

67) Done in class

68) Iterate $x^2+1 \pmod n$, starting with 2 for $n=937251$:

2, 5, 26, 677, 458330, 8172493, 643303, 6004665

7625946, 2091966, 8911313, 6839734, 530783, ...

Observe $\gcd(n, 8911313 - 7625946) = 127$

$\gcd(n, 6004665 - 530783) = 223$

and $n/(127 \cdot 223) = 331$. Furthermore all three factors are prime.

70) Then $X_m - X_n \equiv (m-n) \pmod n$, this is not random and thus does not have expected runtime \sqrt{p} .