Conjecture de Goldbach (7 juin 1742)

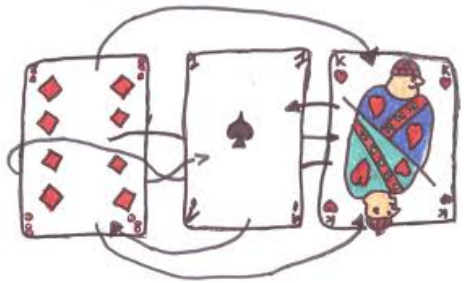
- 271 ans
- **Énoncé** : Tout entier pair (n) supérieur à 2 est la somme de deux nombres premiers.
- $\Longleftrightarrow$ Tout entier supérieur à 1 est la moyenne de deux nombres premiers $(\frac{1}{2}p_1 + \frac{1}{2}p_2)$.
- Échanger, permuter
- notations : CG, dg

Représenter les nombres par des mots de restes

- *Base modulaire* : (3,5,7)
- $98 = (2,3,0)$
- $dg \rightarrow 19 = (1,4,5)$
- $86 = (2,1,2)$
- dg trivial $\rightarrow 43 = (1,3,1)$

Échanger, permuter

- Jeu du bonneteau



- Jeu du taquin ou pousse-pousse (cf Bicentenaire)

- Pouss-Pouss (La tige en plastique finit par prendre la place de la glace à l'intérieur du cylindre.)

Permuter deux variables en informatique

- $X \leftrightarrow Y$
- *méthode 1* :

$X \leftarrow 1$
$Y \leftarrow 0$

$X \leftarrow Y$
$Y \leftarrow X$

X ? Y ?

X=0, Y=0

Permuter deux variables en informatique

- *méthode 2* :

$X \leftarrow 1$
$Y \leftarrow 0$

$Z \leftarrow X$
$X \leftarrow Y$
$Y \leftarrow Z$

X ? Y ?

X=0, Y=1

Permuter les lettres de mots dans les anagrammes

- Galilée envoie un cryptogramme à Kepler :

  smaismrmilmepoetaleumibunenugttauiras

  $\rightarrow$ Salve umbistineum geminatum Martia proles. (Kepler)

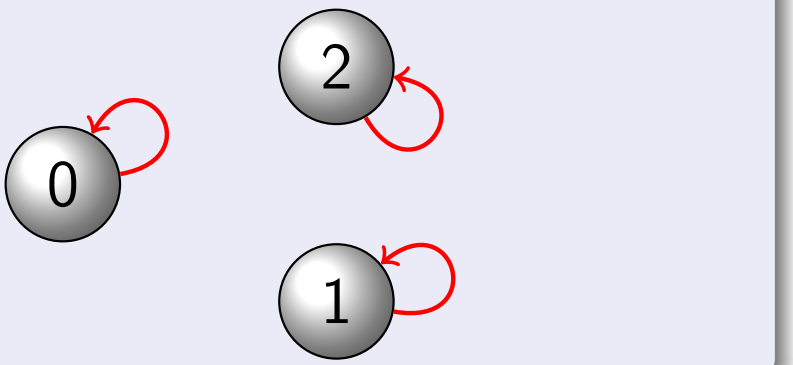
  (Salut, double protection du bouclier, enfants de Mars.)

  $\rightarrow$ Altissimum planetam tergeminum observavi. (Galilée)

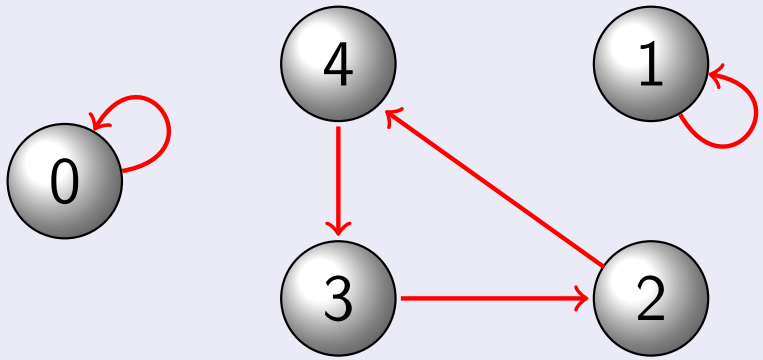
  (J'ai observé que la planète la plus lointaine est en forme de trois.)

Echanger les racines dans la théorie de Galois

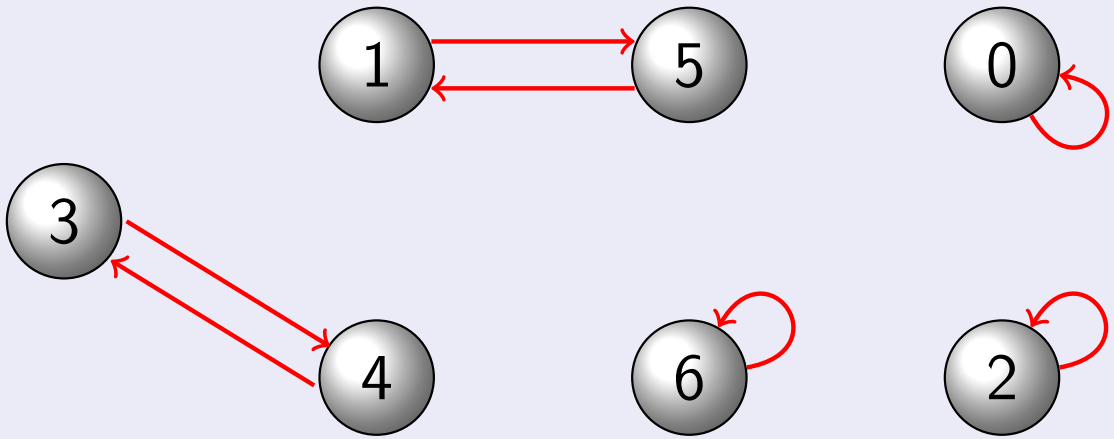
$\mathbb{Z}/3\mathbb{Z}$



$\mathbb{Z}/5\mathbb{Z}$



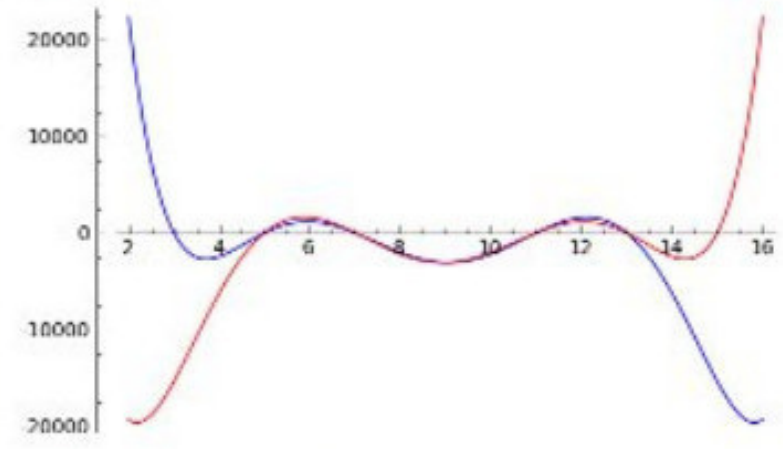
$\mathbb{Z}/7\mathbb{Z}$



Les *dg* sont solutions d'une équation polynomiale

- On le postule.
- Galois cite Libri.
- On peut fabriquer cette équation en "remontant" des solutions :
  - une première éq. poly. de racines les nombres premiers ($\leqslant n$),
  - une deuxième obtenue en remplaçant x par $n - x$ dans la première ($x \mapsto n - x$),
  - solutions communes aux deux équations.
- Nullité du déterminant d'une matrice de Sylvester

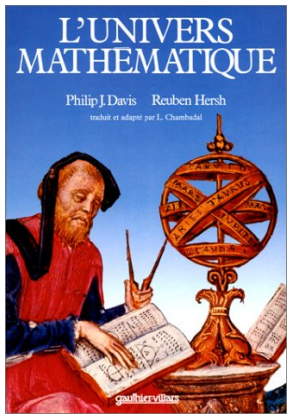
```
x=var('decomp18')
f=plot(x^6-56*x^5+1237*x^4-13712*x^3+79891*x^2-230456*x+255255,(x,2,16),rgbcolor=(0,0,1))
g=plot(x^6-52*x^5+1057*x^4-10552*x^3+52891*x^2-118420*x+75075,(x,2,16),rgbcolor=(1,0,0))
```




```
h=plot(2*x^6-108*x^5+2294*x^4-24264*x^3+132782*x^2-348876*x+330330,(x,2,16),rgbcolor=(0,1,0))
show(h)
```

Le partage de *dg*

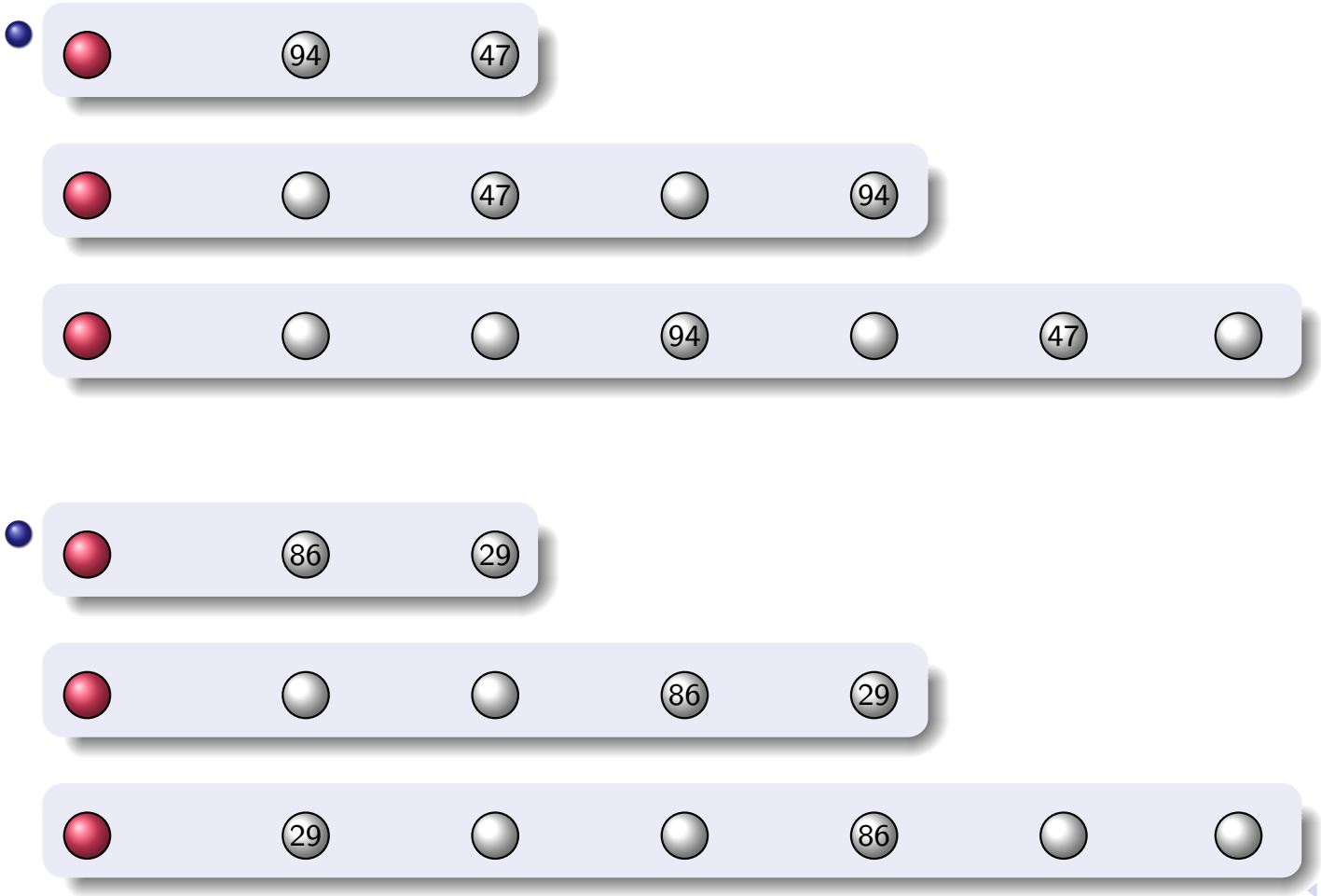
- $20902 = 3 + 20899$ $20962 = 3 + 20959$
  $20904 = 5 + 20899$ $20964 = 5 + 20959$
  $20906 = 3 + 20903$ $20966 = 3 + 20963$
  $20908 = 5 + 20903$ $20968 = 5 + 20963$
  $20910 = 7 + 20903$ $20970 = 7 + 20963$
  $20912 = 13 + 20899$ $20972 = 13 + 20959$
  $20914 = 11 + 20903$ $20974 = 11 + 20963$
  $20916 = 13 + 20903$ $20976 = 13 + 20963$
  $20918 = 19 + 20899$ $20978 = 19 + 20959$
  $20920 = 17 + 20903$ $20980 = 17 + 20963$
  $20922 = 19 + 20903$ $20982 = 19 + 20963$
  $20924 = 3 + 20921$ $20984 = 3 + 20981$



- Des causes différentes produisent les mêmes effets (écart de 60, congrus mod 3 et 5).

Utiliser une solution triviale

- faire découler l'existence d'un *dg* pour un pair double de composé de l'existence obligatoire d'un *dg* trivial pour un double de premier en permutant les classes.



Permutations des racines

- $$\begin{array}{ccc} 2p_i & \xrightarrow{f} & 2c \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ p_i & \xrightarrow{f} & p_j \end{array}$$

- $$\begin{array}{ccc} 94 = (1,4,3) & \xrightarrow{f} & 88 = (1,3,4) \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ 47 = (2,2,5) & \xrightarrow{f} & 29 = (2,4,1) \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ \mathbb{Z}/3\mathbb{Z} \setminus \{0,1\} \times \mathbb{Z}/5\mathbb{Z} \setminus \{0,4\} \times \mathbb{Z}/7\mathbb{Z} \setminus \{0,3\} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z} \setminus \{0,1\} \times \mathbb{Z}/5\mathbb{Z} \setminus \{0,3\} \times \mathbb{Z}/7\mathbb{Z} \setminus \{0,4\} \end{array}$$

Permutations des racines

- $$\begin{array}{ccc} 94 = (1,4,3) & \xrightarrow{f} & 88 = (1,3,4) \\ \downarrow g_t & & \downarrow g \\ 47 = (2,2,5) & \xrightarrow{f} & 29 = (2,4,1) \end{array}$$

- $\mathbb{Z}/3\mathbb{Z} \to Id$,
  $\mathbb{Z}/5\mathbb{Z} \to \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 3 \end{pmatrix}$,
  $\mathbb{Z}/7\mathbb{Z} \to \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$

Outils

- Théorie des groupes (moins fois moins égal plus, impair plus impair égal pair).
- Le nombre de bijections d'un ensemble de cardinal n dans lui-même est $n!$
- **Première idée** : on veut passer d'une décomposition triviale $2p_k = p_k + p_k$ aux décompositions pour tous les pairs qui "sont touchés" par la même base, i.e. entre deux carrés de premiers consécutifs.

Outils

- **Question :** Pourquoi trouve-t-on toujours un double de premier entre 2 carrés de premiers ? (celui qui va servir de "modèle")

$$p_k^2 + 1 \quad \leqslant 2p \quad < p_{k+1}^2 + 1 \quad ?$$

- **Théorème de Tchebychev** : on trouve toujours un premier entre un nombre et son double.

$$\forall x \in \mathbb{N}^*,\ \exists p \textit{ premier},\ x \leqslant p \leqslant 2x$$

Corollaire :

$$\frac{2}{5}\, n \ln n < p_n < 3\, n \ln n$$

- **Conjecture de Legendre** : on trouve toujours un premier entre deux carrés d'entiers consécutifs.

$$\forall x \in \mathbb{N}^*,\ \exists p \textit{ premier},\ x^2 \leqslant p \leqslant (x+1)^2$$

- **Problème** : la **question** est toujours ouverte, il faut une autre idée.

Récurrence

- On va faire passer une solution triviale $2p_k = p_k + p_k$ à tous les pairs inférieurs à $2p_k$ et supérieurs à $2p_{k-1}$
- Soit on travaillera dans le même produit cartésien de corps premiers qui a servi de base modulaire, soit on travaillera dans un sous-produit cartésien de la base.
- Remarque : les restes non-nuls et non égaux à ceux du pair double de premier doivent sûrement pouvoir être permutés avec d'autres (il y a de la marge) de manière à ce que les contraintes assez "légères" que sont la non-nullité et la non-égalité aux restes du double de composé puissent être vérifiées.

Congruences

- Les $6k$ ont des *dg* dans les deux ensembles de nombres premiers en progression arithmétique, soit de la forme $6k+1$, soit de la forme $6k-1$.
- Les $6k+2$ ont des *dg* uniquement dans l'ensemble des premiers de la forme $6k+1$ (car les $6k+2$ et les $6k-1$ sont congrus à 2 (mod 3)).
- Les $6k+4$ ont des *dg* uniquement dans l'ensemble des premiers de la forme $6k-1$ (car les $6k+4$ et les $6k+1$ sont congrus à 1 (mod 3)).
- On sépare ces trois cas de manière à ne s'occuper que des congruences selon les modules supérieurs ou égaux à 5. Cela permet d'obtenir un traitement homogène selon tous les modules.
- Je crois que le nombre de bijections est à calculer sur des ensembles dans lesquels on élimine 3 congruences (pour que les permutations respectent et la non-nullité des restes du *dg* et leur non-égalité aux restes de n).
- De l'existence d'un *dg trivial* pour un seul pair, je crois qu'on peut déduire l'existence d'un *dg* pour $\prod_p (p-3)!$ nombres, ce qui est beaucoup...

Conjecture

- Tout nombre pair n supérieur à 12 partage l'un de ses dg avec $n - 6$.

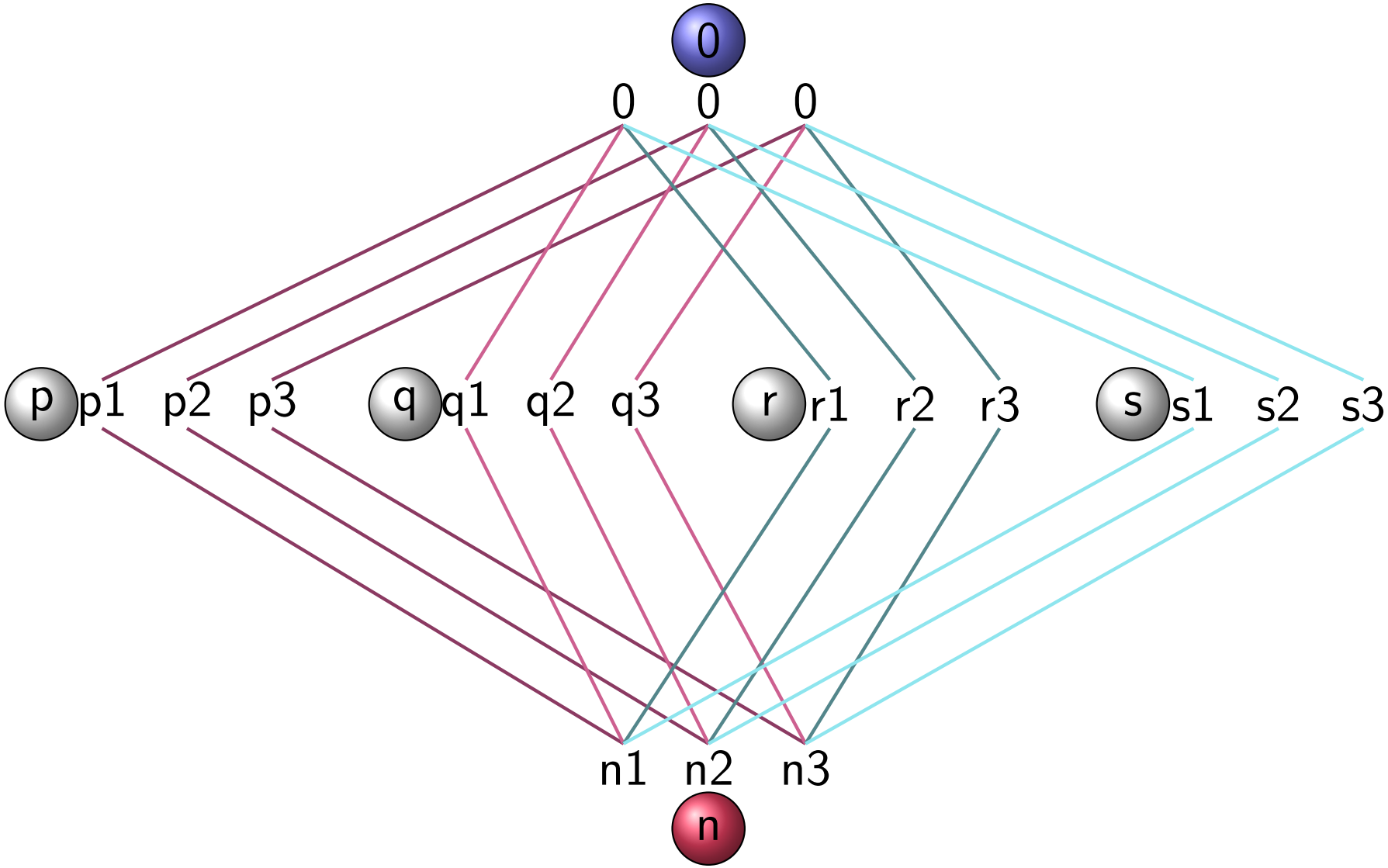
- vérifiée par ordinateur jusqu'à 4.10^6.

Passer entre les gouttes : les $6k+2$

26 $(2,1)$	$\to 7$	$(1,2)$	*ou*	13	$(1,3)$	(t)
32 $(2,2)$	$\to 13$	$(1,3)$				
38 $(2,3)$	$\to 19$	$(1,4)$ (t)				
44 $(2,4)$	$\to 7$	$(1,2)$	*ou*	13	$(1,3)$	
50 $(2,0,1)$	$\to 13$	$(1,3,6)$	*ou*	7	$(1,2,0)$	
56 $(2,1,0)$	$\to 19$	$(1,4,5)$	*ou*	13	$(1,3,6)$	
62 $(2,2,6)$	$\to 7$	$(1,2,0)$	*ou*	19	$(1,4,5)$	
68 $(2,3,5)$	$\to 31$	$(1,1,3)$	*ou*	7	$(1,2,0)$	
74 $(2,4,4)$	$\to 7$	$(1,2,0)$	*ou*	37	$(1,2,2)$	(t)

- Galois $\to$ Sagiol : au bout de combien d'applications revient-on à Galois ? (merci Norbert Verdier).
- Jeu plus petit / plus grand dans les réels en élémentaire.

Congruences



Notion d'invariant en informatique

- *trouver le double d'un nombre n* :

```
X ← 0 ;
Y ← n ;
while (y > 0) {
  Y ← Y-1 ;
  X ← X+2 ;
}
```

Invariant de boucle : $(Y{=}0) \vee (X{=}2(n{-}Y))$.

Conclusion

- **Hilbert** :

  Wir mussen wissen, wir werden wissen (pas d'ignorabimus en mathématiques.)

- **Poincaré** :

  Le terrain le plus naturel et le plus favorable pour cette étude est l'arithmétique élémentaire, c'est à dire les opérations mettant en jeu des nombres entiers. Quand nous analysons des opérations telles que l'addition et la multiplication, nous nous rendons compte qu'un type de raisonnement se "retrouve à chaque pas", c'est la démonstration "par récurrence" : "on établit d'abord un théorème pour n égal à 1 ; on montre ensuite que, s'il est vrai de $n-1$, il est vrai de n, et on en conclut qu'il est vrai pour tous les nombres entiers." C'est là le "raisonnement mathématique par excellence". Sa particularité est "qu'il contient, sous une forme condensée, une infinité de syllogismes", et qu'il permet de passer du particulier au général, du fini à l'infini, concept qui apparaît dès les premiers pas de l'arithmétique élémentaire et sans lequel "il n'y aurait pas de science parce qu'il n'y aurait rien de général", mais uniquement des énoncés particuliers.

Conclusion

- **Poincaré** :

  D'où nous vient ce "raisonnement pas récurrence" ?

  Certainement pas de l'expérience. Celle-ci peut nous suggérer que la règle est vraie pour les dix ou les cent premiers nombres, mais elle est désarmée face à l'infinité de tous les nombres naturels. Le principe de contradiction (on dirait aujourd'hui le raisonnement par l'absurde) est aussi impuissant : il nous permet d'obtenir certaines vérités, mais non d'en enfermer une infinité en une seule formule. "Cette règle (le raisonnement par récurrence), inaccessible à la démonstration analytique et à l'expérience, est le véritable type du jugement synthétique a priori. L"'irrésistible évidence" avec laquelle ce "principe" s'impose n'est autre que "l'affirmation de la puissance de l'esprit qui se sait capable de concevoir la répétition indéfinie d'un même acte dès que cet acte est une fois possible"... *(extrait de la biographie "Poincaré : mathématicien et philosophe" d'Umberto Bottazzini, éd. Belin Pour la Science)*

Conclusion

- On a utilisé un SNURPF : un Système de NUmération par les Restes dans les Parties Finies de $\mathbb{N}$.

- On se situe dans une théorie lexicale des nombres, selon laquelle les nombres sont des mots.