Weds
2/19

Week 5

Today we want to talk about how to test if $M_n = 2^n - 1$ is prime or not.

Brute-force method

Ex 49: Is 7 prime?

$2 \nmid 7$

$3 \nmid 7$

$4 \nmid 7$

$5 \nmid 7$

$6 \nmid 7$

There is no $1 < m < 7$ with $m \mid 7$

So, 7 is prime

So to test if x is prime you look for divisors m of x with $1<m<x$
If there are no such m then x is prime.

The first shortcut is we only need to look for divisors m of x in the range $1<m\leq\sqrt{x}$

This is because divisors come in "pairs."

Ex 50:

$x=385$, $\sqrt{x}=\sqrt{385}\approx 19.62$

divisors of 385

$\sqrt{385}\approx 19.62$

1, 5, 7, 11 | 35, 55, 77, 385

$11\cdot 35=385$

$7\cdot 55=385$

$5\cdot 77=385$

$1\cdot 385=385$

So, its sufficient to look on either the left or right side of the dotted line corresponding to $\sqrt{385}$ to find a divisor of 385.

Ex 51: $X = 25$

divisors of 25

1, 5, 25

$\sqrt{25}$

This example shows why we must test in the range $1 < m \leq \sqrt{x}$

Prop 52:

Let x be an integer with $x \geq 2$.

If x is composite (not prime), then there exists a divisor m of x with $1 < m \leq \sqrt{x}$.

Proof: Let $x \geq 2$ be a composite integer (not prime).

Then there exist $a, b \in \mathbb{Z}$ where $x = ab$ and $1 < a < x$ and $1 < b < x$.

What would happen if both $\sqrt{x} < a$ and $\sqrt{x} < b$?

If this happened then $x = ab > \sqrt{x}\sqrt{x} = x$.

Then $x > x$ which is impossible.

So either $1 < a \leq \sqrt{x}$ or $1 < b \leq \sqrt{x}$.

$\blacksquare$

Ex 53:

Is $M_7 = 2^7 - 1 = 127$ prime?

$x = 127$, $\sqrt{x} = \sqrt{127} \approx 11.2694\ldots$

test divisors $1 < m \leq 11$

$2 \nmid 127$	$7 \nmid 127$
$3 \nmid 127$	$8 \nmid 127$
$4 \nmid 127$	$9 \nmid 127$
$5 \nmid 127$	$10 \nmid 127$
$6 \nmid 127$	$11 \nmid 127$

In fact, since 127 is odd you don't have to test any even m.

$M_7 = 2^7 - 1$ is prime since it has no divisors m in the range $1 < m \leq \sqrt{2^7 - 1}$

This method is okay unless x is really big.

For example, the biggest known Mersenne prime (2018) is

$$2^{82,589,933} - 1$$

which has

24,862,048

digits.

One other shortcut

Prop 54: If $x \geq 2$ is a composite integer, then there exists a prime p that divides x with $1 < p \leq \sqrt{x}$.

pf: Let $x \geq 2$ be a composite integer. By Prop 52, there exists $m \in \mathbb{Z}$ with $m|x$ and $1 < m \leq \sqrt{x}$.

Since $1 < m$, by the FTOA (Thm 18) there exists

→ a prime p that divides m.

Since $p|m$ and $m|x$ we know that $p|x$.

Since $p|m$, we know $1 < p \leq m \leq \sqrt{x}$. ▨

Side-example

$x = 24, \sqrt{x} \approx 4.899$

$m = 4$

$p = 2$

Ex 55:

$M_7 = 2^7 - 1 = 127$

$\sqrt{127} \approx 11.2694\ldots$

only need to check primes $1 < p \leq 11$

$2 \nmid 127$	$5 \nmid 127$	$11 \nmid 127$
$3 \nmid 127$	$7 \nmid 127$	

So, $M_7 = 2^7 - 1$ is prime.

Fermat discovered two more theorems.

Thm 56° If p is an odd prime, then any prime divisor of $M_p = 2^p - 1$ must be of the form

$2kp+1$ where $k \in \mathbb{Z}$.

Thm 57° If p is an odd prime, then any prime divisor q of $M_p = 2^p - 1$ must satisfy $q \equiv \pm 1 \pmod 8$,

This means:

$q \equiv 1 \pmod 8$

OR

$q \equiv 7 \pmod 8$

Ex 58: Is $M_{13} = 2^{13} - 1$ prime?

$M_{13} = 2^{13} - 1 = 8191$

$p = 13$

$\sqrt{8191} \approx 90.5041\ldots$

We only need to test primes q that satisfy:

(i) $1 < q \leq 90$ ~~Thm 52~~ Prop 54

(ii) $q = 2kp + 1 = 26k + 1$ ($p = 13$) Thm 56

(iii) $q \equiv 1 \pmod 8$ or $q \equiv 7 \pmod 8$ Thm 57

Use (i) and (ii) to generate a list.

k	$q = 26k+1$	
1	$q = 27$ ←	not prime $27 = (3)(9)$
2	$q = 53$	
3	$q = 79$	
4	$q = 105 > 90$	

→ Only $q = 53$ and $q = 79$ are primes satisfying (i) and (ii).

Now use (iii)

$$\begin{array}{r} 6 \\ 8\overline{)53} \\ -48 \\ \hline (5) \end{array}$$

$$\begin{aligned} 53 &= 8 \cdot 6 + 5 \\ &\equiv 0 + 5 \pmod 8 \\ &\equiv 5 \pmod 8 \end{aligned}$$

$$\boxed{53 \not\equiv \pm 1 \pmod 8}$$

$$\begin{array}{r} 9 \\ 8\overline{)79} \\ -72 \\ \hline (7) \end{array}$$

$79 = (8)(9) + 7$

$\boxed{\begin{array}{l} 79 \equiv 7 \pmod 8 \\ 79 \equiv -1 \pmod 8 \end{array}}$

Result: The only prime q that satisfies (i), (ii), and (iii) is $q = 79$.

Does 79 divide $M_{13} = 2^{13} - 1 = 8191$?

$$\begin{array}{r} 103 \\ 79\overline{)8191} \\ -79 \\ \hline 291 \\ -237 \\ \hline (54) \end{array}$$

← remainder

So, $79 \nmid M_{13}$.

$\boxed{M_{13} \text{ is prime.}}$ There are no prime divisors of M_{13} satisfying (i), (ii), (iii).