



COURS ET PROBLÈMES GUIDÉS

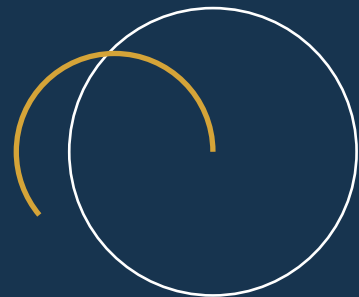
CONGRUENCES

Calculer avec les restes,
raisonner sur les grands nombres.

COLLÈGE AVANCÉ / LYCÉE

Préparation aux olympiades de mathématiques

Calcul modulaire · Puissances
Divisibilité · Preuves d'impossibilité



Comprendre. Puis résoudre.

22 pages · 8 exercices supplémentaires corrigés

Explications courtes · Raisonnements complets

LE PARCOURS

Sommaire et mode d'emploi

L'objectif

Remplacer de grands nombres par de petits représentants sans changer le reste, puis utiliser cette idée pour calculer et démontrer.

Partie	Pages
Définition et règles de calcul	3–6
Cycles et grands exposants	7–11
Divisibilité et impossibilités	12–16
Huit exercices supplémentaires	17–18
Corrigés et fiches méthodes	19–22

Comment travailler ?

Lire une fiche, puis cacher le corrigé d'un exemple et refaire le raisonnement. Pour les exercices, écrire les étapes sur une copie avant de vérifier les réponses.

Le niveau

Les premiers exemples installent les bases. Les problèmes suivants demandent de combiner plusieurs idées. Les résultats restent justifiés, même lorsque la solution est courte.

Note d'édition. Adaptation française du fichier *Congruences vos 8 12.txt*. Les méthodes mathématiques lisibles sont reprises. Plusieurs formules affichées ne figurent pas dans la transcription : les exemples concernés sont signalés comme adaptés. Les exercices d'entraînement et les compléments sont ajoutés.

COURS · 1

Avoir le même reste

Définition

Pour des entiers a, b et un entier $m \geq 2$,

$$a \equiv b \pmod{m} \iff m \mid (a - b).$$

Cela signifie que a et b ont le même reste dans la division euclidienne par m .

Exemple

$$17 \equiv 12 \equiv 7 \equiv 2 \equiv -3 \pmod{5}.$$

Tous les nombres de cette ligne s'écrivent $5k + 2$, avec k entier.

Représentant et reste : deux mots distincts

Le nombre -3 est un représentant de la même classe que 17 modulo 5. Mais le reste euclidien est 2, car un reste doit vérifier $0 \leq r < 5$.

$$-3 = 5(-1) + 2.$$

Reconnaître la divisibilité

$$a \equiv 0 \pmod{m} \iff m \mid a.$$

Par exemple $84 \equiv 0 \pmod{7}$, car $84 = 7 \times 12$.

Attention. « a divise b » s'écrit $b \equiv 0 \pmod{a}$, et non l'inverse. Pour un modulo, on utilise ici un entier positif au moins égal à 2.

COURS • 2

Les opérations autorisées

Si $a \equiv b \pmod{m}$ **et** $c \equiv d \pmod{m}$

$$a + c \equiv b + d, \quad a - c \equiv b - d, \quad ac \equiv bd \pmod{m}.$$

Pour tout entier $n \geq 1$, on a aussi $a^n \equiv b^n \pmod{m}$.

Exemple de calcul

Calculer le reste de $38 \times 27 + 19$ modulo 7 :

$$38 \times 27 + 19 \equiv 3 \times (-1) + 5 \equiv 2 \pmod{7}.$$

Le reste est donc 2.

Pourquoi les puissances sont compatibles

La différence se factorise :

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1}).$$

Comme m divise $a - b$, il divise aussi $a^n - b^n$.

Châîner les congruences

Si $a \equiv b$ et $b \equiv c$ modulo m , alors $a \equiv c$ modulo m . En effet, $a - c = (a - b) + (b - c)$ est un multiple de m .

Idée clé. Réduire après chaque addition ou multiplication garde les calculs petits. Choisir un représentant négatif est souvent plus rapide.

COURS · 3

Simplifier demande une condition

La règle sûre

Si $ca \equiv cb \pmod{m}$ et $\text{PGCD}(c, m) = 1$, alors

$$a \equiv b \pmod{m}.$$

Sans cette coprimauté, on ne peut pas conserver automatiquement le même modulo.

Un contre-exemple

On a $16 \equiv 12 \pmod{4}$. Diviser par 4 donnerait $4 \equiv 3 \pmod{4}$, ce qui est faux.

La règle générale

Pour $c \neq 0$, posons $g = \text{PGCD}(c, m)$. Alors

$$ca \equiv cb \pmod{m} \iff a \equiv b \pmod{m/g}.$$

La condition signifie $m \mid c(a-b)$. Après division de m et c par g , les facteurs restants sont premiers entre eux, ce qui justifie la simplification.

Exemple complémentaire

$$6x \equiv 12 \pmod{15} \iff 2x \equiv 4 \pmod{5} \iff x \equiv 2 \pmod{5}.$$

Modulo 15, cela correspond à $x \equiv 2, 7$ ou 12 .

Attention. On ne divise pas une congruence comme une égalité réelle. Il faut vérifier le PGCD avec le modulo.

COURS · 4

Résoudre une congruence linéaire

Exemple complémentaire pour s'entraîner.

Exemple 1 : un inverse existe

Résoudre $7x \equiv 3 \pmod{11}$. Comme $7 \times 8 = 56 \equiv 1 \pmod{11}$, on multiplie par 8 :

$$x \equiv 24 \equiv 2 \pmod{11}.$$

Toutes les solutions sont $x = 11k + 2$, avec $k \in \mathbb{Z}$.

Exemple 2 : réduire le modulo

$$6x \equiv 8 \pmod{14} \iff 3x \equiv 4 \pmod{7}.$$

Comme $3 \times 5 \equiv 1 \pmod{7}$, on obtient

$$x \equiv 20 \equiv 6 \pmod{7}.$$

Modulo 14, les classes solutions sont donc 6 et 13.

Exemple 3 : aucune solution

$6x \equiv 5 \pmod{14}$ est impossible : cela voudrait dire $6x - 5 = 14k$, avec un membre impair et l'autre pair.

Le critère utile

$ax \equiv b \pmod{m}$ possède des solutions exactement lorsque $\text{PGCD}(a, m)$ divise b . Dans ce cas, diviser d'abord a, b, m par ce PGCD, puis chercher l'inverse du nouveau coefficient.

MÉTHODE · 1

Trouver une période

Le bon raccourci

Si $a^t \equiv 1 \pmod{m}$ et si $n = qt + r$ avec $0 \leq r < t$, alors

$$a^n \equiv (a^t)^q a^r \equiv a^r \pmod{m}.$$

On réduit l'exposant modulo t , pas automatiquement modulo m .

Exemple complémentaire : les puissances de 3 modulo 7

n	1	2	3	4	5	6
$3^n \bmod 7$	3	2	6	4	5	1

Puisque $2024 = 6 \times 337 + 2$,

$$3^{2024} \equiv 3^2 \equiv 2 \pmod{7}.$$

Une puissance qui vaut -1

On a déjà $3^3 \equiv -1 \pmod{7}$. Donc $3^6 \equiv 1$, ce qui évite parfois de remplir tout le tableau.

Quand le nombre n'est pas premier avec le modulo

La suite peut avoir un début particulier. Modulo 8, les puissances de 2 donnent 2, 4, 0, 0, ... ; aucune puissance positive n'est congrue à 1.

Attention. Une période doit être prouvée. Tester deux valeurs égales ne suffit pas toujours à décrire le début de la suite.

EXEMPLES GUIDÉS · 1

Profiter de 1 et de -1

1. Calculer 8^{100} modulo 9

Comme $8 \equiv -1 \pmod{9}$:

$$8^{100} \equiv (-1)^{100} = 1 \pmod{9}.$$

Le reste est $\boxed{1}$. Pour 8^{101} , le représentant est -1 , donc le reste est $\boxed{8}$.

2. Calculer 9^{1990} modulo 11

Comme $9 \equiv -2 \pmod{11}$, cherchons une petite puissance de 2 :

$$2^5 = 32 \equiv -1 \pmod{11}, \quad 2^{10} \equiv 1.$$

L'exposant 1990 est pair et multiple de 10. Ainsi

$$9^{1990} \equiv 2^{1990} = (2^{10})^{199} \equiv 1 \pmod{11}.$$

3. Revenir à un reste positif

Si un calcul donne $N \equiv -17 \pmod{12}$, ajouter deux fois 12 :

$$-17 + 24 = 7, \quad 0 \leq 7 < 12.$$

Le reste est 7.

Idée clé. Chercher d'abord une puissance congrue à 1 ou -1 . Le reste du calcul dépend alors surtout de la division de l'exposant.

EXEMPLE GUIDÉ · 2

Des exposants très grands

Exemple adapté : l'énoncé de la transcription est incomplet.

Calculer le reste modulo 7 de

$$N = \sum_{k=1}^9 10^{10^k}.$$

1. Trouver la période de la base

$$10^3 = 1000 \equiv -1 \pmod{7}, \quad 10^6 \equiv 1 \pmod{7}.$$

Il suffit donc de connaître chaque exposant 10^k modulo 6.

2. Réduire l'exposant

On a $10 \equiv 4 \pmod{6}$ et $4^2 \equiv 4 \pmod{6}$. Par multiplication successive,

$$10^k \equiv 4 \pmod{6} \quad (k \geq 1).$$

3. Réduire chaque terme

$$10^{10^k} \equiv 10^4 \equiv 10(-1) \equiv -3 \equiv 4 \pmod{7}.$$

Il y a neuf termes dans la somme :

$$N \equiv 9 \times 4 = 36 \equiv 1 \pmod{7}.$$

Résultat

Le reste est 1.

Idée clé. Pour une puissance de puissance, deux modulus interviennent : celui du nombre final, puis celui de la période utilisée pour son exposant.

EXEMPLE GUIDÉ · 3

Les deux derniers chiffres de 2^{999}

Traduire la question

Les deux derniers chiffres d'un entier sont son reste modulo 100, écrit avec deux chiffres si nécessaire.

1. Une puissance commode

$$2^{10} = 1024 \equiv 24 \pmod{100}, \quad 2^{20} \equiv 24^2 \equiv 76.$$

Or $76^2 = 5776 \equiv 76 \pmod{100}$. Toute puissance positive de 76 reste donc congrue à 76.

2. Découper l'exposant

$$999 = 20 \times 49 + 19.$$

Ainsi $2^{999} \equiv 76 \times 2^{19} \pmod{100}$. On a $2^{19} = 524288 \equiv 88 \pmod{100}$, d'où

$$2^{999} \equiv 76 \times 88 = 6688 \equiv 88 \pmod{100}.$$

Résultat

Les deux derniers chiffres sont 88.

Pourquoi cela ne vaut pas 1

$2^{20} \equiv 76$ et non 1 modulo 100. Ici, on a utilisé la stabilité des puissances de 76 ; on n'a pas appliqué la règle des périodes de la page 7.

Attention. Un nombre ayant un facteur commun avec le modulo demande de la prudence dans la réduction de l'exposant.

EXEMPLE GUIDÉ · 4

Les deux derniers chiffres de 23^{2023}

1. Monter par carrés

Tous les calculs suivants sont modulo 100 :

Puissance	Reste
23^2	29
23^4	$29^2 \equiv 41$
23^8	$41^2 \equiv 81$
23^{10}	$81 \times 29 \equiv 49$
23^{20}	$49^2 \equiv 1$

2. Réduire l'exposant

Comme $2023 = 20 \times 101 + 3$,

$$23^{2023} \equiv (23^{20})^{101} 23^3 \equiv 23^3 \pmod{100}.$$

3. Terminer par un petit produit

$$23^3 \equiv 23 \times 29 = 667 \equiv 67 \pmod{100}.$$

Résultat

Les deux derniers chiffres sont 67.

Idée clé. Les carrés successifs donnent rapidement $a^2, a^4, a^8, \dots$. En combinant ces puissances, on atteint l'exposant utile sans calculer le grand nombre.

PREUVE D'IMPOSSIBILITÉ

Quatre chiffres égaux à la fin ?

Problème

Une puissance de 2 peut-elle avoir au moins quatre chiffres et se terminer par quatre chiffres identiques ?

1. Traduire les quatre derniers chiffres

Si ces chiffres sont tous égaux à d , avec $0 \leq d \leq 9$, alors

$$2^n = 10000q + 1111d.$$

Comme le nombre a au moins quatre chiffres, on a $n \geq 10$, donc 2^n est divisible par 16. De plus, $16 \mid 10000$.

2. Passer modulo 16

$$0 \equiv 1111d \equiv 7d \pmod{16}.$$

Puisque 7 et 16 sont premiers entre eux, on obtient $d \equiv 0 \pmod{16}$. Comme d est un chiffre, cela impose $d = 0$.

3. Éliminer le dernier cas

Une puissance de 2 ne peut pas se terminer par 0000 : elle serait divisible par 5. Or sa décomposition ne contient que le facteur premier 2.

Résultat

C'est impossible.

Idée clé. Le modulo 16 vient de deux propriétés : il divise 10^4 et il divise les puissances de 2 assez grandes. Le bon modulo rend la contradiction visible.

COMPLÉMENT · 1

Les critères de divisibilité

Exemple complémentaire pour s'entraîner.

Écrivons un entier en base 10 :

$$N = d_0 + 10d_1 + 10^2d_2 + \cdots + 10^k d_k.$$

Modulo 3 ou modulo 9

Comme $10 \equiv 1$, toutes les puissances de 10 sont congrues à 1 :

$$N \equiv d_0 + d_1 + \cdots + d_k \pmod{9}.$$

La même preuve fonctionne modulo 3. Un entier est donc divisible par 9 (ou par 3) exactement lorsque la somme de ses chiffres l'est.

Modulo 11

Comme $10 \equiv -1 \pmod{11}$:

$$N \equiv d_0 - d_1 + d_2 - \cdots + (-1)^k d_k \pmod{11}.$$

On utilise la somme alternée des chiffres.

Par blocs de trois chiffres

$1001 = 7 \times 11 \times 13$. Ainsi $1000 \equiv -1$ modulo chacun de ces trois nombres. Par exemple

$$123456 \equiv 456 - 123 = 333 \equiv 4 \pmod{7}.$$

Idée clé. Les critères usuels ne sont pas des règles isolées : ils viennent du reste de la base 10 ou d'une petite puissance de 10.

COMPLÉMENT · 2

Reconnaître un carré impossible

Exemple complémentaire pour s'entraîner.

Les carrés modulo 4

Un entier est pair ou impair. S'il est pair, son carré vaut 0 modulo 4. S'il est impair, on écrit $n = 2k + 1$:

$$n^2 = 4k(k + 1) + 1 \equiv 1 \pmod{4}.$$

Les seuls restes possibles d'un carré modulo 4 sont donc 0 et 1.

Application

L'équation $x^2 = 4y + 3$ n'a aucune solution entière, car son membre de droite vaut 3 modulo 4.

Les carrés modulo 8

Pour un entier impair,

$$n^2 = 4k(k + 1) + 1 \equiv 1 \pmod{8},$$

car $k(k + 1)$ est pair. Pour un entier pair, le carré vaut 0 ou 4 modulo 8. Les restes possibles sont donc 0, 1, 4.

Exemple

Un entier congru à 5 modulo 8 ne peut pas être un carré. En particulier, $8t + 5$ n'est jamais un carré entier.

Attention. Une condition nécessaire n'est pas toujours suffisante. Un nombre congru à 1 modulo 8 peut ne pas être un carré : 17 en est un exemple.

APPROFONDISSEMENT

Faire apparaître un facteur 3 de plus

Exemple adapté : l'énoncé de la transcription est incomplet.

Montrer que, pour tout entier $r \geq 0$,

$$3^{r+1} \mid 4^{3^r} - 1.$$

1. Initialiser

Pour $r = 0$, on a $4^{3^0} - 1 = 3$, divisible par 3^1 .

2. Passer d'un rang au suivant

Supposons $3^{r+1} \mid 4^{3^r} - 1$. Posons $A = 4^{3^r}$. Alors $A \equiv 1 \pmod{3}$. La différence de cubes donne

$$4^{3^{r+1}} - 1 = A^3 - 1 = (A - 1)(A^2 + A + 1).$$

Le premier facteur est divisible par 3^{r+1} , par hypothèse. Le second est divisible par 3, car

$$A^2 + A + 1 \equiv 1 + 1 + 1 \equiv 0 \pmod{3}.$$

Le produit est donc divisible par 3^{r+2} .

3. Conclure

Le raisonnement se répète à partir du cas $r = 0$. La propriété est vraie pour tout $r \geq 0$: c'est une preuve par récurrence.

Idée clé. Pour prouver une divisibilité par une puissance croissante d'un nombre premier, chercher une factorisation qui ajoute un facteur premier à chaque étape.

EXEMPLE GUIDÉ · 5

Calculer 7^{103} modulo 17

Exemple adapté : l'énoncé de la transcription est incomplet.

1. Rechercher une petite puissance égale à -1

$$\begin{aligned}7^2 &= 49 \equiv -2 \pmod{17}, & 7^4 &\equiv 4 \pmod{17}, \\7^8 &\equiv 16 \equiv -1 \pmod{17}, & 7^{16} &\equiv 1 \pmod{17}.\end{aligned}$$

2. Découper 103

$$103 = 6 \times 16 + 7.$$

On obtient donc

$$7^{103} \equiv 7^7 \pmod{17}.$$

3. Recomposer la petite puissance

$$7^7 = 7^4 \cdot 7^2 \cdot 7 \equiv 4 \cdot (-2) \cdot 7 = -56 \equiv 12 \pmod{17}.$$

Résultat

Le reste est 12.

Pourquoi écrire $7 = 4 + 2 + 1$?

Les puissances 7^4 , 7^2 et 7 sont déjà connues. Cette décomposition évite de calculer les puissances intermédiaires.

Idée clé. Garder les petits restes obtenus en chemin : ils servent souvent à reconstruire la dernière puissance.

ENTRAÎNEMENT • 1/2

Quatre calculs de restes

Exercices supplémentaires. Écrire les congruences utilisées et donner un reste compris entre 0 et $m - 1$. Corrigés page 19.

1 • Un représentant négatif

Donner le reste de $(-23)^5$ dans la division par 7.

2 • Une période

Calculer 3^{2024} modulo 7.

3 • Un modulo à réduire

Résoudre $6x \equiv 8 \pmod{14}$ et donner toutes les classes solutions modulo 14.

4 • Deux puissances

Calculer le reste de $2^{100} + 3^{100}$ dans la division par 5.

Pour débloquer la recherche

- Exercice 1 : -23 peut être remplacé par un petit entier.
- Exercice 2 : une puissance de 3 vaut 1 modulo 7.
- Exercice 3 : 6 et 14 ont un facteur commun.
- Exercice 4 : traiter les deux puissances séparément, puis additionner.

Attention. Une congruence ne donne pas encore le reste final si le représentant obtenu est négatif ou supérieur au modulo.

ENTRAÎNEMENT • 2/2

Quatre raisonnements courts

Exercices supplémentaires. Justifier chaque conclusion ; une simple liste d'essais ne suffit pas toujours. Corrigés page 20.

5 • Un carré impossible

Montrer que $4n + 3$ n'est jamais un carré entier lorsque $n \geq 0$.

6 • Un exposant minimal

Trouver le plus petit entier $t > 0$ tel que $7^t \equiv 1 \pmod{10}$.

7 • Deux conditions à réunir

Trouver le plus petit entier positif x tel que $x \equiv 2 \pmod{3}$ et $x \equiv 4 \pmod{5}$.

8 • Une base bien choisie

Calculer le reste de 257^{33} dans la division par 16.

Pour débloquent la recherche

- Exercice 5 : classer les carrés modulo 4.
- Exercice 6 : la première puissance qui donne 1 est importante.
- Exercice 7 : écrire $x = 5k + 4$, puis utiliser la condition modulo 3.
- Exercice 8 : commencer par réduire 257.

Idée clé. Pour un minimum, construire une solution ne suffit pas : expliquer pourquoi toutes les valeurs plus petites échouent.

CORRIGÉS · 1/2

Réduire, puis calculer

1. Un représentant négatif

$-23 \equiv -2 \pmod{7}$, donc

$$(-23)^5 \equiv (-2)^5 = -32 \equiv 3 \pmod{7}.$$

Le reste est $\boxed{3}$.

2. Une période

$3^6 \equiv 1 \pmod{7}$ et $2024 = 6 \times 337 + 2$:

$$3^{2024} \equiv 3^2 \equiv \boxed{2} \pmod{7}.$$

3. Un modulo à réduire

Diviser les trois entiers 6, 8 et 14 par 2 donne

$$3x \equiv 4 \pmod{7}.$$

Multiplier par 5, inverse de 3 modulo 7, donne $x \equiv 6 \pmod{7}$. Les deux classes modulo 14 sont donc

$$\boxed{x \equiv 6 \text{ ou } 13 \pmod{14}}.$$

4. Deux puissances

$2^4 \equiv 1$ et $3^4 \equiv 1$ modulo 5. Comme $100 = 4 \times 25$:

$$2^{100} + 3^{100} \equiv 1 + 1 \equiv \boxed{2} \pmod{5}.$$

Idée clé. Toutes les opérations ont lieu avec le même modulo, sauf lorsqu'une simplification justifiée réduit explicitement ce modulo.

CORRIGÉS · 2/2

Prouver et trouver le minimum

5. Un carré impossible

Un carré vaut 0 ou 1 modulo 4 selon que sa base est paire ou impaire. Or $4n + 3 \equiv 3 \pmod{4}$. C'est impossible.

6. Un exposant minimal

Les puissances successives de 7 modulo 10 donnent

$$7, \quad 9, \quad 3, \quad 1.$$

Les exposants 1, 2 et 3 ne conviennent pas ; 4 convient. Donc $\boxed{t = 4}$.

7. Deux conditions à réunir

Écrire $x = 5k + 4$. Modulo 3, cela donne

$$2k + 1 \equiv 2 \pmod{3}, \quad 2k \equiv 1 \pmod{3}, \quad k \equiv 2 \pmod{3}.$$

Donc $k = 3t + 2$ et $x = 15t + 14$. Les solutions sont congrues à 14 modulo 15 ; la plus petite positive est $\boxed{14}$.

8. Une base bien choisie

Comme $257 = 16 \times 16 + 1$, on a

$$257^{33} \equiv 1^{33} \equiv \boxed{1} \pmod{16}.$$

Attention. Il était inutile de développer 257^{33} . La taille du nombre disparaît dès que l'on réduit sa base.

FICHE MÉTHODE

Comment choisir le modulo ?

On demande un reste

Le diviseur annoncé fournit directement le modulo. Réduire la base, puis chercher une période pour les puissances.

On demande les derniers chiffres

Un chiffre : modulo 10. Deux chiffres : modulo 100. Trois chiffres : modulo 1000. On peut parfois séparer en facteurs premiers entre eux.

On veut prouver une impossibilité

Tester un petit modulo où les formes présentes ont peu de restes possibles : 4 ou 8 pour les carrés, 3 pour certaines puissances, 16 pour les quatre derniers chiffres d'une puissance de 2.

On veut prouver une divisibilité

Traduire l'objectif $m \mid N$ en $N \equiv 0 \pmod{m}$. Chercher une simplification, une factorisation ou un raisonnement par récurrence.

On a deux conditions de reste

Écrire le nombre sous la forme $x = mk + r$ grâce à la première condition, puis déterminer k avec la seconde. Lorsque les modulus sont premiers entre eux, une seule classe modulo leur produit convient.

Le contrôle

Un calcul de restes doit finir avec $0 \leq r < m$. Une preuve d'impossibilité doit montrer que les restes exigés ne peuvent pas coïncider.

FICHE DE SYNTHÈSE

Les six règles à retenir

1. **Définition** : $a \equiv b \pmod{m}$ signifie $m \mid a - b$.
2. **Calcul** : additionner, soustraire, multiplier et élever à une puissance entière positive sont des opérations compatibles.
3. **Simplification** : annuler un facteur tout en gardant le modulo exige qu'il soit premier avec ce modulo.
4. **Puissances** : si $a^t \equiv 1 \pmod{m}$, on peut réduire l'exposant modulo t .
5. **Représentants** : un nombre négatif est autorisé pendant le calcul ; le reste final est entre 0 et $m - 1$.
6. **Preuve** : une condition modulaire peut exclure un candidat. Elle ne suffit pas toujours à prouver que ce candidat existe.

Un calcul modèle

$$19^{2026} \equiv (-1)^{2026} \equiv 1 \pmod{20}.$$

La base devient -1 , la parité de l'exposant termine le calcul.

Idée clé. Les congruences gardent exactement l'information utile : le reste. Le grand nombre lui-même peut rester inconnu.