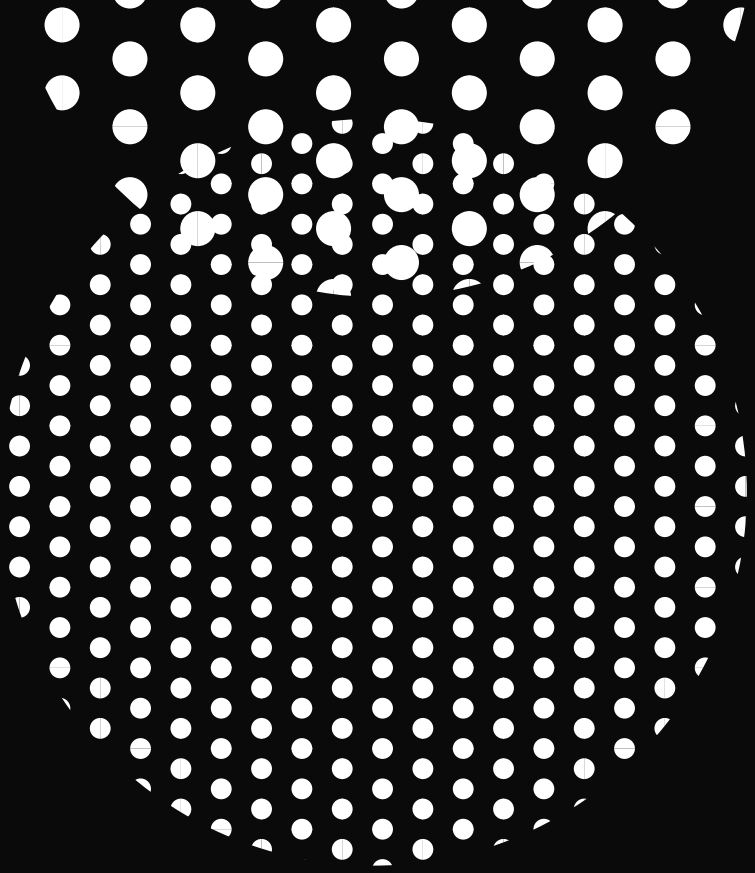

Thm: Tout $n \geq 2$ se décompose $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

pv: Sinon.

$\bar{E} = \{ n$ qui ne se décomposent pas en produit de premiers $\}$

Par l'abs. $\bar{E} \neq \emptyset$ Soit $\bar{n} \in \bar{E}$ minimal

Obs: $\bar{n}$ n'est pas premier ($\bar{n} = p$)

Donc $\bar{n} = dm$ $\bar{n}$ a un diviseur d

avec $1 < d < \bar{n}$ pas premier

$\Downarrow$ $1 < m < \bar{n}$

Comme $d, m < \bar{n}$, $d, m \notin \bar{E}$

donc $d = p_i^{\alpha_i} \dots p_j^{\alpha_j}$

$m = p_i^{\alpha_i} \dots p_j^{\alpha_j}$

$\Downarrow$

$\bar{n} = dm$ = produit de nombres premiers CONTRAD

$p_1 < p_2 < \dots < p_n$ nombres premiers

Thm 2: $p_1^{\alpha_1} \dots p_{r_2}^{\alpha_{r_2}} = n = q_1^{\beta_1} \dots q_s^{\beta_s}$ $\Rightarrow$ $s = r_2$

$p_1 = q_1$

$p_2 = q_2$

$\alpha_i = \beta_i$ $\forall\, 1 \leq i \leq r_2$

EXTRAIRE

pv: $p_1^{\alpha_1} p_2^{\alpha_2} \cdot p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2} = q_1^{\beta_1} \dots q_s^{\beta_s}$

donc $p_i \mid \underbrace{q_1 \cdot q_1}_{\beta_1} \dots \underbrace{q_s \cdot q_s}_{\beta_s}$

Thm Euclide

$p_i =$ l'un des $q_1, \dots, q_s$

càd $\forall\, 1 \leq i \leq r_2$ $p_i \in \{q_1, \dots, q_s\}$ EXO $\Rightarrow$ $\{p_1, \dots, p_{r_2}\} = \{q_1, \dots, q_s\}$

de manière symétrique $\{p_1, \dots, p_{r_2}\}$ card $\Rightarrow$ $r_2 = s$

Comme $p_1 < \dots < p_{r_2}$

Comme $q_1 < \dots < q_s = r_2$

$\Rightarrow p_i = q_i$ $\forall\, 1 \leq i \leq r_2$

Suite $p_1^{\alpha_1} \cdots p_i^{\alpha_i} \cdots p_n^{\alpha_n} = p_1^{\beta_1} \cdots p_i^{\beta_i} \cdots p_2^{\beta_2}$ $\quad \forall p_i = q_i$

$p_i \mid \beta_i$ $\qquad$ $p_i \mid \beta_i$

S: $\alpha_i \neq \beta_i$ $\qquad$ (1) $\alpha_i > \beta_i$
(2) $\alpha_i < \beta_i$

Cas 1: $p_1^{\alpha_1} \cdots p_i^{\alpha_i - \beta_i} \cdots p_2^{\alpha_2} = p_1^{\beta_1} \cdots 1 \cdots p_2^{\beta_2}$
≥ 1

cela dit $p_i \mid p_1^{\beta_1} \cdots 1 \cdots p_2^{\beta_2}$ Contredit Euclide

$\alpha_i \geq \beta_i$
symétrique
$\alpha_i \leq \beta_i$
Donc $\alpha_i = \beta_i$
□

Thm: Card $\{p \geq 2$ premiers$\}$ = Card $\mathcal{P} = +\infty$

pv: Sinon, il existe seulement un nombre fini k de nombres premiers

Poser $N := 1 + p_1 \cdot p_k \cdot p_k \Rightarrow \forall\, 1 \leq k \leq k$ $N \equiv 1 \mod p_k$
Mais $N = p_{i_1}^{\alpha_{i_1}} \cdots p_{i_2}^{\alpha_{i_2}}$ avec $1 \leq i_1 < \cdots < i_2 \leq k$
$\alpha_{i_1}, \ldots, \alpha_{i_2} \geq 1$
Contradit

$\Rightarrow N \equiv 0 \mod p_{i_1}$ et aussi $N \equiv 0 \mod p_i^{\alpha_i}$

Exp: Soit $p \in \mathcal{P}$ Soit $\alpha \geq 1$ exposant. Les seuls diviseurs de p^α sont $1, p, p^2, \ldots, p^{\alpha-1}, p^\alpha$ (α fois)

pv: $q \in \mathcal{P}$ divise p^α càd $q \mid \underbrace{p \cdots p}_{\alpha \text{ fois}}$ Euclide $q =$ l'un des p
$q = p$
...
□

$397 \in \mathcal{P}$ Q : $5^{400} \equiv ?$ mod 397

Thm : $5^{397} \equiv 5$ mod 397

$5^{400} = 5^{397} \cdot 5^3 = 5 \cdot 5^3 = 25 \cdot 25 = 625$ mod 397 $\equiv 328$ mod 397

Thm Fermat-Bis : $\forall p \in \mathcal{P}$ premier $\forall a \in \mathbb{Z}$

$a^p \equiv a \mod p$

Thm Fermat : $\forall p \in \mathcal{P}$ $\forall a \in \mathbb{Z}$ avec $a \wedge p = 1$ pgcd(a, p)

$\Leftrightarrow p \nmid a$ p n'est pas un facteur de a

$\Leftrightarrow a \not\equiv 0 \mod p$

$\Leftrightarrow$ a n'est pas multiple de p

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

Prp : Fermat $\Leftrightarrow$ Fermat-Bis

pv : $\Rightarrow$: Soit $a \in \mathbb{Z}$ Si $a \not\equiv 0 \mod p$,

Hyp que Fermat ↳ $a^{p-1} \equiv 1 \mod p$ BON donne $a \left(\begin{array}{l} a^{p-1} \equiv 1 \mod p \\ a^{p-1} = 1 + kp \end{array} \right.$

$a^p \equiv a \mod p$

↳ F bis seul + avec $a \wedge p = 1$

Si $a \equiv 0 \mod p \overset{\text{RÉC}}{\Rightarrow} a^k \equiv 0 \mod p \overset{\forall k \geq 1}{\Rightarrow}$

$\Rightarrow a^p \equiv 0 \mod p$

$\Rightarrow a^p \equiv 0 \equiv a \equiv 0 \mod p$

F bis dans le cas où $p \mid a$

$\Leftarrow$: Hyp : $a^p \equiv a \mod p$ $\forall a \in \mathbb{Z}$

Prendre a avec $a \wedge p = 1$ comme de Fermat

Ecrire $a^p - a \equiv 0 \mod p$

$a(a^{p-1} - 1) = 0 + kp$ d'où $p \mid a(a^{p-1} - 1)$ Mais $p \nmid a$

$\overset{\text{GAUSS}}{\Rightarrow}$ $p \mid (a^{p-1} - 1) \Leftrightarrow a^{p-1} - 1 \equiv 0 \mod p$ Fermat □

On démontre le théorème de Fermat Bis par Réc en utilisant le binome de Newton.

pv F-bis: $0^p \equiv 0 \mod p$ oui
$1^p \equiv 1 \mod p$ oui
$2^p \equiv 2 \mod p$! Ex: $2^{97} \equiv 2 \mod 97$

Réc: Si $p \in \mathbb{P}$ premier, alors $\forall a \in \mathbb{Z}$ on a
Magie $(a+1)^p = a^p + 1 \mod p$

Alors $2^p = (1+1)^p = 1^p + 1 = 2 \mod p$

$3^p = (2+1)^p \equiv 2^p + 1 \mod p$ (RÉC)
$\equiv 2 + 1 \mod p$
$\equiv 3 \mod p$

pv - magie: $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + a^1\binom{p}{1} + 1^p \mod p$
$\binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + a^1\binom{p}{1} \equiv 0 \mod p$

Lm: Pour $1 \le k \le p-1$ on a $\binom{p}{k} \equiv 0 \mod p$

pv: $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p\cdot(p-1)!}{1\cdot 2\cdots k \cdot 1\cdot 2\cdots(p-k)}$ $\in \mathbb{N}$
ici $k \le p-1$ et $p-k \le p-1$

p en haut ne peut pas être simplifié par un facteur en bas $2 \le k \le p-1 \Rightarrow k \nmid p$ (p premier)
donc le résultat est mult de p $\equiv 0 \mod p$ □

Résumé: □ $\mathbb{Z}$ anneau $(+,\times)$ — $a+25=0 \Rightarrow a=-25$
$a\cdot 25 = 1$ $a = \frac{1}{25} \in \mathbb{Q}$ & $\mathbb{Z}$
$\times$ pas d'inverse

□ $\mathbb{Z}/n\mathbb{Z}$ anneau $(+,\times)$
Ex: $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

$\bar{1}$ a l'inverse mult $\bar{1}$
$\bar{1}^{-1} = \bar{1}$
$\bar{2}\cdot\bar{2} = \bar{1}$ car $\bar{2}^{-1} = \bar{2}$!

Obs · ngc : $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \setminus \{\bar{0}\} = \{\bar{1}, \bar{2}\}$

est un groupe de multiplication x, i.e x associative
id. est $\exists$ élém^t neutre T
$\forall x \neq 0 \ \exists x' \text{ tq } xx' = \bar{1}$

$(\bar{1})^{-1} = \bar{1}$
$(\bar{2})^{-1} = \bar{2}$

associative : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
commutative : $a \cdot b = b \cdot a$

Déf* : Un anneau $A = (A, +, \times)$ muni de $+, \times$ tq
(1) $(A, +)$ est groupe associativité de $+$
commutativité de $+$
$0 + a = a \ \forall a \in A$
$\forall a \in A \ \exists -a \text{ tq } a + (-a) = 0$

(2) $\times$ distributive / $+$ $a \times (b + c) = a \times b + a \times c$

(3) $\times$ associative, commutative, avec $a \cdot 1_A = 1_A \cdot a = a$ $\forall a \in A$

~~MAIS $\forall a \neq 0 \ \exists a' \text{ avec } a \cdot a' = 1_A$~~

Ex : $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$

commutatif

Déf : Un corps, c'est un anneau $(A, +, \times)$, 0_A, 1_A (0_A : l'élément neutre pour l'addition ; 1_A : l'élément neutre pour mult)
$(k, +, \times)$ qui a en plus la ptés
$0_k, 1_k$ $\forall a \neq 0_k \ \exists a' \in k \text{ tq } a \cdot a' = 1_k = a' \cdot a$
$a' \neq 0$ Sinon si $a' = 0$, $a \cdot 0 = 0$

Rqs : a' est unique
NV : Deux inverses de a : $a \cdot a' = 1$
Soustr $a \cdot a'' = 1$
$a(a' - a'') = 0 \Rightarrow a' - a'' = 0$ □

Obs : $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$ est un corps MIEUX QU'UN ANNEAU

$\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Obs :
$\bar{2} \cdot \bar{1} = \bar{2}$
$\bar{2} \cdot \bar{2} = \bar{0}$
$\bar{2} \cdot \bar{3} = \bar{2}$

AÏE 1 $\bar{2} \neq \bar{0}$ mais $\bar{2} \cdot \bar{2} = \bar{0}$

AÏE 2 $\bar{2}$ n'a pas d'inverse pour $\times$

je vais le conceptualiser ☺

Déf : Un anneau $(A,+,\times)$ intègre si

(i) $\forall a \neq 0 \quad \forall b \neq 0 \Rightarrow a \cdot b \neq 0$ $\quad \mathbb{Z}/4\mathbb{Z}$ pas intègre car $\bar{2}\cdot\bar{2}=\bar{0}$

$\Updownarrow$

(ii) $(a=0$ ou $b=0) \quad \Leftarrow \quad ab=0$

$\Updownarrow$

(iii) $\quad b=0 \quad \Leftarrow \quad (a\cdot b=0$ avec $a\neq 0)$

Lm : Si $a\neq 0$ et si $a\cdot b = a\cdot c$ alors $b=c$

pv : Soustr $\quad a(b-c)=0 \Rightarrow b-c=0$ □

	Corps
$\mathbb{Z}/2\mathbb{Z}$	V
$\mathbb{Z}/3\mathbb{Z}$	V
$\mathbb{Z}/4\mathbb{Z}$	X
$\mathbb{Z}/5\mathbb{Z}$	V
$\mathbb{Z}/6\mathbb{Z}$	X

Prop : Tout corps $(K,+,\times)$ est un anneau intègre (Mon déf) ; $\exists a'$ car $(K,+,\times)$ corps

pv : Soient $a, b \in K$ avec $a\neq 0$ tq $a'(a\cdot b=0)$

$\Rightarrow \underbrace{a'\cdot a}_{1}\cdot b = 0$

$\Rightarrow \quad b=0$ □

Thm (*7) : Pour $n \geq 2$ entre, on a équivalence entre

$\Updownarrow$ (i) $n=p \in \mathcal{P}$ est premier

anneau $\Updownarrow$ (ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre

anneau (iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps

pv : (i) $\Rightarrow$ (ii) $\Leftrightarrow$ (iii)

(ii) $\Updownarrow$ (iii) $\Leftarrow$ Prop vue, ok

pv : (i) $\Updownarrow$ (iii)

Soit $n=p$ premier Soient $x,y \in \mathbb{Z}/p\mathbb{Z}$ avec $x\cdot y=0$

But $(x=0$ ou $y=0)$

càd $x\cdot y \equiv 0 \mod p$

càd $x\cdot y = {}^{\exists}k\cdot p$

$\Rightarrow p \mid x\cdot y \Rightarrow p\mid x$ ou $p\mid y$ d'après euclide

$\Leftrightarrow x\equiv 0 \mod p$ ou $y\equiv 0 \mod p$

$\Leftrightarrow (x=0$ dans $\mathbb{Z}/p\mathbb{Z}$ ou $y=0$ dans $\mathbb{Z}/p\mathbb{Z})$

pv : (i) ⇓ (iii) :
Soit $x \in \{1, 2, \dots, n-1\}$ qlcq
But trouver x' avec $x'x = 1$
Hyp : $\mathbb{Z}/n\mathbb{Z}$ intègre
Nécessairement $x' \neq 0$, il faut trouver x' dans $[\bar{1}, \dots, \overline{n-1}]$ mod n

Ass° : L'ensemble $\{x \cdot k : k = 0, 1, 2, \dots, n-1\}$ a n éléments distincts
=> L'ensemble $\{x \cdot k : k = 1, 2, \dots, n-1\}$ a n-1 éléments distincts
On admet à l'avance l'Assertion
Si cela est vrai on déduit que que $\{x\cdot 1, x\cdot 2, \dots, x(n-1)\}$
$= \{1, 2, \dots, n-1\}$
$= \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$
nécessaire : il existe à gauche k avec $x \cdot k = 1$
↑ x' cherché

pv Ass° : $0 \leq k_1 \neq k_2 \leq n-1$ => $x \cdot k_1 \not\equiv x \cdot k_2$ mod n
$\Leftrightarrow x(k_1 - k_2) \neq \bar{0}$ dans $\mathbb{Z}/n\mathbb{Z}$
Rappel : $x \neq 0$ et $k_1 \neq k_2$
$\Leftrightarrow k_1 \cdot k_2 \neq 0$
$(a \neq 0$ et $b \neq 0) \Rightarrow a \cdot b \neq 0$
Hyp : $\mathbb{Z}/n\mathbb{Z}$ intègre □

pv : (i) ?? (iii) : $\Leftrightarrow$ non (i) ⇓ non (ii)
Contraposition
$(P \Rightarrow Q) \Leftrightarrow (\neg P \Leftarrow \neg Q)$

non(i) - non n = $n \in \mathcal{P}$ càd n pas premier càd $n = dm$ avec $1 < d < n$, $1 < m < n$

Dans $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/dm\mathbb{Z}$ on a : $d \neq 0$ car $d \in [\bar{1}, \bar{2}, \dots, \overline{n-1}]$
$m \neq 0$ car $m \in [\bar{1}, \bar{2}, \dots, \overline{n-1}]$

MAIS $d \cdot m = n = 0$ dans $\mathbb{Z}/n\mathbb{Z}$
$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$ dans $\mathbb{Z}/4\mathbb{Z}$ AÏE !

$\mathbb{Z}/n\mathbb{Z}$ pas intègre non(ii)
□

Possible que certains $a \in \mathbb{Z}/n\mathbb{Z}$ aient un inverse multiplicatif, même quand $n \in \mathbb{P}$

Thm: Soit $n \geq 2$ Pour tout $a \in \mathbb{Z}$:

$\Updownarrow$ (i) $a \wedge n = 1$ $\quad a \cdot a' = 1 \bmod n$

$\Updownarrow$ (ii) $\exists a' \in \mathbb{Z}/n\mathbb{Z}$ avec $a\,a' = 1$

Pv: Bezout

$a \wedge n = 1 \iff ua + vn = 1$ $\quad \exists\, u, v \in \mathbb{Z}$

($vn = 0 \bmod n$ car multiple de n)

réduction mod n

$\Rightarrow ua \equiv 1 \bmod n$

Cela dit que u est l'inverse multiplicatif de a dans $\mathbb{Z}/n\mathbb{Z}$ □

Déf: $(\mathbb{Z}/n\mathbb{Z})^\times$ = Groupe des inversibles dans $\mathbb{Z}/n\mathbb{Z}$

$= \{a \in \mathbb{Z}/n\mathbb{Z},\ \exists a' \in \mathbb{Z}/n\mathbb{Z} \text{ avec } a \cdot a' = 1\}$

$\overset{\text{THM}}{=} \{a \in \mathbb{Z}/n\mathbb{Z} \quad a \wedge n = 1\}$

Indicatrice d'Euler
$\varphi(n)$ → prend un nombre et donne un nombre des nombres entre 1 et n qui sont premiers à n.
Ex: $\varphi(5) = 3$ car 2, 3, 4 sont premiers à 5

Déf: Indicatrice d'Euler

$\varphi(n) = a \cdot n \qquad 1 \leq a \leq n : a \wedge n = 1$

Thm: [Restes chinois] Soient $n_1, n_2, \dots, n_r \geq 1$ premiers entre eux

$n_i \wedge n_j = 1 \qquad (\forall 1 \leq i \neq j \leq r)$

Alors pour tous $a_1, a_2, \dots, a_r \in \mathbb{Z}$, les éqts : $\exists x$

$$x \equiv a_1 \bmod n_1$$
$$\vdots$$
$$x \equiv a_r \bmod n_r$$

ont tjrs une solution.

Si x' est une autre sol alors $x - x' \equiv 0 \bmod (n_1 \cdot n_2)$

Pv : Poser $n := n_1 \dots n_{i-1} n_i n_{i+1} \dots n_r$

pour i fixé $\hat{n}_i = \frac{n}{n_i} = n_1 \dots n_{i-1} 1 n_{i+1} \dots n_r$

Obs : $n_i \wedge \hat{n}_i = 1$ car $n_i \wedge n_j = 1 \quad \forall 1 \leq i \neq j \leq r$

Bezout : $\exists u_i n_i + \exists v_i \hat{n}_i = 1 \mid \mod n_i \mid_{\mod n_j \; j \neq i}$ $\Rightarrow e_i \equiv 1 \mod n_i$

$\vdots$

$e_j \equiv 0 \mod n_j \quad \forall j \neq i$

Poser $e_i := v_i \hat{n}_i$

Sol : $x := a_1 e_1 + \dots + a_i e_i + \dots + a_n e_n$ on vérifie $x \equiv a_i \mod n_i$

$\forall 1 \leq i \leq r$

□