Un chapitre de l'héritage de Pierre de Fermat

Paris – KafeMath

Jean-Marie De Koninck

Le 23 mai 2019

Pierre de Fermat
(1601-1665)

L'empreinte de Pierre de Fermat

L'empreinte de Pierre de Fermat

- Son *grand théorème* concernant la non existence de solutions entières positives de l'équation $x^n + y^n = z^n$ pour chaque entier $n \geq 3$

L'empreinte de Pierre de Fermat

- Son *grand théorème* concernant la non existence de solutions entières positives de l'équation $x^n + y^n = z^n$ pour chaque entier $n \geq 3$

- Son *petit théorème*, à l'effet que $2^{p-1} \equiv 1 \pmod{p}$ pour chaque nombre premier impair p

L'empreinte de Pierre de Fermat

- Son *grand théorème* concernant la non existence de solutions entières positives de l'équation $x^n + y^n = z^n$ pour chaque entier $n \geq 3$
- Son *petit théorème*, à l'effet que $2^{p-1} \equiv 1 \pmod{p}$ pour chaque nombre premier impair p
- Une caractérisation des entiers pouvant s'écrire comme la somme de deux carrés

L'empreinte de Pierre de Fermat

- Son *grand théorème* concernant la non existence de solutions entières positives de l'équation $x^n + y^n = z^n$ pour chaque entier $n \geq 3$
- Son *petit théorème*, à l'effet que $2^{p-1} \equiv 1 \pmod{p}$ pour chaque nombre premier impair p
- Une caractérisation des entiers pouvant s'écrire comme la somme de deux carrés
- Sa méthode de descente infinie qui permet de démontrer l'inexistence de solutions de certaines équations diophantiennes

L'empreinte de Pierre de Fermat

L'empreinte de Pierre de Fermat

- Fondateur (avec Blaise Pascal) de la théorie des probabilités

L'empreinte de Pierre de Fermat

- Fondateur (avec Blaise Pascal) de la théorie des probabilités
- Un précurseur du calcul différentiel par sa méthode de recherche des maximums et des minimums d'une fonction

L'empreinte de Pierre de Fermat

- Fondateur (avec Blaise Pascal) de la théorie des probabilités
- Un précurseur du calcul différentiel par sa méthode de recherche des maximums et des minimums d'une fonction
- Sa méthode de factorisation des entiers

Savoir factoriser des grands nombres – Important ?

Savoir factoriser des grands nombres – Important ?

Important pour la transmission sécuritaire

des messages secrets

La cryptographie

La cryptographie

Jules César:

$$\begin{array}{cccccc} A & B & C & D & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \\ C & D & E & F & \cdots \end{array}$$

La cryptographie

La cryptographie

Deuxième guerre mondiale

Arthur Scherbius

Machine Enigma

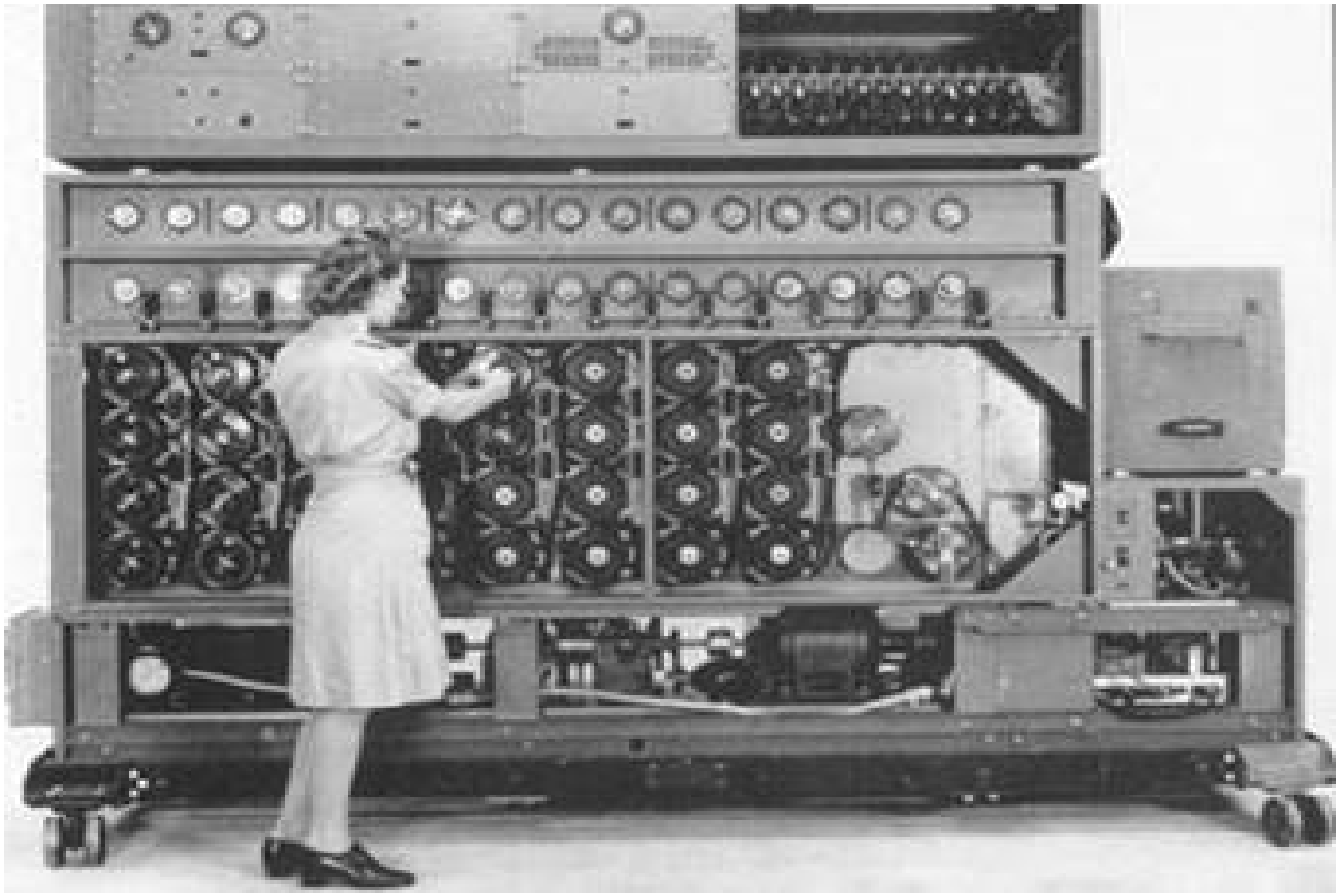
La cryptographie

La cryptographie

Alan Turing

La cryptographie

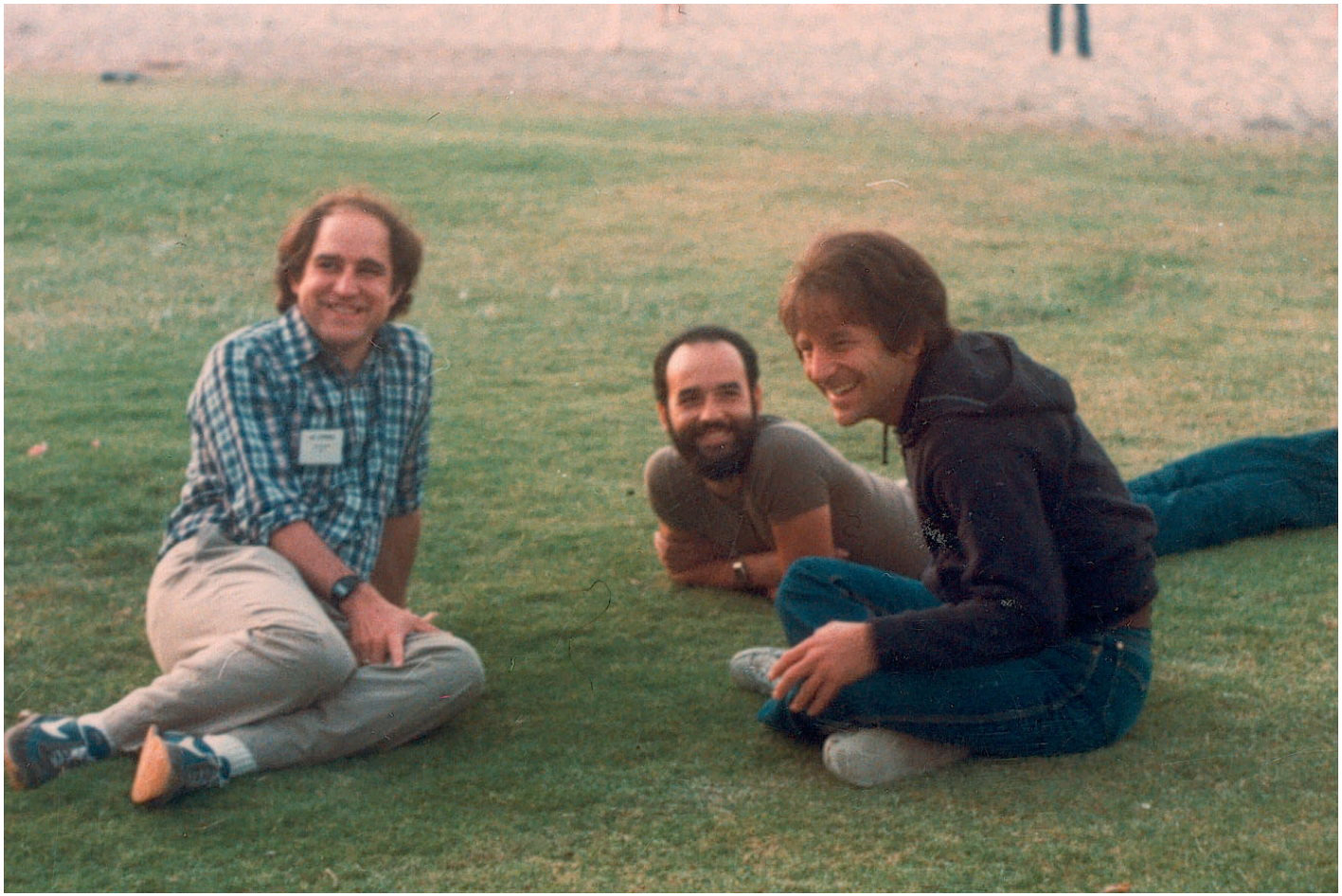
La cryptographie



La Bombe

La méthode RSA

La méthode RSA



Ron Rivest, Adi Shamir, Leonard Adleman

La méthode RSA – Rivest - Shamir - Adleman

La méthode RSA – Rivest - Shamir - Adleman

- On sait facilement multiplier deux nombres

La méthode RSA – Rivest - Shamir - Adleman

- On sait facilement multiplier deux nombres
- On sait difficilement faire l'inverse: "factoriser"

La méthode RSA – Rivest - Shamir - Adleman

- On sait facilement multiplier deux nombres
- On sait difficilement faire l'inverse: "factoriser"
- 1978: Rivest, Shamir, Adleman mettent au point la méthode RSA

Des débuts difficiles

Des débuts difficiles

- En 1644, Marin Mersenne étudie les nombres $M_p := 2^p - 1$

Des débuts difficiles

- En 1644, Marin Mersenne étudie les nombres $M_p := 2^p - 1$
- Mersenne croit que le nombre M_{251} est composé

Des débuts difficiles

- En 1644, Marin Mersenne étudie les nombres $M_p := 2^p - 1$
- Mersenne croit que le nombre M_{251} est composé
- En 1976, on estime qu'il faudrait plus de 10^{20} années pour factoriser M_{251}, un nombre de 76 chiffres

Des débuts difficiles

- En 1644, Marin Mersenne étudie les nombres $M_p := 2^p - 1$
- Mersenne croit que le nombre M_{251} est composé
- En 1976, on estime qu'il faudrait plus de 10^{20} années pour factoriser M_{251}, un nombre de 76 chiffres
- En 1984, 32 heures de calcul sur un Cray-1 permettent de factoriser M_{251}

La factorisation complète de $2^{251} - 1$

La factorisation complète de $2^{251} - 1$

Factorisation maison en 55 secondes:

$$\begin{aligned} 2^{251} - 1 &= 503 \times 54217 \times 1782302872140632895 11 \\ &\quad \times 6167688219869525750 1367 \\ &\quad \times 120703961782498930399696 81 \end{aligned}$$

La méthode de factorisation de Fermat

La méthode de factorisation de Fermat

On constate que

$$899 = 900 - 1 = 30^2 - 1^2 = (30 - 1)(30 + 1) = 29 \times 31$$

La méthode de factorisation de Fermat

On constate que

$$899 = 900 - 1 = 30^2 - 1^2 = (30 - 1)(30 + 1) = 29 \times 31$$

Pour tout nombre composé impair n, il existe $a > b \geq 1$ tels que

$$n = a^2 - b^2$$

La méthode de factorisation de Fermat

On constate que

$$899 = 900 - 1 = 30^2 - 1^2 = (30 - 1)(30 + 1) = 29 \times 31$$

Pour tout nombre composé impair n, il existe $a > b \geq 1$ tels que

$$n = a^2 - b^2$$

En effet, supposons que $n = r \times s$ avec $1 < r < s$

La méthode de factorisation de Fermat

On constate que

$$899 = 900 - 1 = 30^2 - 1^2 = (30 - 1)(30 + 1) = 29 \times 31$$

Pour tout nombre composé impair n, il existe $a > b \geq 1$ tels que

$$n = a^2 - b^2$$

En effet, supposons que $n = r \times s$ avec $1 < r < s$

Il suffit alors de choisir $a = \dfrac{s + r}{2}$ et $b = \dfrac{s - r}{2}$

La méthode de factorisation de Fermat

La méthode de factorisation de Fermat

Comme $n = a^2 - b^2 < a^2$, on a $a > \sqrt{n}$, auquel cas $a \geq \lfloor \sqrt{n} \rfloor + 1$

La méthode de factorisation de Fermat

Comme $n = a^2 - b^2 < a^2$, on a $a > \sqrt{n}$, auquel cas $a \geq \lfloor \sqrt{n} \rfloor + 1$

On commence donc avec $a = \lfloor \sqrt{n} \rfloor + 1$; si $a^2 - n = b^2$, alors $n = a^2 - b^2$

La méthode de factorisation de Fermat

Comme $n = a^2 - b^2 < a^2$, on a $a > \sqrt{n}$, auquel cas $a \geq \lfloor \sqrt{n} \rfloor + 1$

On commence donc avec $a = \lfloor \sqrt{n} \rfloor + 1$; si $a^2 - n = b^2$, alors $n = a^2 - b^2$

Sinon, on choisit $a = \lfloor \sqrt{n} \rfloor + 2$

La méthode de factorisation de Fermat

Comme $n = a^2 - b^2 < a^2$, on a $a > \sqrt{n}$, auquel cas $a \geq \lfloor \sqrt{n} \rfloor + 1$

On commence donc avec $a = \lfloor \sqrt{n} \rfloor + 1$; si $a^2 - n = b^2$, alors $n = a^2 - b^2$

Sinon, on choisit $a = \lfloor \sqrt{n} \rfloor + 2$

Éventuellement, avec $a = \lfloor \sqrt{n} \rfloor + k$, on aura $a^2 - n = b^2$, auquel cas $n = a^2 - b^2$

L'exemple choisi par Fermat

L'exemple choisi par Fermat

Fermat choisit le nombre $n = 2\,027\,651\,281$

L'exemple choisi par Fermat

Fermat choisit le nombre $n = 2\,027\,651\,281$

Il obtient $\lfloor \sqrt{n} \rfloor = 45\,029$ et pose d'abord $a = 45\,029 + 1 = 45\,030$

L'exemple choisi par Fermat

Fermat choisit le nombre $n = 2\,027\,651\,281$

Il obtient $\lfloor \sqrt{n} \rfloor = 45\,029$ et pose d'abord $a = 45\,029 + 1 = 45\,030$

Comme $45\,030^2 - 2\,027\,651\,281 = 49\,619$ n'est pas un carré parfait,

L'exemple choisi par Fermat

Fermat choisit le nombre $n = 2\,027\,651\,281$

Il obtient $\lfloor \sqrt{n} \rfloor = 45\,029$ et pose d'abord $a = 45\,029 + 1 = 45\,030$

Comme $45\,030^2 - 2\,027\,651\,281 = 49\,619$ n'est pas un carré parfait,

il pose ensuite $a = 45\,031$, qui ne produit pas non plus de carré parfait

L'exemple choisi par Fermat

Fermat choisit le nombre $n = 2\,027\,651\,281$

Il obtient $\lfloor \sqrt{n} \rfloor = 45\,029$ et pose d'abord $a = 45\,029 + 1 = 45\,030$

Comme $45\,030^2 - 2\,027\,651\,281 = 49\,619$ n'est pas un carré parfait,

il pose ensuite $a = 45\,031$, qui ne produit pas non plus de carré parfait

et ainsi de suite jusqu'à ce qu'il pose $a = 45\,041$, qui donne

$$b = \sqrt{45\,041^2 - 2\,027\,651\,281} = \sqrt{1\,040\,400} = 1\,020$$

L'exemple choisi par Fermat

Fermat choisit le nombre $n = 2\,027\,651\,281$

Il obtient $\lfloor \sqrt{n} \rfloor = 45\,029$ et pose d'abord $a = 45\,029 + 1 = 45\,030$

Comme $45\,030^2 - 2\,027\,651\,281 = 49\,619$ n'est pas un carré parfait,

il pose ensuite $a = 45\,031$, qui ne produit pas non plus de carré parfait

et ainsi de suite jusqu'à ce qu'il pose $a = 45\,041$, qui donne

$$b = \sqrt{45\,041^2 - 2\,027\,651\,281} = \sqrt{1\,040\,400} = 1\,020$$

Fermat conclut alors que

$$\begin{aligned} n &= 2\,027\,651\,281 = 45\,041^2 - 1\,020^2 \\ &= (45\,041 - 1\,020)(45\,041 + 1\,020) = 44\,021 \times 46\,061 \end{aligned}$$

La méthode de Fermat programmée

La méthode de Fermat programmée

```
n = 2 027 651 281; a = Floor[Sqrt[n]] + 1;
While[!IntegerQ[b = Sqrt[a^2 - n]], a++];
Print["a=",a,"et b=",b,"⟶ n =",a - b, " × ",a + b]
```

La méthode de Fermat programmée

```
n = 2 027 651 281; a = Floor[Sqrt[n]] + 1;
While[!IntegerQ[b = Sqrt[a^2 - n]], a++];
Print["a=",a,"et b=",b,"⟶ n =",a - b, " × ",a + b]
```

ce qui donne

$$a = 45\,041 \text{ et } b = 1\,020 \longrightarrow n = 44\,021 \times 46\,061.$$

Le nombre d'étapes nécessaires pour factoriser un nombre en utilisant la méthode de Fermat

Le nombre d'étapes nécessaires pour factoriser un nombre en utilisant la méthode de Fermat

Si $n = d_1 d_2$, où $d_1 < \sqrt{n} < d_2$ sont les diviseurs milieux de n

Le nombre d'étapes nécessaires pour factoriser un nombre en utilisant la méthode de Fermat

Si $n = d_1 d_2$, où $d_1 < \sqrt{n} < d_2$ sont les diviseurs milieux de n

Exemple: $n = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$; $d_1 = 33$, $d_2 = 35$ sont les diviseurs milieux de n, car

$$33 < \sqrt{n} = \sqrt{1155} = 33,9 < 35$$

Le nombre d'étapes nécessaires pour factoriser un nombre en utilisant la méthode de Fermat

Si $n = d_1 d_2$, où $d_1 < \sqrt{n} < d_2$ sont les diviseurs milieux de n

Exemple: $n = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$; $d_1 = 33$, $d_2 = 35$ sont les diviseurs milieux de n, car

$$33 < \sqrt{n} = \sqrt{1155} = 33,9 < 35$$

Alors le nombre k d'étapes pour factoriser un nombre n est

$$k = \frac{d_1 + d_2}{2} - \lfloor \sqrt{d_1 d_2} \rfloor = \frac{d_1 + d_2}{2} - \lfloor \sqrt{n} \rfloor$$

Le nombre d'étapes nécessaires pour factoriser un nombre en utilisant la méthode de Fermat

Si $n = d_1 d_2$, où $d_1 < \sqrt{n} < d_2$ sont les diviseurs milieux de n

Exemple: $n = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$; $d_1 = 33$, $d_2 = 35$ sont les diviseurs milieux de n, car

$$33 < \sqrt{n} = \sqrt{1155} = 33,9 < 35$$

Alors le nombre k d'étapes pour factoriser un nombre n est

$$k = \frac{d_1 + d_2}{2} - \lfloor \sqrt{d_1 d_2} \rfloor = \frac{d_1 + d_2}{2} - \lfloor \sqrt{n} \rfloor$$

Méthode de Fermat efficace si $d_2 - d_1$ est petit

Accélérer la méthode de Fermat

Accélérer la méthode de Fermat

- Si $n = r \times s$, alors $n_1 = uv \times n = uv \times rs = ur \times vs$ avec possiblement $ur < \sqrt{n_1} < vs$ et $vs - ur$ petit

Accélérer la méthode de Fermat

- Si $n = r \times s$, alors $n_1 = uv \times n = uv \times rs = ur \times vs$ avec possiblement $ur < \sqrt{n_1} < vs$ et $vs - ur$ petit
- 1974: R.S. Lehman $\longrightarrow$ factorise n en moins de $n^{1/3}$ étapes

Accélérer la méthode de Fermat

- Si $n = r \times s$, alors $n_1 = uv \times n = uv \times rs = ur \times vs$ avec possiblement $ur < \sqrt{n_1} < vs$ et $vs - ur$ petit
- 1974: R.S. Lehman $\longrightarrow$ factorise n en moins de $n^{1/3}$ étapes
- 1999: J.F. McKee $\longrightarrow$ factorise n en moins de $n^{1/4}$ étapes

L'approche de Maurice Kraitchik

L'approche de Maurice Kraitchik

Au lieu de chercher a et b tels que $n = a^2 - b^2$, on cherche u et v tels que $u^2 \equiv v^2 \pmod{n}$

L'approche de Maurice Kraitchik

Au lieu de chercher a et b tels que $n = a^2 - b^2$, on cherche u et v tels que $u^2 \equiv v^2 \pmod{n}$
Rappelons que $u^2 \equiv v^2 \pmod{n}$ veut dire $n \mid (u^2 - v^2)$

L'approche de Maurice Kraitchik

Au lieu de chercher a et b tels que $n = a^2 - b^2$, on cherche u et v tels que $u^2 \equiv v^2 \pmod{n}$
Rappelons que $u^2 \equiv v^2 \pmod{n}$ veut dire $n \mid (u^2 - v^2)$

Soit $n = 1081$. On constate que $127^2 \equiv 80^2 \pmod{n}$

L'approche de Maurice Kraitchik

Au lieu de chercher a et b tels que $n = a^2 - b^2$, on cherche u et v tels que $u^2 \equiv v^2 \pmod{n}$
Rappelons que $u^2 \equiv v^2 \pmod{n}$ veut dire $n \mid (u^2 - v^2)$

Soit $n = 1081$. On constate que $127^2 \equiv 80^2 \pmod{n}$

On a donc que

$$n \mid 127^2 - 80^2 = (127 - 80)(127 + 80) = 47 \times 207$$

L'approche de Maurice Kraitchik

Au lieu de chercher a et b tels que $n = a^2 - b^2$, on cherche u et v tels que $u^2 \equiv v^2 \pmod{n}$
Rappelons que $u^2 \equiv v^2 \pmod{n}$ veut dire $n \mid (u^2 - v^2)$

Soit $n = 1081$. On constate que $127^2 \equiv 80^2 \pmod{n}$

On a donc que

$$n \mid 127^2 - 80^2 = (127 - 80)(127 + 80) = 47 \times 207$$

Comme tout facteur de n est un facteur de 47 ou de 207, et comme $207 = 9 \times 23$, on conclut que

$$n = 23 \times 47$$

L'approche de Maurice Kraitchik

L'approche de Maurice Kraitchik

Autre exemple: $n = 9701$. On pose $a = \lfloor \sqrt{n} \rfloor + 1 = 99$ et $f(x) := x^2 - n$

L'approche de Maurice Kraitchik

Autre exemple: $n = 9701$. On pose $a = \lfloor \sqrt{n} \rfloor + 1 = 99$ et $f(x) := x^2 - n$

Examinons quelques termes de la suite $f(99)$, $f(100), \ldots$, en conservant seulement les nombres $f(r)$ dont le plus grand facteur premier est ≤ 5

L'approche de Maurice Kraitchik

Autre exemple: $n = 9701$. On pose $a = \lfloor \sqrt{n} \rfloor + 1 = 99$ et $f(x) := x^2 - n$

Examinons quelques termes de la suite $f(99)$, $f(100), \ldots$, en conservant seulement les nombres $f(r)$ dont le plus grand facteur premier est ≤ 5

Le tout premier terme de cette suite donne $f(99) = 99^2 - 9701 = 100 = 2^2 \times 5^2$, un carré parfait !

L'approche de Maurice Kraitchik

Autre exemple: $n = 9701$. On pose $a = \lfloor \sqrt{n} \rfloor + 1 = 99$ et $f(x) := x^2 - n$

Examinons quelques termes de la suite $f(99)$, $f(100), \ldots$, en conservant seulement les nombres $f(r)$ dont le plus grand facteur premier est ≤ 5

Le tout premier terme de cette suite donne $f(99) = 99^2 - 9701 = 100 = 2^2 \times 5^2$, un carré parfait !

Cette fois, la factorisation de 9701 nous saute aux yeux, puisque $(99 - 10)(99 + 10) \equiv 0 \pmod{9701}$, auquel cas $9701 = 89 \times 109$

L'approche de Maurice Kraitchik

L'approche de Maurice Kraitchik

Plus généralement, comment fait-on pour trouver u et v tels

$$u^2 \equiv v^2 \pmod{n} \quad ?$$

L'approche de Maurice Kraitchik

Plus généralement, comment fait-on pour trouver u et v tels

$$u^2 \equiv v^2 \pmod{n} \quad ?$$

Un exemple: $n = 11\,111$

L'approche de Maurice Kraitchik

Plus généralement, comment fait-on pour trouver u et v tels

$$u^2 \equiv v^2 \pmod{n} \quad ?$$

Un exemple: $n = 11\,111$

On considère alors le polynôme $f(x) := x^2 - n$

L'approche de Maurice Kraitchik

Plus généralement, comment fait-on pour trouver u et v tels

$$u^2 \equiv v^2 \pmod{n} \quad ?$$

Un exemple: $n = 11\,111$

On considère alors le polynôme $f(x) := x^2 - n$

On pose $a = \lfloor \sqrt{n} \rfloor + 1 = 106$

L'approche de Maurice Kraitchik

Plus généralement, comment fait-on pour trouver u et v tels

$$u^2 \equiv v^2 \pmod{n} \quad ?$$

Un exemple: $n = 11\,111$

On considère alors le polynôme $f(x) := x^2 - n$

On pose $a = \lfloor \sqrt{n} \rfloor + 1 = 106$

On examine la suite $f(106), f(107), f(108), \ldots$, en conservant seulement les nombres $f(r)$ dont le plus grand facteur premier n'excède par 11

L'approche de Maurice Kraitchik

Rappelons que $n = 11\,111$ et $f(x) = x^2 - n$

L'approche de Maurice Kraitchik

Rappelons que $n = 11\,111$ et $f(x) = x^2 - n$

La suite $f(106), f(107), f(108), \ldots$, où on conserve exclusivement les nombres $f(r)$ dont le plus grand facteur premier n'excède par 11

L'approche de Maurice Kraitchik

Rappelons que $n = 11\,111$ et $f(x) = x^2 - n$

La suite $f(106), f(107), f(108), \ldots$, où on conserve exclusivement les nombres $f(r)$ dont le plus grand facteur premier n'excède par 11

donne

r	$f(r)$	factorisation de $f(r)$
106	125	$= 5^3$
109	770	$= 2 \times 5 \times 7 \times 11$
111	1210	$= 2 \times 5 \times 11^2$
122	3773	$= 7^3 \times 11$
131	6050	$= 2 \times 5^2 \times 11^2$

L'approche de Maurice Kraitchik

Rappelons que $n = 11\,111$ et $f(x) = x^2 - n$

La suite $f(106), f(107), f(108), \ldots$, où on conserve exclusivement les nombres $f(r)$ dont le plus grand facteur premier n'excède par 11

donne

r	$f(r)$	factorisation de $f(r)$
106	125	$= 5^3$
109	770	$= 2 \times 5 \times 7 \times 11$
111	1210	$= 2 \times 5 \times 11^2$
122	3773	$= 7^3 \times 11$
131	6050	$= 2 \times 5^2 \times 11^2$

Aucun carré parfait !

L'approche de Maurice Kraitchik

Rappelons que $n = 11\,111$ et $f(x) = x^2 - n$

La suite $f(106), f(107), f(108), \ldots$, où on conserve exclusivement les nombres $f(r)$ dont le plus grand facteur premier n'excède par 11

donne

r	$f(r)$	factorisation de $f(r)$
106	125	$= 5^3$
109	770	$= 2 \times 5 \times 7 \times 11$
111	1210	$= 2 \times 5 \times 11^2$
122	3773	$= 7^3 \times 11$
131	6050	$= 2 \times 5^2 \times 11^2$

Aucun carré parfait ! Malheur ?

L'approche de Maurice Kraitchik

r	$f(r)$	factorisation de $f(r)$
106	125	$= 5^3$
109	770	$= 2 \times 5 \times 7 \times 11$
111	1210	$= 2 \times 5 \times 11^2$
122	3773	$= 7^3 \times 11$
131	6050	$= 2 \times 5^2 \times 11^2$

L'approche de Maurice Kraitchik

r	$f(r)$	factorisation de $f(r)$
106	125	$= 5^3$
109	770	$= 2 \times 5 \times 7 \times 11$
111	1210	$= 2 \times 5 \times 11^2$
122	3773	$= 7^3 \times 11$
131	6050	$= 2 \times 5^2 \times 11^2$

On retient seulement les nombres $r_1, r_2, \ldots, r_k$ tels que le produit correspondant $f(r_1)f(r_2)\cdots f(r_k)$ est un carré parfait, disons v^2. En posant $u = r_1 r_2 \cdots r_k$, on aura alors

$$\begin{aligned} u^2 &= r_1^2 r_2^2 \cdots r_k^2 \equiv (r_1^2 - n)(r_2^2 - n)\cdots(r_k^2 - n) \\ &= f(r_1)f(r_2)\cdots f(r_k) = v^2 \pmod{n} \end{aligned}$$

L'approche de Maurice Kraitchik

r	$f(r)$	factorisation of $f(r)$
106	125	$= 5^3$
109	770	$= 2 \times 5 \times 7 \times 11$
111	1210	$= 2 \times 5 \times 11^2$
122	3773	$= 7^3 \times 11$
131	6050	$= 2 \times 5^2 \times 11^2$

L'approche de Maurice Kraitchik

r	$f(r)$	factorisation of $f(r)$
106	125	$= 5^3$
109	770	$= 2 \times 5 \times 7 \times 11$
111	1210	$= 2 \times 5 \times 11^2$
122	3773	$= 7^3 \times 11$
131	6050	$= 2 \times 5^2 \times 11^2$

Le produit des lignes 2, 3 et 4 donne le carré parfait $(2 \times 5 \times 7^2 \times 11^2)^2$

L'approche de Maurice Kraitchik

En effectuant le produit des lignes 2, 3 et 4, on obtient

$$\begin{aligned}
(r_2 \times r_3 \times r_4)^2 &\equiv f(r_2)f(r_3)f(r_4) \pmod{n},\\
(109 \times 111 \times 122)^2 &\equiv (2 \times 5 \times 7^2 \times 11^2)^2 \pmod{n},\\
9426^2 &\equiv 3735^2 \pmod{n},\\
(9426 - 3735) \times (9426 + 3735) &\equiv 0 \pmod{n},\\
5691 \times 13161 &\equiv 0 \pmod{n}.
\end{aligned}$$

L'approche de Maurice Kraitchik

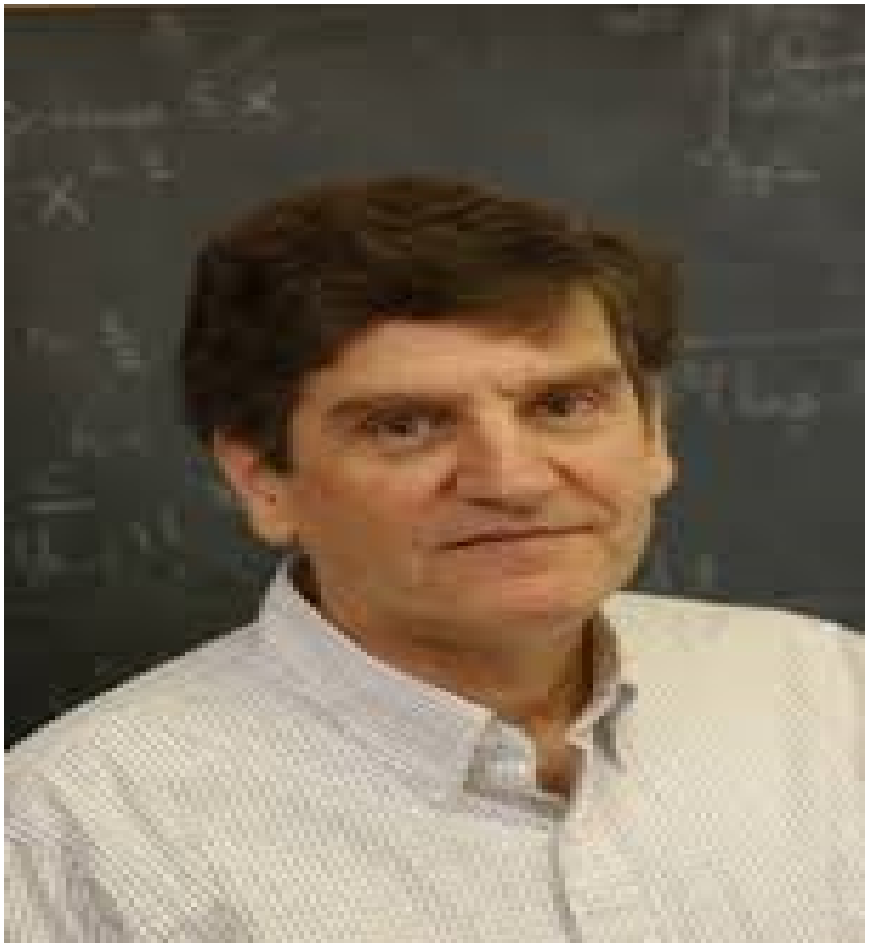
En effectuant le produit des lignes 2, 3 et 4, on obtient

$$\begin{aligned}
(r_2 \times r_3 \times r_4)^2 &\equiv f(r_2)f(r_3)f(r_4) \pmod{n},\\
(109 \times 111 \times 122)^2 &\equiv (2 \times 5 \times 7^2 \times 11^2)^2 \pmod{n},\\
9426^2 &\equiv 3735^2 \pmod{n},\\
(9426 - 3735) \times (9426 + 3735) &\equiv 0 \pmod{n},\\
5691 \times 13161 &\equiv 0 \pmod{n}.
\end{aligned}$$

Comme $\text{pgcd}(5691, n) = 271$ et $\text{pgcd}(13161, n) = 41$, on conclut que $n = 11\,111 = 41 \times 271$

Le crible quadratique – 1981

Le crible quadratique – 1981



Carl Pomerance

Le crible quadratique

Le crible quadratique

Pour factoriser n, au lieu de prendre $f(x) = x^2 - n$, on choisit

$$f(x) = (x + \lfloor \sqrt{n} \rfloor)^2 - n$$

Le crible quadratique

Pour factoriser n, au lieu de prendre $f(x) = x^2 - n$, on choisit

$$f(x) = (x + \lfloor \sqrt{n} \rfloor)^2 - n$$

Avantage: pour x petit, $f(x) \approx 2x\sqrt{n}$, donc petit

Le crible quadratique

Pour factoriser n, au lieu de prendre $f(x) = x^2 - n$, on choisit

$$f(x) = (x + \lfloor \sqrt{n} \rfloor)^2 - n$$

Avantage: pour x petit, $f(x) \approx 2x\sqrt{n}$, donc petit

Ce faisant, on arrive à factoriser un nombre n en seulement

$$e^{\sqrt{\log n \ \log\log n}} \quad \text{étapes}$$

Le crible quadratique

Pour factoriser n, au lieu de prendre $f(x) = x^2 - n$, on choisit

$$f(x) = (x + \lfloor \sqrt{n} \rfloor)^2 - n$$

Avantage: pour x petit, $f(x) \approx 2x\sqrt{n}$, donc petit

Ce faisant, on arrive à factoriser un nombre n en seulement

$$e^{\sqrt{\log n \ \log\log n}} \quad \text{étapes}$$

Exemple: $n \approx 10^{75}$; on a $n^{1/3} \approx 10^{25}$ et $e^{\sqrt{\log n \ \log\log n}} < 10^{13}$

Quels sont les compétiteurs du crible quadratique ?

Il y a essentiellement deux compétiteurs:

Quels sont les compétiteurs du crible quadratique ?

Il y a essentiellement deux compétiteurs:

- La méthode des courbes elliptiques de H.W. Lenstra

Quels sont les compétiteurs du crible quadratique ?

Il y a essentiellement deux compétiteurs:

- La méthode des courbes elliptiques de H.W. Lenstra
- La méthode du corps des nombres

La méthode des courbes elliptiques de Lenstra

La méthode des courbes elliptiques de Lenstra

- Elle provient de la méthode de Pollard $p-1$

La méthode des courbes elliptiques de Lenstra

- Elle provient de la méthode de Pollard $p-1$
- Or, celle-ci est basée sur le petit théorème de Fermat

La méthode des courbes elliptiques de Lenstra

- Elle provient de la méthode de Pollard $p-1$
- Or, celle-ci est basée sur le petit théorème de Fermat
- Rappelons le petit théorème de Fermat:

$$p > 2 \Longrightarrow 2^{p-1} \equiv 1 \pmod{p}$$

La méthode des courbes elliptiques de Lenstra

- Elle provient de la méthode de Pollard $p-1$
- Or, celle-ci est basée sur le petit théorème de Fermat
- Rappelons le petit théorème de Fermat:

$$p > 2 \Longrightarrow 2^{p-1} \equiv 1 \pmod{p}$$

- Exemple: avec $p = 5$, on a bien $2^{5-1} \equiv 1 \pmod{5}$

La méthode de Pollard $p-1$

La méthode de Pollard $p-1$

Soit n impair composé et soit $p \mid n$, où p est inconnu

La méthode de Pollard $p-1$

Soit n impair composé et soit $p \mid n$, où p est inconnu

Soit k un entier assez grand pour que $p-1 \mid k!$

La méthode de Pollard $p-1$

Soit n impair composé et soit $p \mid n$, où p est inconnu

Soit k un entier assez grand pour que $p-1 \mid k!$

Dans ce cas, puisque $2^{p-1} \equiv 1 \pmod{p}$, on a

$$2^{k!} = 2^{(p-1)\frac{k!}{p-1}} \equiv 1^{k!/(p-1)} = 1 \pmod{p}$$

de sorte que p divise $2^{k!}-1$

La méthode de Pollard $p-1$

Soit n impair composé et soit $p \mid n$, où p est inconnu

Soit k un entier assez grand pour que $p-1 \mid k!$

Dans ce cas, puisque $2^{p-1} \equiv 1 \pmod{p}$, on a

$$2^{k!} = 2^{(p-1)\frac{k!}{p-1}} \equiv 1^{k!/(p-1)} = 1 \pmod{p}$$

de sorte que p divise $2^{k!}-1$

Soit a la valeur de $2^{k!}-1 \pmod{n}$

La méthode de Pollard $p-1$

Soit n impair composé et soit $p \mid n$, où p est inconnu

Soit k un entier assez grand pour que $p-1 \mid k!$

Dans ce cas, puisque $2^{p-1} \equiv 1 \pmod{p}$, on a

$$2^{k!} = 2^{(p-1)\frac{k!}{p-1}} \equiv 1^{k!/(p-1)} = 1 \pmod{p}$$

de sorte que p divise $2^{k!}-1$

Soit a la valeur de $2^{k!}-1 \pmod{n}$

Comme $p \mid n$ et $p \mid a$, on a $p \mid \text{pgcd}(a,n)$

La méthode de Pollard $p-1$

La méthode de Pollard $p-1$

Exemple: Factoriser $2^{2^6}+1 = 18\,446\,744\,073\,709\,551\,617$

La méthode de Pollard $p-1$

Exemple: Factoriser $2^{2^6}+1 = 18\,446\,744\,073\,709\,551\,617$

En programmant avec Mathematica, on a

```
n=2^(2^6)+1;k=100;i=2;q=3;
While[i<=k,{q=PowerMod[q,i,n];i++}];a=q-1;p=GCD[a,n];
Print[p]
```

La méthode de Pollard $p-1$

Exemple: Factoriser $2^{2^6}+1 = 18\,446\,744\,073\,709\,551\,617$

En programmant avec Mathematica, on a

```
n=2^(2^6)+1;k=100;i=2;q=3;
While[i<=k,{q=PowerMod[q,i,n];i++}];a=q-1;p=GCD[a,n];
Print[p]
```

ce qui révèle le facteur premier $p = 274177$. Comme $n/p = 67280421310721$ est premier, on a obtenu

$$2^{2^6}+1 = 274\,177 \times 67\,280\,421\,310\,721$$

La méthode de Pollard $p-1$

Exemple: Factoriser $2^{2^6}+1 = 18\,446\,744\,073\,709\,551\,617$

En programmant avec Mathematica, on a

```
n=2^(2^6)+1;k=100;i=2;q=3;
While[i<=k,{q=PowerMod[q,i,n];i++}];a=q-1;p=GCD[a,n];
Print[p]
```

ce qui révèle le facteur premier $p = 274177$. Comme $n/p = 67280421310721$ est premier, on a obtenu

$$2^{2^6}+1 = 274\,177 \times 67\,280\,421\,310\,721$$

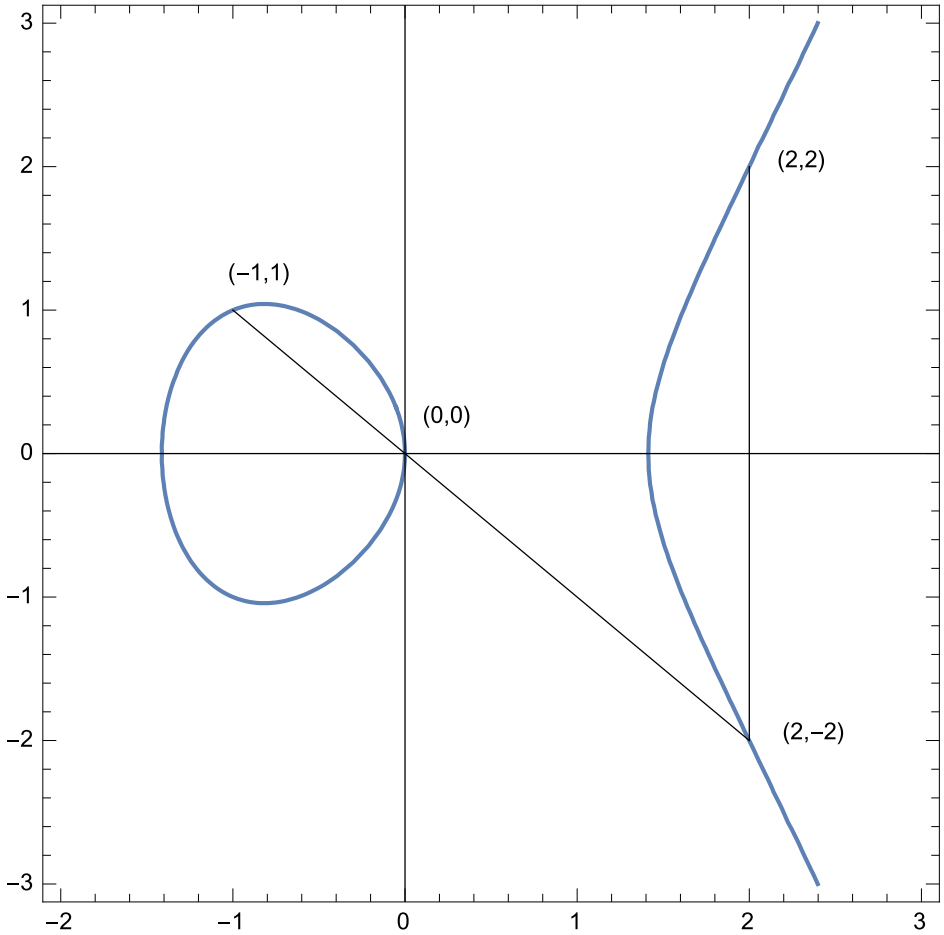
La méthode fonctionne bien parce que $p-1 = 274176 = 2^8 \cdot 3^3 \cdot 7 \cdot 17$

La méthode des courbes elliptiques de Lenstra

La méthode des courbes elliptiques de Lenstra

Hendrik W. Lenstra

La méthode des courbes elliptiques de Lenstra



$$y^2 = x^3 - 2x$$

La méthode des courbes elliptiques de Lenstra

La méthode des courbes elliptiques de Lenstra

Soit n un nombre à factoriser

La méthode des courbes elliptiques de Lenstra

Soit n un nombre à factoriser

On considère une courbe elliptique $E : y^2 = x^3 + ax + b$
et les points $P = (x, y)$ modulo n sur cette courbe

La méthode des courbes elliptiques de Lenstra

Soit n un nombre à factoriser

On considère une courbe elliptique $E : y^2 = x^3 + ax + b$
et les points $P = (x, y)$ modulo n sur cette courbe

On prend un point P sur cette courbe et on calcule

$$P, 2P, 3P, \ldots$$

jusqu'à ce que $kP = O$

La méthode des courbes elliptiques de Lenstra

Soit n un nombre à factoriser

On considère une courbe elliptique $E : y^2 = x^3 + ax + b$
et les points $P = (x, y)$ modulo n sur cette courbe

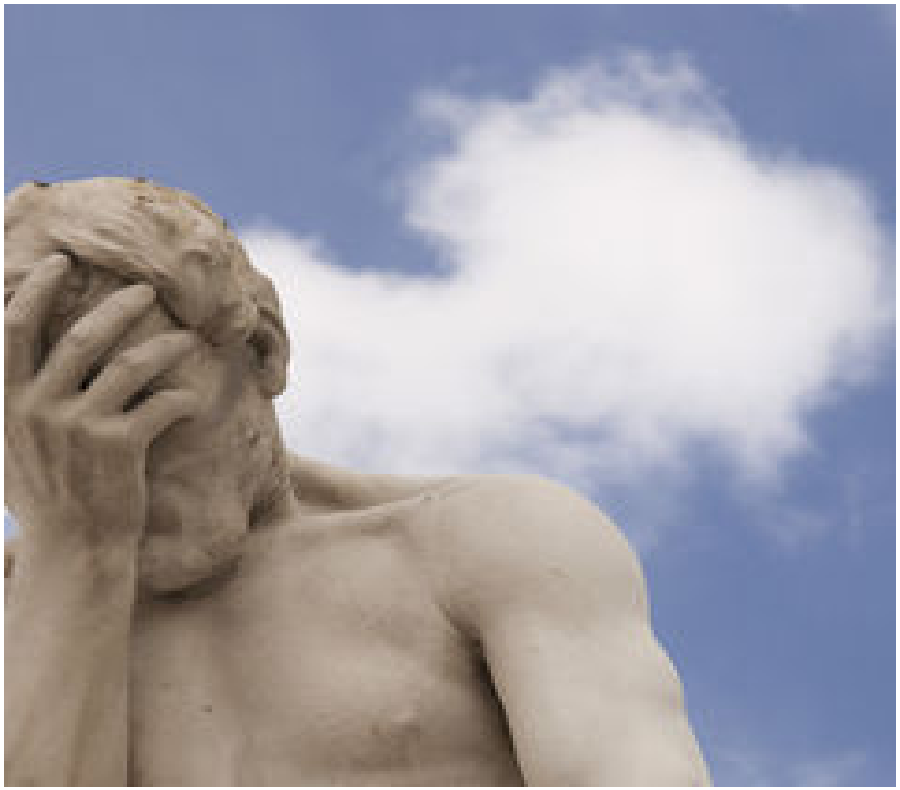
On prend un point P sur cette courbe et on calcule

$$P, 2P, 3P, \ldots$$

jusqu'à ce que $kP = O$

On en déduit un facteur de n

De quoi réfléchir...



Merci !

www.jeanmariedekoninck.mat.ulaval.ca