Fermat primes and Pepin's test.

$$F_n = 2^{2^n} + 1 \quad \text{when is this prime?}$$

it is for $n = 1, 2, 3, 4$

(see video)

Related to a basic problem in geometry.

missing on worksheet

Pepin's Test: F_n $n \geq 1$ is prime $\iff 3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$.

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

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

$$3^{\frac{F_4 - 1}{2}} = 3^{2^{16}/2} = 3^{2^{15}} = 3^{32678} \equiv ? \mod 65537$$

$$3^{2^{15}} = \left(3^{2^{14}}\right)^2$$

$$\left(3^{2^{14}}\right) = \left(3^{2^{13}}\right)^2$$

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

$\therefore$ - use successive squaring

$$3^{2^0} \equiv 3^1 \equiv 3 \mod 65537$$

$$3^{2^1} \equiv 3^2 \equiv 9$$

$$3^{2^2} \equiv 9^2 \equiv 81$$

$$3^{2^3} \equiv 81^2 \equiv 6561$$

$$3^{2^4} \equiv 6561^2 \equiv 54449$$

$$3^{2^5} \equiv 54449^2 \equiv 61869$$

$$3^{2^6} \equiv 61869^2 \equiv 19139$$

$$3^{2^7} \equiv (19139)^2 \equiv 15028$$

$\vdots$

up to $3^{2^{15}}$

(2) Let $n \geq 2$, show that $F_n \equiv 2 \mod 5$.

Want $\underbrace{2^{2^n} + 1}$ $\equiv 2 \mod 5$

$\Updownarrow$

$2^{2^n} \equiv 1 \mod 5.$

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

$2^{2^1} = 2^2 = \underline{4}$

$2^{2^2} = 2^{(2\cdot 2)} = (2^2)^2 = \underline{4^2} \equiv \underline{1} \mod 5.$

$2^{2^3} = (2^4)^2 \equiv \underline{1^2} \equiv \underline{1} \mod 5$

Observe: $2^{2^n} = 2^{4 \cdot 2^{n-2}} = (2^4)^{n-2}$

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

$= 16^{n-2}$

$\equiv 1^{n-2} \mod 5$

$\equiv 1 \mod 5.$

$(p^2-1) = (p+1)(p-1).$

Exercise 2:

$\mathbb{F}_p[i]$ be sums $a+bi$ where $a, b \in \mathbb{F}_p$

$i^2 = -1.$

Can also view as: $\mathbb{F}_p[x]/(x^2+1)$ or $\mathbb{Z}[i]/p$

$x \leftrightarrow i$

$x^2+1=0 \leftrightarrow x^2=-1$

⚠ Not always a field.

But it is a field when $p \equiv 3 \mod 4$.

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

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

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

$|\mathbb{F}_{p^2}^\times| = p^2-1$

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

(1) Find a prim root in $\mathbb{F}_3[i]$, write down the discrete log.

Looking for $g \in \mathbb{F}_3[i]^\times$ such that

$g^8 = 1$, $g^d \neq 1$ for any $d \mid 8$, $d \neq 8$.
i.e. $d = 4, 2, 1$

true for any g by Lagrange since $|\mathbb{F}_3[i]^\times| = 8$.

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!).

$g = 1+i$

$k \in \mathbb{Z}/8\mathbb{Z}$	0	1	2	3	4	5	6	7
$(1+i)^k \in \mathbb{F}_3[i]^\times$	1	$1+i$	$2i$	$1+2i$	2	$2+2i$	i	$2+i$

$x \in \mathbb{F}_3[i]^\times$	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
$I(x)$	0	4	6	2	1	3	7	8