Ch. 10 Great Thm

thm A $a = 2k$, $p \nmid a$, $p \mid a+1$ $\Rightarrow p = 2k+1$

two is the only odd prime.
$p \nmid a \Rightarrow p \neq 2k$, so $p = 2k+1$
(all factors of odds are odd)

thm B $a = 2k$, $p \nmid a$, $p \mid a^2+1$ $\Rightarrow p = 4k+1$

proof: a even $\Rightarrow$ a^2 even
Apply thm A $\Rightarrow$ $p = 2k+1$

I. $p = 4k+1$ ⟶ yes!
II. $p = 4k+3$
F.L.T. $\Rightarrow$ $p \mid a^{p-1} - 1 \Rightarrow p \mid a^{4k+2} - 1$

$a^p \equiv a \pmod p$
$a^{p-1} \equiv 1 \pmod p$

Algebra: $a^{4k+2} + 1 = (a^2+1)(a^{4k} - a^{4k-2} + a^{4k-4} - \dots + a^4 - a^2 + 1)$

↑ since p divides this term, it divides the product. So

p divides both $a^{4k+2}+1$ & $a^{4k+2} - 1$, so it divides their difference

$$p \mid (a^{4k+2}+1) - (a^{4k+2} - 1) \Rightarrow p \mid 2$$ ⊗

Ex pick a even.

$a = 18$ $\quad a^2+1 = 18^2+1 = 325 = 5^2 \cdot 13$ $\quad 5 = 4k+1$, $13 = 4k+1$

thm C $\left.\begin{array}{l} a = 2k \\ p \nmid a \\ p \mid a^4+1 \end{array}\right\} \Rightarrow p = 8k+1$

proof: $a^4 = (a^2)^2+1$. Apply thm B $\Rightarrow p = 4k+1$

So $p = 8k$ ✗ | $p = 8k+1$ | $p = 8k+5$

$8k+2$, $8k+4$, $8k+6$

$p = 8k+3$
$= 4(2k)+3$ ✗

$p = 8k+7$
$4(2k)+4+3$
$4(2k+1)+3$ ✗

If $p = 8k+5$

FLT $p \mid a^{p-1} - 1 \Rightarrow p \mid a^{8k+4} - 1$

Algebra $a^{8k+4}+1 = \underbrace{(a^4+1)}_{p \text{ divides}}(a^{8k} - a^{8k-4} + a^{8k+4} - \dots + a^8 - a^4 + 1)$

So $p \mid a^{8k+4}+1$ & $p \mid a^{8k+4}-1 \Rightarrow p \mid 2 \Rightarrow$ ✗

$\Rightarrow p = 8k+1$

---

continuing ...

$p \mid a^{16}+1 \Rightarrow p = 32k+1$

$p \mid a^{32}+1 \Rightarrow p = 64k+1$

$p \mid a^{2^n}+1 \Rightarrow p = (2^{n+1})k+1$

thm: $2^{32}+1$ is not prime.

proof: suppose $p \mid 2^{32}+1$. the $p = 64k+1$

let k grow incrementally, check each case.

$k = 10 \quad 64 \cdot 10 + 1 = 641$ & $2^{32}+1 = 641 \times 6{,}700{,}417$ □

Fermat:

Recall: $a^2 + b^2 = c^2$

Last theorem: 1600's ... 2005 (Andrew Wiles)

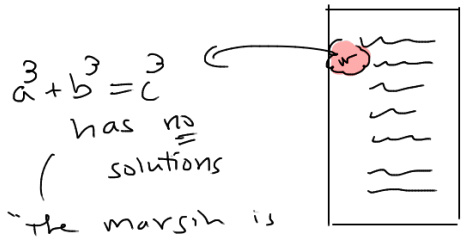
Little theorem:

$a^p \equiv a \pmod p$

$\Updownarrow$

$a^{p-1} \equiv 1 \pmod p$

remainder when ÷ by p.



a = # } 12
p = prime } 7

$12^{7-1} = 12^6 = 298594$

$298594 \div 7 \hookrightarrow$ remainder $= 1$

Euler's Proof of Fermat's Little Theorem

Thm: If p = prime & $a \in \mathbb{N}$ for which $p \nmid a$ $\Rightarrow$ $\boxed{p \mid a^{p-1} - 1}$

(recall $a \mid b \Rightarrow b = a \cdot n$)

Tools: ① Euclid's Lemma: If $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

② Binomial Coeff: $(a+b)^p = a^p + p a^{p-1} b + \frac{p(p-1)}{2!} a^{p-2} b + \frac{p(p-1)(p-2)}{3!} a^{p-3} b^3 + \dots + b^p$

& primes

point: b/c p = prime, there's no cancel culture

Thm ① p prime $a \in \mathbb{N}$ $\Rightarrow$ $(a+1)^p - (a^p + 1)$ is divisible by p.

proof: First + Last terms of ① are ↑, rest are binomial coeffs $\mid \frac{p(p-1)\dots}{n!}$

Thm ② Induction Step: If $\overbrace{a^p - a}^{\text{on ladder}}$ is divisible by p then

$\underbrace{(a+1)^p - (a+1)}_{\text{climb}}$ is also divisible by p.

use induction hyp:

Assume: $a^p - a$ is divisible by $p \Rightarrow a^p - a = p \cdot n$ For $n \in \mathbb{N}$

reinterpret goal given inductive hyp ... so $a = a^p - pn$,

$$(a+1)^p - (a+1) = (a+1)^p - (a^p - pn + 1)$$

$$= \underbrace{(a+1)^p - (a^p + 1)}_{} + pn$$

using Thm ①, entire RHS is divisible by p.

Thm ③: Induct on a: $p \mid a^{p-1} - 1$ } get a ladder: } $p = 3$, $a = 2$ } $3 \mid 2^{3-1} - 1 \equiv 3 \mid 2^2 - 1 \equiv 3 \mid 3 \Rightarrow$ true

Now we're on ladder

Thm 3 $\Rightarrow$ we can climb

$\Rightarrow$ By induction true $\forall$ a.

In gen'l: let p = given prime. choose $a = 1$

$$p \mid a^{p-1} - 1 \Rightarrow p \mid 1^{p-1} - 1 \Rightarrow p \mid 1 - 1 \Rightarrow p \mid 0 \ \&\ 0 = p \cdot m$$

$\Rightarrow$ 1 works for all p.

$\Rightarrow$ we're on ladder for all p. Now induct, Thm ②. $\Rightarrow$ Induction $p \mid a^{p-1} - 1$ $\forall a, p$

Great thm

Fermat:

- Last Thm
- Little thm
- Conjecture all #'s like this are prime

$$2^{2^p}+1$$

$p=1 \Rightarrow 2^{2^1}+1 = 5$

$p=2 \Rightarrow 2^{2^2}+1 = 17$

$p=3 \Rightarrow 2^{2^3}+1 = 257$

$p=4 \Rightarrow 2^{2^4}+1 = 65{,}537$ prime (Fermat knew)

$p=5 \Rightarrow 2^{2^5}+1 = 2^{32}+1 \approx 4.2$ billion