FONDEMENTS DES MATHÉMATIQUES

AYBERK ZEYTİN

1. DIVISIBILITÉ

Comment on peut écrire un entier naturel comme un produit des petits entiers? Cette question a une infinitude d'interconnexions entre les nombres naturels que les mathématiciens ont étudié pendant des milliers d'années. L'aventure commence par rappeler l'arithmétique de nos jeunes et la regarder à nouveau.

Dans ce chapitre on commence notre étude des entiers naturels par la définition de divisibilité et on présente les idées de la division euclidienne, le plus grand commun diviseurs, et l'algorithme d'Euclide. On utilise l'algorithme d'Euclide pour trouver entier résolution à equations lineaires. Ces id'ées sont commandées en en une longue liste ascendante, mais de nombreuses expériences dans la vie quotidienne sont cycliques: heures dans la journée, jours de la semaine, les mouvements des planètes. Ce concept de cyclicité a pour résultat l'idée de l'arithmétique modulaire qui formalise l'idée intuitive de nombres sur un cycle.

Dans ce chapitre, on va introduire l'idee simple d'arithmétique et on va développer ces idée plus loin dans les chapitres à venir. Vous venez de développer des compétences en théorèmes prouvant, y compris démontrer des théorèmes par induction alors que vous explorez les questions de divisibilité des nombres entiers et des questions sur l'arithmétique modulaire.

1.1. Définitions et Exemples.

Les entiers naturels sont utilisé pour compter que l'on a vu dans notre enfance.

Définition 1. *Les entiers naturels sont les nombres* $\mathbf{N} = \{1, 2, 3, \ldots\}$.

L'entier 0 et les entiers negatifs sont les abstractions des entiers naturels.

Définition 2. *Les entiers sont* $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Avoir cette définition formelle de la divisibilité vous permettra de dire clairement pourquoi certains théorèmes sur la divisibilité sont vraies. Se souvenant de la définition formelle de la divisibilité sera utile tout au long du cours.

Il y a plusieurs des relations entre entiers mais dans ce chapitre on va étudier la divisibilité d'un nombre par un autre.

Définition 3. *Soient* a *et* d *entiers. On dit que* d *divise* a *(où* d *est un diviseur de* a *) s'il existe un entier* k *telle que* $a = k \cdot d$. *On le note par* $d|a$.

Nous passons ensuite à une définition plus complexe qui capture l'idée de nombres disposés dans un schéma cyclique. Par exemple, si on a écrit les nombres naturels autour d'une horloge, vous mettriez 13 au lieu de 1 et 14 au lieu de 2, etc. L'idée est ce qui est formalisé dans la définition de la congruence:

Définition 4. *Supposons que* a, b *et* n *sont entiers avec* $n > 0$. *On dit que* a *et* b *sont congrus modulo* n *si et seluement si* $n|(a - b)$. *On le note par* $a \equiv b$ *mod* n.

Exercice 5. *Soit* n *un entier. Montrer que si* $6|n$ *alors* $3|n$.

Résolution. Si $6|n$ alors il existe un entier k telle que $n = 6 \cdot k = 2 \cdot 3 \cdot k$. Donc, $n = 3 \cdot k'$ où $k' = 2 \cdot k$ est un entier.

Exercice 6. *Soit n un entier. Si $n \equiv 7$ mod 2 alors $n \equiv 3$ mod 2*

Résolution. On commence par $n \equiv 7 \bmod 2$. Par définition, $2|(n-7)$ c'est-à-dire qu'il existe un entier k avec $2 \cdot k = (n-7)$. On a $2 \cdot k + 4 = (n-7) + 4$ que on dit $2k' = 2 \cdot (k+2) = n-3$; où $k' = k+2$ est un entier. Alors $2|n-3$.

On peut utiliser les définitions et le théorèmes qui on a vu. Mais on ne peut pas montrer un théorème ou résout un exercice avec l'aide d'une proposition ou déclaration que on n'a pas montré.

1.2. **Divisibilité et Congruence.** Les théorèmes suivantes répondent à questions concernant divisibilité et les operations arithmetiques: addition, multiplication etc. Une bonne stratégie de poser bonne questions est de poser considérer un concept et étudier les relations avec les autres concepts.

Théorème 7. *Soient a, b et c entiers. Si $a|b$ et $a|c$ alors $a|(b-c)$.*

Théorème 8. *Soient a, b et c entiers. Si $a|c$ et $a|c$ alors $a|(b+c)$.*

Théorème 9. *Soient a, b et c entiers. Si $a|b$ et $a|c$ alors $a|bc$.*

Tout théorème a une hypothèse et une conclusion. Cette structure de théorèmes suggère automatiquement des questions: par exemple, est-ce que nous pouvons deduire le même résultat en utilisant une hypothèse faible? Si nous sommes en mesure de déduire le même résultat avec moins ou plus faible hypothèses, alors nous avons construit un théorème plus fort. De même, si nous sommes en mesure de déduire une conclusion forte à partir des mêmes hypothèses, alors nous avons construit un théorème plus fort. Donc tenter d'affaiblir l'hypothèse et toujours obtenir la même conclusion, ou de garder les mêmes hypothèses et déduire une conclusion fort sont deux méthodes à suivre lorsque nous cherchons de nouvelles vérités. Essayons donc cette stratégie avec le théorème précédent.

Lorsque vous envisagez de savoir si une hypothèse particulière implique une conclusion particulière, vous envisagez une conjecture. Trois résultats sont possibles. Vous pouvez prouver, dans ce cas, la conjecture est transformé en un théorème. Vous pouvez trouver un exemple spécifique (appelé un contre-exemple) où les hypothèses sont vraies, mais la conclusion est fausse. Ce contre-exemple serait alors montrer que la conjecture est fausse. Souvent, vous ne pouvez pas résoudre le conjecture de toute façon. Dans ce cas, vous pouvez essayer changeant la conjecture en renforçant l'hypothèse, ce qui affaiblit la conclusion, ou envisagent par ailleurs une conjecture connexe.

Question 10. *Est-ce que vous pouvez montrer théorème 9 en utilisant une hypothèse faible? Est-ce que vous pouvez montrer $a^2|bc$ avec la même hypothèse.*

Si vous considérez une conjecture et découvrir qu'elle est fausse, ce n'est pas la fin de la route. Au lieu de cela, vous avez alors le défi d'essayer de trouver un peu différentes hypothèses et les conclusions qui pourraient être vrai. Toutes ces stratégies d'exploration conduisent à de nouvelles mathématiques.

Question 11. *Est-ce que vous pouvez écrire votre conjecture analogue à Théorème 9 et le montrer?*

Le théorème suivant est une exemple:

Théorème 12. *Soient a, b et c entiers. Si $a|b$ alors $a|bc$.*

On considére maintenant l'arithmétique modulaire. Pour commencer la regardons d'abord quelques exemples concrets d'acquérir une certaine expérience avec congruence modulo un nombre. Faire des exemples précis est souvent une bonne stratégie pour développer l'intuition d'un sujet.

Exercice 13. *Décider si les déclarations suivantes sont vrai ou faux. Prouver votre résolution.*

- *Est-ce que* $45 \equiv 9 \pmod 4$*?*
- *Est-ce que* $37 \equiv 2 \pmod 5$*?*
- *Est-ce que* $37 \equiv 3 \pmod 5$*?*
- *Est-ce que* $31 \equiv -3 \pmod 5$*?*

Vous pouvez contruire exercices en attendant que vous êtes sûr comment on décider si une congruence est vraie ou non. Avec l'expérience on commence à voir des tendances. L'exercice suivant vous demande de trouver un modèle qui permet de clarifier ce que les groupes d'entiers sont équivalentes à l'autre sous le concept de congruence modulo n.

Exercice 14. *Pour chacune des congruences suivantes, caractériser tous les entiers* m *qui satisfont la congruence:*

- $m \equiv 0 \pmod 3$,
- $m \equiv 1 \pmod 3$,
- $m \equiv 2 \pmod 3$,
- $m \equiv 3 \pmod 3$,
- $m \equiv 4 \pmod 3$,

Pour comprendre la définition de la congruence, une stratégie est de examiner la mesure dans laquelle la congruence se comporte de la même façon que l'égalité. Par exemple, nous savons que tous les entiers sont égal à lui-même. Ainsi, nous pouvons demander: «Est-cue que tous les entiers sont congru à lui-même?". C'est une question naturel parce que la congruence a une définition spécifique, de sorte que nous devons savoir si cette définition spécifique nous permet de déduire que tous les entiers sont congru à lui-même.

Théorème 15. *Soient* a *et* n *entiers avec* $n > 0$*. Alors,* $a \equiv a \pmod n$*.*

Nous allons explorer plusieurs cas où les propriétés de l'égalité ordinaire suggérer des questions quant à savoir si la congruence fonctionne de la même façon. Par exemple, dans l'égalité, l'ordre de la gauche contre la droite d'un signe égal n'a pas d'importance. Est-ce la même chose pour congruence?

Théorème 16. *Soient* a, b *et* n *entiers avec* $n > 0$*. Si* $a \equiv b \pmod n$*, alors* $b \equiv a \pmod n$*.*

On sait que si a est égal à b et b est égal à c alors a est égal à c. Mais est-ce que la définition de congruence nous permettre de conclure la même chose au sujet d'une chaîne de congruences? Il le fait.

Théorème 17. *Soient* a, b, c *et* n *entiers avec* $n > 0$*. Si* $a \equiv b \pmod n$ *et* $b \equiv c \pmod n$*, alors* $a \equiv c \pmod n$*.*

Note: Si vous êtes familier avec les relations d'équivalence, vous pouvez noter que les trois théorèmes précédents établissent que la congruence modulo n définit une relation d'équivalence sur l'ensemble des entiers, $\mathbf{Z}$. Dans l'exercice avant que ces théorèmes, vous avez décrit les classes d'équivalence modulo 3.

Les théorèmes suivants explorent la mesure dans laquelle congruences se comportent de la même chose que l'égalité ordinaire en ce qui concerne les opérations arithmétiques. Nous allons systématiquement à travers les opérations d'addition, la soustraction et la multiplication. Division, comme nous allons le voir, cela exige plus de réflexion.

Théorème 18. *Soient* a, b, c, d *et* n *entiers avec* $n > 0$*. Si* $a \equiv b \pmod n$ *et* $c \equiv d \pmod n$*, alors* $a + c \equiv b + d \pmod n$*.*

Théorème 19. *Soient* a, b, c, d *et* n *entiers avec* $n > 0$*. Si* $a \equiv b \pmod n$ *et* $c \equiv d \pmod n$*, alors* $a - c \equiv b - d \pmod n$*.*

Théorème 20. *Soient* a, b, c, d *et* n *entiers avec* $n > 0$. *Si* $a \equiv b$ *mod* n *et* $c \equiv d$ *mod* n, *alors* $ac \equiv bd$ *mod* n.

Congruences fonctionnent aussi bien avec les exposants, comme nous le verrons dans le Théorème 24. Une façon d'montrer est de commencer avec les cas simples et de voir comment le cas général peut être prouvé. Les exercices suivants présentent une stratégie de raisonnement connu comme preuve par induction (mathématique).

Exercice 21. *Soient* a, b *et* n *entiers avec* $n > 0$. *Montrer que si* $a \equiv b$ *mod* n, *alors* $a^2 \equiv b^2$ *mod* n.

Exercice 22. *Soient* a, b *et* n *entiers avec* $n > 0$. *Montrer que si* $a \equiv b$ *mod* n, *alors* $a^3 \equiv b^3$ *mod* n.

Exercice 23. *Soient* a, b, k *et* n *entiers avec* $n > 0$ *et* $k > 1$. *Montrer que si* $a \equiv b$ *mod* n, *alors* $a^k \equiv b^k$ *mod* n.

Théorème 24. *Soient* a, b, k *et* n *entiers avec* $n > 0$ *et* $k > 0$. *Montrer que si* $a \equiv b$ *mod* n, *alors* $a^k \equiv b^k$ *mod* n.

Vous avez prouvé plusieurs théorèmes qui établissent que les congruences comportement similaire à l'égalité ordinaire par rapport à l'addition, la soustraction, la multiplication et les exposants. Pour faire toutes ces théorèmes plus significative, il est utile de voir ce qu'ils veulent dire avec les entiers. Faire exemples est un bon moyen de développer l'intuition.

Exercice 25. *Illustrer 18 - 24 par un exemple.*

Remarquér que, nous n'avons pas encore examiné l'opération arithmétique de division. Nous vous demandons de considérer la conjecture naturelle ici.

Question 26. *Soient* a, b, c *et* $n > 0$ *entiers telle que* $ac = bc$ *mod* n. *Est-ce qu'on peut déduire que* $a \equiv b$ *mod* n. *Si votre réponse est "Oui." montrer, si "Non." donner un contre-exemple.*

Nous allons continiue la discussion de la division à un stade postérieur. Nous avons trouvé que le concept de congruence et les théorèmes sur l'addition, soustraction, multiplication, et les exposants nous permettent de démontrer certains faits intéressants concernant les entiers. Vous avez déjà vu comment-on dire quand un nombre est divisible par 3 ou par 9. Par exemple, 1131 est divisible par 3 car 3 divise $1 + 1 + 3 + 1$. Dans les prochains théorèmes vous prouver que ces techniques de vérification de la divisibilité.

Théorème 27. *Soit un entier naturel* n *exprimé en base* 10 *comme* $n = a_k a_{k-1} \dots a_0$ *où* a_i *est un chiffre de* n *et soit* $m = a_k + a_{k-1} + \dots + a_1 + a_0$, *alors* $n \equiv m$ *mod* 3.

Théorème 28. 3 *divise un entier naturel* n *si et seulement si la somme de ses chiffres est divisible par* 3.

Note: Une "si et seulement si" déclaration de théorème est vraiment deux théorèmes distincts qui ont besoin de deux démonstrations distinctes. Une bonne pratique consiste à écrire chaque relevé séparément de sorte que l'hypothèse et la conclusion sont claires dans chaque cas. On l'a fait dans le cas suivant pour illustrer la pratique.

Théorème 29. *Si* 3 *divise un entier* n *alors la somme de ses chiffres (éxprime en base* 10*) est divisible par* 3.

Théorème 30. *Si la somme de ses chiffres d'un entier* n *(éxprime en base 10) est divisible par* 3 *alors* $3|n$.

Aprés démontrer un théorème, c'est une bonne idée de essayer de trouver s'il ya d'autres théorèmes connexes qui peut être prouvable avec la même technique. Nous vous encourageons à trouver plusieurs de ces critères de divisibilité dans le prochain exercice.

Exercice 31. *Prouver autres critères de divisibilité similaires à la précédente.*

1.3. **L'Algorithme d'Euclide.** Nous passons ensuite notre attention sur un théorème appelé la division euclidienne. Avant que nous affirmons, nous rappelons un fait sur les nombres naturels qui est évidemment vrai. En fait, c'est tellement évident que c'est un axiome, ce qui signifie une déclaration que nous acceptons comme vrai sans preuve. La raison pour laquelle nous ne pouvons pas vraiment donner une preuve, c'est que nous n'avons pas vraiment défini les nombres naturels, mais ils sont simplement les utiliser comme des objets familiers que nous avons connus nos vies à tous. Si nous prenons une approche très abstraite et formelle de la théorie des nombres où nous avons défini les nombres naturels en termes de théorie des ensembles, par exemple, la déclaration suivante peut être l'un des axiomes nous utiliser pour définir les nombres naturels. Au lieu de cela, nous allons simplement supposer que l'axiome du bon ordre (ou théorème de Zermelo) suivant pour les nombres naturels est vrai.

Axiome 32. *Toute partie non vide de* $\mathbf{N}$ *admet un plus petit élément.*

Puisque nous acceptons ce fait comme vrai, on doit on sentir libre de l'utiliser quand on le souhait. La valeur de cet axiome est qu'il permet parfois nous de cerner la raison pour laquelle certains affirmation est vraie dans une démonstration. Voici un exemple de comment on peut l'axiome du bon ordre des nombres naturels.

Théorème 33. *Étant donné un entier naturel* n*, il existe un entier naturel* k *telle que* $n - 7k < 7$*.*

Démonstration. Soit S l'ensemble des nombres $7i$, où i est un entier naturel, telles que $7i$ est supérieur ou égal à n:

$$S = \{\ell = 7i \in \mathbf{N} \mid 7i \geq n\}$$

. Par l'axiome du bon ordre des nombres naturels, S a un plus petit élément. On le appele $7j$. Puis $7j$ diffère de n de moins de 7, sinon $7(j-1)$ serait un plus petit élément de S. □

Cet exemple donne une idée de la façon dont l'axiome du bon ordre des nombres naturels est utilisé; on définit une partie non vide approprié des nombres naturels et regardons plus petit élément de cette partie de déduire quelque chose qu'on veut. On peut envisager d'utiliser l'axiome du bon ordre des nombres naturels à prouver l'algorithme d'Euclide ci-dessous.

L'algorithme d'Euclide est une observation utile sur les nombres naturels. Souvent il capte exactement ce que nous devons savoir pour prouver des théorèmes sur les nombres entiers. Après l'avoir lu attentivement, on verra qu'il capte une propriété de base sur la division ordinaire.

Théorème 34. *Soient* n *et* m *des entiers naturels. Ensuite:*

(l'existence) *il existe des entiers* q *(pour quotient) et* r *(pour le reste), de telle sorte que* $m = nq + r$ *et* $0 \leq r \leq n - 1$,

(l'unicité) *si* q, q' *et* r, r' *sont des nombres entiers qui satisfont* $m = nq + r = nq' + r'$ *avec* $0 \leq r, r' \leq n-1$, *alors* $q = q'$ *et* $r = r'$.

Comme d'habitude, on examine quelques exemples pour comprendre l'déclaration.

Exercice 35. *Illustrer l'algorithme d'Euclide pour:*

- $m = 25$, $n = 7$
- $m = 277$, $n = 4$
- $m = 33$, $n = 11$
- $m = 33$, $n = 45$

Exercice 36. *Montrer l'existence de l'algorithme d'Euclide. (Indication: Étant donné* m *et* n *comment on peut définir* q *et* r*?)*

Exercice 37. *Montrer l'unicité de l'algorithme d'Euclide. (Indication: Si* $nq + r = nq' + r'$*, alors* $nq - nq' = r' - r$*. Qu'est-ce qu'on sait sur* r *et* r'*.)*

Le théorème suivant relie les notions de congruence modulo n avec des restes comme se produire dans l'algorithme d'Euclide. Il dit que si les restes sont les mêmes lorsque divisé par le module, alors que les entiers sont congruents.

Théorème 38. *Soient* a, b *et* n *entiers avec* $n > 0$. *Alors* $a \equiv b \mod n$ *si et seulement si* a *et* b *ont le même reste en divisant par* n. *Il est équivalent de dire que* $a \equiv b \mod n$ *si et seulement si quand on a* $a = nq_1 + r_1$ $(0 \leq r_1 \leq n-1)$ *et* $b = nq_2 + r_2$ $(0 \leq r_2 \leq n-1)$, *on déduire* $r_1 = r_2$.

1.4. **Les Plus grands communs diviseurs et les équations diophantiennes linéaires.** Les diviseurs d'un entier nous disent quelque chose sur sa structure. Une des stratégies de mathématiques est d'étudier les points communs. Dans le cas des diviseurs, nous passons maintenant de regarder les diviseurs d'un nombre unique à regarder diviseurs communs d'une paire de nombres. Cette stratégie contribue à éclairer les relations et les caractéristiques communes des nombres.

Définition 39. *Un* diviseur commun *des entiers* a *et* b *est un entier* d *telle que* $d|a$ *et* $d|b$.

On a défini dénominateur commun et maintenant on procède à explorer ses implications. La première question est: combien de diviseurs communs ont une paire d'entier?

Question 40. *Est-ce que deux entiers ont au moins un diviseur commun?*

Question 41. *Il est possible de trouver deux entiers qui ont une infinité de diviseurs communs?*

Le plus grand commun diviseur, abrégé en général **pgcd**, est un concept qui joue un rôle central dans l'étude d'un grand nombre de nos futurs sujets.

Définition 42. *Le plus grand commun diviseur de deux entiers* a *et* b, *mais pas les deux sont égal à* 0, *est le plus grand entier* d *tel que* $d|a$ *et* $d|b$. *Le plus grand diviseur commun de deux nombres entiers* a *et* b *est notée* $\gcd(a, b)$, *ou plus brièvement* (a, b).

Avoir plus de diviseurs en commun montre une certaine similitude entre les entiers, mais ayant presque aucun diviseur commun indique que les entiers ne partagent pas de nombreux facteurs. Une paire d'entiers qui n'ont pas de diviseurs communs supplémentaires ont un rôle particulier à jouer et par conséquent sont donné un nom, premiers entre eux ou copremiers.

Définition 43. *Soit* a *et* b *deux entiers. On dit que* a *et* b *sont premiers entre eux ou copremiers si* $\gcd(a, b) = 1$.

Comme d'habitude, on examine quelques exemples sur ce concept.

Exercice 44. *Trouver le plus grand commun diviseur de:*

- $a = 36$ $b = 22$
- $a = 45$ $b = -15$
- $a = -296$ $b = -88$
- $a = 0$ $b = 115$
- $a = 15$ $b = 28$
- $a = -1$ $b = 25634$

Quelles paires sont premiers entre eux?

Les théorèmes suivants explorer les conditions dans lesquelles différentes paires d'entiers ont les mêmes grands communs diviseurs. Notez que dans les théorèmes suivantes qui, bien qu'ils ressemblent à l'équation que on a vu dans l'algorithme d'Euclide, on utilise entiers plutôt que des entiers naturels. Aussi, il y a aucune hypothèse au sujet de la taille de r dans ces théorèmes.

Théorème 45. *Soient* a, n, b, r *et* k *entiers. Si* $a = nb + r$ *et* $k|a$ *et* $k|b$, *alors* $k|r$.

Théorème 46. *Soient* a, b n_1 *et* r_1 *entiers avec* a *et* b *mais pas les deux sont égal à* 0. *Si* $a = n_1 b + r_1$ *alors* $(a, b) = (b, r_1)$.

Exercice 47. *A titre d'illustration du théorème ci-dessus, noter que:*

$$\begin{aligned} 51 &= 3 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 \end{aligned}$$

Montrer que si $a = 51$ *et* $b = 15$ *alors* $(a, b) = (6, 3) = 3$ *en utilisant le théorème précedént.*

Exercice 48 (L'algorithme d'Euclide)**.** *En utilisant le théorème précédent et l'algorithme d'Euclide successivement, élaborer une procédure pour trouver le plus grand commun diviseur de deux entiers.*

La méthode que vous avez probablement imaginé pour trouver le plus grand commun diviseur de deux entiers est effectivement très célèbre. Il remonte à la troisième siècle av. J.-C. et on l'appelle l'algorithme d'Euclide.

Exercice 49. *Trouver*

- $(96, 112)$
- $(175, 24)$
- $(0, 115)$
- $(-288, -166)$
- $(1, 25634)$

en utilisant l'algorithme d'Euclide.

L'exercice suivant illustre le fait que les techniques que vous développez pour trouver diviseurs communs peuvent également être utilisés pour trouver des solutions à des équations entières.

Exercice 50. *Trouver les entiers* x *et* y *telle que* $175x + 24y = 1$.

Cet exemple est en fait un cas particulier d'un théorème général qui concerne nombres premiers entre eux et résolution d'équations dans entiers.
Note: Dans le théorème suivant, rappelez-vous qu'avant qu'un "si et seulement si" déclaration de théorème est vraiment deux théorèmes distincts. Comme d'habitude, de garder les choses soient claires, c'est une bonne pratique d'écrire chacun séparément. Nous l'avons fait pour vous retrouver dans ce cas pour illustrer la pratique.

Théorème 51. *Soient* a *et* b *entiers. Alors* a *et* b *sont premiers entre eux (i.e* $(a, b) = 1$*) si et seulement s'il existe entiers* x *et* y *telle que* $ax + by = 1$.

Ici, écrit séparément, les deux théorèmes vous devez prouver:

Théorème 52. *Soient* a *et* b *deux entiers. Si* $(a, b) = 1$ *alors il existe des entiers* x *et* y *de telle sorte que* $ax + by = 1$. *(Indication: Utiliser l'algorithme Euclide. Faites quelques exemples en prenant quelques paires d'entiers premiers entre eux, faisant l'algorithme d'Euclide, et de voir comment trouver le* x *et* y. *C'est une bonne idée de commencer avec un exemple où l'algorithme d'Euclide prend juste une étape, puis faire un exemple où l'algorithme d'Euclide s'effectue en deux étapes, puis trois étapes, puis chercher une procédure générale.)*

Théorème 53. *Soient* a *et* b *sont entiers. S'il existe entiers* x *et* y *avec* $ax + by = 1$ *alors* $(a, b) = 1$.

Après démontrér un théorème, on cherche à trouver des extensions ou des modifications de celui-ci qui sont tout aussi vrai. Dans ce cas, nous venons de démontrer un théorème sur les nombres premiers entre eux. Il est donc naturel de se demander ce que nous pouvons dire dans le cas où une paire de nombres n'est pas premiers entre eux. On trouve qu'un théorème analogue est vrai.

Théorème 54. *Pour tous entiers* a *et* b *n'est pas* 0 *tous les deux, il existe entiers* x *et* y *de telle sorte que*

$$ax + by = (a, b).$$

Les trois théorèmes suivants apparaissent ici pour deux raisons: premièrement, parce que vous pourriez utiliser certains des résultats précédents à prouver, et, deux, parce qu'ils seront utiles pour théorèmes à venir.

Théorème 55. *Soit* a, b *et* c *entiers. Si* $a|bc$ *et* $(a, b) = 1$, *alors* $a|c$

Théorème 56. *Soit* a, b *et* n *entiers. Si* $a|n$, $b|n$ *et* $(a, b) = 1$, *alors* $ab|n$.

Théorème 57. *Soit* a, b *et* n *entiers. Si* $(a, n) = 1$ *et* $(b, n) = 1$ *alors* $(ab, n) = 1$.

Notre analyse jusqu'ici d'équations diophantiennes linéaires va se révéler très utile dans la résolution de notre problème en suspens avec l'annulation en arithmétique modulaire. On a montré l'existence d'entiers a, b, c et n ($c \neq 0$) pour lequel $ac \equiv bc \pmod{n}$ et l'instant a n'est pas congruente à b modulo n.

Question 58. *Quelles hypothèses au sujet de* a, b, c *et* n *peut être ajoutés afin que* $ac \equiv bc$ *(mod* n*) impliquerait* $a \equiv b$ *(mod* n*)? Énoncer un théorème appropriée et prouver avant continuer.*

Le théorème suivant répond à la question précédente, alors n'hésitez pas à répondre à la Question 58 AVANT de lire plus loin. La réponse implique le concept d'être premiers entre eux.

Théorème 59. *Soient* a, b, c *et* n *entiers avec* $n > 0$. *Si* $ac \equiv bc$ *(mod* n*) et* $(c, n) = 1$ *alors* $a \equiv b$ *(mod* n*).*

Théorèmes 54 et 53 commencent à répondre à la question: nombres entiers donnés a, b, et c, quand pensez existe des entiers x et y qui vérifient l'équation $ax + by = c$? Quand nous cherchons des solutions entières de l'équation, l'équation est appelée une *équation diophantienne*.

Question 60. *Supposons que* a, b, *et* c *sont des nombres entiers, et qu'il existe une solution a l'équation* $ax+by = c$, *c-à-d, supposons qu'il y sont des nombres entiers* x *et* y *qui satisfont à l'équation* $ax+by = c$. *Quelle condition doit satisfaire* c *en termes de* a *et* b*?*

Question 61. *Est-ce que vous pouvez faire une conjecture en complétant la déclaration suivante?*

Conjecture. *Étant donné des entiers* a, b *et* c, *il existe des entiers* x *et* y *qui satisfont à l'équation* $ax+by = c$ *si et seulement si .....*

Essayer de montrer la conjecture avant de lire plus loin.

Le théorème suivant résume les circonstances dans lesquelles une équation $ax + by = c$ a des solutions entières. Il s'agit d'un "si et seulement si" théorème, donc, comme toujours, on doit écrire les deux théorèmes distincts qui doivent être prouvés.

Théorème 62. *Étant donné des entiers* a, b *et* c, *avec* a *et* b *pas tous les deux* 0, *il existe deux entiers* x *et* y *qui satisfont à l'équation* $ax + by = c$ *si et seulement si* $(a, b)|c$.

Ce théorème nous dit dans quelles conditions notre équation linéaire a une solution, mais il ne nous dit pas sur toutes les solutions qu'une telle équation peut avoir, il soulève une question.

Question 63. *Pour les nombres entiers* a, b *et* c, *on considére le linéaire Diophantine équation* $ax+by = c$. *On suppose que les entiers* x_0 *et* y_0 *satisfont l'équation, c'est-à-dire* $ax_0 + by_0 = c$. *Quels sont les autres valeurs* $x = x_0 + h$ *et* $y = y_0 + k$ *satisfont également* $ax + by = c$*? Formuler une hypothèse qui répond à cette question. Concevoir des exemples pour justifier votre exploration. Par exemple,* $6 \cdot (-3)15 \cdot 2 = 12$. *Pouvez-vous trouver d'autres entiers* x *et* y *tels que* $6x + 15y = 12$*? Combien d'autres paires d'entiers* x *et* y *peuvent vous trouver? Pouvez-vous trouver une infinité d'autres solutions?*

La question suivante a été conçu par le célèbre mathématicien Leonhard Euler (1707-1783). Il présente une situation de vie réelle impliquant chevaux et des bœufs afin que nous puissions tous nous identifier avec le problème. Pouvez-vous voir comment le problème d'Euler est liée aux questions précédentes?

Exercice 64. *Un agriculteur expose la somme de 1770 couronnes dans l'achat de chevaux et des bœufs. Il paie 31 couronnes pour chaque cheval et 21 couronnes pour chaque bœuf. Quels sont les nombres possibles de chevaux et des bœufs que l'agriculteur a acheté?*

Le théorème suivant vous montre comment générer de nombreuses solutions pour notre équation diophantienne linéaire, une fois que vous avez une solution.

Théorème 65. *Soient* a, b c x_0 *et* y_0 *des entiers avec* a *et* b *pas les deux* 0 *tel que* $ax_0 + by_0 = c$. *Alors, les entiers*

$$x = x_0 + \frac{b}{(a,b)} \text{ et } y = y_0 - \frac{a}{(a,b)}$$

satisfont l'équation $ax + by = c$.

Exercice 66. *Trouver toutes les résolutions entières de l'équation* $24x + 9y = 33$.

Le théorème précédent complète notre analyse de l'équation diophantienne linéaire

$$ax + by = c.$$

L'analyse des solutions de cette équation diophantienne a fait bon usage du plus grand commun diviseur. Nous pouvons maintenant démontrer un théorème sur grands communs diviseurs qui est difficile à prouver devant on a analysé ces équations diophantiennes. Toutefois, il est intéressant d'essayer de prouver cette affirmation qui semble simple, sans utiliser nos théorèmes sur les équations diophantiennes.

Théorème 67. *Si* a *et* b *sont des entiers, pas tous les deux* 0, *et* k *est un entier naturel, puis*

$$\text{pgcd}(ka, ka) = k\text{pgcd}(a, b).$$

Nous complétons ce chapitre en prenant l'idée de plus grand commun diviseur et l'examen d'une idée connexe. Diviseurs communs de deux nombres divisent les deux entiers. Une sorte de question inverse est la suivante: Supposons que vous êtes donné deux nombres naturels. Quels sont les entiers font ces deux entiers à la fois fracture, en d'autres termes, pouvons-nous décrire les multiples communs? En particulier, ce qui est le moins commun, multiple positif de deux nombres naturels? Le premier défi est d'écrire une définition appropriée.

Exercice 68. *Pour* a *et* b *entiers naturels donner une définition appropriée pour* plus petit commun multiple *de* a *et* b, *notée* $\text{ppcm}(a, b)$. *Construire et calculer quelques exemples.*

Le théorème suivant concerne les idées du plus petit commun multiple et le plus grand commun diviseur.

Théorème 69. *Si* a *et* b *sont entiers naturels, alors* $\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = a \cdot b$

Corollaire 70. *Si* a *et* b *sont entiers naturels, alors* $\text{ppcm}(a, b) = a \cdot b$ *si et seulement si* a *et* b *sont premiers entre eux*

Après avoir terminé une œuvre, il est satisfaisante et utile de rassembler les idées dans votre esprit. Nous vous exhortons à prendre cette mesure en considérant la question suivante.

Question 71. *Dans ce chapitre, nous avons exploré les notions de divisibilité, le plus grand diviseur commun, et des solutions aux équations diophantiennes linéaires. Comment sont toutes ces idées liées? Résumer les relations.*

2. Les Nombres Premiers

Une des stratégies de principe par lequel nous arrivons à comprendre notre monde physique ou conceptuelle est de briser les choses en morceaux, décrire les morceaux les plus élémentaires, puis décrivent comment les pièces sont assemblées pour créer l'ensemble. Notre objectif est de comprendre les nombres naturels, donc ici nous adopter cette stratégie réductionniste et penser à briser nombres naturels en morceaux.

On commence par penser à la façon entiers naturels peuvent être combinés pour créer d'autres nombres naturels. La méthode la plus fondamentale est par ailleurs. Donc, nous allons penser à briser nombres naturels dans leurs morceaux les plus élémentaires du point de vue de l'addition. Quels sont les "éléments" pour ainsi dire par rapport à l'addition des nombres naturels? La réponse est qu'il n'y a qu'un seul élément, le numéro 1. Tout autre nombre naturel peut être décomposé en plus petits nombres naturels qui ajoutent ensemble pour créer le nombre que on a commencé avec. Chaque nombre naturel est simplement la somme de $1 + 1 + 1 + \ldots + 1$. Bien sûr, cette idée n'est pas trop éclairante puisque chaque nombre naturel ressemble beaucoup à un autre de ce point de vue. Toutefois, elle souligne la propriété la plus fondamentale des nombres naturels, à savoir qu'ils se présentent tous de la procédure de simple ajout d'1 certain nombre de fois. En fait, cette propriété des nombres naturels est au cœur des processus inductifs à la fois pour construire les nombres naturels et souvent pour démontrer des théorèmes à leur sujet.

Un moyen plus intéressant de construire des nombres naturels plus grands à partir de plus petits est d'utiliser multiplication. Pensons à ce que les particules élémentaires, pour ainsi dire, sont des nombres naturels à l'égard de multiplication. Autrement dit, quels sont les nombres naturels qui ne peuvent être décomposés en plus petits nombres naturels à travers la multiplication. Quels nombres naturels ne sont pas le produit des nombres naturels plus petits? La réponse, bien sûr, ce sont les nombres premiers.

L'étude des nombres premiers est l'un des principaux axes de la théorie des nombres. Comme on va le prouver, chaque nombre naturel supérieur à 1 est soit premier ou il peut être exprimée comme un produit de nombres premiers. Nombres premiers sont les blocs de construction multiplicateurs de tous les nombres naturels.

2.1. Théorème fondamental de l'arithmétique.

Le rôle des définitions en mathématiques ne peut pas être surestimée. Ils nous obligent à être précis dans notre langage et le raisonnement. Quand une nouvelle définition est introduite, on doit prendre le temps de se familiariser avec ses détails. Essayer d'obtenir à l'aise avec son sens. Regarder les exemples. Même le mémoriser.

Définition 72. *Un entier naturel* $p > 1$ *est appelé premier si et seulement si* p *n'est pas un produit des nombres naturels inférieurs à* p.

Définition 73. *Un nombre naturel* n *est appelé* composé, *si et seulement si* n *est un produit de nombres naturels inférieurs à* n.

Le théorème suivant nous dit que chaque entier naturel supérieur à 1 a au moins un facteur premier.

Théorème 74. *Si* n *est un entier supérieur à* 1 *alors il existe un nombre premier tel que* $p|n$.

Pour s'habituer à nombres premiers, c'est une bonne idée d'en trouver.

Exercice 75. *Trouver les nombres premiers inférieurs à* 100 *sans l'aide d'une calculatrice ou une table de nombres premiers et de réfléchir à la façon dont vous décidez si chaque entier naturel que vous choisissez est premier ou non.*

Vous avez probablement identifié les premiers dans l'exercice précédent par la division de première instance. Par exemple, pour déterminer si oui ou non 91 était premier, vous pourriez avoir

d'abord essayé en le divisant par 2. Une fois convaincu que 2 ne divise pas 91, vous avez probablement passé à 3, puis 4, puis 5, puis 6. Enfin, vous avez atteint 7 et découvert que, en fait, 91 n'est pas un nombre premier. Vous étiez probablement soulagé, car vous pourriez avoir secrètement craindre que vous auriez à poursuivre la tâche ardue de division de première instance 91 fois! Le théorème suivant nous dit que vous ne devez pas avoir été trop préoccupé.

Théorème 76. *Un entier naturel est un nombre premier si et seulement si pour tous les nombres premiers* $p \leq \sqrt{n}$, p *ne divise pas* n.

Exercice 77. *Utiliser le théorème précedent de verifier* 101 *est un nombre premier.*

La recherche de nombres premiers a une longue et fascinante histoire qui continue à se dérouler aujourd'hui. Récemment, la recherche de nombres premiers a pris une importance pratique car nombres premiers sont utilisés tous les jours à faire des communications Internet sécurisé, par exemple. Et on va voir quelques techniques modernes d'identification des nombres premiers. Mais on va commencer avec une ancienne méthode pour trouver des nombres premiers. L'exercice suivant présente une méthode très tôt des nombres premiers identification attribué au savant Eratosthène (276-194 avant JC).

Exercice 78 (Crible d'Ératosthène)**.** *Écrivez tous les nombres naturels de* 1 *à* 100*, peut-être sur un* 10×10 *tableau. Encerclez le chiffre* 2*, le plus petit nombre premier. Rayez tous les nombres divisibles par* 2*. Circle* 3*, le prochain numéro qui n'est pas barrée. Rayez tous les plus grands nombres qui sont divisibles par* 3*. Continuer de faire le tour le plus petit nombre qui n'est pas biffé et rayer ses multiples. Répéter. Pourquoi les chiffres sont encerclés de tous les nombres premiers inférieurs à* 100*?*

Grâce à notre liste des nombres premiers, on peut commencer à étudier combien de nombres premiers existent et quelle est la proportion des nombres naturels sont premiers.

Exercice 79. *Pour chaque entier naturel* $<$*, définir* $\pi(n)$ *comme le nombre des nombres premiers inférieur ou égal à* n*.*

- *Trouver* $\pi(n)$ *pour* $n = 1, \ldots, 100$*.*
- *Faire une proposition sur environ la taille* $\pi(n)$ *est relatif au* n*. En particulier, vous pensez que* $\frac{\pi(n)}{n}$ *est généralement une fonction croissante ou une fonction décroissante? Vous pensez que cela se rapproche un nombre spécifique (comme une limite) quand* n *tend vers l'infini? Faire une conjecture et d'essayer de le prouver. Prouver votre conjecture est un défi difficile à relever. Vous pouvez utiliser un ordinateur pour étendre votre liste de nombres premiers à un nombre beaucoup plus important et de voir si votre conjecture semble tenir en place.*

Les mathématiciens ne donnent pas le titre de "Théorème Fondamental" trop souvent. En fait, vous avez peut-être seulement rencontré un ou deux dans votre vie (le théorème fondamental de l'algèbre et le théorème fondamental de l'analyse). On peut penser de ces théorèmes comme quelque chose de très important. Si c'est le cas, nous serions correct. Ce qui fait un théorème important? Une réponse pourrait être qu'il capture une relation de base et qu'il est largement applicable à expliquer un large éventail de mathématiques. On va voir que le théorème fondamental de l'arithmétique possède certainement ces qualités.

On va écrire le théorème fondamental de l'arithmétique en deux parties: la partie de l'existence et de la part d'unicité. La partie existence dit que chaque nombre naturel plus grand que 1 peut s'écrire comme le produit de nombres premiers et la partie unicité dit essentiellement qu'il n'y a qu'une seule façon de le faire. Par exemple, $24 = 2^3 \cdot 3 = 3 \cdot (-2)^3$.

Théorème 80 (Théorème fondamental de l'arithmétique - Existence part)**.** *Chaque entier naturel supérieur à* 1 *est soit un nombre premier ou il peut être exprimé comme un produit fini de nombres premiers. Autrement dit, pour chaque nombre naturel* n *supérieur à* 1*, il existe des nombres premiers distincts*

$p_1, p_2, \ldots, p_m$ *et nombres naturels* $r_1, r_2, \ldots, r_m$ *tels que*

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_m^{r_m}.$$

Le lemme suivant pourrait être utile pour prouver le part d'unicité du théorème fondamental de l'arithmétique.

Lemme 81. *Soit* p *et* $q_1, q_2, \ldots, q_n$ *nombres premiers et soit* k *un entier naturel tel que* $p \cdot k = q_1 \cdot q_2 \cdot \ldots \cdot q_n$. *Alors* $p = q_i$ *pour un certain* i.

Théorème 82 (Théorème fondamental de l'arithmétique-unicité part)**.** *Soit* n *un entier naturel. Soit* $\{p_1, p_2, \ldots, p_m\}$ *et* $\{q_1, q_2, \ldots, q_s\}$ *des ensembles de nombres premiers avec* $p_i \neq p_j$ *si* $i \neq j$ *et* $q_i \neq q_j$ *si* $i \neq j$. *Soit* $\{r_1, r_2, \ldots, r_m\}$ *et* $\{t_1, t_2, \ldots, t_s\}$ *des ensembles d'entiers naturels tels que*

$$\begin{aligned} n &= p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_m^{r_m} \\ &= q_1^{t_1} \cdot q_2^{t_2} \cdot \ldots \cdot q_s^{t_s}. \end{aligned}$$

Alors $m = s$ *et* $\{p_1, p_2, \ldots, p_m\} = \{q_1, q_2, \ldots, q_s\}$. *Autrement dit, les ensembles de nombres premiers sont égaux, mais leurs éléments ne sont pas nécessairement énumérés dans le même ordre, c'est-à-dire* p_i *peut ou ne peut pas correspondre* q_i. *En outre, si* $p_i = q_j$ *alors* $r_i = t_j$. *En d'autres termes, si nous exprimons le même entier naturel comme un produit de puissances de nombres premiers distincts, alors les expressions sont identiques à l'exception de l'ordre des facteurs.*

Mettant l'existence et l'unicité des pièces ensemble, on obtient la formulation ensemble du théorème fondamental de l'arithmétique:

Théorème 83 (Théorème fondamental de l'arithmétique)**.** *Chaque entier naturel supérieur à* 1 *est un nombre premier ou il peut être exprimée comme un produit fini de nombres premiers où l'expression est unique à l'ordre des facteurs.*

On prend un moment pour réfléchir à un petit problème au sujet de notre définition de la "premier". Les humains prennent des décisions au sujet de ce que les définitions de faire. Réfléchissons sur les choix que nous avons faits dans la définition de "premier". Une notion de "premier" est l'incapacité à se décomposer plus loin. Sûrement 1 répond à ce critère. Pourtant, notre choix de la définition de premier omet 1. Quel est l'avantage de ne pas choisir d'inclure 1 parmi les nombres premiers? Si 1 ont été appelés une prime, pourquoi le théorème fondamental de l'arithmétique ne plus être vrai?

Le théorème fondamental de l'arithmétique nous dit que chaque entier naturel plus grand que 1 est un produit de nombres premiers. Voici quelques exercices qui aident à montrer ce que cela signifie dans certains cas spécifiques.

Exercice 84. *Écrire* $n = 12!$ *comme un produit de nombres premiers.*

Exercice 85. *Determiner le nombre de zéros à la fin de* $25!$.

Le théorème fondamental de l'arithmétique dit que pour tout entier naturel $n > 1$, il existe nombres premiers distincts $p_1, p_2, \ldots, p_m$ et entiers naturels $r_1, r_2, \ldots r_m$ de telle sorte que

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_m^{r_m}$$

et d'ailleurs, la décomposition est unique à l'ordre des facteurs. Lorsque la p_i sont triés afin que $p_1 < p_2 < \ldots < p_m$, nous dira que $p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_m^{r_m}$ est *la décomposition unique* de n.

2.2. **Applications du Théorème fondamental de l'arithmétique.** Une application du théorème fondamental de l'arithmétique, c'est que si nous connaissons les facteurs premiers de deux nombres naturels, c'est une question simple pour déterminer si l'on divise l'autre. Ce qui suit est une caractérisation de la divisibilité en termes de nombres premiers. Il y a beaucoup de lettres et de nombreux indices, mais une fois compris, ce théorème a un sens.

Théorème 86. *Soient* a *et* b *des nombres naturels supérieurs à* 1 *et soient* $p_1^{r_1}p_2^{r_2}\dots p_m^{r_m}$ *la factorisation unique en nombres premiers de* a *et soit* $q_1^{t_1}q_2^{t_2}\dots q_s^{r_s}$ *la factorisation unique en nombres premiers de* b. *Alors* $a|b$ *si et seulement si pour tout* $i \leq m$ *il existe* $a_j \leq s$ *tels que* $p_i = q_j$ *et* $r_i \leq t_j$.

En utilisant la décomposition en produit de facteurs premiers il est facile de prouver certaines affirmations qui pourraient être autrement plus difficile.

Théorème 87. *Soient* a, b *entiers naturels et* $a^2|b^2$. *Alors,* $a|b$.

Décomposition en produit de facteurs premiers peuvent nous aider à trouver le plus grand commun diviseur et plus petit commun multiple de deux nombres naturels. Voici quelques exemples.

Exercice 88. *Trouver* $(3^{14}\cdot 7^{22}\cdot 11^5\cdot 17^3, 5^2\cdot 11^4\cdot 13^8\cdot 17)$

Exercice 89. *Trouver* $\mathrm{ppcm}(3^{14}\cdot 7^{22}\cdot 11^5\cdot 17^3, 5^2\cdot 11^4\cdot 13^8\cdot 17)$

Après avoir fait quelques exemples, nous cherchons instinctivement la tendance générale. Autrement dit, nous cherchons à faire une déclaration générale qui capte la raison pour laquelle la méthode que nous utilisons dans les exemples spécifiques fonctionne.

Exercice 90. *Faire une conjecture qui généralise les idées que vous avez utilisé pour résoudre les deux exercices précédents.*

Question 91. *Pensez-vous que cette méthode est toujours mieux, toujours pire, et parfois mieux, parfois pire que d'utiliser l'algorithme d'Euclide pour trouver* (a, b)*? Pourquoi ?*

Le théorème suivant nécessite une utilisation intelligente du théorème fondamental de l'arithmétique.

Théorème 92. *Étant donné* $N+1$ *entiers naturels, par exemple* $a_1, a_2, \dots a_{N+1}$, *tout inférieur ou égal à* $2N$, *alors il existe une paire, disons* a_i *et* a_j *avec* $i \neq j$, *tel que* $a_i|a_j$.

Le théorème fondamental de l'arithmétique peut être utilisé pour prouver que certaines équations n'ont pas de solutions entières .

Théorème 93. *Il n'existe pas de entiers naturels* m *et* n *tels que* $7m^2 = n^2$.

Théorème 94. *Il n'existe pas de entiers naturels* m *et* n *tels que* $24m^3 = n^3$.

Jusqu'à ici, on a parlé exclusivement sur des entiers naturels et entiers. Nos indications sur les nombres naturels et entiers peuvent réellement nous aider à comprendre les types plus généraux de nombres comme des nombres rationnels et des nombres irrationnels.

Sur l'ensemble $P = \mathbf{Z}\times(\mathbf{Z}\backslash\{0\})$, on définit la relation: $(p, q) \sim (r, s)$ si et seulement si $ps - rq = 0$. On le note par $(p, q) \sim (r, s)$.

Exercice 95. *Trouver tous les éléments de* P *qui sont equivalent á*

- $(7, 1)$
- $(1, 7)$
- $(0, 1)$

Question 96. *Pourquoi l'élément* $(n, 0)$ *est exclu, où* $n \in \mathbf{Z}$*? Qu'est-ce qu'il se passe si on considére* $\mathbf{Z}\times\mathbf{Z}$ *au lieu de* P.

Exercice 97. *Montrer que la relation $\sim$ est une relation d'équivalence.*

Définition 98. *Un class d'équivalence d'un élément $(p, q) \in P$ est noteé par $\frac{p}{q}$ et appelé un nombre rationnel. L'ensemble de nobres rationnels est noteé par $\mathbf{Q}$.*

Exercice 99. *On définit l'addition et la multiplication sur $\mathbf{Q}$ comme:*

$$\frac{p}{q} + \frac{r}{s} := \frac{p_o s_o + r_o q_o}{s_o q_o} \qquad \frac{p}{q} \cdot \frac{r}{s} := \frac{p_o r_o}{s_o q_o};$$

où $(p_o, q_o) \in \frac{p}{q}$ et $(r_o, s_o) \in \frac{r}{s}$. Montrer que le résultat ne depend pas le représentant choisi.

Question 100. *L'ensemble d'entiers est un sous-ensemble de $\mathbf{Q}$, naturellement. Comment?*

On revient maintenant au monde des nombres entiers. Ce qui suit est un théorème qu'on a démontré dans le Chapitre 1. Ici, nous répétons le théorème avec l'idée que le théorème fondamental de l'arithmétique pourrait aider à fournir une autre preuve.

Théorème 101. *Soient a, b et n entiers. Si $a|n$ $b|n$ et $(a, b) = 1$ alors $ab|n$.*

Les entiers sont divisible par un nombre premier p ou par les entiers qui sont premiers à p.

Théorème 102. *Soit p un nombre premier et soit a un entier. Ensuite p ne divise pas n si et seulement si $(a, p) = 1$.*

On note que $9|6 \cdot 12$ et encore 9 ne divise pas 6 ou 12. Toutefois, si un premier divise un produit de deux entiers, alors il doit diviser l'un ou l'autre.

Théorème 103. *Soit p un nombre premier et soient a et b entiers. Si $p|ab$, alors $p|a$ ou $p|b$.*

Les théorèmes suivants explorent les relations entre le plus grand commun diviseur et diverses opérations arithmétiques. Vous pourriez envisager de faire la preuve d'au moins deux façons, l'une utilisant le théorème fondamental de l'arithmétique et l'autre utilisant les techniques du chapitre 1.

Théorème 104. *Soient a, b et c entiers. Si $(b, c) = 1$, alors $(a, bc) = (a, b)\Delta(a, c)$.*

Théorème 105. *Soient a, b et c entiers. Si $(a, b) = 1$ et $(a, c) = 1$, alors $(a, bc) = 1$.*

Théorème 106. *Soient a et b deux entiers. Si $(a, b) = d$, alors $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Théorème 107. *Soient a, b, u et v des entiers. Si (a, b) = 1 et $u \mid a$ et $v \mid n$, alors (u, v) = 1.*

2.3. **L'infinitude de nombres premiers.** Une des questions les plus fondamentales qu'on peut se demander sur les nombres premiers est : "Combien sont-ils?" Dans cette section, nous montrons qu'il existe une infinitude d'autres. Pour prouver qu'il existe une infinitude de nombres premiers, on doit montrer qu'il ya un grand nombres naturels qui ne sont pas le produit des nombres naturels plus petits. Nos premiers points d'observation remarquer que les nombres entiers naturels consécutifs ne peuvent pas partager diviseurs communs supérieurs à 1.

Théorème 108. *Pour tous les entiers n on a $(n, n + 1) = 1$.*

Pouvez-vous penser à un entier naturel qui est divisible par 2, 3, 4 et 5? Pouvez-vous penser à un entier naturel qui a un reste de 1 lorsqu'il est divisée par 2, 3, 4 et 5? Si vous pensez à des moyens systématiques pour répondre à ces questions, vous serez bien sur votre façon de prouver le théorème suivant.

Théorème 109. *Soit k un entier naturel. Alors il existe un entier naturel n (qui sera beaucoup plus grand que k) de telle sorte qu'aucune nombre naturel inférieur à k et supérieur à 1 divise n.*

Le théorème précédent nous montre comment produire des nombres naturels qui sont spécifiquement pas divisible par certains nombres naturels. Cette prise de conscience nous aide à trouver des nombres naturels qui ne sont pas divisible par aucun des nombres naturels autres qu'eux-mêmes et 1, en d'autres termes, les nombres premiers.

Théorème 110. *Soit* k *un entier naturel. Alors il existe une prime supérieure à* k*.*

Le théorème d'infinitude du nombres premiers est un des résultats de base des mathématiques. Il a été prouvé dans les temps anciens et est reconnu comme l'un des théorèmes fondamentaux. Au début, vous pourriez penser: "Bien sûr , il doit y avoir une infinité de nombres premiers. Comment pourrait-il pas y avoir une infinité de nombres premiers car il ya une infinité de nombres naturels?". Mais n'oubliez pas que la même prime peut être utilisé plusieurs fois. Par exemple, on peut construire arbitrairement grands nombres naturels tout en augmentant de 2 à de grandes puissances. Il est donc concevable que certains nombre fini de nombres premiers suffirait à produire tous les nombres naturels. Cependant, en fait, il ya une infinité de nombres premiers, comme vous allez maintenant prouver.

Théorème 111 (Infinitude de Nombres Premiers)**.** *Il y a une infinité de nombres premiers.*

Après avoir mis au point une preuve ou les preuves ou appris une preuve, il est satisfaisant de réfléchir sur la logique de l'argumentation et apprécier la beauté ou intelligence du raisonnement.

Question 112. *Quelles étaient les parties les plus intelligents ou les plus difficiles de votre preuve de le théorème d'infinitude du nombres premiers?*

L'un des principaux moyens que les nouvelles mathématiques créé est de prendre une suite et voir si elle peut être prolongée ou des variantes de celle-ci peut être prouvé. Dans le cas de l'infinité de nombres premiers, on peut se demander s'il existe une infinité de nombres premiers d'un certain type. Nous commençons par faire une observation sur le nombre congru à 1 modulo 4, qui sera ensuite on aide à prouver qu'il existe une infinité de nombres premiers de la forme $4k + 3$.

Théorème 113. *Si* $r_1, r_2, \ldots, r_m$ *sont des entiers naturels et chacun est congru à* 1 *modulo* 4*, alors le produit* $r_1 \cdot r_2 \cdot \ldots \cdot r_m$ *est aussi congru à* 1 *modulo* 4*.*

Pour prouver le théorème suivant, rappelez-vous la preuve de le théorème d'infinitude de nombres premiers et voyez comment la stratégie de cette preuve peut être adapté à démontrer le théorème suivant plus difficile .

Théorème 114 (Théorème d'infinitude de nombres premiers de la forme $4k + 3$)**.** *Il ya une infinité de nombres premiers congrus à* 3 *modulo* 4*.*

Lorsque on a prouvé le théorème précédent, on peut se-même forcé de comprendre une technique de démontrer des théorèmes sur l'existence d'une infinité de nombres premiers d'un certain type. Maintenant on va voir dans quelle mesure cette technique peut être poussé. En d'autres termes demandez-vous combien de théorèmes comme le précédent sont prouvables en utilisant une idée similaire .

Question 115. *Y at-il d'autres théorèmes comme la précédente que vous pouvez prouver?*

En fait, le théorème beaucoup plus générale qui suit est vrai. Sa preuve dans toute sa généralité, cependant, est assez difficile et nous ne tentera PAS dans ce cours.

Théorème 116. *Si* a *et* b *sont des nombres naturels premiers entre eux, alors il existe une infinité de nombres naturels* k *pour lequel* $ak + b$ *est un nombre premier.*

Le théorème précédent est souvent appelé du théorème de *Dirichlet* sur les nombres premiers dans une progression arithmétique et est due à Lejeune Dirichlet (1805-1859). Une *progression arithmétique* est une suite de nombres de la forme $ak + b$,$k = 1, 2, 3, \ldots$, où b est un entier quelconque, et a est un nombre naturel. Il s'agit d'une suite de nombres qui sont tous congru à b modulo a. L'étude des nombres premiers dans les progressions arithmétiques est un domaine encore actif aujourd'hui. Prenons le récent résultat suivant dû à Ben Green et Tao Terrence .

Théorème 117 (Green et Tao, 2005)**.** *Il y a des progressions arithmétiques arbitrairement longues de nombres premiers .*

Cela signifie que pour tout entier naturel n, il existe un nombre premier p et un entier naturel a tel que p , $p + a$, $p + 2a$, $p + 3a$, $\ldots$, $p + na$, sont tous premiers. À titre d'exemple, une progression arithmétique de nombres premiers de longueur cinq se trouve en choisissant $p = 5$ et $a = 6$, ce qui donne la séquence 5, 11, 17, 23, 29. Le plus long progess arithmétique des nombres premiers connus comme de Juillet 2004 a une longueur de 23 et est donnée par

$$56211383760397 + k44546738095860, k = 0, 1, \ldots, 22$$

. Terrence Tao a reçu la médaille Fields en partie pour son travail lié à ce résultat. Médailles Fields, l'équivalent mathématique du prix Nobel, est décerné une fois tous les quatre ans à des mathématiciens en circulation sous l'âge de 40 ans.

Exercice 118. *Trouvez le record actuel de la plus longue progression arithmétique de nombres premiers .*

2.4. **Nombres Premiers de Forme Spéciale.** Le plus grand nombre premier connu est d'un type spécial appelé un nombre premier de Mersenne, qui est un premier de la forme $2^n - 1$. Les théorèmes ici montrent certaines fonctionnalités de nombres premiers de Mersenne.

Exercice 119. *Utiliser division polynomiale de pour calculer* $(x^m - 1)/(x - 1)$.

Théorème 120. *Si* n *est un entier naturel et* $2^n - 1$ *est un nombre premier, alors* n *doit être un nombre premier.*

Théorème 121. *Si* n *est un entier naturel et* $2^n + 1$ *est premier, alors* n *doit être une puissance de* 2*.*

Définition 122. *Un nombre premier de Mersenne est un nombre premier de la forme* $2^p - 1$*, où* p *est un nombre premier. Un premier de la forme* $2^{2^k} + 1$ *est appelé un nombre premier de Fermat.*

Exercice 123. *Trouver* 5 *nombres premiers de Mersenne et* 5 *nombres premiers de Fermat.*

Exercice 124. *Pour un A dans la classe et d'un doctorat en mathématiques, montrer qu'il existe une infinité de nombres premiers de Mersenne (ou nombres premiers de Fermat) ou prouver qu'il n'y a pas (au choix).*

2.5. **La distribution des nombres premiers.** Comment les nombres premiers réparties entre les nombres naturels? Y at-il quelque motif de leur distribution? Il existe une infinité de nombres premiers, mais comment sont-ils rare chez les entiers naturels? Quelle est la proportion des nombres naturels sont des nombres premiers? Pour explorer ces questions, la meilleure façon de commencer est de regarder les nombres naturels et les nombres premiers entre eux. Voici donc quelques gammes de nombres naturels avec les premiers imprimés en caractères gras:

$$1, \mathbf{2}, \mathbf{3}, 4, \mathbf{5}, 6, \mathbf{7}, 8, 9, 10, \mathbf{11}, 12, \mathbf{13}, 14, 15, 16, \mathbf{17}, 18, \mathbf{19}, 20, 21, 22, \mathbf{23}, 24, \ldots$$

$$\ldots, 300, 301, 302, 303, 304, 305, 306, \mathbf{307}, 308, 309, 310, \mathbf{311}, 312, \mathbf{313}, 314, 315, 316, \ldots$$

$$\ldots, 2025, 2026, \mathbf{2027}, 2028, \mathbf{2029}, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, \ldots$$

Quelles observations peut-on faire? Tout d'abord, on peut noter que la proportion de nombres premiers devenir de plus. Autrement dit, nombres premiers ont tendance à être plus clairsemée que nous allons plus loin dans la séquence des entiers naturels. Dit d'une autre façon, on a tendance à voir plus et plus longtemps séries de nombres composés consécutifs.

Théorème 125. *Il existe arbitrairement longues chaînes des nombres composés. C'est-à-dire, pour tout entier naturel* n*, il existe une chaîne de plus de* n *nombres composés consécutifs.*

D'autre part, nous observons toujours des nombres premiers regroupés, par exemple 311 et 313 , ou 2027 et 2029. C'est une fameuse question ouverte de savoir si oui ou non ce comportement se poursuit indéfiniment. Si vous avez déjà réglé la question précédente à propos de nombres premiers de Mersenne, puis résoudre la question suivante vous donnera un autre Ph.D.

Question 126 (Conjecture des nombres premiers jumeaux)**.** *Y at-il une infinité de paires de nombres premiers qui diffèrent les uns des autres par deux? (Les paires* 11 *et* 13 *, 29 et* 31 *, 41 et* 43 *sont des exemples de certains de ces paires.)*

Dans les 24 premièrs nombres naturels, 9 d'entre eux sont des nombres premiers. On voit que $\frac{9}{24}$ des 24 premièrs 24 entiers naturels sont des nombres premiers , c'est juste un peu plus d'un tiers. On a vu comment cette fraction changements que n augmente dans le tamis de l'exercice Eratosthène.

n	$\pi(n)$	$\frac{n}{\log n}$	$\frac{\pi(n)}{n}$	$\frac{1}{\log n}$	$\frac{\pi(n)}{n/\log n}$
10	4	4.3...	0.4	0.43429...	0.92104...
10^2	25	21.7...	0.25	0.21714...	1.15133...
10^3	168	144.7...	0.168	0.14476...	1.16054...
10^4	1229	1085.7...	0.1229	0.10857...	1.13199...
10^5	9592	8685.8...	0.09592	0.08685...	1.10443...
10^6	78498	72382.4...	0.078498	0.07238...	1.08452...
10^7	664579	620420.7...	0.0664579	0.06204...	1.07121...
10^8	5761455	5428681.0...	0.05761455	0.05428...	1.06144...
10^9	50847534	48254942.4...	0.050847534	0.04825...	1.05385...

TABLE 1. Proportions du nombres premiers

Avant d'ordinateurs à haute vitesse sont disponibles, le calcul (ou juste estimation) la proportion des nombres premiers dans les nombres naturels est une tâche difficile. En fait, il y a "ordinateurs" années étaient en fait des êtres humains qui ont fait des calculs. Ces gens étaient étonnamment précise, mais nécessitaient beaucoup de temps et de dévouement pour accomplir ce que les ordinateurs d'aujourd'hui peuvent faire en quelques secondes. Un arithmetician autrichien du XVIIIe siècle sous le nom de JP Kulik a passé 20 années de sa vie à créer, à la main, un tableau des 100 premiers millions de nombres premiers. Son tableau n'a jamais été publié et, malheureusement, le volume contenant les nombres premiers entre 12642600 et 22852800 a disparu depuis.

Aujourd'hui, il ya des programmes qui calculent le nombre de nombres premiers inférieurs à n, notée $\pi($n, pour de plus grandes valeurs de n et imprimer la proportion : $\frac{\pi(n)}{n}$. Comme nous l'avons observé plus haut, la proportion des primes semble aller lentement vers le bas. Autrement dit, le pourcentage de numéros moins d'un million qui sont premiers est plus petit que le pourcentage de numéros moins d'un millier qui sont premiers. Les premiers, dans un certain sens, se clairsemée et clairsemée parmi les plus grands nombres.

Dans le début des années 1800, bien avant que les ordinateurs ont même imaginé, Carl Friedrich Gauss (1777-1855), connu par beaucoup comme le prince des mathématiques, et Adrien -Marie Legendre (1752-1833) a fait une observation perspicace sur les nombres premiers. Ils ont remarqué que même si les premiers ne semblent pas se produire dans n'importe quel schéma prévisible, la proportion des primes est liée au logarithme naturel.

Gauss et Legendre conjecturèrent que la proportion de nombres premiers parmi les n premiers entiers naturels est d'environ $\frac{1}{\log n}$. Le Tableau 1 montre le nombre de nombres premiers jusqu'à n, les proportions des nombres premiers, et une comparaison avec $\frac{1}{\log n}$.

Remarquér comment la dernière colonne semble devenir de plus en plus proche de 1. C'est-à-dire, la proportion de nombres premiers dans les n premiers entiers naturels est d'environ 1 et la fraction $\frac{\pi(n)}{n}$ est de plus en plus proche de $\frac{1}{\log n}$.

Théorème 127 (Théorème des nombres premiers)**.** *Lorsque n tend vers l'infini, la proportion de nombres premiers inférieur ou égal à n, noteé $\frac{\pi(n)}{n}$, s'approche de $\frac{1}{\log n}$. C'est-à-dire,*

$$\lim_{n \longrightarrow \infty} \left(\frac{\pi(n)/n}{1/\log n} \right) = 1.$$

Les démonstrations de ce théorème sont difficiles, et au-delà de la portée de ce livre. Enfin, nous mentionnons ici encore une question ouverte célèbre concernant nombres premiers.

Exercice 128. *Exprimer chacun des 20 premiers entiers naturels pairs supérieurs à 2 comme une somme de deux nombres premiers. (Par exemple: $8 = 5 + 3$).*

Dans une lettre à Euler, en date du 7 Juin 1742, Christian Goldbach (1690-1764) a affirmé que chaque entier naturel supérieur à 2 est la somme de trois nombres premiers. C'était convention au moment d'inscrire l'entier 1 comme étant parmi les nombres premiers. La conjecture a été ré-exprimé par Euler comme suit:

Conjecture (La conjecture de Goldbach)**.** *Chaque positif, même entier supérieur à 2 peut être écrit comme la somme de deux nombres premiers.*

La conjecture de Goldbach a été vérifiée par ordinateur, à partir de Juin 2006, pour tous les nombres pairs jusqu'à $400,000,000,000,000,000$. Comme les entiers naturels pairs deviennent plus grandes, il semble y avoir d'autres façons de les écrire comme une somme de deux nombres premiers. Par exemple, l'entier $100,000,000$ peut s'écrire comme la somme de deux nombres premiers de $219,400$ façons différentes. Mais on ne sait pas comment prouver que, en général tous les nombres pairs naturelles sont la somme de deux nombres premiers. Peut-être un nombre pair avec 10 billions de chiffres n'est pas la somme de deux nombres premiers. Jusqu'à ce que on a une méthode générale de la preuve qui s'appliquera à tous les nombres pairs, on ne sait pas si un tel nombre naturel ne pourrait pas exister.

2.6. **De l'Antiquité à Internet.** L'intérêt pour les propriétés multiplicatif des nombres naturels sûrement précédé les œuvres d'Euclide (Éléments, Livres VII , VIII, IX), mais c'est ici que nous trouvons la première étude écrite. Par exemple, la Proposition 20 du Livre IX donne la première preuve connue de l'infinité de nombres premiers. L'intérêt des Grecs dans les premiers peut-être été plus engendré par la connexion qu'ils partageaient avec les nombres parfaits. Un entier naturel est dit être parfait si elle est égale à la somme de ses diviseurs propres. Par exemple, le plus petit nombre parfait est 6, depuis le $6 = 1 + 2 + 3$, et les quatre premiers nombres parfaits sont

$$\begin{aligned}
6 &= 2^{2-1}(2^2 - 1) = 1 + 2 + 3 \\
28 &= 2^{3-1}(2^3 - 1) = 1 + 2 + 4 + 7 + 14 \\
496 &= 2^{5-1}(2^5 - 1) = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 \\
28 &= 2^{7-1}(2^7 - 1) = 1 + 2 + 4 + 8 + 16 + \ldots + 2032 + 4064
\end{aligned}$$

Dans le livre IX de ses Eléments d'Euclide fut la suivante: si pour un certain n , 2^n-1 est premier, alors $2^{n-1}(2^n-1)$ est parfait. Cela a établi le lien entre les nombres parfaits et nombres premiers de la forme 2^n-1.

L'étude sérieuse des nombres parfaits et nombres premiers de formes spéciales a été reprise au XVIIe siècle par les goûts de René Descartes (1596-1650), Pierre de Fermat (1601-1665), et Marin Mersenne (1588-1648). Dans une lettre à Mersenne 1638, Descartes a déclaré qu'il pensait qu'il pouvait prouver que tout nombre pair parfaite était de la forme donnée par le théorème d'Euclide, mais aucune preuve n'a été donnée. En outre, dans une lettre à Mersenne, datée 1640, Fermat a indiqué qu'il avait prouvé la suivante: si n est un entier composé, alors 2^n-1 est composé aussi, mais si n est premier, alors $2n-1$ est pas forcément un nombre premier, avec deux exemples étant $2^{11}-1 = 23 \cdot 89$, et $2^{23}-1 = 47 \cdot 178481$.

En 1647, Mersenne a donné la liste suivante de 11 nombres premiers p pour lesquels il croyait 2^p-1 était premier aussi : 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. Il a commis une erreur en incluant seulement 67 (et en excluant 61, 89 et 107). A ce jour, nombres premiers de la forme 2^p-1 sont appelés nombres premiers de Mersenne, et il est encore inconnu s'il existe un infinité de nombre premiers de Mersenne. Dans un article publié à titre posthume, Euler finalement réussi à prouver que tous les nombres parfaits pairs sont du type d'Euclide, donnant une bijection entre nombres premiers de Mersenne et de nombres parfaits. Curieusement, on ne sait pas si des nombres parfaits impairs existent.

La recherche de nouveaux nombres premiers de Mersenne continue à ce jour. En fait, n'importe qui avec un ordinateur à la maison et une connexion Internet peut rejoindre l' Internet Grande Mersenne Prime Search (GIMPS). La liste de Mersenne a seulement été augmenté pour contenir 44 exemples comme de Septembre 2006, avec le plus grand ayant plus de 9,8 millions de chiffres.

Exercice 129. *Trouvez le record actuel pour le plus grand nombre premier de Mersenne connu.*

Il ya une récompense financière de 100,000$ pour la première personne (ou groupe) de trouver un nombre premier de Mersenne avec au moins 10 millions de chiffres . Bon chasse!

3. Systèmes de Congruence Linéaire

Dans le Chapitre 1, on a établi les bases de l'arithmétique modulaire. On procéde maintenant à voir comment l'arithmétique modulaire se rapporte à d'autres constructions algébriques familières telles que les fonctions et les équations, et comment il peut nous aider à mieux comprendre les nombres premiers et nombres composés.

Arithmétique modulaire est intéressant comme un sujet abstrait dans la théorie des nombres, mais elle joue également un rôle important dans la vie réelle. Il est la base de la cryptographie à clé publique (ou cryptographie asymétrique) et les chiffres de contrôle associées à la détection d'erreur. Ici, nous développons la théorie de l'arithmétique modulaire et explorer plus tard certaines de ses applications en dehors des mathématiques.

3.1. **Puissances et polynômes modulo n.** Rappeler la définition suivante de la congruence du Chapitre 1.

Définition 130. *Supposons que a, b et n sont des entiers avec $n > 0$. On dit que a et b sont congrus modulo n si et seulement si $n|(a - b)$. On le note par $a \equiv b$ (mod n) et lire ces symboles comme "a est congru à b modulo n".*

Voici quelques exercices qui encouragent à vous rafraîchir la mémoire sur certains des théorèmes d'arithmétique modulaire que vous avez prouvé dans Chapitre 1.

Exercice 131. *Montrer que 41 divise $2^{20} - 1$ en suivant ces étapes. Expliquez pourquoi chaque étape est vrai.*

- $2^5 \equiv -9$ *(mod 41)*
- $(2^5)^4 \equiv (-9)^4$ *(mod 41)*
- $2^{20} \equiv (-1)^2$ *(mod 41)*

Question 132. *Dans votre tête, est-ce que vous pouvez trouver l'entier naturel k, $0 \leq k \leq 11$, tel que $k \equiv 39^{453}$ (mod 12)? (Indication: Ne pas essayer de multiplier les , puis divisez par 12 Bien sûr , cette astuce est une plaisanterie plutôt boiteux , car si vous pouviez multiplier 39^{453} dans votre tête, vous ne seriez pas prendre un cours de théorie des nombres vous ... serait réalisant des exploits mentale dans certains "sideshow carnaval".)*

La question suivante continue à vous montrer la valeur de la pensée (et de l'arithmétique modulaire) plutôt que la force brutale .

Question 133. *Dans votre tête ou en utilisant du papier et un crayon, mais aucun calculatrice, pouvez-vous trouver un entier k, $0 \leq k \leq 6$, tel que $2^{50} \equiv k$ (mod 7).*

La question suivante vous demande de calculer une puissance plus grande (453) d'un nombre modulo 12. Essayez de penser à comment le faire efficacement. Voici un indication. Si vous voulez élever un nombre à la 16e puissance, vous pouvez premier carré, puis place le résultat, puis place le résultat, puis place le résultat. Alors que quatre multiplications accomplir élevant à la puissance 16ème, plutôt que d'utiliser 16 multiplications. Aussi, n'oubliez pas que vous pouvez réduire réponses modulo 12, de sorte que vous n'aurez jamais à multiplier les nombres plus grand que 11. Tout en faisant l'exercice suivant, pensez à systématiser votre stratégie. En particulier, vous pouvez voir pourquoi votre stratégie pourrait impliquer exprimer 453 comme une somme de puissances de 2? Voyez si vous pouvez faire le problème suivant sans jamais multipliant le nombre de plus de 12 ans et sans faire plus de 10 étapes de la multiplication de deux nombres inférieurs à 12 et réduire les réponses modulo 12.

Question 134. *L'utilisation de papier et un crayon, mais aucun calculatrice, pouvez-vous trouver un entier naturel k , $0 \leq k \leq 11$, de sorte que $39^{453} \equiv k$ (mod 12).*

Maintenant vous avez développé le pouvoir de prendre des puissances, voici un autre exercice qui prend avantage de votre méthode.

Exercice 135. *Montrer que* 39 *divise* $17^{48} - 5^{24}$.

En ce moment, on a développé quelques idées sur la façon d'augmenter efficacement le nombre de puissances en arithmétique modulaire. La question suivante vous invite à cristalliser votre méthode et décrire clairement.

Question 136 (Décrire technique)**.** *Soient* a, n *et* r *entiers naturels. Décrivez comment on peut trouver un entier* k $(0 \leq k \leq n-1)$ *tel que* $k \equiv a^r$ *(mod* n*) soumis à la contrainte que vous ne multipliez le nombre plus grand que* n *et que vous avez seulement à faire sur* $\log_2(r)$ *tel multiplications.*

La technique que vous venez de développer et décrite permet aux ordinateurs de traiter en prenant de très grands entiers (contenant plusieurs centaines de chiffres) et de les élever à des puissances énormes modulo autres entiers énormes. La capacité des ordinateurs pour faire face à ces défis arithmétiquement -niques se révèle être un ingrédient essentiel dans les méthodes modernes de transmission sécurisée de données utilisé sur Internet tous les jours.

Nous nous tournons maintenant notre attention sur les polynômes et comment ils se comportent, vu du point de vue de l'arithmétique modulaire. Nous commençons par un exemple concret.

Question 137. *Soit* $f(x) = 13x^{49} - 27x^{27} + x^{14} - 6$. *Est-il vrai que* $f(98) \equiv f(-100)$(*mod* 99)*?*

Comme d'habitude, après avoir fait un exemple précis, nous pensons à ce déclaration plus générale l'exemple spécifique suggère.

Théorème 138. *Supposons que* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *est un polynôme de degré* $n > 0$ *avec des coefficients entiers. Soient* a, b *et* m *des entiers avec* $m > 0$. *Si* $a \equiv b$(*mod* m), *alors* $f(a) \equiv f(b)$(*mod* m).

Les prochaines corollaires sont des répétitions des résultats du chapitre 1 sur les critères permettant de déterminer si un nombre naturel est divisible par 3 ou 9. Ici, vous êtes invités à reconnaître un nombre naturel que l'évaluation d'un polynôme, et d'en déduire les déclarations suivantes du théorème précédent.

Corollaire 139. *Soit le nombre naturel* n *est exprimé en base* 10 *comme* $n = a_k a_{k-1} \cdots a_1 a_0$. *Soit* $m = a_k + a_{k-1} + \cdots + a_1 + a_0$. *Puis* $9|n$ *si et seulement si* $9|m$.

Corollaire 140. *Soit le nombre naturel* n *est exprimé en base* 10 *comme* $n = a_k a_{k-1} \cdots a_1 a_0$. *Soit* $m = a_k + a_{k-1} + \cdots + a_1 + a_0$. *Puis* $3|n$ *si et seulement si* $3|m$.

Au cours de votre travail sur le chapitre 1, vous avez peut-être imaginé d'autres critères de divisibilité. Si oui, est-ce polynôme vue de ces théorèmes de divisibilité vous aider à comprendre pourquoi vos méthodes sont vraies? Pouvez-vous penser maintenant de nouveaux théorèmes de divisibilité comme celle-ci?

Les deux prochaines théorèmes ne comportent pas de l'arithmétique modulaire. Ils affirment plus ou moins que tout polynôme devient grand.

Théorème 141. *Supposons que* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *est un polynôme de degré* $n > 0$ *et supoosons que* $a_n > 0$. *Ensuite, il existe un entier* k *tel que si* $x > k$, *alors* $f(x) > 0$.

Note: Nous supposons que le coefficient du terme de plus haut degré est supérieur à zéro. Les autres coefficients peuvent être positifs ou négatifs ou nuls.

Le théorème suivant étend l'idée que les polynômes obtenir positif et indique à peu près que non seulement obtiennent-ils positifs, mais ils deviennent grands et grand séjour de quelque point. Notez que le théorème ne vous demande pas d'être efficace et de trouver la première place après

que le polynôme reste supérieure à une certaine valeur. Il demande juste vous prouver que finalement ce qui se passe.

Théorème 142. *Supposons que* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *est un polynôme de degré* $n > 0$ *et supposons* $a_n > 0$*. Ensuite, pour tout nombre* M *il existe un entier* k *(qui dépend de* M*) de telle sorte que, si* $x > k$*, alors* $f(x) > M$*.*

Le théorème suivant relie polynômes avec des nombres premiers. Il dit que tout polynôme à coefficients entiers produit de nombres composites. Il n'y a pas de polynôme qui ne produit que des nombres premiers. Pour prouver la théorème suivant, il pourrait être utile de réfléchir à l'arithmétique modulaire. Rappelez-vous que si un nombre est congru à 0 modulo n, alors n divise le nombre, et étant divisible est la question fondamentale d'être composite. La preuve du théorème suivant est un défi, mais si vous regardez juste, alors vous pouvez donner une preuve convaincante. Donc, l'astuce consiste à utiliser les théorèmes 138 et 142.

Théorème 143. *Supposons que* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *est un polynôme de degré* $n > 0$ *avec des coefficients entiers. Alors* $f(x)$ *est un nombre composé pour une infinité d'entiers* x*.*

Note: Ce théorème implique que nous ne pouvons pas trouver un polynôme magique qui ne produit que des valeurs de choix pour chaque entrée entière. Mais, certains polynômes font assez bien. Le polynôme $f(x) = x^2 + x + 41$ a une valeur nominale (c'est-à-dire $f(n)$ est un nombre premier) pour 80 entrées entières consécutives , $n = -40, -39, \cdots, 38, 39$. Essayez un peu de valeurs à tester cette affirmation.

Quand on pense à un nombre naturel modulo n, elle est conforme à un entier non négatif inférieur à n. Les prochaines broches théorème que l'idée vers le bas.

Théorème 144. *Étant donné un entier et un nombre naturel* n*, il existe un entier* t *déterminé uniquement dans l'ensemble* $\{0, 1, 2, ..., n-1\}$ *telle que* $a \equiv t(\ mod\ n)$*.*

3.2. **Congruences Linéaires.** Dans le premier chapitre, nous avons discuté de quelques questions sur la recherche de solutions pour les équations diophantiennes linéaires. Maintenant, nous allons prendre des questions analogues au sujet de trouver des solutions aux équations en arithmétique modulaire. Plus précisément, notre prochain objectif est de déterminer quand il existe des solutions à la congruence linéaire général

$$ax \equiv b(\ \mathrm{mod}\ n)$$

et la façon de trouver toutes les solutions. Une solution est une valeur entière de x qui rend la congruence vrai. Nous allons commencer par quelques exemples.

Exercice 145. *Trouver toutes les solutions dans le canonique système complet de résidus modulo n appropriée qui satisfont aux congruences linéaires suivantes:*

- $26x \equiv 14(\ mod\ 3)$
- $2x \equiv 3(\ mod\ 5)$
- $4x \equiv 7(\ mod\ 8)$
- $24x \equiv 123(\ mod\ 213)$ *(Cette congruence est fastidieux de faire par essais et erreurs, donc peut-être par nous devrions reporter travail sur elle pour l'instant et au lieu d'essayer de développer des techniques qui pourraient aider.)*

Ce théorème suivant relie clairement la question de savoir comment résoudre congruences linéaires avec les techniques de résolution d'équations diophantiennes linéaires que nous avons développés dans le chapitre 1 .

Théorème 146. *Soient* a*,* b *et* n *des entiers avec* $n > 0$*. Montrer que la* $ax \equiv b(\ mod\ n)$ *a une solution si et seulement s'il existe des entiers* x *et* y *tels que* $ax + ny = b$*.*

Ces théorèmes vous encourager à vous souvenir de votre travail du chapitre 1.

Théorème 147. *Soient* a, b *et* n *des entiers avec* $n > 0$. *L'équation* $ax \equiv b(\ mod\ n)$ *a une solution si et seulement si* $(a, n)|b$.

En ce moment, nous avons une condition spécifique qui indique si une congruence linéaire sera ou ne sera pas une solution . Nous pouvons utiliser ce critère pour voir si notre congruence différée dans l'exercice 145 a ou n'a pas de solution.

Question 148. *Étudier la 4e équation dans l'exercice 145 en utilisant théorème 147.*

Maintenant, nous allons effectivement résoudre la congruence de façon systématique . Comme d'habitude, ce travail est attacher de nouveau dans le travail que nous avons à résoudre des équations diophantiennes linéaires dans le chapitre 1 .

Utilisez l'algorithme d'Euclide pour trouver un x qui satisfait $24x \equiv 123(\ \mathrm{mod}\ 213)$. Trouver tous les x qui satisfont $24x \equiv 123(\ \mathrm{mod}\ 213)$.

Après avoir fait un exemple précis, comme d'habitude nous prenons du recul et essayons de décrire une procédure générale.

Question 149. *Soient* a, b *et* n *des entiers avec* $n > 0$. *Combien de solutions sont là pour la congruence linéaire* $ax \equiv b(\ mod\ n)$ *dans les entiers naturels avec* $x < n$? *Pouvez-vous décrire une technique pour les trouver?*

Le théorème suivant donne la réponse, alors essayez de penser à travers sur votre propre avant de lire. Alors que penser de cette question, la cristallisation des idées sur les équations diophantiennes linéaires aidera.

Théorème 150. *Soient* a, b *et* n *des entiers avec* $n > 0$. *Ensuite:*

(1) *La congruence* $ax \equiv b(\ mod\ n)$ *est résoluble en entiers si et seulement si* $(a, n)|b$.
(2) *Si* x_0 *est une résolution de la congruence* $ax \equiv b(\ mod\ n)$, *alors toutes les solutions sont donnés par:*

$$x_0 + \left(\frac{n}{(a,n)} \cdot m\right)\ (\ mod\ n)$$

où $m = 0, 1, \ldots (a, n) - 1$.
(3) *Si* $ax \equiv b(\ mod\ n)$ *a une résolution, alors il y a exactement* (a, n) *ré solutions distinctes.*

3.3. **Systèmes de congruences linéaires: le théorème des restes chinois.** Parfois, dans la vie réelle, nous sommes confrontés à des problèmes impliquant des congruences linéaires simultanées. Quelque chose comme ce qui suit est probablement arrivé à vous.

Exercice 151. *Une bande de 17 pirates ont volé un sac de pièces d'or. Quand ils ont essayé de diviser la fortune en parties égales, 3 pièces sont restés. Dans la bagarre qui a suivi sur qui devrait obtenir les pièces supplémentaires, un pirate a été tué. Les pièces ont été redistribuées, mais cette fois 10 pièces sont restés. Encore une fois ils se sont battus pour savoir qui devrait obtenir les pièces restantes et un autre pirate a été tué. Maintenant, heureusement, les pièces peuvent être répartis équitablement entre les survivants 15 pirates. Quel était le plus petit nombre de pièces qui auraient pu être dans le sac?*

Peut-être votre expérience est moins violente et plus bucolique. Des œufs doivent compter aussi.

Exercice 152. *Lorsque les œufs dans un panier sont éliminés deux, trois, quatre, cinq ou six à la fois, il reste, respectivement, un, deux, trois, quatre, ou cinq œufs. Quand ils sont sortis sept à la fois, qu'aucun ne sont pas restés. T rouver le plus petit nombre d'œufs qui auraient pu être contenus dans le panier.*

Ces exercices sont difficiles mais amusant à faire. La question est maintenant de savoir si nous pouvons formuler des déclarations générales qui nous disent quand il existe des solutions à ces problèmes et comment ces solutions peuvent être trouvées. Ce premier théorème donne un critère pour quand nous pouvons trouver un résolution unique qui est conforme à deux valeurs différentes modulo deux modules différents. Cette résolution unique est appelé une solution à un système de deux congruences linéaires. Plus tard, nous allons envisager des solutions à arbitrairement grands systèmes de congruences linéaires.

Théorème 153. *Soient* a, b, m *et* n *sont des entiers avec* $m > 0$ *et* $n > 0$. *Ensuite, le système:*

$$\begin{aligned} x &\equiv a(\ mod\ n) \\ x &\equiv b(\ mod\ m) \end{aligned}$$

a une résolution si et seulement si $(n, m)|(a - b)$.

Le théorème suivant affirme que, dans le cas où $(m, n) = 1$, la solution est unique modulo le produit mn.

Théorème 154. *Soient* a, b, m *et* n *des entiers avec* $m > 0$, $n > 0$, *et* $(m, n) = 1$. *Ensuite, le système:*

$$\begin{aligned} x &\equiv a(\ mod\ n) \\ x &\equiv b(\ mod\ m) \end{aligned}$$

a une résolution unique $(\ mod\ mn)$.

Le théorème le plus célèbre le long de ces lignes est le théorème des restes chinois. Voici les modules sont premiers, mais il peut y avoir un nombre quelconque d'entre eux. Le problème de pirate est un problème du théorème des restes chinois dans le déguisement (éventuellement avec un bandeau sur l'œil). Le théorème des restes chinois se concerne L différentes congruences linéaires. Chaque fois que vous voyez un théorème ou d'un problème qui a un nombre élevé, c'est une bonne idée de commencer à penser aux cas où L est 1 ou 2 ou 3. Faire ces cas particuliers est un excellent moyen de vous apprendre à faire le cas général. Le théorème précédent vous permet de démarrer en faisant le cas $L = 2$. En outre, vous pourriez penser à induction en essayant de faire ensuite le cas général.

Théorème 155 (Théorème des restes chinois)**.** *Supposons que* $n_1, n_2, \ldots n_L$ *sont entiers naturels qui sont deux à deux premiers entre eux, c'est-à-dire* $(n_i, n_j) = 1$ *pour* $i \neq j\ 1 \leq i, j \leq L$. *Alors, le système de congruences:*

$$\begin{aligned} x &\equiv a_1(\ mod\ n_1) \\ x &\equiv a_2(\ mod\ n_2) \\ &\vdots \\ x &\equiv a_L(\ mod\ n_L) \end{aligned}$$

a une résolution unique modulo $n_1 \cdot n_2 \cdot \ldots \cdot n_L$.

4. Petit théorème de Fermat et Théorème d'Euler

4.1. **Ordres d'un entier modulo n.** Nous commençons ici d'explorer la façon puissances des nombres se comportent modulo n. Nous allons trouver une structure parmi les entiers modulo n qui est intéressant, a des applications en cryptographie et codes entre autres, et conduit à des idées centrales de la théorie des groupes. Comme d'habitude, nous allons faire des exemples précis afin de nous aider à développer une certaine intuition de ce que nous pourrions nous attendre.

Exercice 156. *Pour $i = 0, 1, 2, 3, 4, 5$, et 6, se trouve un entier qui 2^i est congru modulo 7. En d'autres termes, compter 2^0(mod 7), 2^1(mod 7), $\cdots$, 2^6(mod 7).*

Prenant puissances d'un entier ne peut pas créer des facteurs communs avec un autre entier s'il n'en existait pas pour commencer.

Théorème 157. *Soient a et n des entiers naturels avec $(a, n) = 1$. Puis $(a^j, n) = 1$ pour tout $j \in \mathbb{N}$.*

Réduire un entier modulo n ne peut pas créer un facteur commun avec n.

Théorème 158. *Soient a, b et n sont des entiers avec $n > 0$ et $(a, n) = 1$. Si $a \equiv b$(mod n), puis $(b, n) = 1$.*

Si on prend un certain nombre de différentes puissances d'un entier, on voit parfois obtenir les mêmes valeurs modulo n.

Théorème 159. *Soient a et n des entiers naturels. Ensuite, il existe des entiers naturels i et j, avec $i \neq j$, tel que $a^i \equiv a^j$(mod n).*

Le théorème suivant répète un théorème que nous avons vu avant, mais il est l'un des théorèmes les plus utilisés dans l'exploration des puissances, de sorte que vous devrait avoir sa déclaration et la preuve au bout de vos doigts.

Théorème 160. *Soient a, b, c et n sont des entiers avec $n > 0$. Si $ca \equiv bc$(mod n) et $(c, n) = 1$, alors $a \equiv b$(mod n).*

Le théorème suivant nous dit que si nous prenons un entier naturel qui est premier avec n, alors un certain puissance de celui-ci sera congru à 1 modulo n. Une conséquence de ce théorème est que, après une puissance arrive à 1, les puissances vont tout simplement recycler.

Théorème 161. *Soient a et n des entiers naturels avec $(a, n) = 1$. Alors il existe un entier naturel k tel que $a^k \equiv 1$(mod n).*

Le théorème précédent nous dit que chaque entier naturel premier avec un module n a un exposant naturellement associée, à savoir, le plus petit exposant qui fait la puissance congru à 1. Ce concept est si utile que nous lui donnons un nom.

Définition 162. *Soient a et n des entiers avec $(a, n) = 1$. Le plus petit entier naturel k tel que $k \equiv 1$(mod n) est appelé l'ordre de a modulo n et est noté $\mathrm{ord}_n(a)$.*

4.2. **Le Petit Théorème de Fermat.** Le théorème culminant de cette section est petit théorème de Fermat. Il nous donne des informations sur ce que la puissance d'un certain entier sera congru à 1 modulo un nombre premier. Nous allons aborder ce théorème en trouvant d'abord une sorte de limite sur la taille de l'ordre d'un nombre naturel. Expérimenter avec des chiffres réels est une bonne façon de commencer.

Question 163. *Choisir deux entiers naturels qui sont premier entre eux, a et n, et calculer l'ordre de a modulo n. Créez une conjecture sur la façon grande de l'ordre de un modulo n peut être, en fonction de n.*

En faisant vos expériences de prendre un certain nombre de puissances, vous avez sans doute remarqué que jusqu'à ce que le puissance était congru à 1 modulo n, les valeurs modulo n ne se répète jamais. Cette observation est le contenu du théorème suivant.

Théorème 164. *Soient* a *et* n *des entiers naturels avec* $(a, n) = 1$ *et soit* $k = \mathrm{ord}_n(a)$. *Ensuite, les nombres* $a^1, a^2, \ldots, a^k$ *sont deux à deux incongrues modulo* n.

Prenant puissances d'un entier naturel au-delà de son ordre ne pourra jamais produire des entiers différents modulo n.

Théorème 165. *Soient* a *et* n *des entiers naturels avec* $(a, n) = 1$ *et soit* $k = \mathrm{ord}_n(a)$. *Pour tout entier naturel* m , a^m *est congruent modulo* n *à l'un des nombres* $a^1, a^2, \ldots, a^k$.

Les seules puissances d'un entier naturel qui donnent 1 modulo n sont des puissances qui sont des multiples de l'ordre.

Théorème 166. *Soient* a *et* n *des entiers naturels avec* $(a, n) = 1$, *soit* $k = \mathrm{ord}_n(a)$, *et soit* M *un entier naturel. Alors suis* $a^m \equiv 1 (\ mod\ n)$ *si et seulement si* $k|m$.

Ce théorème suivant peut-être ce que vous conjecturé quand vous avez fait vos expériences concernant l'ordre dans la première question de cette section. Il indique que l'ordre d'un entier naturel, c'est-à-dire la puissance que vous obtient d'abord à 1 modulo n, est inférieur à n.

Théorème 167. *Soient* a *et* n *des entiers naturels avec* $(a, n) = 1$. *Puis* $\mathrm{ord}_n(a) < n$.

La question suivante vous demande de faire quelques expériences qui pourraient vous conduire à faire une conjecture sur les puissances des entiers modulo des nombres premiers. Vous aurez probablement faire la conjecture que nous verrons plus tard est en fait un théorème, le petit théorème de Fermat.

Exercice 168. *Calculer* $a^{p-1} (\ mod\ p)$ *pour différents nombres premiers* p *et entiers* a, *et faire une conjecture.*

Multipliant tous les entiers naturels inférieurs à un nombre premier p donnera le même résultat modulo p en multipliant un multiple fixe de un de ces entiers.

Théorème 169. *Soit* p *un nombre premier et soit* a *un entier non divisible par* p. *Puis*

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) (\ mod\ p)$$

Ce théorème peut être utilisée pour prouver le petit théorème de Fermat, qui suit. Nous affirmons deux versions du petit théorème de Fermat, mais vous demandons de prouver que les deux versions sont équivalentes à l'autre. Deux d'entre eux nous disent les faits importants et applicables sur les puissances des entiers naturels modulo un nombre premier.

Théorème 170 (Le petit théorème de Fermat, v1)**.** *Si* p *est un nombre premier et* a *est un entier naturel avex* $(a, p) = 1$, *alors* $a^{p-1} \equiv 1 (\ mod\ p)$.

Théorème 171. *Si* p *est un nombre premier et* a *est un entier naturel avex* $(a, p) = 1$, *alors* $a^p \equiv a (\ mod\ p)$.

Théorème 172. *Les deux versions du petit théorème de Fermat indiquées ci-dessus sont équivalentes à l'autre, c'est-à-dire chacun peut être déduite de l'autre.*

Le petit théorème de Fermat affirme qu'un entier naturel non divisible par p, élevé à la $(p-1)$-ième puissance, est congru à 1 modulo p. Rappelons que l'ordre d'un entier naturel est la plus petite puissance qui est congru à 1 modulo p. Le théorème suivant indique que l'ordre de chaque numéro doit diviser $(p-1)$.

Théorème 173. *Soit* p *un nombre premier et soit* a *un entier. Si* $(a, p) = 1$, *alors* $\mathrm{ord}_p(a)$ *divise* $p - 1$, *c'est-à-dire* $\mathrm{ord}_p(a)|(p - 1)$.

Une des applications impressionnantes du petit théorème de Fermat est qu'il nous permet de faire des calculs impliquant arithmétique modulaire qui serait impossible autrement.

Exercice 174. *Calculer chacun des exercices suivants, sans l'aide d'une calculatrice ou un ordinateur:*

- 512^{372}(*mod* 13)
- 3444^{3233}(*mod* 17)
- 123^{456}(*mod* 23)

Exercice 175. *Trouver le reste de la division de* 314^{159} *par* 31.

Le petit théorème de Fermat nous dit d'informations sur les modules principaux, mais comment allons-nous faire face à des modules qui ne sont pas premier? Une stratégie consiste à décomposer un composite (non premier) module en parties qui sont premiers entre eux. Le théorème suivant montre qu'un entier naturel qui est conforme à un entier fixe modulo deux modules différents, relativement premier est conforme à ce même numéro modulo le produit des modules. Par exemple, si vous avez un entier naturel qui est congru à 12 modulo 15 et le même nombre est congru à 12 modulo 8, ce nombre est aussi conforme à 12 modulo $120 (= 8 \cdot 15)$.

Théorème 176. *Soient* n *et* m *des entiers naturels qui sont premier entre eux, et soit* a *un entier. Si* $x \equiv a$(*mod* n) *et* $x \equiv a$(*mod* m), *alors* $x \equiv a$(*mod* mn).

Exercice 177. *Trouver le reste lorsque* 472 *est divisé par* 91.

Quand on voit des pouvoirs et un module, c'est une bonne idée de penser à le module comme un produit de nombres premiers et ensuite voir si vous pouvez utiliser le petit théorème de Fermat à son avantage.

Exercice 178. *Trouver l'entier naturel* $k < 117$ *tel que* $2^{117} \equiv k$(*mod* 117). *(Indication: Notez que 117 n'est pas premier.)*

UNIVERSITÉ GALATASARAY