2. Miller Rabin primality test

1. For each integer $n = 561,\ 41041,\ 67867,\ 7777853,\ 8768767$, choose an $a \in \mathbf{Z}_n^*$ and compute $a^{n-1} \bmod n$. What can you deduce about the primality of n from the results of the computations?

2. Verify that $n = 8911$ is 3-pseudoprime, but **not** 2-pseudoprime and **not** 5-pseudoprime.

3. (*Carmichael numbers*) Let n be a composite integer with the following properties

$$\begin{cases} \text{it is squarefree,} \\ \text{if } p \text{ divides } n, \text{ then } p-1 \text{ divides } n-1. \end{cases}$$

   Verify that n passes the Little Fermat Theorem test, for all integers a with $\gcd(a, n) = 1$.

4. Verify that the following Carmichael numbers

   321197185, 9746347772161, 8767496993623482137601, 32809426840359564991177172754241

   do not pass the Miller-Rabin test.

5. (a) Show that the number of classes $a \in \mathbf{Z}_9^*$ for which 9 is a-pseudoprime is $> \varphi(9)/4$.
   (b) Do the same for all the composite numbers between 10 and 20. Verify that in all cases the number of such classes is $\leq \varphi(n)/4$.

6. Discrete logarithm problem

1. *Primitive root criterium.* Let $\bar{x} \in \mathbf{Z}_p^*$, with p prime. Then $\bar{x}$ is a primitive root in $\mathbf{Z}_p^*$ if and only if $\bar{x}^{\frac{p-1}{d}} \not\equiv \bar{1} \mod p$, for all prime divisors d of $p-1$.

2. Let p be a prime and let $\bar{a}$ and $\bar{b}$ be primitive roots in $\mathbf{Z}_p^*$. Prove that $\log_{\bar{a}} \bar{b}$ is invertible modulo $p-1$.

3. Let $p = 47$. Determine a primitive root $\bar{a} \in Z_{47}^*$. Compute $\log_{\bar{a}} 11$.

4. Let $p = 439$.
   (a) Verify that $\bar{a} = \overline{17}$ is the smallest primitive root in $\mathbf{Z}_p^*$.
   (b) Compute $\log_{\bar{a}} \overline{100}$.

5. Let $p = 227$.
   (a) Verify that $\bar{a} = \bar{2}$ is a primitive root in $\mathbf{Z}_p^*$.
   (b) Compute $\log_{\bar{a}} \bar{3}$, $\log_{\bar{a}} \bar{5}$, $\log_{\bar{a}} \bar{7}$, using the relations modulo p

$$2^{20} \equiv 3^2 \cdot 7, \qquad 2^{57} \equiv 3 \cdot 5, \qquad 2^{128} \equiv 3 \cdot 7^2.$$

   (c) Compute $\log_{\bar{a}} \overline{100}$.

6. Let $p = 1061$.
   (a) Determine a primitive root $\bar{a}$ in $\mathbf{Z}_p^*$;
   (b) Compute $\log_{\bar{a}} \overline{101}$.