2/24
Monday
Week 6

Last time we talked about ways to check if $M_p = 2^p - 1$ is prime or not.

The methods we discussed aren't good when P gets really big.

In the 1880's Lucas found another method.

Calculations

$S_1 = S_0^2 - 2 = 4^2 - 2 = 14$

$S_2 = S_1^2 - 2 = 14^2 - 2 = 194$

Luc

S_0

S_n

Lucas considered the following sequence:

$$S_0 = 4$$
$$S_n = S_{n-1}^2 - 2, \quad n \geq 1$$

Def 59

4, 14, 194, 37,634, 1,416,317,954, 2,005,956,546,822,746,144, ...

S_0 S_1 S_2 S_3 S_4 S_5

Thm 60 (Lucas-Lehmer)

Let p be an odd prime.

$M_p = 2^p - 1$ is prime

iff $\underbrace{s_{p-2} \equiv 0 \pmod{M_p}}$

That is: M_p divides s_{p-2}

Ex 61

$p = 3$

Is $M_3 = 2^3 - 1 = 7$ prime ??

Q: Is

$s_{3-2} \equiv 0 \pmod{M_3}$??

$s_1 = 14 \equiv 0 \pmod{7}$

So, $M_3 = 7$ is prime.

Ex 62

p=5

Is $M_5 = 2^5 - 1 = 31$ prime ?

Is $S_{5-2} = S_3 \equiv 0 \pmod{\underbrace{31}_{M_5}}$?

Method 1

$S_0 = 4$

$S_1 = 4^2 - 2 = 14$

$S_2 = 14^2 - 2 = 194$

$S_3 = 194^2 - 2 = 37,634$

$S_3 \equiv 0 \pmod{M_5}$

So, $M_5 = 31$ is prime

M_5

S_3

M_5 divides S_3

remainder

```
   1214
31 | 37634
   -31
   ----
    66
   -62
   ----
     43
    -31
    ---
     124
    -124
    ----
       0
```

Method 2

Is $M_5 = 2^5 - 1 = 31$ prime ?

Test if $S_3 \equiv 0 \pmod{M_5}$.

* Mod as you go *

31

$S_0 \equiv 4 \pmod{31}$

$S_1 \equiv (4^2 - 2) \pmod{31} \equiv 14 \pmod{31}$

$S_2 \equiv (S_1^2 - 2) \pmod{31}$

$\equiv (14^2 - 2) \pmod{31}$

$\equiv 194 \pmod{31}$

$\equiv 8 \pmod{31}$

$$\begin{array}{r} 6 \\ 31\overline{)194} \\ -186 \\ \hline 8 \end{array}$$

remainder

$194 = (31)(6) + 8$

$S_3 \equiv (S_2^2 - 2) \pmod{31}$

$\equiv (8^2 - 2) \pmod{31}$

$\equiv 62 \pmod{31} \equiv 0 \pmod{31}$

$$\begin{array}{r} 2 \\ 31\overline{)62} \\ -62 \\ \hline 0 \end{array}$$

So,

$S_3 \equiv 0 \pmod{31}$

$\equiv 0 \pmod{M_5}$

So, $M_5 = 2^5 - 1$ is prime.

Ex 63:

p = 11

Is $M_{11} = 2^{11} - 1 = 2047$ prime?

$S_0 \equiv 4 \pmod{2047}$

$S_1 \equiv (4^2 - 2) \pmod{2047} \equiv 14 \pmod{2047}$

$S_2 \equiv 194 \pmod{2047}$

$S_3 \equiv (194^2 - 2) \pmod{2047}$

$\equiv 37{,}634 \pmod{2047}$

$\equiv \boxed{788 \pmod{2047}}$

$$\begin{array}{r} 18 \\ 2047 \overline{)\,37634} \\ -2047 \\ \hline 17164 \\ -16376 \\ \hline 788 \end{array}$$

$S_4 \equiv (788^2 - 2) \pmod{2047}$

$\equiv 620{,}942 \pmod{2047}$

$\equiv \boxed{701 \pmod{2047}}$

$$\begin{array}{r} 303 \\ 2047 \overline{)\,620{,}942} \\ -6141 \\ \hline 6842 \\ -6141 \\ \hline 701 \end{array}$$

$S_5 \equiv (701^2 - 2) \pmod{2047}$

$\equiv 491{,}399 \pmod{2047}$

$\equiv \boxed{119 \pmod{2047}}$

$S_6 \equiv (119^2 - 2) \pmod{2047}$

$\equiv 14{,}159 \pmod{2047}$

$\equiv \boxed{1877 \pmod{2047}}$

$$S_7 \equiv (1877^2 - 2) \pmod{2047}$$
$$\equiv 3,523,127 \pmod{2047}$$
$$\equiv \boxed{240 \pmod{2047}}$$

$$\frac{3,523,127}{2047} \approx 1721.117\ldots$$

remainder $= 3,523,127 - (2047)(1721)$
$= 3,523,127 - 3,522,887$
$= 240$

$$S_8 \equiv (240^2 - 2) \pmod{2047}$$
$$\equiv 57,598 \pmod{2047}$$
$$\equiv \boxed{282 \pmod{2047}}$$

$$S_9 \equiv (282^2 - 2) \pmod{2047}$$
$$\equiv 79,522 \pmod{2047}$$
$$\equiv \boxed{1736 \pmod{2047} \neq 0 \pmod{2047}}$$

Since $S_9 \not\equiv 0 \pmod{M_{11}}$

We have that

$M_{11} = 2047$

is not prime

(2047)

GIMPS

Using Mathematica

$M_{109} = 2^{109} - 1$ not prime

$2^{109} - 1 = 649,037,107,316,853,$
$453,566,312,041,$
$152,511$