Plaquette 3 – Nombres premiers, valuations et factorielles

Arithmétique dans Z — Licence 1 (L1)

Corrections détaillées

Boîte à outils

Décomposition et valuations. Tout $n \geq 2$ s'écrit de façon unique $n = \prod_p p^{v_p(n)}$, où $v_p(n)$ est l'exposant de p.

$$v_p(ab) = v_p(a) + v_p(b), \qquad a \mid b \Leftrightarrow \forall p,\ v_p(a) \leq v_p(b)$$

— $v_p(\mathrm{pgcd}(a,b)) = \min(v_p(a), v_p(b))$ et $v_p(\mathrm{ppcm}(a,b)) = \max(v_p(a), v_p(b))$.

— **Nombre de diviseurs** : $d(n) = \prod_p (v_p(n) + 1)$.

— **Lemme d'Euclide** : p premier, $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

— **Test** : $n \geq 2$ non premier admet un diviseur premier $p \leq \sqrt{n}$.

Formule de Legendre (valuation d'une factorielle) :

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$$

— p premier et $1 \leq k \leq p-1$: $p \mid \binom{p}{k}$.

— **Petit théorème de Fermat** : $a^p \equiv a \pmod p$; si $p \nmid a$, $a^{p-1} \equiv 1 \pmod p$.

Correction de l'exercice 1 – Premiers de la forme 4k + 3

a) Si $p_1, \dots, p_k$ étaient tous les premiers, $N = p_1 \cdots p_k + 1 \geq 2$ aurait un facteur premier $p = p_i$. Alors p_i diviserait $N - p_1 \cdots p_k = 1$: absurde.

b) Si $a \equiv 1$ et $b \equiv 1 \pmod 4$, alors $ab \equiv 1 \times 1 = 1 \pmod 4$; par récurrence, tout produit fini de tels entiers est $\equiv 1 \pmod 4$.

c) $N \equiv -1 \equiv 3 \pmod 4$, N est **impair** et $N \geq 3$. Ses facteurs premiers sont impairs, donc congrus à 1 ou 3 modulo 4.

— S'ils étaient **tous** $\equiv 1 \pmod 4$, leur produit N serait $\equiv 1 \pmod 4$ par b) : faux. Donc N a un facteur premier $q \equiv 3 \pmod 4$.

— q est l'un des p_i ; alors q divise $4p_1 \cdots p_k - N = 1$: **contradiction**.

Il existe une infinité de nombres premiers $p \equiv 3 \pmod 4$

— **Exemple** : avec $\{3, 7\}$, $N = 4 \times 21 - 1 = 83$, premier et $\equiv 3 \pmod 4$, absent de la liste ✓

d) Avec $N = 4p_1 \cdots p_k + 1 \equiv 1 \pmod 4$, rien n'empêche N d'avoir des facteurs $\equiv 3 \pmod 4$ (deux facteurs $\equiv 3$ donnent un produit $\equiv 1$). L'argument « un facteur doit être de la bonne forme » ne marche plus. On le contourne avec $N = (2p_1 \cdots p_k)^2 + 1$ et le résultat de l'exercice « Diviseurs premiers de n² + 1 ».

Réponse. $N = 4p_1 \cdots p_k - 1 \equiv 3 \pmod 4$ a un facteur premier $\equiv 3 \pmod 4$ hors de la liste : il y en a une infinité.

Correction de l'exercice 2 – Test de primalité par la racine

a) $n = ab$ avec $1 < a \leq b < n$. Alors $a^2 \leq ab = n$. Tout facteur premier p de a vérifie $p \leq a$, donc $p^2 \leq a^2 \leq n$ et $p \mid n$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

$$n \text{ composé} \Longrightarrow \exists p \text{ premier},\ p \mid n,\ p \leq \sqrt{n}$$

b) $\sqrt{221} \approx 14{,}9$: on teste $2, 3, 5, 7, 11, 13$. $221 = 13 \times 17$: **composé**.

— $\sqrt{223} \approx 14{,}93$: 223 est impair ; somme des chiffres 7 (pas multiple de 3) ; ne finit ni par 0 ni par 5 ; $223 = 7 \times 31 + 6$; $223 = 11 \times 20 + 3$; $223 = 13 \times 17 + 2$. Aucun diviseur : **premier**.

c) Il suffit de tester les premiers ≤ 100 (le premier suivant, 101, vérifie $101^2 = 10\,201 > 10\,007$) : 25 **divisions** au plus.

d) Écrivons $n = p_1 p_2 \cdots p_r$ (premiers, avec répétition). Chaque $p_i > \sqrt[3]{n}$. Si $r \geq 3$, alors $n \geq p_1 p_2 p_3 > (\sqrt[3]{n})^3 = n$: absurde.

— Donc $r \leq 2$: n est premier ($r = 1$) ou produit de deux premiers ($r = 2$).

— **Portée** : c'est le principe des algorithmes de factorisation par « petits facteurs d'abord » ; le coût dépend de $\sqrt{n}$, ce qui devient énorme pour les nombres de 300 chiffres de la cryptographie.

Réponse. Un composé a un facteur premier $\leq \sqrt{n}$; $221 = 13 \times 17$, 223 premier ; 25 divisions pour 10 007.

Correction de l'exercice 3 – Longues suites de nombres composés

a) Pour $2 \leq k \leq n$, k divise $n!$ (c'est un facteur du produit $1 \times 2 \times \ldots \times n$), donc :

$$k \mid n! + k \quad \text{et} \quad 2 \leq k < n! + k$$

— $n! + k$ a un diviseur k strictement compris entre 1 et lui-même : il est **composé**.

b) Pour avoir L entiers consécutifs composés, on prend $n = L + 1$: les L entiers $(L+1)! + 2, \ldots, (L+1)! + L + 1$ conviennent.

c) $6! = 720$: $722 = 2 \times 361$, $723 = 3 \times 241$, $724 = 4 \times 181$, $725 = 5 \times 145$, $726 = 6 \times 121$. Cinq composés consécutifs ✓

— Beaucoup plus petits : $24, 25, 26, 27, 28$ (entre les premiers 23 et 29) ; et même 90 à 96 pour sept consécutifs.

— **Remarque** : la construction par $n!$ garantit l'existence mais ne donne pas les plus petits exemples.

d) Non : les « trous » entre premiers consécutifs peuvent être arbitrairement grands, mais il y a toujours des premiers **après** chaque trou. Les deux résultats sont compatibles ; ils disent que les premiers se **raréfient** (en moyenne, l'écart près de n est de l'ordre de $\ln n$).

Réponse. $k \mid n! + k$ pour $2 \leq k \leq n$; 722 à 726 ; plus petits : 24 à 28.

Correction de l'exercice 4 – Formule de Legendre

a) Les multiples de p^k dans $\{1, \ldots, n\}$ sont $p^k, 2p^k, \ldots, qp^k$ avec q le plus grand entier tel que $qp^k \leq n$, c'est-à-dire $q = \left\lfloor \dfrac{n}{p^k} \right\rfloor$.

b) Par additivité de v_p : $v_p(n!) = \sum_{m=1}^{n} v_p(m)$. Un entier m avec $v_p(m) = j$ est multiple de $p, p^2, \ldots, p^j$ et pas de p^{j+1} : il est compté **exactement j fois** dans la somme

$$\sum_{k \geq 1} \operatorname{card}\left\langle m \leq n : p^k \mid m \right\rangle = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

— Les deux sommes sont donc égales (la somme est finie : les termes sont nuls dès que $p^k > n$).

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

c) Le nombre de zéros finaux est $v_{10}(100!) = \min(v_2(100!), v_5(100!))$. Par Legendre :

— $v_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor + \left\lfloor \frac{100}{125} \right\rfloor = 20 + 4 + 0 = 24$.

d) $v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$.

— Le minimum est $v_5 = 24$: 100! se termine par 24 **zéros**. Les 5 sont le facteur limitant (il y a beaucoup plus de 2).

— **Piège** : compter seulement les multiples de 5 donne 20 ; il faut ajouter 25, 50, 75, 100 qui apportent **deux** facteurs 5.

Réponse. $v_p(n!) = \sum_k \lfloor n/p^k \rfloor$; $v_5(100!) = 24$, $v_2(100!) = 97$: 24 zéros.

Correction de l'exercice 5 – Binôme modulo p et Fermat

a) Avec $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, on vérifie $k\binom{p}{k} = p\binom{p-1}{k-1}$. Donc p divise $k\binom{p}{k}$.

— Pour $1 \le k \le p-1$, $p \nmid k$ ($0 < k < p$), donc $p \wedge k = 1$ (p premier). Par **Gauss**, $p \mid \binom{p}{k}$.

b) Binôme de Newton :

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p \equiv a^p + b^p \pmod{p}$$

— Tous les termes intermédiaires sont multiples de p par a).

c) Initialisation : $0^p = 0$ ✓ **Hérédité** : si $a^p \equiv a$, alors par b) avec $b = 1$:

— $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$ ✓

— La propriété vaut pour tout $a \in \mathbb{N}$, puis pour $a < 0$ (car $a \equiv a + kp$ avec $a + kp \ge 0$).

— Si de plus $p \nmid a$, on simplifie $a \cdot a^{p-1} \equiv a \cdot 1$ par a (inversible modulo p) : $a^{p-1} \equiv 1 \pmod{p}$.

d) $3^5 = 243 = 48 \times 5 + 3 \equiv 3 \pmod{5}$ ✓ ; $2^7 = 128 = 18 \times 7 + 2 \equiv 2 \pmod{7}$ ✓

— $p = 4$ (non premier) : $\binom{4}{2} = 6$ n'est pas divisible par 4. La primalité sert exactement à l'étape « $p \wedge k = 1$ ».

Réponse. $p \mid \binom{p}{k}$; $(a+b)^p \equiv a^p + b^p$ [p] ; $a^p \equiv a$ [p] ; $\binom{4}{2} = 6$ contre-exemple pour $p = 4$.

Correction de l'exercice 6 – Nombres de Fermat

a) $F_n - 2 = 2^{2^n} - 1$. Différence de deux carrés :

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = (F_n - 2)F_n$$

— Récurrence : $F_1 - 2 = 3 = F_0$ ✓ ; si $F_0 \cdots F_{n-1} = F_n - 2$, alors $F_0 \cdots F_n = (F_n - 2)F_n = F_{n+1} - 2$ ✓

b) Soit $m < n$ et $d = \text{pgcd}(F_m, F_n)$. F_m est l'un des facteurs de $F_0 \cdots F_{n-1} = F_n - 2$, donc $d \mid F_n - 2$. Comme $d \mid F_n$, $d \mid 2$.

— Les F_n sont **impairs** : $d = 1$.

c) Chaque F_n a un facteur premier q_n. Les F_n étant deux à deux premiers entre eux, les q_n sont **distincts** : on obtient une infinité de nombres premiers.

d) $F_5 = 2^{32} + 1 = 4\,294\,967\,297$. On calcule $641 \times 6\,700\,417 = 4\,294\,967\,297$ ✓

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— **Astuce d'Euler** : $641 = 5 \times 2^7 + 1 = 5^4 + 2^4$. Modulo 641, $5 \times 2^7 \equiv -1$, donc $5^4 \times 2^{28} \equiv 1$, et $5^4 \equiv -2^4$ donne $-2^{32} \equiv 1$, soit $641 \mid 2^{32} + 1$.

— **Leçon** : vérifier quatre cas (F_0 à F_4 premiers) ne prouve rien ; il faut une démonstration.

Réponse. $F_0 \cdots F_{n-1} = F_n - 2$; les F_n sont deux à deux premiers entre eux ; $F_5 = 641 \times 6\,700\,417$.

Correction de l'exercice 7 – Nombre de diviseurs

a) Si $m \mid n$, alors $v_p(m) \leq v_p(n)$ pour tout p, et m n'a pas d'autre facteur premier que les p_i. Réciproquement, un tel produit divise n. Par unicité de la décomposition, chaque choix $(\beta_1, \ldots, \beta_r)$ donne un diviseur différent :

$$d(n) = \prod_{i=1}^{r} (\alpha_i + 1)$$

b) Le produit est impair si et seulement si chaque $\alpha_i + 1$ est impair, c'est-à-dire chaque α_i **pair** : n est un carré.

c) $12 = 12 = 6 \times 2 = 4 \times 3 = 3 \times 2 \times 2$. On attribue les plus grands exposants aux plus petits premiers :

— $2^{11} = 2\,048$; $2^5 \times 3 = 96$; $2^3 \times 3^2 = 72$; $2^2 \times 3 \times 5 = 60$.

— Le plus petit est 60 (diviseurs : $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$ ✓).

d) La porte m change d'état une fois par diviseur k de m : $d(m)$ fois. Elle finit ouverte si $d(m)$ est **impair**, c'est-à-dire si m est un carré (b).

— Portes ouvertes : $1, 4, 9, 16, 25, 36, 49, 64, 81, 100$ (dix portes).

— **Explication intuitive** : les diviseurs vont par paires $\left(k, \frac{m}{k}\right)$, sauf $k = \sqrt{m}$ quand m est un carré.

Réponse. $d(n) = \prod (\alpha_i + 1)$, impair $\Leftrightarrow$ n carré ; plus petit entier à 12 diviseurs : 60 ; portes ouvertes : les carrés.

Correction de l'exercice 8 – Identité de Sophie Germain

a) On complète le carré : $n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2 - 2n)(n^2 + 2 + 2n)$ (différence de deux carrés).

b) Pour que le produit soit premier, le plus petit facteur doit valoir 1 (les deux sont ≥ 1 : $n^2 - 2n + 2 = (n-1)^2 + 1 \geq 1$).

— $(n-1)^2 + 1 = 1 \Leftrightarrow n = 1$. Alors $n^4 + 4 = 5$, premier ✓

— $n = 0$ donne 4, non premier. **Seul** $n = 1$ convient.

c) Même méthode : $a^4 + 4b^4 = (a^2 + 2b^2)^2 - 4a^2b^2$, d'où

$$a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)$$

— Si n est pair, $n^4 + 4^n$ est pair et > 2 : composé.

— Si n est impair, $n = 2m + 1$: $4^n = 4 \times \left(2^m\right)^4$, soit $b = 2^m$. Le petit facteur vaut $(n-b)^2 + b^2 \geq b^2 = 4^m \geq 4$ pour $m \geq 1$: composé.

— **Exemple** $n = 3$: $81 + 64 = 145 = 5 \times 29$ ✓ (avec $b = 2$: facteurs $9 - 12 + 8 = 5$ et $9 + 12 + 8 = 29$).

d) $n^2 - 1 = (n-1)(n+1)$. Premier impose $n - 1 = 1$, soit $n = 2$: $n^2 - 1 = 3$ ✓

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— **Méthode** : pour montrer qu'une expression est rarement première, on la **factorise** et on force un facteur à valoir 1.

Réponse. n^4+4 premier $\Leftrightarrow n=1$; $a^4+4b^4=(a^2+2ab+2b^2)(a^2-2ab+2b^2)$; n^2-1 premier $\Leftrightarrow n=2$.

Correction de l'exercice 9 – Carré d'un premier modulo 24

a) Les restes modulo 6 sont $0,\dots,5$. Si $p\equiv 0,2,4$, p est pair ; si $p\equiv 3$, $3\mid p$. Pour $p\geq 5$ premier, il reste $p\equiv 1$ ou $5\equiv -1 \pmod 6$.

b) p est impair : $p-1$ et $p+1$ sont deux **pairs consécutifs**, donc l'un est multiple de 4. Leur produit est multiple de $2\times 4=8$.

c) Parmi $p-1$, p, $p+1$ (trois entiers consécutifs), l'un est multiple de 3 ; ce n'est pas p. Donc $3\mid (p-1)(p+1)$.

$$8\mid p^2-1,\quad 3\mid p^2-1,\quad 8\wedge 3=1 \implies 24\mid p^2-1$$

d) $p^2-q^2=(p^2-1)-(q^2-1)$ est une différence de deux multiples de 24.

— $p=11$, $q=7$: $121-49=72=3\times 24$ ✓ ; et $p^2-1=120=5\times 24$ ✓

— **Piège** : l'hypothèse $p\geq 5$ est nécessaire : $3^2-1=8$ n'est pas multiple de 24.

Réponse. $24\mid p^2-1$ pour tout premier $p\geq 5$; $121-49=72=3\times 24$.

Correction de l'exercice 10 – PGCD et PPCM par les valuations

a) Pour deux réels x, y : $\{\min(x,y),\max(x,y)\}=\{x,y\}$, donc $\min+\max=x+y$. Par la lecture des valuations :

$$v_p(\text{pgcd}\times\text{ppcm})=\min(v_p(a),v_p(b))+\max(v_p(a),v_p(b))=v_p(ab)$$

— Deux entiers positifs de mêmes valuations pour **tout** p sont égaux (décomposition unique).

b) On compare exposant par exposant (2 : 3 et 5 ; 3 : 4 et 1 ; 5 : 0 et 2 ; 7 : 1 et 0) :

— $\text{pgcd}=2^3\times 3=24$; $\text{ppcm}=2^5\times 3^4\times 5^2\times 7=453\,600$.

— **Contrôle** : $a=4\,536$, $b=2\,400$, $ab=10\,886\,400=24\times 453\,600$ ✓

c) $v_p(a^2)=2v_p(a)$ et $\min(2x,2y)=2\min(x,y)$: les valuations de $\text{pgcd}(a^2,b^2)$ sont celles de $\text{pgcd}(a,b)^2$.

d) $a^2\mid b^2\Leftrightarrow\forall p,\ 2v_p(a)\leq 2v_p(b)\Leftrightarrow\forall p,\ v_p(a)\leq v_p(b)\Leftrightarrow a\mid b$.

— $a^2\mid b^3$ **n'entraîne pas** $a\mid b$: $a=8$, $b=4$: $64\mid 64$ mais $8\nmid 4$ (valuations : $6\leq 6$ mais $3>2$).

— **Méthode** : toute question de divisibilité entre produits et puissances devient une **inégalité entre exposants**.

Réponse. pgcd × ppcm $=ab$; en b) 24 et 453 600 ; $a^2\mid b^2\Leftrightarrow a\mid b$; contre-exemple $a=8$, $b=4$ pour $a^2\mid b^3$.

Correction de l'exercice 11 – Triplets de premiers

a) On regarde les restes modulo 3 : p, $p+2$, $p+4\equiv p+1$ ont les restes p, $p+2$, $p+1$ modulo 3, soit **les trois restes** $0,1,2$ dans un certain ordre.

— L'un des trois est donc multiple de 3 ; étant premier, il vaut 3. Comme $p+2\geq 4$ et $p+4\geq 6$, c'est $p=3$.

— $(3,5,7)$ est bien un triplet de premiers ✓ C'est le **seul**.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

b) Si $p \neq 3$, alors $p \equiv \pm 1 \pmod 3$ et $p^2 \equiv 1$, donc $p^2 + 2 \equiv 0 \pmod 3$, avec $p^2 + 2 > 3$: composé.

— Donc $p = 3$, et $3^2 + 2 = 11$ est premier ✓

c) Même idée : si $p \neq 3$, $p^2 \equiv 1 \pmod 3$ et $8p^2 + 1 \equiv 8 + 1 = 9 \equiv 0 \pmod 3$, avec $8p^2 + 1 > 3$: composé.

— $p = 3$: $8 \times 9 + 1 = 73$, premier ($\sqrt{73} < 9$; 73 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7) ✓

d) On choisit un **petit module** (3) et on montre qu'une des quantités est forcément divisible par ce module ; elle ne peut alors être première que si elle **égale** le module.

$$x^2 \equiv 1 \pmod 3 \text{ pour tout } x \not\equiv 0 \pmod 3$$

Réponse. Seuls $p = 3$: $(3, 5, 7)$, $3^2 + 2 = 11$, $8 \times 9 + 1 = 73$.

Correction de l'exercice 12 – Premiers entre n et 2n

a) $p \leq 2n$ est l'un des facteurs de $(2n)! = 1 \times 2 \times \ldots \times 2n$: $p \mid (2n)!$.

— $(n!)^2$ est un produit d'entiers tous $\leq n < p$; aucun n'est divisible par p, donc (lemme d' **Euclide**) $p \nmid (n!)^2$.

— $(2n)! = N(n!)^2$: p divise $N(n!)^2$ sans diviser $(n!)^2$, et p est premier, donc $p \mid N$.

b) Les premiers de $]n\,;2n]$ sont distincts, donc deux à deux premiers entre eux ; chacun divise N, donc leur produit aussi (corollaire de Gauss).

c) N est l'un des termes (positifs) de la somme $\sum_{k=0}^{2n} \binom{2n}{k} = (1+1)^{2n} = 4^n$, donc $N \leq 4^n$.

$$\prod_{n < p \leq 2n} p \leq \binom{2n}{n} \leq 4^n$$

d) $n = 5$: un seul premier dans $]5\,;10]$, 7 ; $N = 252 = 7 \times 36$ ✓ et $7 \leq 1\,024$.

— $n = 10$: $11 \times 13 \times 17 \times 19 = 46\,189$; $N = 184\,756 = 4 \times 46\,189$ ✓ ; $46\,189 \leq 4^{10} = 1\,048\,576$.

— **Portée** : cette majoration est une étape de la preuve de Chebyshev-Erdős du **postulat de Bertrand** (il y a toujours un premier entre n et $2n$).

Réponse. Les premiers de $]n\,;2n]$ divisent $\binom{2n}{n} \leq 4^n$; $n = 10$: $46\,189 \mid 184\,756$.

Correction de l'exercice 13 – Diviseurs premiers de n² + 1

a) Si $p \mid n$, alors $p \mid (n^2 + 1) - n^2 = 1$: absurde. Et $p \mid n^2 + 1$ s'écrit $n^2 \equiv -1 \pmod p$.

b) On élève à la puissance $\dfrac{p-1}{2}$ (entier, car p est impair), puis on applique Fermat ($p \nmid n$) :

$$(-1)^{\frac{p-1}{2}} \equiv \left(n^2\right)^{\frac{p-1}{2}} = n^{p-1} \equiv 1 \pmod p$$

— $(-1)^{(p-1)/2}$ vaut ± 1 ; s'il valait -1, on aurait $-1 \equiv 1$, soit $p \mid 2$, impossible (p impair). Donc $(-1)^{(p-1)/2} = 1$: $\dfrac{p-1}{2}$ est **pair**, $p \equiv 1 \pmod 4$.

c) 17 (premier, $\equiv 1$) ; $26 = 2 \times 13$ ($13 \equiv 1$) ; $65 = 5 \times 13$ (tous deux $\equiv 1$) ; $145 = 5 \times 29$ ($29 \equiv 1$) ✓ Le seul premier pair possible est 2.

d) Supposons que $p_1, \ldots, p_k$ soient tous les premiers $\equiv 1 \pmod 4$ et posons $N = (2p_1 \cdots p_k)^2 + 1 \geq 5$, impair.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— Un facteur premier q de N est impair et divise m^2+1 avec $m = 2p_1 \cdots p_k$: par b), $q \equiv 1 \pmod 4$, donc q est un p_i.

— Mais alors $q \mid m$, donc $q \mid N - m^2 = 1$: **contradiction**. Il y a une infinité de premiers $\equiv 1 \pmod 4$.

Réponse. Tout premier impair divisant n^2+1 est $\equiv 1 \pmod 4$; il y a une infinité de tels premiers.

Correction de l'exercice 14 – Valuation 2-adique d'une puissance de 3

a) Différence de deux carrés, avec $3^{2^{n+1}} = \left(3^{2^n}\right)^2$:

$$u_{n+1} = \left(3^{2^n}\right)^2 - 1 = \left(3^{2^n} - 1\right)\left(3^{2^n} + 1\right)$$

b) Pour $n \geq 1$, $3^{2^n} = 9^{2^{n-1}}$ et $9 \equiv 1 \pmod 4$, donc $3^{2^n} \equiv 1 \pmod 4$.

— Alors $3^{2^n} + 1 \equiv 2 \pmod 4$: il est pair mais pas multiple de 4, donc $v_2 = 1$.

c) Par additivité de v_2 et a) : $v_2(u_{n+1}) = v_2(u_n) + v_2\left(3^{2^n}+1\right)$.

— Pour $n \geq 1$, cela donne $v_2(u_{n+1}) = v_2(u_n) + 1$. Avec $v_2(u_1) = v_2(8) = 3$, une récurrence donne $v_2(u_n) = n+2$ pour $n \geq 1$.

— **Cas** $n = 0$: $u_0 = 2$, $v_2(u_0) = 1 \neq 0 + 2$. La formule est fausse au rang 0, car $3^{2^0} + 1 = 4$ a une valuation 2 et non 1 (b ne s'applique pas).

d) $u_1 = 8 = 2^3$ ✓ ; $u_2 = 80 = 2^4 \times 5$ ✓ ; $u_3 = 3^8 - 1 = 6\,560 = 2^5 \times 205$ ✓

— **Leçon** : une récurrence doit être **initialisée au bon rang** ; le rang de départ est dicté par l'hypothèse utilisée dans l'hérédité.

Réponse. $v_2\left(3^{2^n} - 1\right) = n + 2$ pour $n \geq 1$ (et 1 pour $n = 0$) ; $6\,560 = 2^5 \times 205$.

Correction de l'exercice 15 – Synthèse : théorème de Wilson

a) $x^2 \equiv 1 \Leftrightarrow p \mid (x-1)(x+1)$. Par le lemme d'**Euclide**, $p \mid x-1$ ou $p \mid x+1$: $x \equiv \pm 1$.

— Modulo 8 (non premier) : $1^2 = 1$, $3^2 = 9 \equiv 1$, $5^2 = 25 \equiv 1$, $7^2 = 49 \equiv 1$: **quatre** solutions. Le lemme d'Euclide est faux pour 8 ($8 \mid 2 \times 4$ sans diviser ni 2 ni 4).

b) Chaque $x \in \{1, \ldots, p-1\}$ est premier avec p, donc inversible : il existe un unique $x' \in \{1, \ldots, p-1\}$ avec $xx' \equiv 1$.

— $x' = x \Leftrightarrow x^2 \equiv 1 \Leftrightarrow x \in \{1, p-1\}$ par a). Pour $2 \leq x \leq p-2$, on a donc $x' \neq x$ et $x' \in \{2, \ldots, p-2\}$ (car $x' \neq 1$ et $x' \neq p-1$).

— L'application $x \mapsto x'$ échange les éléments deux à deux : ils se regroupent en paires.

c) Dans $(p-1)! = 1 \times (2 \times \ldots \times (p-2)) \times (p-1)$, chaque paire donne 1 :

$$(p-1)! \equiv 1 \times 1 \times (p-1) \equiv -1 \pmod p$$

— Le cas $p = 2$ se vérifie à part : $1! \equiv -1 \pmod 2$ ✓

d) $4! = 24 = 25 - 1$ ✓ ; $6! = 720 = 721 - 1$ et $721 = 7 \times 103$ ✓ ; $10! = 3\,628\,800$ et $3\,628\,801 = 11 \times 329\,891$ ✓

— Si $n = ab$ avec $1 < a < b < n$, a et b figurent dans $(n-1)!$: $n \mid (n-1)!$. Si $n = a^2$ avec $a \geq 3$, alors a et $2a$ sont distincts et $< n$: $n = a^2 \mid a \times 2a$, qui divise $(n-1)!$.

— **Bilan** : pour $n \geq 6$ composé, $(n-1)! \equiv 0$; pour n premier, $\equiv -1$. ($n = 4$ est une exception : $3! = 6 \equiv 2 \pmod 4$.)

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Réponse. $x^2 \equiv 1\ [p] \Leftrightarrow x \equiv \pm 1$; $(p-1)! \equiv -1 \pmod{p}$; pour $n \geq 6$ composé, $(n-1)! \equiv 0 \pmod{n}$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).