Worksheet on Primality Testing

March 16, 2019

1 Two Theorems

Theorem 1 (Fermat's Little Theorem)**.** .

Let n be prime. Then

(FLT) $\boxed{\begin{array}{l}\textit{If } a \not\equiv 0 \pmod{n},\\ \textit{then } a^{n-1} \equiv 1 \pmod{n}.\end{array}}$

Theorem 2 (Roots of 1 Property)**.** .

Let n be prime. Then

(ROO) $\boxed{\begin{array}{l}\textit{If } x^2 \equiv 1 \pmod{n},\\ \textit{then } x \equiv \pm 1 \pmod{n}.\end{array}}$

Proof. Suppose $x^2 \equiv 1 \pmod{n}$. Then

$$0 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod{n}.$$

In other words, $n \mid (x-1)(x+1)$. Since n is prime, if it divides a product, then it divides one or the other other factor. Hence,

$$n \mid x-1 \quad \text{or} \quad n \mid x+1.$$

In other words, $x \equiv \pm 1 \pmod{n}$. □

Carefully read the two theorems and the proof.

2 Collect some data

Fill in the tables. Tips: exploit symmetry to reduce the work.

n = 5

a	a^{n-1}
0	0
1	1
2	1
3	
4	

x	x^2
0	0
1	1
2	4
3	
4	

Is n prime? YES / NO

Does n satisfy (FLT)? YES / NO
If not, which a value(s) is/are the *witness(es)*?

Does n satisfy (ROO)? YES/ NO
If not, which x value(s) is/are the *witness(es)*?

n = 8

a	a^{n-1}
0	0
1	1
2	0
3	3
4	0
5	
6	
7	

x	x^2
0	0
1	1
2	4
3	1
4	
5	
6	
7	

Is n prime? YES / NO

Does n satisfy (FLT)? YES / NO
If not, which a value(s) is/are the *witness(es)*?

Does n satisfy (ROO)? YES/ NO
If not, which x value(s) is/are the *witness(es)*?

n = 9

a	a^{n-1}
0	0
1	1
2	4
3	0
4	
5	
6	
7	
8	

x	x^2
0	0
1	1
2	4
3	
4	
5	
6	
7	
8	

Is n prime? YES / NO

Does n satisfy (FLT)? YES / NO
If not, which a value(s) is/are the *witness(es)*?

Does n satisfy (ROO)? YES/ NO
If not, which x value(s) is/are the *witness(es)*?

3 Now your challenge.

Is n prime or composite? For each n below, try to decide with good certainty using as few computations as possible. You may use Single Cell Sage Server (`sagecell.sagemath.org`; works on a phone; app also exists) and type `Mod(a,n)` to find a modulo n. Keep track of all the computations you tried before you were convinced about your answer. Give a confidence estimate of your answer (e.g. "I'm 95% certain" meaning 95% of the time you will be right in a similar situation).

1. Is 1723 prime or composite?

2. Is 1727 prime or composite?

3. Is 1729 prime or composite?

4 Further challenges

1. Looking at the proof of ROO carefully for guidance on how to do so, construct an example of n and x with $x \not\equiv \pm 1 \pmod{n}$ but $x^2 \equiv 1 \pmod{n}$. (The point is not to find one by guessing, but to see how to construct as many examples as you may want by using the proof to inspire a general method.)

2. Prove that ROO holds for $n = 9$ even though $n = 9$ is composite. (Hint: consider the two factors modulo 3).

3. Find an infinite family of other n for which ROO holds, and give a proof.

4. Can you characterize exactly for which n ROO will hold?