits from X_0^2. For instance, if $X_0 = 35385906$, we find that $X_0^2 = 1252162343440836$ so that our next number is $X_1 = 16234344$. If we repeat this a few times we find the numbers in the table on the right.

X_0	16234344
X_1	55392511
X_2	33027488
X_3	81496359
X_4	65653025
X_5	31969165
X_6	02751079
X_7	56843566
X_8	19099559
X_9	79315399

Since it is difficult, at first glance, to find a pattern in these numbers, we may think that this is an appropriate way to find random numbers. In other words, we have created the illusion of randomness through a deterministic process. Further study shows, however, that this is not a good random number generator. Each term in the sequence depends only on its immediate predecessor and there are only a finite number of possible terms. This means that the sequence will inevitably repeat. The problem is that the sequence can get caught in relatively short cycles. For instance, if the number 31360000 appears in the sequence at some point, we end up with this number again after another 99 iterations and this cycle continues indefinitely.

From *Random Numbers : Nothing Left to Chance*,
an AMS Feature Column, by David Austin

Questions

1. Why is it impossible to create really random numbers with a computer ?
2. Explain why any sequence of numbers generated with Von Neumann's procedure will inevitably repeat.
3. Use Von Neumann's procedure to generate 10 "random" two-digit numbers with a seed $X_0 = 81$. Zeros may have to be added in front of each square to make it four-digits long. What problem is encountered after these ten numbers ?
4. What is the lowest two-digit number whose square is a real four-digit number ?
5. Try to find a two-digit number such that Von Neumann's procedure will always generate the same number. Show all your ideas, even if they seem fruitless.