

ACTIVITY 11. PRIMALITY TESTING

The idea behind primality testing is to find a way to test whether a given number n is a prime, without having to try to factor the number, which can be a long and tedious task.

Simply put, in order to determine whether a number is a prime, find out whether it “acts like” a prime.

Okay, so “how to primes act?” you wonder.

(a) Complete the following table:

n	2^n	2^n mod 3	2^n mod 5	2^n mod 7	2^n mod 11	2^n mod 13
1	2	2	2	2	2	2
2	4	1	4	4	4	4
3	8	2	3	1	8	
4	16	1			5	
5	32				x	
6	64				y	
7	128					
8	256					
9	512					
10	1024					
11	2048					
12	4096					

Some of the entries are filled in for you.

An easy way to fill in the table is to work your way down each column, doubling each entry in the previous row, and reducing by the corresponding clock number.

For column $2^n \bmod 11$ the entry x in the table is $2 \times 5 = 10$.

Note that $2^5 = 32 = 10 \bmod 11$.

The entry y just below x is $2 \times 10 = 20 = 9 \bmod 11$.

Note that $2^6 = 64 = 9 \bmod 11$.

(b) Circle the entries: $2^2 \bmod 3$, $2^4 \bmod 5$, $2^6 \bmod 7$, $2^{10} \bmod 11$, $2^{12} \bmod 13$.

If you didn’t make any mistakes in filling out the table, these five entries should all be 1.

This is not a coincidence.

Fermat’s Little Theorem. If n is an odd prime, then

$$\boxed{2^{n-1} = 1 \bmod n}.$$

This gives us a way to test n for primality, since if n is prime, then it must satisfy Fermat's Little Theorem.

The Fermat Primality Test base 2:

To test whether a particular number n is prime, compute

$$2^{n-1} \bmod n$$

If the answer is 1, then n is a *likely candidate* for being prime. If the answer is not 1, then you *can be sure* that n is composite. Why?

(c) Compute 2^{n-1} for $n = 15$ and $n = 21$.

(d) The big question: do any composite numbers ever pass the the Fermat test?

The answer is: rarely, but it happens.

Compute $2^{10} \bmod 341$. What does this tell you about $2^{340} \bmod 341$? Is 341 prime or composite? (Hint: try dividing it by 11.)

Composite numbers, like 341, which satisfy the Fermat test are called pseudo-primes base 2.

In the field of medicine, a **false positive** happens when a person being screened for a disease tests positive, but further tests show that the person does not have the disease. Good news for that person. A **false negative** occurs when a person who actually has the disease tests negatively.

In using Fermat's Little Theorem to test for primality (not that being a prime is a disease), a composite number, like 341, which passes the test constitutes a false positive. There are no false negatives (unless there is an error in computation) because **all** primes **must** satisfy Fermat's Little Theorem.