Thm: Si $a \wedge b = 1$ $\quad a, b \in \mathbb{Z}$

Alors $\forall c$, $a | bc \Rightarrow a | c$

pv: Soient $a, b, c \in \mathbb{Z}$ tq $a \wedge b = 1$ et $a | bc$

Or $a \wedge b = 1$, alors $\exists u, v \in \mathbb{Z}$
tq $ua + vb = 1$
$\Leftrightarrow c(ua + vb) = c$
$\Leftrightarrow uac + vbc = c$

On a : $a | uac$ trivialement
$a | vbc$ par hyp : $a | bc$
donc $a | (uac + vbc)$ ($= c$)

donc $a | c$

[Bézout]

Thm : Soient $a, b \in \mathbb{Z}$

(i) $a \wedge b = 1$

(ii) $\exists u, v \in \mathbb{Z} \quad au + bv = 1$

Gauss

Thm : Soient $a, b, c \in \mathbb{Z}$

$$a \wedge b = 1 \text{ et } a \mid bc \Rightarrow a \mid c$$

pv : $a \wedge b = 1$ et $a \mid bc$

$a \wedge b = 1 \Rightarrow \exists u, v \quad au + bv = 1$ (par Bézout)

$acu + bcv = c$

$a \mid acu$ trivialement acu multiple de a

$a \mid bcv$ car $a \mid bc$ par hyp $a \mid c$

Prop : $a \wedge c = 1$ et $b \wedge c = 1 \Rightarrow ab \wedge c = 1$

pv : $\exists u, v \quad au + cv = 1$

$\exists l, n \quad bl + cn = 1$

$(au + cv)(bl + cn) = 1 \cdot 1$

$\Leftrightarrow (ab)(ul) + c(vbl + aun + cvn) = 1$ On pose $ul = m_1$ ... $= m_2$

$(ab)m_1 + cm_2 = 1$

Donc $ab \wedge c = 1$ par Bézout.

Exc : Soit $n \in \mathbb{Z}$ tq $3 \mid 5n$

$3 \cdot 5 = 15$

$6 \cdot 5 = 30$

$2 \cdot 3 \wedge 7 = 1$ $\quad$ $5 \cdot 11 \wedge 57$

Fermat
Thm: Si $p \in \mathbb{P}$, $\forall a \in \mathbb{Z}$ $p \nmid a$

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

F bis
Thm: Si $p \in \mathbb{P}$, $\forall a \in \mathbb{Z}$

$$a^p \equiv a \mod p$$

Prop: Thm F $\Leftrightarrow$ Thm F-bis

PV:

$\Rightarrow$: hyp: $p \in \mathbb{P}$, $a \in \mathbb{Z}$ tq $p \nmid a$

$a^{p-1} \equiv 1 \mod p$
$a^p \equiv a \mod p$ → Fermat bis □

Supp $p \mid a$ alors $a \equiv 0 \mod p$
$a^p \equiv 0^p \equiv 0 \mod p$ F-bis vrai □

$\Leftarrow$: hyp: $p \in \mathbb{P}$ $a \in \mathbb{Z}$ tq $p \nmid a$

$a^p \equiv a \mod p$
$\Leftrightarrow a^p - a \equiv 0 \mod p$
$\Leftrightarrow a(a^{p-1} - 1) \equiv 0 \mod p$ or $p \nmid a \Leftrightarrow a \not\equiv 0 \mod p$
$\Leftrightarrow (a^{p-1} - 1) \equiv 0 \mod p$
$\Leftrightarrow a^{p-1} \equiv 1 \mod p$ F □

F-bis:

Lm: $(a+1)^p \equiv a^p + 1$

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} 1^1 + \binom{p}{2} a^{p-2} 1^2 \dots 1^p$$

$\forall k \leq p-1$ $\binom{p}{k} \equiv 0 \mod p$

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} = \frac{(p-1)!\,p}{k!\,(p-k)!}$$

$k \geq 1$
$k \leq p-1$ $\qquad$ $p-k \leq p-1$ $\qquad$ de plus p est premier

donc $\nexists$ dans $\{1 \dots k\}$ $\qquad$ $i \mid p$
ou $\{1 \dots (p-k)\}$

Donc $\binom{p}{k}$ est divisible par p donc $\binom{p}{k} \equiv 0 \bmod p$

ce qui donne $(a+1)^p = a^p + \binom{p}{1} a^{p-1} 1^1 + \dots + 1^p$
$\equiv a^p + 0 + 0 + \dots + 0 + 1 \bmod p$
$\equiv a^p + 1 \bmod p$

$a^p \equiv a \bmod p$

Rec: $0^p \equiv 0 \bmod p$
$1^p \equiv 1 \bmod p$

Hyp: $P(a)$: $a^p \equiv a \bmod p$
$P(a+1)$: $(a+1)^p \equiv a+1 \bmod p$

$(a+1)^p \equiv a^p + 1 \bmod p$
$a^p \equiv a \bmod p$ par hyp de rec

$(a+1)^p \equiv a^p + 1 \bmod p$ par Ln
$\equiv a+1 \bmod p$ par hyp de rec

↳ cqfd

Donc $F \Rightarrow b$ □

RV de F: par la prop d'équivalence de F et F-b's

Exc: $5^3 - 5 = 120$ est divisible par 3

$2^5 - 2 = 30$ est divisible par 5

Utilité : chercher l'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$

Thm : Soient $a, b \in \mathbb{Z}$

$\Leftrightarrow$ (i) $a \wedge b = 1$

$\Leftrightarrow$ (ii) $\exists u, v \in \mathbb{Z}$ $ua + vb = 1$

Thm : Soient $a, b, c \in \mathbb{Z}$

$a \wedge b = 1$ et $a \mid bc \Rightarrow a \mid c$

PV !

$a \wedge b = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ $(au + bv = 1)^c$

$acu + bcv = c$

$a \mid acu$

$a \mid bcv$ $\quad a \mid bc$ par hyp

$a \mid (acu + bcv)$

$\| c$

$a \mid c$ □

Prop : $a \wedge c = 1$ et $b \wedge c = 1 \Rightarrow ab \wedge c = 1$ $\quad a, b, c \in \mathbb{Z}$

PV : $a \wedge c = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ $|au + cv| = 1$

$b \wedge c = 1 \Rightarrow \exists k, l \in \mathbb{Z}$ $|bk + cl| = 1$

$(au + cv)(bk + cl) = 1 \cdot 1 = 1$

$(ab)(uk) + c(vbk + aul + cvl) = 1$

$:= m_1$ $\quad := m_2$

$(ab) m_1 + c \cdot m_2 = 1 \Rightarrow ab \wedge c = 1$

$2 \cdot 3 = 6 \wedge 7$

1) Soit $p \in \mathcal{P}$, $\forall a \in \mathbb{Z}$ tq $p \nmid a$

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

2) Soit $p \in \mathcal{P}$ $\forall a \in \mathbb{Z}$

$$a^p \equiv a \mod p$$

3) Propi: Thm F $\subset$ Thm FB

Pv:

$\Rightarrow$ $p \in \mathcal{P}$ $a \in \mathbb{Z}$, $p \nmid a$ $a^{p-1} \equiv 1 \mod p$

$$a^{p-1} \cdot a \equiv 1 \cdot a \mod p$$
$$\subset\!\!\Rightarrow a^p \equiv a \mod p$$

$\Leftarrow$ $p \in \mathcal{P}$ $a \in \mathbb{Z}$ $p \nmid a$ $a^p \equiv a \mod p$

$\subset\!\!\Rightarrow a^p - a \equiv 0 \mod p$

$\subset\!\!\Rightarrow a(a^{p-1} - 1) \equiv 0 \mod p$ Or $p \nmid a$, donc $a \not\equiv 0 \mod p$

$$a^{p-1} - 1 \equiv 0 \mod p$$
$$\subset\!\!\Rightarrow a^{p-1} \equiv 1 \mod p$$

□

Lm: $\forall 1 \leq k \leq p-1$ $\binom{p}{k} \equiv 0 \mod p$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{(p-1)! \cdot p}{k!(p-k)!}$$

$\forall i \in \{1, \dots, k\}$ $i \nmid p$ $1 \leq i \leq p-1$

$\forall j \in \{1, \dots, p-k\}$ $j \nmid p$ $1 \leq p-k \leq p-1$

$$\binom{p}{k} \equiv 0 \mod p$$

Thm F-B:

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{p-2}a^1 + a^0 \cdot 1^p$$
$$+1$$

$$= a^p + 0 + 0 + 0 + \dots + 1 \quad \text{mod } p$$

$$\Rightarrow (a+1)^p \equiv a^p + 1 \text{ mod } p$$

Par rec :

$P(a)$: $a^p \equiv a \text{ mod } p$

$0^p \equiv 0 \text{ mod } p$
$1^p \equiv 1 \text{ mod } p$

$P(a+1)$: $(a+1)^p \equiv a^p + 1 \text{ mod } p$
$\equiv a \text{ mod } p$

$(a+1)^p \equiv a + 1 \text{ mod}$

cqfd □

$a^p \equiv a \text{ mod } p$

$5^3 \equiv 5 \text{ mod } 3$

$5^3 - 5 \equiv 0 \text{ mod } 3$

$125 - 5 = 120$

$2^5 - 2 = 30$ est div. 5

$\mathbb{Z}/7\mathbb{Z}$ $\quad p = 7 \quad a = 3$

$3^7 \equiv 3 \text{ mod } p$
$\Leftrightarrow 3^6 \equiv 1 \text{ mod } p$
$3^5 \cdot 3 \equiv 1 \text{ mod } p \Leftrightarrow$ 3^5 - l'inverse de 3 dans $\mathbb{Z}/7\mathbb{Z}$

$3^5 = 3^2 \cdot 3^2 \cdot 3$ $\quad 9 \equiv 2 \text{ mod } 7$

$\equiv 2 \cdot 2 \cdot 3 \text{ mod } 7$
$\equiv 12 \text{ mod } 7$
$\equiv 5 \text{ mod } 7$

$3 \cdot 5 \cdot 15 \equiv 1 \text{ mod } 7$
$\Leftrightarrow$ l'inverse de 3 mod 7