Fermat primes and Pepin's test.

\[ F_n = 2^{2^n} + 1 \]

when is this prime?

it is for \( n=1, 2, 3, 4 \) (see video)

Related to a basic problem in geometry.

Pepin's test: \( F_n \) is prime \( \iff \) \( 3 \frac{F_n - 1}{2} \equiv -1 \mod F_n \)

Exercise 1. (1), (2), (3)

(1) \( F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537 \)

\[ 3 \frac{F_n - 1}{2} = 3 \frac{2^{16} - 1}{2} = 3 \cdot 2^{15} = 3 \cdot 32768 = 3 \cdot 7 = ? \mod 65537 \]
\[ 3^{2^{14}} = \left(3^{2^{13}}\right)^2 \]

\[ (3^{2^{13}})^2 = \left(3^{2^{12}}\right)^2 \]

- Use successive squaring

\[ 3^{2^0} = 3^1 = 3 \quad \text{and} \quad 63577 \]
\[ 3^{2^1} = 3^2 = 9 \]
\[ 3^{2^2} = 9^2 = 81 \]
\[ 3^{2^3} = 81^2 = 6561 \]
\[ 3^{2^4} = 6561^2 = 4304641 \]
\[ 3^{2^5} = 4304641^2 = 184753834641 \]
\[ 3^{2^6} = 184753834641^2 = 3399639881780785041 \]
\[ 3^{2^7} = (19139)^2 = 36596041 \]

\[ \uparrow \text{to } 3^{2^{15}} \]
Let \( n \geq 2 \). Show that \( F_n = 2 \text{ mod } S \).

We want
\[
2^{2^n} + 1 \equiv 2 \text{ mod } S
\]

\[
\Rightarrow 2^{2^n} \equiv 1 \text{ mod } S.
\]

If you don't see why, just start computing for small \( n \) and see what happens.

\[
2^2 = 4 = \eta
\]

\[
2^{2^2} = 2^{(2^2)} = (2^2)^2 = \eta^2 \equiv 1 \text{ mod } S.
\]

\[
2^{2^3} = (2^{2^2})^2 = 1^2 \equiv 1 \text{ mod } S
\]
Observe: \[ 2^{2n} = 2^4 \cdot 2^{n-2} = (2^4)^{n-2} = 16^{n-2} = 1^{n-2} \mod 5 = 1 \mod 5, \]

(Uses \( n \geq 2 \) to factor out \( 2^2 \) from \( 2^n \) in the exponent.

Exercise 2:

\[ (p^2 - 1) = (p+1)(p-1). \]

\( \mathbb{F}_p[i] \) be sum \( a+bi \) where \( a, b \in \mathbb{F}_p \).

\( i^2 = -1. \)

Can also view as:

\[ \mathbb{F}_p[i] \cong \mathbb{F}_p[x]/(x^2 + 1) \]

or \( \mathbb{Z}[i] / \mathbb{F}_p \)

\( x \leftrightarrow i \)

\( x^2 + 1 = 0 \leftrightarrow x^2 = -1 \)
Not always a field, but it is a field when $p \equiv 3 \mod 4$.

(C. e. g. using $x^2 + 1$ is irreducible polynomial in $\mathbb{F}_p(x)$)

Has $p^2$ elements. (3 choices for $a$, $p$ choices for $b$).

$\mathbb{F}_p^x$ has a discrete logarithm that identifies this with $\mathbb{Z}/(p^2 - 1)\mathbb{Z}$

(i.e. there is a primitive $(p^2 - 1)$th root of unity)

(1) Find a prin root in $\mathbb{F}_3[\sqrt{i}]$, write down the discrete log.
Looking for $g \in F_3[i] x$ such that $g^8 = 1$, $g^d \neq 1$ for any $d \mid 8$, $d \neq 8$. 

\[ g^8 = 1 \]

true for any $g$ by Lagrange since $|F_3[i] x| = 8$.

e.g. $2^2 = 1$ so 2 doesn't work

\[ i^4 = (i^2)^2 = (-1)^2 = 1 \] so $i$ doesn't work

any of $g = \{ 1+i, 2+i, 1+2i, 2+2i \}$ will work!

\[
\begin{array}{ccccccc}
\hline
x & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\hline
(1+i)^x \in F_3[i] x & 1 & 1+i & 2 & 1+2i & 2+i & 1+2i & 2 & 1+i \\
\hline
\end{array}
\]
\[ x \in \mathbb{R}^3 \cap i\mathbb{R}^3 \]

\[ I(x) \]

\[ \begin{array}{cccccccc}
0 & 1 & 2 & i & 2i & 1+i & 1+2i & 2+i & 2+2i \\
\end{array} \]