Name: Moldovan Vasilica
Group: 935

Assignment A
Primality check using the Miller-Rabin test

① Test for $n = 2393$ and $k=3$ (at most 3 repetitions)

Step 0. Write $n-1 = 2^s t$, where t is odd.

$n-1 = 2392 = 8\cdot 299 = 2^3 \cdot 299 \Rightarrow \begin{cases} s=3 \\ t=299 \end{cases}$

$i=1$.

Step 1. Choose a such that $1<a<n$.
Choose $a=2$.

Step 2. Compute (by the repeated squaring modular exponentiation) the following sequence (modulo n):

$a^t, a^{2t}, \dots, a^{2^s t} \Leftrightarrow 2^{299}, 2^{2\cdot 299}, 2^{2^2\cdot 299}, 2^{2^3\cdot 299}$

$2^{299} = 2392 = -1 \pmod{2393}$ (repeated squaring modular exponentiation)

$2^{2\cdot 299} = (2^{299})^2 = (-1)^2 = 1 \pmod{2393}$

$2^{2^2\cdot 299} = (2^{2\cdot 299})^2 = 1^2 = 1 \pmod{2393}$

$2^{2^3\cdot 299} = (2^{2^2\cdot 299})^2 = 1^2 = 1 \pmod{2393}$

Step 3
The obtained sequence is $[-1,1,1,1]$ and since we obtain the value 1 and its previous value is -1, we repeat the steps 1-3 (because $i=1<3=k$, we still have to do at most two repetitions). (1)

$i=2$

Step 1
Choose $a=13$.

Step 2 Compute the following sequence (modulo n):

$a^t, a^{2t}, \dots, a^{2^s t} \Leftrightarrow 13^{299}, 13^{2\cdot 299}, 13^{2^2\cdot 299}, 13^{2^3\cdot 299}$

$13^{299} = 1422 \pmod{2393}$

$13^{2\cdot 299} = (13^{299})^2 = (1422)^2 = 2392 = -1 \pmod{2393}$

$13^{2^2\cdot 299} = (13^{2\cdot 299})^2 = (-1)^2 = 1 \pmod{2393}$

$13^{2^3\cdot 299} = (13^{2^2\cdot 299})^2 = 1^2 = 1 \pmod{2393}$

Step 3.
The obtained sequence is $[1422,-1,1,1]$ and since we obtain the valu 1 and its previous value is -1, we repeat the steps 1-3 (because $i=1<3=k$). (2

$i=2$

Step 1

Choose $a=157$.

Step 2 Compute the following sequence (modulo n):

$a^t, a^{2t}, \dots, a^{2^s t} \Leftrightarrow 157^{299}, 157^{2\cdot 299}, 157^{2^2\cdot 299}, 157^{2^3\cdot 299}$

$157^{299} = 2392 = -1 \pmod{2393}$

$157^{2\cdot 299} = (157^{299})^2 = (-1)^2 = 1 \pmod{2393}$

$157^{2^2\cdot 299} = (157^{2\cdot 299})^2 = 1^2 = 1 \pmod{2393}$

$157^{2^3\cdot 299} = (157^{2^2\cdot 299})^2 = 1^2 = 1 \pmod{2393}$

Step 3

The obtained sequence is $[-1,1,1,1]$ and since we obtain the value 1 and its previous value is -1, and $i=3=k$, we can stop the algorithm, because n is probable prime. (3)

From (1) + (2) + (3), we can conclude that 2393 is ~~is~~ probable prime, with a probability of error of $\frac{1}{4^k} = \frac{1}{4^3} = \frac{1}{64} = 0{,}015625$.

② Test for $n=781$ and $k=3$.

Step 0. Write $n-1 = 2^s t$, where t is odd.

$n-1 = 780 = 4\cdot 195 = 2^2\cdot 195 \Rightarrow \begin{cases} s=2 \\ t=195 \end{cases}$

$i=1$

Step 1. Choose a such that $1<a<n$.

Choose $a=2$.

Step 2. Compute the following sequence (modulo n):

$a^t, a^{2t}, \dots, a^{2^s t} \Leftrightarrow 2^{195}, 2^{2\cdot 195}, 2^{2^2\cdot 195}$

$2^{195} = 758 \pmod{781}$ (repeated squaring modular exponentiation)

$2^{2\cdot 195} = (2^{195})^2 = (758)^2 = 529 \pmod{781}$

$2^{2^2\cdot 195} = (2^{2\cdot 195})^2 = (529)^2 = 243 \pmod{781}$

Step 3:

The obtained sequence is $[758, 529, 243]$ and since we haven't obtain any value of 1, we can stop the algorithm and conclude that n is composite.

Hence, $n=781$ is surely composite.