Alexandre Junod
Lycée Denis-de-Rougemont (Neuchâtel), alexandre.junod@rpn.ch

Congruences entre les nombres de Fibonacci

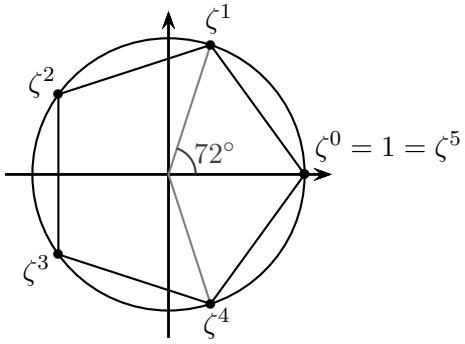
Cet article est dédié à Alain M. Robert, Professeur émérite de l'Université de Neuchâtel, décédé le 7 mars 2025 à l'âge de 83 ans. Auteur de nombreuses publications, dont des ouvrages de référence en analyse non standard et en analyse p-adique, il a dirigé plusieurs thèses concernant des congruences.

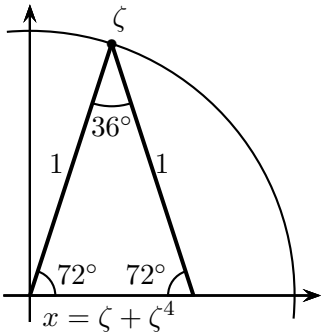
Un nombre premier p et un entier $n \geqslant 1$ étant donnés, nous établissons entre les nombres de Fibonacci quelques congruences modulo $np\mathbb{Z}_{(p)}$, où $\mathbb{Z}_{(p)}$ est l'ensemble des nombres rationnels dont le dénominateur n'est pas divisible par p. Un lien avec les périodes de Pisano est ensuite établi.

1 La formule de Binet revisitée

Les nombres de Fibonacci sont définis par $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-2} + F_{n-1}$ pour tout entier $n \geqslant 2$. La formule de Binet permet d'exprimer $F_n = \frac{1}{\sqrt{5}}(\varphi^n - \widehat{\varphi}^n)$, où $\varphi > \widehat{\varphi}$ sont les solutions de l'équation $x^2 = x + 1$. Elle peut être démontrée facilement par soustraction avec les relations $\varphi^n = F_n\varphi + F_{n-1}$ et $\widehat{\varphi}^n = F_n\widehat{\varphi} + F_{n-1}$ pour $n \geqslant 1$ (voir [1]). Nous donnons une reformulation à l'aide des racines cinquièmes de l'unité, en nous basant sur un échange trouvé dans un forum sur internet (`https://math.stackexchange.com/questions/3162413`).

D'un point de vue géométrique, les puissances de $\zeta = \cos(72°) + i\sin(72°)$ forment sur le cercle trigonométrique un pentagone régulier symétrique par rapport à l'axe réel (voir la figure de gauche ci-dessous). On a la relation $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$ car $z = \zeta$, qui ne vaut pas 1, annule le polynôme $P(z) = z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1)$.





Le nombre $x = \zeta + \zeta^4 = \zeta + \overline{\zeta} = 2\,\mathrm{Re}(\zeta) = 2\cos(72°)$ est un réel positif et on peut remarquer que $x^2 + x - 1 = (\zeta^2 + 2\zeta^5 + \zeta^8) + (\zeta + \zeta^4) - 1 = \zeta^2 + 2 + \zeta^3 + \zeta + \zeta^4 - 1 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$. On en déduit que $x = \frac{-1+\sqrt{5}}{2}$ (l'autre solution de l'équation $x^2 + x - 1 = 0$ est négative) et donc

$$\frac{1}{\sqrt{5}} = \frac{\sqrt{5}}{5} = \frac{2x+1}{5}, \qquad \varphi = \frac{1+\sqrt{5}}{2} = 1 + x, \qquad \widehat{\varphi} = \frac{1-\sqrt{5}}{2} = -x.$$

Comme $x = \zeta + \zeta^4 = -(1 + \zeta^2 + \zeta^3)$, la formule de Binet devient

$$F_n = \frac{1 + 2\zeta + 2\zeta^4}{5}\left((1 + \zeta + \zeta^4)^n - (1 + \zeta^2 + \zeta^3)^n\right).$$

Comme $(1+\zeta+\zeta^4)(1+\zeta^2+\zeta^3) = (1+x)(-x) = -(x^2+x) = -1$, les nombres $1+\zeta+\zeta^4$ et $-(1+\zeta^2+\zeta^3)$ sont inverses réciproques. On retrouve ainsi la relation $F_{-n} = (-1)^{n+1}F_n$ pour tout entier $n \geqslant 0$.

2 Congruences

On considère de manière générale un ensemble $\mathcal{A}$ muni de trois lois de composition :

- une "addition" $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$ $((x;y) \mapsto x+y)$ commutative, associative, qui admet un élément neutre (noté $0_{\mathcal{A}}$) et telle que tout élément $x \in \mathcal{A}$ admet un inverse (noté $-x$) dans $\mathcal{A}$,
- une "multiplication externe" $\mathbb{Z} \times \mathcal{A} \to \mathcal{A}$ $((n;x) \mapsto n \cdot x)$, définie par $0 \cdot x = 0_{\mathcal{A}}$, $n \cdot x = \underbrace{x+x+\ldots+x}_{n \text{ termes}}$ et $(-n)\cdot x = n \cdot (-x)$ si $n > 0$,
- une "multiplication interne" $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$ $((x;y) \mapsto xy)$ qui est associative et $\mathbb{Z}$-bilinéaire, c'est-à-dire telle que $(m \cdot x_1 + x_2)(n \cdot y_1 + y_2) = mn \cdot (x_1y_1) + m \cdot (x_1y_2) + n \cdot (x_2y_1) + (x_2y_2)$ pour tous les nombres $m, n \in \mathbb{Z}$ et éléments $x_i, y_i \in \mathcal{A}$.

On note $\mathcal{A}_{(p)} = \left\{ \frac{a}{b} \ : \ a \in \mathcal{A},\ b \in \mathbb{Z} \setminus p\mathbb{Z} \right\}$ (anneau de fractions formelles). Par exemple, si $\mathcal{A} = \mathbb{Z}$, alors $\mathcal{A}_{(p)} = \mathbb{Z}_{(p)}$ est l'ensemble des nombres rationnels dont le dénominateur n'est pas divisible par p ("nombres p-entiers"). Au niveau des ensembles de polynômes, si $\mathcal{A} = \mathbb{Z}[x]$, alors $\mathcal{A}_{(p)} = \mathbb{Z}_{(p)}[x]$.

Proposition. On considère un nombre premier p, deux entiers $m, n \geqslant 0$ ainsi que deux éléments $\alpha, \beta \in \mathcal{A}$ qui commutent (c'est-à-dire tels que $\alpha\beta = \beta\alpha$). Si m est divisible par p et si $\alpha \equiv \beta \mod m\mathcal{A}$, alors $\alpha^n \equiv \beta^n \mod mn\mathcal{A}_{(p)}$. La congruence est valable modulo $mn\mathcal{A}$ si n est une puissance de p.

PREUVE. Les conditions initiales permettent d'écrire $\alpha = \beta + m\gamma$ où γ est un élément de $\mathcal{A}$ qui commute avec β. Comme p divise m, on a

$$\alpha^p \ = \ \sum_{k=0}^{p} \binom{p}{k} \beta^{p-k} m^k \gamma^k \ = \ \beta^p + mp\beta^{p-1}\gamma + m^2(\ldots) \ = \ \beta^p + mp\tilde{\gamma} \ \text{ avec } \tilde{\gamma} \in \mathcal{A}.$$

On a donc $\alpha^p \equiv \beta^p \mod mp\mathcal{A}$ et, par induction, $\alpha^{p^k} \equiv \beta^{p^k} \mod mp^k\mathcal{A}$ pour tout entier $k \geqslant 0$. En écrivant $n = lp^k$ avec l non divisible par p, on obtient ainsi $\alpha^n = (\alpha^{p^k})^l \equiv (\beta^{p^k})^l = \beta^n \mod mp^k\mathcal{A}$. Comme $\mathcal{A} \subset \mathcal{A}_{(p)}$, la congruence est valable modulo $mp^k\mathcal{A}_{(p)}$ et comme p ne divise pas l, on a $\mathcal{A}_{(p)} = l\mathcal{A}_{(p)}$. La congruence est donc valable modulo $mn\mathcal{A}_{(p)}$. □

Exemple 1. La congruence $5^n \equiv 1+4n$ modulo $8n\mathbb{Z}$ est valable pour $n = 1$ et pour toute puissance de deux car elle impliquerait (avec la proposition) que $5^{2n} \equiv (1+4n)^2 = 1+8n+16n^2 \equiv 1+8n$ modulo $16n\mathbb{Z}$ (on conclut par induction).

Exemple 2. La congruence $(1+x)^p \equiv 1+x^p \mod p\mathbb{Z}[x]$ est bien connue :

pour $k \in \{1, 2, \ldots, p-1\}$, le coefficient binomial $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$ se trouve dans $\mathbb{Z} \cap p\mathbb{Z}_{(p)} = p\mathbb{Z}$.

Avec la proposition, on a alors $(1+x)^{np} \equiv (1+x^p)^n \mod np\mathbb{Z}_{(p)}[x]$ pour tout entier $n \geqslant 0$. Cela signifie que $\binom{np}{kp} \equiv \binom{n}{k} \mod np\mathbb{Z}_{(p)}$ alors que $\binom{np}{k} \equiv 0 \mod np\mathbb{Z}_{(p)}$ si p ne divise pas k.

Exemple 3. Reprenant le contexte de la section 1, on considère $\mathcal{A} = \mathbb{Z}[\zeta]$, des entiers $a, b, n \geqslant 1$ et un nombre premier $p \neq 5$. Les nombres de Fibonacci sont alors des éléments de $\mathcal{A}_{(p)}$. Comme

$$(1+\zeta^a+\zeta^b)^p \equiv 1+(\zeta^a+\zeta^b)^p \equiv 1+\zeta^{ap}+\zeta^{bp} \mod p\mathcal{A},$$

on a $(1+\zeta^a+\zeta^b)^{np} \equiv (1+\zeta^{ap}+\zeta^{bp})^n \mod np\mathcal{A}_{(p)}$. On peut ainsi écrire

$$\begin{aligned} F_{np} &= \frac{1+2\zeta+2\zeta^4}{5}\left((1+\zeta+\zeta^4)^{np}-(1+\zeta^2+\zeta^3)^{np}\right) \\ &\equiv \frac{1+2\zeta+2\zeta^4}{5}\left((1+\zeta^p+\zeta^{4p})^n-(1+\zeta^{2p}+\zeta^{3p})^n\right) \mod np\mathcal{A}_{(p)}. \end{aligned}$$

Comme $\zeta^5 = 1$, on peut réduire modulo 5 les exposants de ζ. Si $p \equiv 1$ ou $p \equiv 4$ modulo 5, on a

$$F_{np} \equiv \frac{1+2\zeta+2\zeta^4}{5}\left((1+\zeta+\zeta^4)^n-(1+\zeta^2+\zeta^3)^n\right) = F_n \mod np\mathcal{A}_{(p)},$$

alors que si $p \equiv 2$ ou $p \equiv 3$ modulo 5, on obtient

$$F_{np} \equiv \frac{1+2\zeta+2\zeta^4}{5}\left((1+\zeta^2+\zeta^3)^n-(1+\zeta+\zeta^4)^n\right) = -F_n \mod np\mathcal{A}_{(p)}.$$

Les congruences finales $F_{np} \equiv \pm F_n$ modulo $np\mathbb{Z}_{(p)}[\zeta]$ mettent en relation des nombres entiers, elles sont donc valables modulo $np\mathbb{Z}_{(p)}$ sans référence à ζ. On a la reformulation suivante (pour $n \geqslant 1$).

$\dfrac{F_{np}-F_n}{np}$ est p-entier si $p \equiv \pm 1$ modulo 5, $\qquad$ $\dfrac{F_{np}+F_n}{np}$ est p-entier si $p \equiv \pm 2$ modulo 5.

Avec $n = 1$, on trouve un résultat plus connu : $F_p - 1$ est divisible par p lorsque $p \equiv \pm 1$ modulo 5, alors que $F_p + 1$ est divisible par p lorsque $p \equiv \pm 2$ modulo 5.

Améliorations. On peut écrire $(1+\zeta^a+\zeta^b)^{m+np} \equiv (1+\zeta^a+\zeta^b)^m(1+\zeta^{ap}+\zeta^{bp})^n \mod np\mathcal{A}_{(p)}$ (même si $m < 0$ lorsque $(a;b) = (1;4)$ ou $(a;b) = (2;3)$) et adapter le raisonnement précédent.

1) Si $p \equiv \pm 1$ modulo 5, c'est-à-dire si $p \equiv \pm 1$ modulo 10 (puisque p est impair), on trouve

$$F_{m+np} \equiv \frac{1+2\zeta+2\zeta^4}{5}\left((1+\zeta+\zeta^4)^{m+n}-(1+\zeta^2+\zeta^3)^{m+n}\right) = F_{m+n} \mod np\mathcal{A}_{(p)}.$$

La congruence finale $F_{m+np} \equiv F_{m+n}$ est valable modulo $np\mathbb{Z}_{(p)}$, et même modulo $np\mathbb{Z}$ si n est une puissance de p. En particulier, pour un entier $k \geqslant 0$, on a

$$F_{m+(p-1)p^k} = F_{(m-p^k)+p^k\cdot p} \equiv F_m \mod p^{k+1}\mathbb{Z}.$$

La suite de Fibonacci modulo p^{k+1} est donc périodique et sa période divise $(p-1)p^k$. $\qquad (*)$

2) Dans le cas $p \equiv \pm 2$ modulo 5, c'est-à-dire $p = 2$ ou $p \equiv \pm 3$ modulo 10, on trouve

$$F_{m+np} \equiv \frac{1+2\zeta+2\zeta^4}{5}\left((1+\zeta+\zeta^4)^m(1+\zeta^2+\zeta^3)^n-(1+\zeta^2+\zeta^3)^m(1+\zeta+\zeta^4)^n\right) \mod np\mathcal{A}_{(p)}.$$

Comme $(1+\zeta+\zeta^4)(1+\zeta^2+\zeta^3) = \varphi\cdot\widehat{\varphi} = -1$, on a

$$F_{m+np} \equiv \frac{1+2\zeta+2\zeta^4}{5}(-1)^n\left((1+\zeta+\zeta^4)^{m-n}-(1+\zeta^2+\zeta^3)^{m-n}\right) = (-1)^n F_{m-n} \mod np\mathcal{A}_{(p)}.$$

La congruence finale $F_{m+np} \equiv (-1)^n F_{m-n}$ est valable modulo $np\mathbb{Z}_{(p)}$, et même modulo $np\mathbb{Z}$ si n est une puissance de p. En particulier, pour un entier $k \geqslant 0$, on a

$$F_{m+2(p+1)p^k} = F_{(m+2p^k)+2p^k \cdot p} \equiv F_m \mod 2p^{k+1}\mathbb{Z}.$$

La suite de Fibonacci modulo p^{k+1} est donc périodique et sa période divise $2(p+1)p^k$. $(*)$

3 Période de Pisano

On considère un entier $n \geqslant 2$. Comme il n'y a que n^2 réductions modulo n possibles des paires $(F_a; F_{a+1})$, il existe deux paires différentes qui ont la même réduction, c'est-à-dire deux indices $b > a \geqslant 0$ tels que $F_b \equiv F_a$ et $F_{b+1} \equiv F_{a+1}$ modulo n. Par soustraction, on trouve $F_{b-1} \equiv F_{a-1}$, et ainsi de suite jusqu'à obtenir $F_{b-a+1} \equiv F_1 = 1$ et $F_{b-a} \equiv F_0 = 0$. On alors $F_{b-a+k} \equiv F_k$ modulo n pour tout entier k. La suite de Fibonacci modulo n est donc périodique et la période divise $b - a$.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
F_k	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584
mod 2	**0**	**1**	**1**	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
mod 3	**0**	**1**	**1**	**2**	**0**	**2**	**2**	**1**	0	1	1	2	0	2	2	1	0	1	1
mod 4	**0**	**1**	**1**	**2**	**3**	**1**	0	1	1	2	3	1	0	1	1	2	3	1	0

La *période de Pisano* $\pi(n)$ est le plus petit entier positif qui vérifie $F_{k+\pi(n)} \equiv F_k \pmod n$ pour tout entier k. On a en particulier $F_{\pi(n)} \equiv 0$ et $F_{1+\pi(n)} \equiv 1$ modulo n et ces deux congruences suffisent pour caractériser $\pi(n)$. Ainsi, dans le programme Python ci-dessous, on calcule $(F_c \bmod n; F_{c+1} \bmod n)$ à partir de $(F_1; F_2)$ jusqu'à obtenir $(0; 1)$ ou $(1; 0)$, ce dernier cas engendrant $(0; 1)$ à l'étape suivante.

```
def pisano(n):
    a = b = c = 1
    while a+b != 1 :
        a, b, c = b, (a+b)%n, c+1
    return(c+a)
print([pisano(k) for k in range(2,21)])
```

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\pi(n)$	3	8	6	20	24	16	12	24	60	10	24	28	48	40	24	36	24	18	60

Résultats principaux

1) Si m divise n, alors $\pi(m)$ divise $\pi(n)$;

2) Si m et n sont premiers entre eux, alors $\pi(mn) = \text{ppmc}(\pi(m), \pi(n))$.

Tout entier $n \geqslant 2$ admet une unique factorisation en nombres premiers, disons $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ avec $p_1 < p_2 < \cdots < p_m$, et on a alors $\pi(n) = \text{ppmc}(\pi(p_1^{k_1}), \pi(p_2^{k_2}), \ldots, \pi(p_m^{k_m}))$. Il suffit donc d'étudier $\pi(p^k)$ pour tout nombre premier p et tout entier $k \geqslant 1$.

3) $\pi(p^k) = \pi(p)p^s$ avec un certain nombre $s = s_p(k) \in \{0, 1, \ldots, k-1\}$;

4) $\pi(2) = 3$ et $s_2(k) = k - 1$, autrement dit $\pi(2^k) = 3 \cdot 2^{k-1}$;

5) $\pi(5) = 20$ et $s_5(k) = k - 1$, autrement dit $\pi(5^k) = 20 \cdot 5^{k-1} = 4 \cdot 5^k$;

6) Si $p \equiv \pm 1 \pmod{10}$, alors $\pi(p)$ divise $p - 1$;

7) Si $p \equiv \pm 3 \pmod{10}$, alors $\pi(p)$ divise $2(p + 1)$.

PREUVES (inspirées de [2], section 3.1)

1) Si m divise n, les congruences $F_{\pi(n)} \equiv 0$ et $F_{1+\pi(n)} \equiv 1$ modulo n sont aussi valables modulo m.

2) Par le résultat 1), $\pi(mn)$ est divisible par $\pi(m)$ et par $\pi(n)$, donc par leur plus petit multiple commun. A l'inverse, $\pi(mn)$ divise $\mathfrak{p} = \mathrm{ppmc}(\pi(m), \pi(n))$ car pour tout entier k, on a $F_{\mathfrak{p}+k} \equiv F_k$ modulo m et modulo n, donc modulo mn puisque m et n sont premiers entre eux (si un entier est divisible par deux entiers premiers entre eux, alors il est divisible par leur produit).

Pour la suite, on considère l'ensemble $\mathcal{A}$ des matrices 2×2 à coefficients entiers. On peut montrer par induction que les puissances de $M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ sont $M^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}$ et $M^k \equiv I \pmod{n\mathcal{A}}$ signifie que $\pi(n)$ divise k.

3) Pour $k \geqslant 1$, on a $M^{\pi(p^k)} \equiv I$ modulo $p^k\mathcal{A}$. Par la proposition de la section 2, on en déduit que $M^{p\pi(p^k)} = (M^{\pi(p^k)})^p \equiv I$ modulo $p^{k+1}\mathcal{A}$, donc $\pi(p^{k+1})$ divise $p\pi(p^k)$. Il existe un nombre entier n tel que $n\pi(p^{k+1}) = p\pi(p^k)$ et ceci divise $p\pi(p^{k+1})$ par le résultat 1). Il s'ensuit que n divise p, donc $\pi(p^{k+1}) = \pi(p^k)$ ou $\pi(p^{k+1}) = p\pi(p^k)$. On conclut facilement en itérant le raisonnement.

4) L'assertion est vérifiée pour $k \in \{1, 2\}$ et on considère ici un entier $k \geqslant 3$. Dans l'exemple 1 de la section 2, il a été établi que $5^n \equiv 1 + 4n$ modulo $8n\mathbb{Z}$ lorsque n est une puissance de deux. Comme $M^6 = \left(\begin{smallmatrix} 13 & 8 \\ 8 & 5 \end{smallmatrix}\right) \equiv 5\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ modulo $8\mathcal{A}$, on en déduit

$$M^{3\cdot 2^{k-2}} = M^{6\cdot 2^{k-3}} = (M^6)^{2^{k-3}} \equiv 5^{2^{k-3}} I \equiv (1 + 2^{k-1})I \pmod{2^k\mathcal{A}}.$$

On a en particulier $M^{3\cdot 2^{k-2}} \not\equiv I \pmod{2^k\mathcal{A}}$ et $\pi(2^k)$ ne divise pas $3 \cdot 2^{k-2}$. Par le résultat 3), on sait que $\pi(2^k) = 3 \cdot 2^s$ avec $s = s_2(k) \in \{0, 1, \ldots, k-1\}$. La seule possibilité est alors $s_2(k) = k - 1$.

5) L'assertion est valable pour $k = 1$ et on considère ici un entier $k \geqslant 2$. On peut vérifier que

$$(x - y)^5 = x^5 - y^5 - 5xy(x - y)^3 - 5(xy)^2(x - y).$$

En posant $x = \varphi^n$ et $y = \widehat{\varphi}^n$, puis en divisant par $\sqrt{5}$, on obtient (par la formule de Binet "classique") $25F_n^5 = F_{5n} - 25(-1)^n F_n^3 - 5F_n$, autrement dit

$$F_{5n} = 5F_n(5F_n^4 + 5(-1)^n F_n^2 + 1).$$

La plus grande puissance de 5 qui divise F_{5n} est alors $v_5(F_{5n}) = 1 + v_5(F_n)$, donc

$$v_5(F_{4.5^{k-1}}) = 1 + v_5(F_{4.5^{k-2}}) = \ldots = k - 1 + v_5(F_4) = k - 1.$$

Cela signifie que $F_{4.5^{k-1}}$ se divise par 5^{k-1} mais pas par 5^k. En particulier, $\pi(5^k)$ ne divise pas $4 \cdot 5^{k-1} = 20 \cdot 5^{k-2}$. Par le résultat 3), on sait que $\pi(5^k) = 20 \cdot 5^s$ avec $s = s_5(k) \in \{0, 1, \ldots, k-1\}$. La seule possibilité est alors $s_5(k) = k - 1$.

6) et 7) découlent des faits $(*)$ établis dans la section 2 (paragraphe "Améliorations") avec $k = 0$. □

Références

[1] Alexandre Junod, *Nombres de Fibonacci et approximation diophantienne*, Bulletin de la SSPMP N° 152 (mai 2023)

[2] Marc Renault, *The Fibonacci Sequence Under Various Moduli*, 1996
`http://webspace.ship.edu/msrenault/fibonacci/FibThesis.pdf`