TP9 : Factorisation

Résumé du TP

Bertrand Meyer

21 avril 2020

Divisions successives

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, \ldots,$ possibles de n.

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, \ldots,$ possibles de n.

Factorisons, par exemple, $n = 15288$:

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, \ldots$, possibles de n.

Factorisons, par exemple, $n = 15288$:

d	n	facteurs
2	7644	2
	3822	2×2
	1911	$2 \times 2 \times 2$

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, \ldots$, possibles de n.

Factorisons, par exemple, $n = 15288$:

d	n	facteurs
2	7644	2
	3822	2×2
	1911	$2 \times 2 \times 2$
3	637	$2 \times 2 \times 2 \times 3$

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, \dots,$ possibles de n.

Factorisons, par exemple, $n = 15288$:

d	n	facteurs
2	7644	2
	3822	2×2
	1911	$2 \times 2 \times 2$
3	637	$2 \times 2 \times 2 \times 3$
4	637	$2 \times 2 \times 2 \times 3$

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, \ldots,$ possibles de n.

Factorisons, par exemple, $n = 15288$:

d	n	facteurs
2	7644	2
	3822	2×2
	1911	$2 \times 2 \times 2$
3	637	$2 \times 2 \times 2 \times 3$
4	637	$2 \times 2 \times 2 \times 3$
5	637	$2 \times 2 \times 2 \times 3$

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, \ldots$, possibles de n.

Factorisons, par exemple, $n = 15288$:

d	n	facteurs
2	7644	2
	3822	2×2
	1911	$2 \times 2 \times 2$
3	637	$2 \times 2 \times 2 \times 3$
4	637	$2 \times 2 \times 2 \times 3$
5	637	$2 \times 2 \times 2 \times 3$
6	637	$2 \times 2 \times 2 \times 3$

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, ...,$ possibles de n.

Factorisons, par exemple, $n = 15288$:

d	n	facteurs
2	7644	2
	3822	2×2
	1911	$2 \times 2 \times 2$
3	637	$2 \times 2 \times 2 \times 3$
4	637	$2 \times 2 \times 2 \times 3$
5	637	$2 \times 2 \times 2 \times 3$
6	637	$2 \times 2 \times 2 \times 3$
7	91	$2 \times 2 \times 2 \times 3 \times 7$
	13	$2 \times 2 \times 2 \times 3 \times 7 \times 7$

Divisions successives pour factoriser n

On épuise les diviseurs $d = 2, 3, 4, 5, 6, \ldots$, possibles de n.

Factorisons, par exemple, $n = 15288$:

d	n	facteurs
2	7644	2
	3822	2×2
	1911	$2 \times 2 \times 2$
3	637	$2 \times 2 \times 2 \times 3$
4	637	$2 \times 2 \times 2 \times 3$
5	637	$2 \times 2 \times 2 \times 3$
6	637	$2 \times 2 \times 2 \times 3$
7	91	$2 \times 2 \times 2 \times 3 \times 7$
	13	$2 \times 2 \times 2 \times 3 \times 7 \times 7$

Les facteurs sont $13 \times 2 \times 2 \times 2 \times 3 \times 7 \times 7$.

Divisions successives pour factoriser n

On peut aller plus vite en considérant $d = 2$ puis les diviseurs impairs uniquement $d = 3, 5, 7, 9, \ldots,$ possibles de n.

On peut aller encore plus vite en considérant $d = 2$ et $d = 3$ puis les diviseurs non-divisibles par 2 ou 3 uniquement $d = 5, 7, 11, 13, 17 \ldots,$ possibles de n, que l'on obtient par incrément alternatif de 2 ou de 4.

Etc. en privilégiant les k premiers diviseurs au lieu des 2 premiers.

Méthode ρ de Pollard

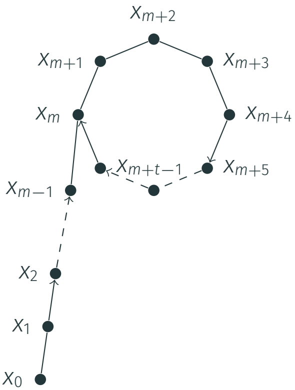
Méthode ρ de Pollard

On veut factoriser $n = p \times q$.

Méthode ρ de Pollard

On veut factoriser $n = p \times q$.

La suite $(x_n)_{n\in\mathbb{N}}$ engendrée par $x \leftarrow x^2 + 1$ boucle dans $\mathbb{Z}/n\mathbb{Z}$.

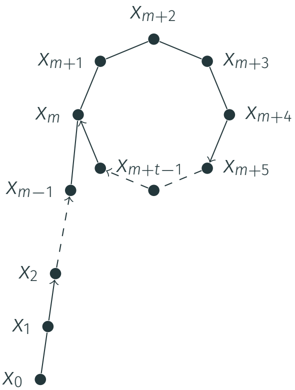


Méthode ρ de Pollard

On veut factoriser $n = p \times q$.

La suite $(x_n)_{n\in\mathbb{N}}$ engendrée par $x \leftarrow x^2 + 1$ boucle dans $\mathbb{Z}/n\mathbb{Z}$.

Les termes étant plutôt uniformément distribuée dans $\mathbb{Z}/p\mathbb{Z}$, on doit y trouver deux termes x_k et $x_{k'}$ égaux modulo p assez vite ($O(\sqrt{p})$ selon le paradoxe des ).

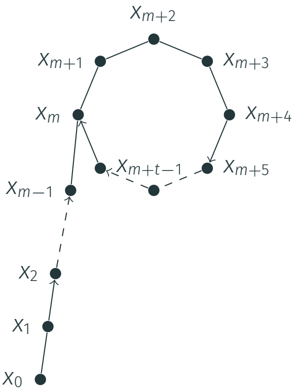


Méthode ρ de Pollard

On veut factoriser $n = p \times q$.

La suite $(x_n)_{n\in\mathbb{N}}$ engendrée par $x \leftarrow x^2 + 1$ boucle dans $\mathbb{Z}/n\mathbb{Z}$.
Les termes étant plutôt uniformément distribuée dans $\mathbb{Z}/p\mathbb{Z}$, on doit y trouver deux termes x_k et $x_{k'}$ égaux modulo p assez vite ($O(\sqrt{p})$ selon le paradoxe des ).

$$x_k \equiv x_{k'} \bmod p \Rightarrow (x_k - x_{k'}) \wedge n \text{ divise } n$$



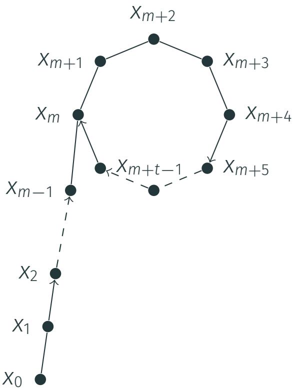
Méthode ρ de Pollard

On veut factoriser $n = p \times q$.

La suite $(x_n)_{n\in\mathbb{N}}$ engendrée par $x \leftarrow x^2 + 1$ boucle dans $\mathbb{Z}/n\mathbb{Z}$.
Les termes étant plutôt uniformément distribuée dans $\mathbb{Z}/p\mathbb{Z}$, on doit y trouver deux termes x_k et $x_{k'}$ égaux modulo p assez vite ($O(\sqrt{p})$ selon le paradoxe des 🎂).

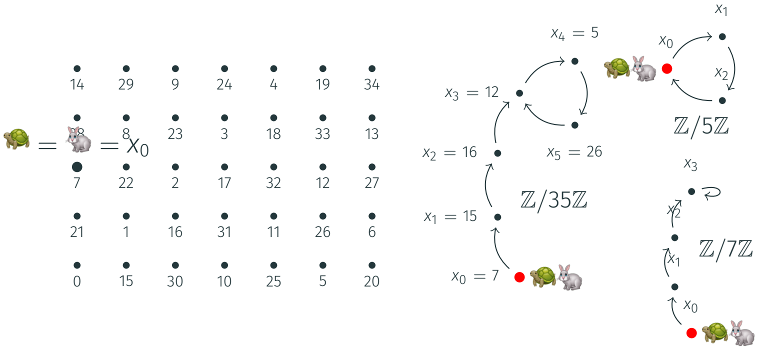
$$x_k \equiv x_{k'} \bmod p \Rightarrow (x_k - x_{k'}) \wedge n \text{ divise } n$$

k et k' s'obtiennent avec l'algorithme du 🐇 et de la 🐢.



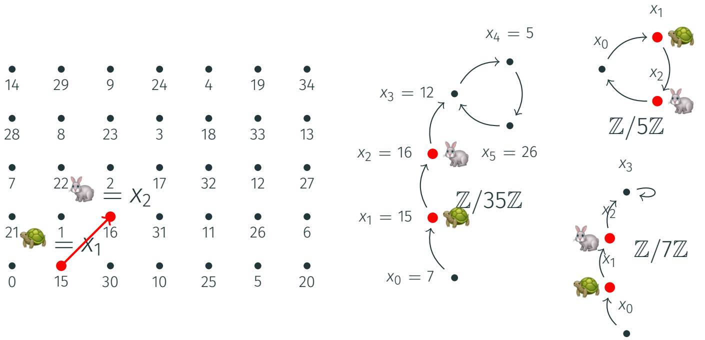
Exemple (factorisons $n = 35$ en partant de $x_0 = 7$)

Étape 0 : 🐢 $= x_0 = 7$, 🐇 $= x_0 = 7$



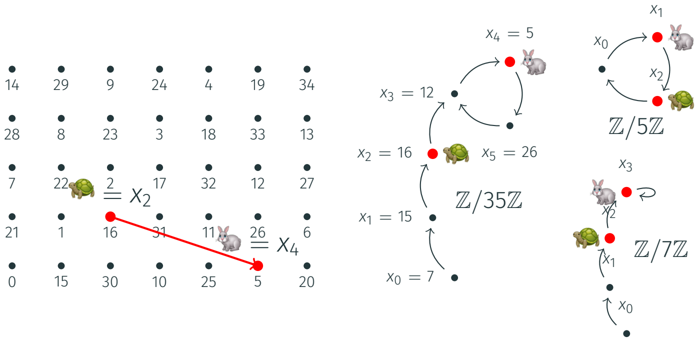
Exemple (factorisons $n = 35$ en partant de $x_0 = 7$)

Étape 1 : 🐢 $= x_1 = 15$, 🐇 $= x_2 = 16$, (🐇 − 🐢) $\wedge\, n = 1$



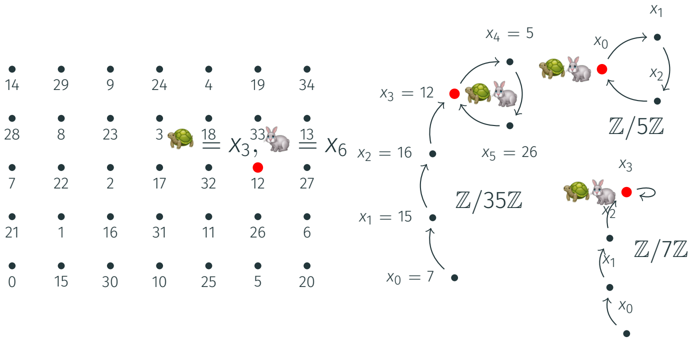
Exemple (factorisons $n = 35$ en partant de $x_0 = 7$)

Étape 2 : 🐢 $= x_1 = 16$, 🐇 $= x_2 = 5$, (🐇 − 🐢) $\wedge\, n = 1$



Exemple (factorisons $n = 35$ en partant de $x_0 = 7$)

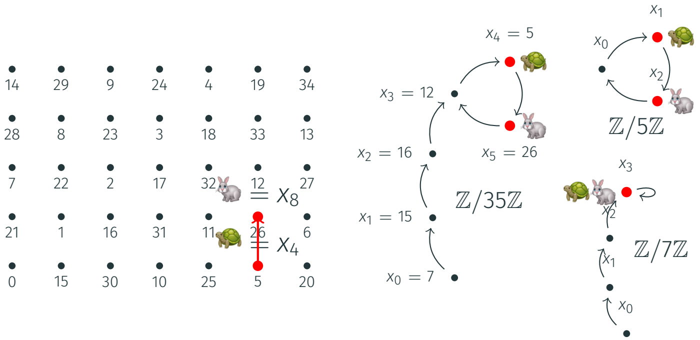
Étape 3 : 🐢 $= x_2 = 12$, 🐇 $= x_4 = 12$, (🐇 − 🐢) $\wedge n = 0$



Méthode ρ de Pollard

Exemple (factorisons $n = 35$ en partant de $x_0 = 7$)

Étape 4 : 🐢 $= x_3 = 5$, 🐇 $= x_6 = 26$, (🐇 $-$ 🐢) $\wedge\, n = 7$



On a repéré un cycle dans $\mathbb{Z}/7ZZ$ et non dans $\mathbb{Z}/5\mathbb{Z}$ ce qui donne un facteur.

Méthode $p-1$ de Pollard

Méthode $p-1$ de Pollard

Petit théorème de Fermat
Si p est premier, alors, pour tout a,

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

Si p est un facteur de n, alors $(a^{\lambda\cdot(p-1)} - 1) \wedge n$ est divisible par p.

Méthode $p-1$ de Pollard

Petit théorème de Fermat
Si p est premier, alors, pour tout a,

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

Si p est un facteur de n, alors $(a^{\lambda\cdot(p-1)} - 1) \wedge n$ est divisible par p.

Méthode $p-1$ de Pollard
Pour a quelconque, calculer

$$(a^m - 1) \wedge n$$

pour des petites valeurs de m, disons $m = \mathrm{ppcm}\{1, 2, 3, \ldots, b\}$ pour un certain b.

Méthode $p-1$ de Pollard

Petit théorème de Fermat
Si p est premier, alors, pour tout a,

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

Si p est un facteur de n, alors $(a^{\lambda\cdot(p-1)} - 1) \wedge n$ est divisible par p.

Méthode $p-1$ de Pollard
Pour a quelconque, calculer

$$(a^m - 1) \wedge n$$

pour des petites valeurs de m, disons $m = \mathrm{ppcm}\{1, 2, 3, \ldots, b\}$ pour un certain b.

On attrape les diviseurs p de n tels que $p-1$ est b-ultrafriable.

Crible quadratique

Crible quadratique

💭 Si y et z vérifient

$$y^2 \equiv z^2 \mod n,$$

alors

$$(y - z) \times (y + z) \equiv 0 \mod n$$

peut révéler une factorisation de n par pgcd.

Crible quadratique

💭 Si y et z vérifient

$$y^2 \equiv z^2 \mod n,$$

alors

$$(y - z) \times (y + z) \equiv 0 \mod n$$

peut révéler une factorisation de n par pgcd.

👀 y et z : on génère des carrés et on combine des produits de leur réduction modulo n pour trouver un autre carré.

Crible quadratique

💭 Si y et z vérifient

$$y^2 \equiv z^2 \mod n,$$

alors

$$(y - z) \times (y + z) \equiv 0 \mod n$$

peut révéler une factorisation de n par pgcd.

👀 y et z : on génère des carrés et on combine des produits de leur réduction modulo n pour trouver un autre carré.

On 🕵️ cet autre carré via de l'algèbre linéaire dans $\mathbb{F}_2$ sur les exposants en se restreignant à une base de petits premiers.

Crible quadratique sur un exemple

Factorisons $n = 2886$.

Crible quadratique sur un exemple

Factorisons $n = 2886$. Avec $\sqrt{n} \simeq 53,7$.

$$\begin{cases} x_0 &= 54^2 = 2916 \equiv 30 \mod n \\ x_1 &= 55^2 = 3025 \equiv 139 \mod n \\ x_2 &= 56^2 = 3136 \equiv 250 \mod n \\ x_3 &= 57^2 = 3249 \equiv 363 \mod n \\ \vdots \end{cases}$$

Crible quadratique sur un exemple

Factorisons $n = 2886$.

$$\begin{cases} x_0 & = & 54^2 = 2916 \equiv 30 & = & 2 \cdot 3 \cdot 5 & = & a_0 & \mod n \\ x_1 & = & 55^2 = 3025 \equiv 139 & = & 139 & = & a_1 & \mod n \\ x_2 & = & 56^2 = 3136 \equiv 250 & = & 2 \cdot 5^3 & = & a_2 & \mod n \\ x_3 & = & 57^2 = 3249 \equiv 363 & = & 3 \cdot 11^2 & = & a_3 & \mod n \\ \vdots \end{cases}$$

On fixe $\{2, 3, 5, 7, 11\}$ comme base de friabilité.

Crible quadratique sur un exemple

Factorisons $n = 2886$.

$$\begin{cases} x_0 & = & 54^2 = 2916 \equiv 30 & = & 2 \cdot 3 \cdot 5 & = & a_0 & \mod n \\ \cancel{x_1} & = & \cancel{55^2 = 3025} \equiv \cancel{139} & = & \cancel{139} & = & \cancel{a_1} & \mod n \\ x_2 & = & 56^2 = 3136 \equiv 250 & = & 2 \cdot 5^3 & = & a_2 & \mod n \\ x_3 & = & 57^2 = 3249 \equiv 363 & = & 3 \cdot 11^2 & = & a_3 & \mod n \\ \vdots & & & & & & & \end{cases}$$

On fixe $\{2, 3, 5, 7, 11\}$ comme base de friabilité.

Crible quadratique sur un exemple

Factorisons $n = 2886$.

$$\begin{cases} x_0 & = & 54^2 = 2916 \equiv 30 & = & 2 \cdot 3 \cdot 5 & = & a_0 & \mod n \\ \cancel{x_1} & = & \cancel{55^2 = 3025} \equiv \cancel{139} & = & \cancel{139} & = & \cancel{a_1} & \mod n \\ x_2 & = & 56^2 = 3136 \equiv 250 & = & 2 \cdot 5^3 & = & a_2 & \mod n \\ x_3 & = & 57^2 = 3249 \equiv 363 & = & 3 \cdot 11^2 & = & a_3 & \mod n \\ \vdots & & & & & & & \end{cases}$$

On fixe $\{2, 3, 5, 7, 11\}$ comme base de friabilité.

On résoud le système dans $\mathbb{F}_2$

$$\begin{cases} e_0 + e_2 & = & 0 & \text{(puissances de 2)} \\ e_0 + e_3 & = & 0 & \text{(puissances de 3)} \\ e_0 + 3e_2 & = & 0 & \text{(puissances de 5)} \\ 2e_3 & = & 0 & \text{(puissances de 11)} \end{cases}$$

Crible quadratique sur un exemple

Factorisons $n = 2886$.

$$\begin{cases} x_0 & = & 54^2 = 2916 \equiv 30 & = & 2 \cdot 3 \cdot 5 & = & a_0 & \mod n \\ \cancel{x_1} & = & \cancel{55^2 = 3025} \equiv \cancel{139} & = & \cancel{139} & = & \cancel{a_1} & \mod n \\ x_2 & = & 56^2 = 3136 \equiv 250 & = & 2 \cdot 5^3 & = & a_2 & \mod n \\ x_3 & = & 57^2 = 3249 \equiv 363 & = & 3 \cdot 11^2 & = & a_3 & \mod n \\ \vdots \end{cases}$$

On fixe $\{2, 3, 5, 7, 11\}$ comme base de friabilité.
Le produit $a_0 a_2 a_3$ a des exposants pairs.

Crible quadratique sur un exemple

Factorisons $n = 2886$.

$$\begin{cases} x_0 & = & 54^2 = 2916 \equiv 30 & = & 2 \cdot 3 \cdot 5 & = & a_0 & \mod n \\ \cancel{x_1} & = & \cancel{55^2 = 3025} \equiv \cancel{139} & = & \cancel{139} & = & \cancel{a_1} & \mod n \\ x_2 & = & 56^2 = 3136 \equiv 250 & = & 2 \cdot 5^3 & = & a_2 & \mod n \\ x_3 & = & 57^2 = 3249 \equiv 363 & = & 3 \cdot 11^2 & = & a_3 & \mod n \\ \vdots \end{cases}$$

On fixe $\{2, 3, 5, 7, 11\}$ comme base de friabilité.
Le produit $a_0 a_2 a_3$ a des exposants pairs. On a trouvé la relation

$$2094^2 = (54 \cdot 56 \cdot 57)^2 \equiv \left(2 \cdot 3 \cdot 5^2 \cdot 11\right)^2 = 1650^2 \mod n.$$

Crible quadratique sur un exemple

Factorisons $n = 2886$.

$$\begin{cases} x_0 & = & 54^2 = 2916 \equiv 30 & = & 2 \cdot 3 \cdot 5 & = & a_0 & \bmod n \\ \cancel{x_1} & = & \cancel{55^2 = 3025} \equiv \cancel{139} & = & \cancel{139} & = & \cancel{a_1} & \bmod n \\ x_2 & = & 56^2 = 3136 \equiv 250 & = & 2 \cdot 5^3 & = & a_2 & \bmod n \\ x_3 & = & 57^2 = 3249 \equiv 363 & = & 3 \cdot 11^2 & = & a_3 & \bmod n \\ \vdots \end{cases}$$

On fixe $\{2, 3, 5, 7, 11\}$ comme base de friabilité.
Le produit $a_0 a_2 a_3$ a des exposants pairs. On a trouvé la relation

$$2094^2 = (54 \cdot 56 \cdot 57)^2 \equiv \left(2 \cdot 3 \cdot 5^2 \cdot 11\right)^2 = 1650^2 \mod n.$$

Or $(2094 - 1650) \wedge n = 13$. D'où une factorisation de $n = 13 \cdot 222$.

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T														

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	1	1	1	1	1	1	1	1	1	1	1	1	1	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/2\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	1	1	1	1	1	1	1	1	1	1	1	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/2\mathbb{Z}$

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x + 54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	1	1	1	1	1	1	1	1	1	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/2\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	1	1	1	1	1	1	1	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/2\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	2	1	1	1	1	1	1	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/2\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \dots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	2	1	2	1	1	1	1	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/2\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	2	1	2	1	2	1	1	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/2\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x + 54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	2	1	2	1	2	1	2	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/2\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	2	1	2	1	2	1	2	1

$f(x)$ ne s'annule pas dans $\mathbb{Z}/4\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	2	1	2	1	2	1	2	1

$f(x)$ ne s'annule pas dans $\mathbb{Z}/4\mathbb{Z}$

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	2	1	2	1	2	1	2	1

$f(x)$ ne s'annule pas dans $\mathbb{Z}/4\mathbb{Z}$

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	2	1	2	1	2	1	2	1	2	1	2	1	2	1

$f(x)$ ne s'annule pas dans $\mathbb{Z}/4\mathbb{Z}$

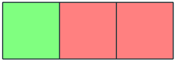
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x + 54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	6	1	2	1	2	1	2	1	2	1	2	1	2	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/3\mathbb{Z}$



Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x + 54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	6	1	2	3	2	1	2	1	2	1	2	1	2	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/3\mathbb{Z}$

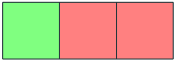
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	6	1	2	3	2	1	6	1	2	1	2	1	2	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/3\mathbb{Z}$



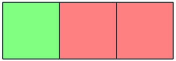
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	6	1	2	3	2	1	6	1	2	3	2	1	2	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/3\mathbb{Z}$



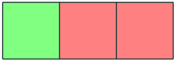
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	6	1	2	3	2	1	6	1	2	3	2	1	6	1

$f(x)$ s'annule en 0 dans $\mathbb{Z}/3\mathbb{Z}$



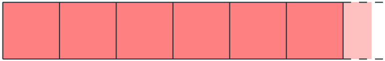
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x + 54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	6	1	2	3	2	1	6	1	2	3	2	1	6	1

$f(x)$ ne s'annule pas dans $\mathbb{Z}/9\mathbb{Z}$



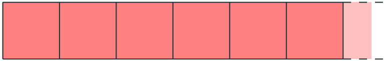
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	6	1	2	3	2	1	6	1	2	3	2	1	6	1

$f(x)$ ne s'annule pas dans $\mathbb{Z}/9\mathbb{Z}$



Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	30	1	10	3	2	1	6	1	2	3	2	1	6	1

$f(x)$ s'annule en 0 et 2 dans $\mathbb{Z}/5\mathbb{Z}$

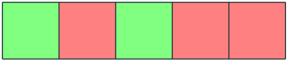
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x + 54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	30	1	10	3	2	5	6	5	2	3	2	1	6	1

$f(x)$ s'annule en 0 et 2 dans $\mathbb{Z}/5\mathbb{Z}$



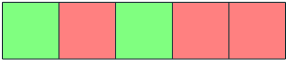
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	30	1	10	3	2	5	6	5	2	3	10	1	30	1

$f(x)$ s'annule en 0 et 2 dans $\mathbb{Z}/5\mathbb{Z}$



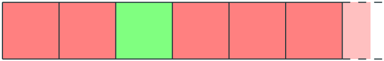
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	30	1	50	3	2	5	6	5	2	3	10	1	30	1

$f(x)$ s'annule en 2 et 15 dans $\mathbb{Z}/25\mathbb{Z}$



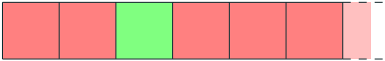
Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots .$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	30	1	250	3	2	5	6	5	2	3	10	1	30	1

$f(x)$ s'annule en 2 et 15 dans $\mathbb{Z}/125\mathbb{Z}$



Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	30	1	250	363	2	35	42	5	2	3	1210	1	1470	7

Et ainsi de suite pour tout $p \leq 11$.

Cribler pour factoriser

Nous voulons repérer les nombres 11-friables parmi

$$f(x) = (x+54)^2 - 2886 \quad \text{pour } x = 0, 1, 2 \ldots.$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f(x)	30	139	250	363	478	595	714	835	958	1083	1210	1339	1470	1603
T	30	1	250	363	2	35	42	5	2	3	1210	1	1470	7

On repère les termes friables : $f(0), f(2), f(3), f(10), f(12)$.