Concours : Troisième CAPES

Section : Mathématiques

Session 2018

Rapport de jury présenté par : Monsieur Loïc FOISSY

Président du jury

Conseil aux futurs candidats

Il est recommandé aux candidats de s'informer sur les modalités du concours.

Les renseignements généraux (conditions d'accès, épreuves, carrière, etc.) sont donnés sur le site du ministère de l'Éducation nationale de l'enseignement supérieur et de la recherche :

http://www.devenirenseignant.gouv.fr/

Le jury du CAPES externe de Mathématiques met à disposition des candidats et des formateurs un site spécifique :

http://capes-math.org/

L'épreuve écrite de cette session s'est tenue le 4 avril 2018.

Les épreuves orales se sont déroulées les 9 et 10 juin 2018, dans les locaux du lycée Henri Loritz de Nancy. Le jury tient à remercier chaleureusement Monsieur le Proviseur et l'ensemble des personnels du lycée pour la qualité de leur accueil. Que soient également remerciés pour leur grande disponibilité les personnels du Département des Examens et Concours de l'académie de Nancy-Metz, ainsi que les services de la Direction Générale des Ressources Humaines qui ont œuvré avec beaucoup de diligence pour que le concours ait lieu dans de bonnes conditions.

Nous tenons à remercier tout particulièrement Messieurs François Avril et Yann Hermans pour la conception et la mise en œuvre du système **CAPES**OS, ainsi que pour leur implication sans faille tout au long du concours.

Table des matières

1 Présentation du concours 4

2 Quelques statistiques 4

2.1 Répartition des notes : épreuve d'admissibilité 4
2.2 Répartition des notes : épreuve d'admission 4
2.3 Répartition des notes : total 5
2.4 Autres données 6

3 Analyse et commentaires 8

3.1 Épreuve écrite 8
3.2 Épreuve orale 11

4 Annexe : ressources diverses 13

1 Présentation du concours

La forme et les programmes des épreuves du concours sont définis par l'arrêté du 19 avril 2013 fixant les sections et les modalités d'organisation des concours du certificat d'aptitude au professorat du second degré (MENH1310120A). Cet arrêté a été publié :

· au journal officiel de la République française nº 0099 du 27 avril 2013 ;
· sur le serveur SIAC2 dans le guide concours personnels enseignants, d'éducation et d'orientation des collèges et lycées.

2 Quelques statistiques

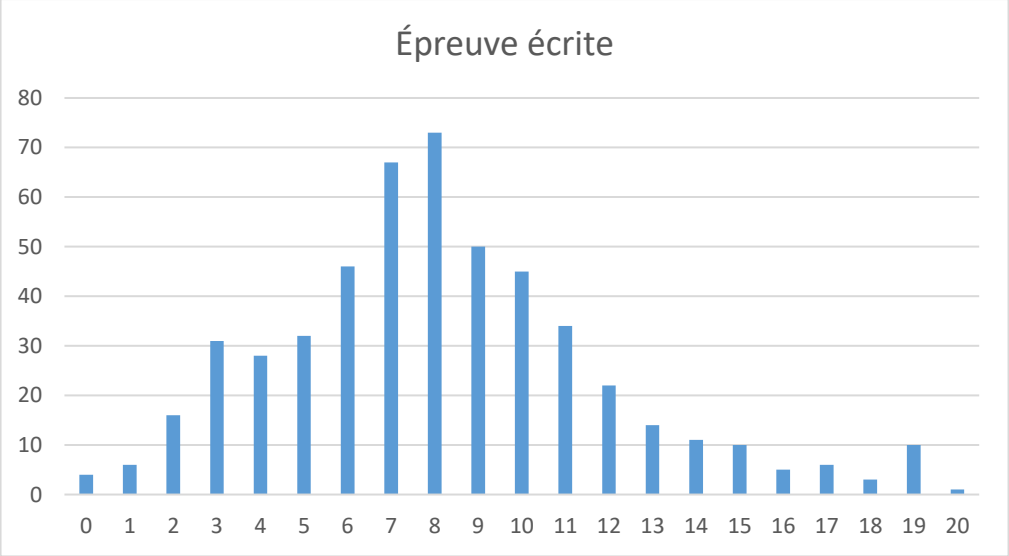
Les données suivantes concernent les concours du CAPES et du CAFEP réunis. Sauf mention contraire, les notes indiquées sont sur 20.

2.1 Répartition des notes : épreuve d'admissibilité

514 candidats se sont présentés à l'épreuve d'admissibilité : 432 pour le CAPES, 82 pour le CAFEP. Parmi eux, 4 ont été éliminés pour avoir obtenu la note 0. La barre d'admissibilité a été fixée à 7,2 pour le CAPES, ce qui a donné 223 admissibles et à 10,2 pour le CAFEP, ce qui a donné 14 admissibles.

Épreuve écrite

Moyenne	Écart type	Quartiles		
		Q1	Q2	Q3
7,69	3,80	5,20	7,36	9,65

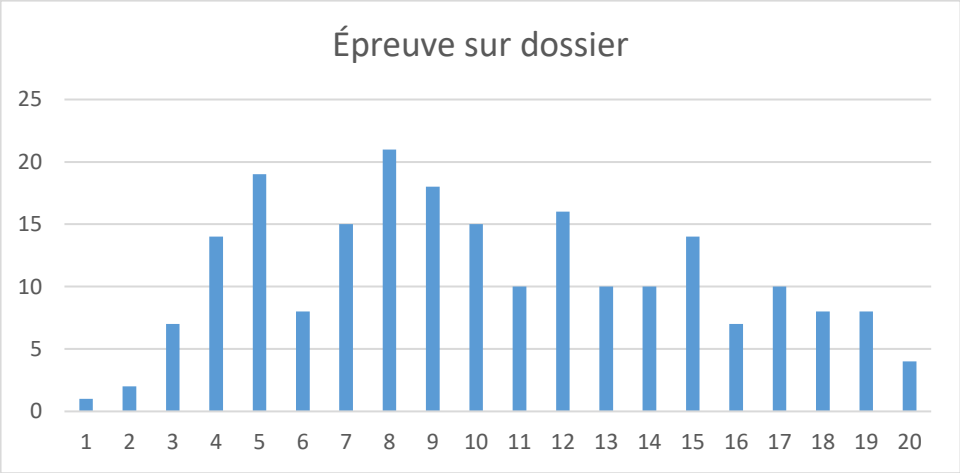


2.2 Répartition des notes : épreuve d'admission

Pour le CAPES, le jury a fixé la barre d'admission à 16,6/40, ce qui a permis de pourvoir 136 postes sur les 145 proposés. Pour le CAFEP, le jury a fixé la barre d'admission à 24/40, ce qui a permis de pourvoir les 7 postes proposés. 20 des 237 admissibles ne se sont pas présentés à l'épreuve orale. Ils ne sont pas comptabilisés dans les tableaux qui suivent.

Épreuve sur dossier

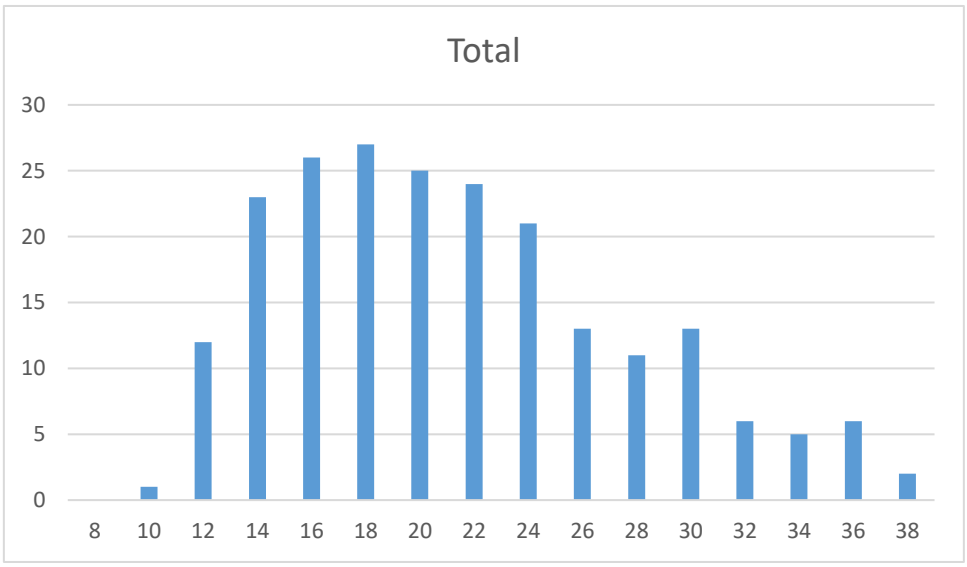
Moyenne	Écart type	Quartiles		
		Q1	Q2	Q3
9,86	4,70	6,21	9,20	13,45

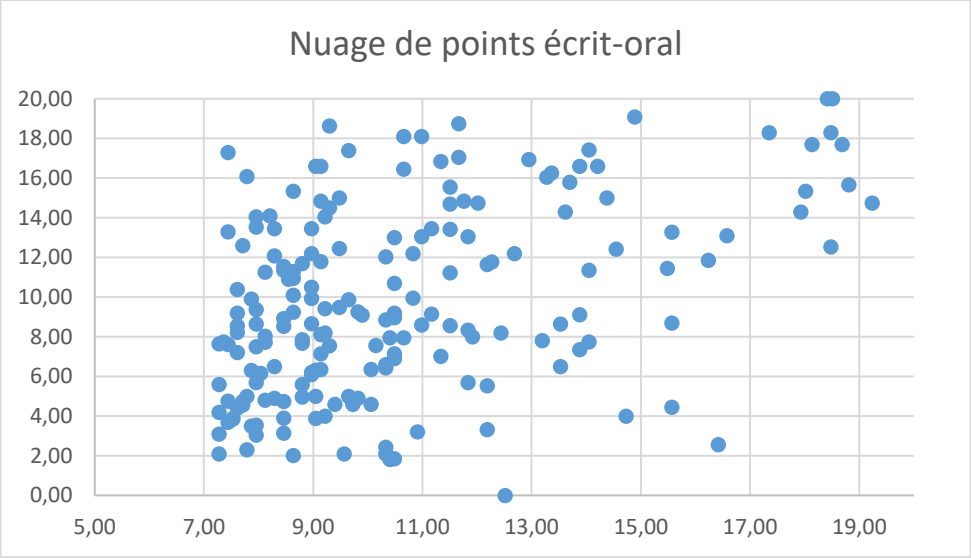


2.3 Répartition des notes : total

Note totale (écrit et oral, sur 40)

Moyenne	Écart type	Quartiles		
		Q1	Q2	Q3
20,54	6,63	15,18	19,60	24,9





Sur ce nuage de points, les notes à l'épreuve d'admissibilité se trouvent en abscisse et les notes à l'épreuve d'admission en ordonnée.

Le coefficient de corrélation entre les épreuves écrite et orale est de 0,46.

2.4 Autres données

Les données suivantes concernent les concours du CAPES et CAFEP réunis, en distinguant les candidats admissibles et les admis. Elles ont été établies à partir des renseignements fournis par les candidats au moment de leur inscription.

	Présents		Admissibles		Admis	
Hommes	345	67%	166	70%	94	66%
Femmes	169	33%	71	30%	49	34%
Total	514		237		143	

ACADEMIE	Présents		Admissibles		Admis	
AIX-MARSEILLE	32	6,23%	13	5,49%	5	3,5%
AMIENS	10	1,95%	1	0,42%	0	0,0%
BESANCON	8	1,56%	3	1,27%	2	1,4%
BORDEAUX	20	3,89%	15	6,33%	9	6,3%
CAEN	11	2,14%	5	2,11%	3	2,1%
CLERMONT-FERRAND	3	0,58%	2	0,84%	1	0,7%
CORSE	1	0,19%	0	0,00%	0	0,0%
CRETEIL-PARIS-VERSAIL.	118	22,96%	59	24,89%	37	25,9%
DIJON	6	1,17%	3	1,27%	1	0,7%
GRENOBLE	28	5,45%	11	4,64%	6	4,2%
GUADELOUPE	2	0,39%	1	0,42%	1	0,7%
GUYANE	1	0,19%	1	0,42%	1	0,7%

LA REUNION	13	2,53%	7	2,95%	4	2,8%
LILLE	24	4,67%	15	6,33%	7	4,9%
LIMOGES	5	0,97%	3	1,27%	3	2,1%
LYON	41	7,98%	20	8,44%	12	8,4%
MARTINIQUE	7	1,36%	3	1,27%	2	1,4%
MAYOTTE	0	0,00%	0	0,00%	0	0,0%
MONTPELLIER	22	4,28%	12	5,06%	8	5,6%
NANCY-METZ	11	2,14%	5	2,11%	4	2,8%
NANTES	27	5,25%	10	4,22%	4	2,8%
NICE	16	3,11%	5	2,11%	3	2,1%
NOUVELLE CALEDONIE	2	0,39%	0	0,00%	0	0,0%
ORLEANS-TOURS	13	2,53%	6	2,53%	2	1,4%
POITIERS	8	1,56%	4	1,69%	3	2,1%
POLYNESIE FRANCAISE	2	0,39%	0	0,00%	0	0,0%
REIMS	4	0,78%	2	0,84%	0	0,0%
RENNES	22	4,28%	8	3,38%	8	5,6%
ROUEN	10	1,95%	4	1,69%	4	2,8%
STRASBOURG	21	4,09%	11	4,64%	6	4,2%
TOULOUSE	26	5,06%	8	3,38%	7	4,9%
TOTAL	514	100,00%	237	100,00%	143	100,0%

PROFESSION	Présents		Admissibles		Admis	
AG NON TIT FONCT HOSPITAL	1	0,2%	1	0,4%	1	0,70%
AG NON TIT FONCT TERRITORIALE	2	0,4%	1	0,4%	1	0,70%
AGRICULTEURS	1	0,2%	0	0,0%	0	0,00%
ARTISANS / COMMERCANTS	6	1,2%	3	1,3%	3	2,10%
ASSISTANT D'EDUCATION	13	2,5%	6	2,5%	3	2,10%
CADRES SECT PRIVE CONV COLLECT	145	28,3%	87	36,7%	57	39,86%
CERTIFIE	2	0,4%	0	0,0%	0	0,00%
CONTRACT ENSEIGNANT SUPERIEUR	2	0,4%	1	0,4%	1	0,70%
CONTRACTUEL 2ND DEGRE	79	15,4%	29	12,2%	16	11,19%
CONTRACTUEL APPRENTISSAGE(CFA)	1	0,2%	0	0,0%	0	0,00%
ENS.STAGIAIRE 2E DEG. COL/LYC	5	1,0%	3	1,3%	1	0,70%
ENSEIG NON TIT ETAB SCOL.ETR	2	0,4%	1	0,4%	1	0,70%
ETUD.HORS ESPE (PREPA CNED)	2	0,4%	1	0,4%	1	0,70%
ETUD.HORS ESPE (PREPA MO.UNIV)	1	0,2%	0	0,0%	0	0,00%
ETUD.HORS ESPE (PREPA PRIVEE)	1	0,2%	0	0,0%	0	0,00%
ETUD.HORS ESPE (SANS PREPA)	3	0,6%	0	0,0%	0	0,00%
ETUDIANT EN ESPE EN 1ERE ANNEE	26	5,1%	22	9,3%	19	13,29%
ETUDIANT EN ESPE EN 2EME ANNEE	1	0,2%	1	0,4%	1	0,70%
FORMATEURS DANS SECTEUR PRIVE	23	4,5%	12	5,1%	7	4,90%
INSTITUTEUR SUPPLEANT	1	0,2%	0	0,0%	0	0,00%
MAITRE AUXILIAIRE	27	5,3%	1	0,4%	0	0,00%
MAITRE DELEGUE	1	0,2%	0	0,0%	0	0,00%
PERS ENSEIG NON TIT FONCT PUB	3	0,6%	2	0,8%	0	0,00%
PERS ENSEIG TIT FONCT PUBLIQUE	1	0,2%	1	0,4%	1	0,70%
PERS FONCT TERRITORIALE	2	0,4%	0	0,0%	0	0,00%
PERS FONCTION PUBLIQUE	5	1,0%	1	0,4%	0	0,00%
PLP	2	0,4%	2	0,8%	0	0,00%
PROF DES ECOLES STAGIAIRE	2	0,4%	1	0,4%	0	0,00%
PROFESSEUR ECOLES	1	0,2%	0	0,0%	0	0,00%
PROFESSIONS LIBERALES	18	3,5%	10	4,2%	4	2,80%

SALARIES SECTEUR INDUSTRIEL	24	4,7%	8	3,4%	4	2,80%
SALARIES SECTEUR TERTIAIRE	51	9,9%	18	7,6%	10	6,99%
SANS EMPLOI	49	9,6%	25	10,5%	12	8,39%
SURVEILLANT D'EXTERNAT	2	0,4%	0	0,0%	0	0,00%
VACATAIRE DU 2ND DEGRE	7	1,4%	0	0,0%	0	0,00%
VACATAIRE ENSEIGNANT DU SUP.	1	0,2%	0	0,0%	0	0,00%
TOTAL	513	100,0%	237	100,0%	143	100,0%

Age	Présents		Admissibles		Admis	
25-29	23	4,5%	11	4,6%	7	4,9%
30-34	66	12,8%	35	14,8%	22	15,4%
35-39	103	20,0%	50	21,1%	33	23,1%
40-44	129	25,1%	55	23,2%	35	24,5%
45-49	112	21,8%	52	21,9%	30	21,0%
50-54	45	8,8%	18	7,6%	8	5,6%
55-59	26	5,1%	12	5,1%	7	4,9%
60-64	10	1,9%	4	1,7%	1	0,7%

L'âge moyen des candidats présents à l'épreuve écrite était de 42,7 ans ; l'âge moyen des candidats admissibles était de 42,2 ans ; l'âge moyen des candidats admis était de 41,5 ans. Le candidat présent le plus jeune avait 26,1 ans et le plus âgé 63,9 ans. Le candidat admissible (puis admis) le plus âgé avait 63,1 ans et le plus jeune, lui aussi admis, 26,5 ans.

3 Analyse et commentaires

Le sujet ainsi qu'un corrigé de l'épreuve écrite se trouve sur le site du jury http://capes-math.org/.

3.1 Épreuve écrite

Le sujet de l'**épreuve d'admissibilité** était composé de deux problèmes indépendants.

Le premier problème envisageait l'étude d'une méthode de chiffrement d'un message, lettre à lettre, construite à partir de fonctions puissances définies comme

$$f_k : R = [\![0;28]\!] \longrightarrow R$$

$$x \longmapsto x^k \bmod 29$$

Le problème était composé de trois parties. La partie A décrivait des premiers essais (pour $k = 3, 7, 19$) et permettait aux candidats de comprendre la méthode de chiffrement proposée. La partie B amenait les candidats à déterminer les *k* pour que les fonctions f_k associées permettent d'assurer le déchiffrement du message. Enfin, la partie C s'intéressait à trois méthodes de calcul de f_{19}.

Le second problème était composé de deux parties. La partie A étudiait d'abord les points constructibles à la règle et au compas dans un plan muni d'un repère orthonormé (*O*, *I*, *J*) puis les nombres constructibles, en tant qu'abscisses dans (*O*, *I*, *J*) de points constructibles. Les candidats devaient démontrer la constructibilité de plusieurs autres éléments, comme la médiatrice d'un segment d'extrémités deux points constructibles, la parallèle et la perpendiculaire à une droite définie par deux points constructibles passant par un point constructible, l'opposé d'un nombre constructible, la somme, la différence, le produit et le quotient de deux nombres constructibles, la racine carrée d'un nombre

constructible... La partie B était centrée sur les polygones réguliers avec l'étude des racines *n*-ième de l'unité, sur les conditions nécessaires et suffisantes de constructibilité des sommets d'un polygone régulier à *n* côtés et sur la construction effective des polygones réguliers à 3, 4 et 6 côtés. Enfin, la partie B s'achevait sur la construction à la règle et au compas du pentagone régulier.

Ces deux problèmes pouvaient permettre d'apprécier, outre les qualités scientifiques des candidats, leur aptitude à se placer dans une optique professionnelle, notamment avec des références explicites aux pratiques d'un élève de troisième (problème 1, A.III) ou à une classe de collège (problème 2, IV).

Le jury a prêté une attention particulière aux compétences suivantes.

— *Divisibilité : utilisation du lemme de Gauss*

Pour cet item, il était demandé aux candidats de répondre correctement à l'une des deux questions B.VII.1 ou B.X.2. Environ 29 % des candidats ont répondu correctement à l'une des deux questions ; environ 41,7 % des candidats n'ont répondu correctement à aucune des deux questions ou de manière incomplète ; environ 29,4 % des candidats n'ont abordé aucune des deux questions.

— *Bonne utilisation du tableur (poignée de recopie)*

Pour cet item, il était demandé aux candidats de répondre correctement à l'une des questions A.III ou C.XIV.1 et C.XV.A ou C.XV.3. Environ 41,5 % des candidats ont validé cet item ; 35,2 % des candidats n'ont pas validé cet item ou de manière incomplète ; environ 23,3 % des candidats n'ont traité aucune des questions examinées.

— *Écrire un algorithme (boucle Tant que)*

Pour cet item, il était demandé aux candidats de répondre correctement à la question B.VIII.4. Environ 8,6 % des candidats ont répondu correctement à la question ; environ 12,5 % des candidats n'ont pas répondu correctement à la question ou de manière incomplète ; environ 78,9% des candidats n'ont pas abordé la question. Environ 40,7% des candidats ayant abordé cette question y ont répondu correctement.

— *Racines n-ièmes de l'unité*

Pour cet item, il était demandé aux candidats de répondre correctement à la question B.IX.1. Environ 11,7 % des candidats ont répondu correctement à la question ; environ 32,1 % des candidats n'ont pas répondu correctement à la question ou de manière incomplète ; environ 56,2 % des candidats n'ont pas abordé la question. Environ 26,7 % ces candidats ayant abordé cette question y ont répondu correctement.

Dans l'ensemble des copies, des compétences ont été régulièrement manifestées comme, dans le problème 1, l'utilisation du tableur ou la résolution de l'équation diophantienne lorsqu'elle est abordée et, pour le problème 2, la rédaction de programmes de construction.

En revanche, d'autres compétences révèlent un degré de maîtrise insuffisant, comme en témoignent les maladresses ou erreurs suivantes : l'utilisation de quantificateurs ou de symboles comme de simples abréviations sans valeur logique (symbole d'implication pour « donc », par exemple), la rédaction très incomplète de démonstrations (hypothèses partielles ou conditions d'utilisation d'un théorème non systématiquement vérifiées, omission des cas particuliers…), la définition de la bijectivité d'une fonction (souvent confondue avec la seule injectivité). Les quantificateurs sont trop souvent absents de l'énoncé des propositions mathématiques et lorsqu'ils sont utilisés, ce n'est pas toujours de manière correcte. De nombreux symboles mathématiques (comme $=, \neq, \in, \notin, \nexists, \exists, \forall$) sont employés à l'intérieur d'une phrase rédigée.

De façon générale, les candidats n'exploitent pas suffisamment les résultats obtenus dans les questions précédentes. *A contrario*, beaucoup de candidats utilisent des résultats qu'il s'agit de démontrer dans les questions suivantes. Nous recommandons de bien lire le sujet de l'épreuve. En outre, les candidats ont trop peu recours à un langage mathématique formalisé et à un lexique approprié. Ils ne vérifient que trop rarement les hypothèses avant d'appliquer une propriété. Trop souvent, les candidats justifient leurs affirmations par des arguments approximatifs introduits par « il est facile de voir que… », « il est clair que… », « c'est évident » ou encore « forcément… », mais pas de manière mathématique et rigoureuse en citant explicitement les définitions ou les théorèmes utilisés. De nombreuses réponses apportées par les candidats sont longues et imprécises. Cela donne souvent l'impression que le candidat souhaite écrire le plus possible pour augmenter ses chances de fournir un élément attendu par le jury. En outre, de nombreuses copies montrent un niveau de langue très insuffisant (orthographe et syntaxe). Nous rappelons que la rédaction doit être argumentée, rigoureuse et claire.

Problème 1

Les candidats ont en général bien réussi le cryptage des messages.

Une partie non négligeable des candidats montre une fragilité certaine en arithmétique : confusion entre « *k* divise *p* » et « *k* est divisible par *p* », identification de la fraction $\frac{a}{b}$ avec le quotient de la division euclidienne de *a* par *b*, confusion entre la division euclidienne de *n* par *p* avec « *p* divise *n* », utilisation de « si *p* divise le produit *ka* alors *p* divise *a* ou *p* divise *k* » sans hypothèse supplémentaire… Les calculs sur les congruences sont peu maitrisés et très mal justifiés (en particulier, la division de deux membres d'une congruence, la confusion entre égalité et congruence).

Peu de candidats utilisent de manière pertinente l'énoncé « si une application entre deux ensembles finis de même cardinalité est injective ou surjective, alors c'est une bijection ». En outre, il y a souvent, à la lecture des copies, une confusion entre « cardinal » d'un ensemble et « dimension » d'un espace (B.X.3).

Peu de candidats ont traité la question B.VIII.1. La propriété « une partie non vide de $\mathbb{N}$ admet un plus petit élément » semble être mal connue.

La question B.VIII.4 – écriture d'un algorithme – semble avoir été évitée par la plupart des candidats. En outre, lorsque la question a été traitée, les candidats ont choisi une boucle « pour » plutôt qu'une boucle « tant que ».

Concernant la question B.IX, les candidats n'apportent que peu de réponses concluantes, lorsque cette question est abordée, pour montrer que $\left(\mathbb{Z}/_{p\mathbb{Z}}\right)^*$ est un groupe cyclique et pour en trouver un générateur.

Enfin, la composition de fonctions n'est pas maitrisée par de nombreux candidats ; beaucoup font la confusion entre le produit de fonctions et la composition (C.XV.2) avec une mauvaise écriture des puissances.

Problème 2

De nombreux candidats ne tiennent pas compte des informations contenues dans le préambule du problème. Ainsi, les définitions (point constructible, nombre constructible, polygone régulier) n'ont pas été bien lues et assimilées par les candidats. Beaucoup de candidats n'ont pas compris ce que le jury attendait d'eux : la constructibilité d'un point n'est que très rarement justifiée à partir de points déjà construits. Aussi, même si les programmes de construction sont correctement rédigés, les candidats ne démontrent que très rarement que les constructions qu'ils proposent correspondent aux objets géométriques demandés.

De nombreux candidats ont confondu le point de coordonnées (*x* ; 0) et le réel *x*. Les notations de géométrie élémentaire ne sont pas maîtrisées : point, segment, demi-droite, droite, longueur.

Le théorème de Thalès est bien utilisé (A.IV.3).

Les calculs sur les nombres complexes sont très diversement maitrisés. Peu de candidats se montrent capables de résoudre l'équation $z^n = 1$. Beaucoup se contentent de donner les solutions $(\mathrm{e}^{\frac{\mathrm{i}2k\pi}{n}})$ sans faire la résolution, ni même préciser les valeurs possibles pour *k*. Enfin, la somme des racines *n*-ième de l'unité (ici, *n* était égal à 5) ne semble pas être un résultat connu.

La réussite à l'**épreuve écrite** nécessite que la préparation des candidats prenne en compte les éléments suivants :

· maîtriser et énoncer avec précision, lorsqu'elles sont utilisées, les connaissances mathématiques de base, indispensables à la prise de recul sur les notions enseignées ;
· rédiger clairement et de manière rigoureuse une démonstration simple, ce qui est une composante essentielle du métier de professeur de mathématiques ;
· exposer avec toute la précision voulue, en mentionnant clairement les étapes successives, les raisonnements, plus particulièrement ceux qui relèvent du collège ou du lycée.

On rappelle aussi l'importance du respect des notations, de la nécessité de conclure une argumentation, mais aussi l'intérêt de la lisibilité d'une copie.

3.2 Épreuve orale

L'épreuve orale vise à apprécier les qualités des candidats en vue d'exercer le métier d'enseignant. Ainsi, il s'agit non seulement de faire la preuve de ses compétences mathématiques, mais également de montrer sa capacité à les transmettre, à en illustrer la portée par des exemples bien choisis et, plus généralement, à susciter l'intérêt des élèves pour la démarche scientifique.

Compte tenu de la complexité du métier d'enseignant, les attentes du jury sont multiples et l'évaluation des candidats prend en compte des critères nombreux et variés, plus particulièrement en termes de **maîtrise**, d'**organisation et clarté**, de **pertinence** et de **réactivité**. Par ailleurs, une certaine connaissance des programmes, une bonne gestion du temps, une élocution claire, un niveau de langue adapté et une attitude d'écoute sont des atouts essentiels.

Cette épreuve s'appuie sur un dossier fourni par le jury portant sur un thème des programmes de mathématiques du collège ou du lycée général ou technologique. Ce thème est illustré par un exercice qui peut être complété par des productions d'élèves, des extraits des programmes officiels, des documents ressources ou des manuels. L'épreuve commence par l'exposé des réponses aux questions (vingt minutes), comprenant la présentation motivée d'exercices sur le thème du dossier, suivi d'un entretien.

Les attentes du jury sont définies avec le texte de l'arrêté définissant l'épreuve. Le jury s'attend notamment à ce que le candidat connaisse et sache prendre en compte les compétences attendues des enseignants. La posture adoptée par le candidat doit exclure l'arrogance, la provocation et l'impatience. Une très bonne maîtrise de la langue française est attendue. Les éléments qui viennent d'être évoqués entrent pour une part significative dans l'évaluation. On cherche à évaluer la capacité du candidat à engager une réflexion pédagogique pertinente et à communiquer efficacement et clairement.

Voici quelques remarques sur le déroulement de cette épreuve pour la session 2018. L'objectif est d'aider les candidats à avoir des repères clairs pour la passation elle-même, mais également pour la préparation des prochaines sessions ; ces remarques sont suivies de quelques conseils pour se préparer à cette épreuve orale du concours.

Le dossier proposé par le jury

La plupart du temps, l'exercice du dossier est bien compris et les productions d'élèves plutôt correctement analysées. De nets progrès ont été accomplis dans l'utilisation des compétences comme angle d'analyse. Notons que certains candidats s'en sortent fort bien en utilisant une liste de compétences propres aux mathématiques ; on pourra à ce propos consulter avec profit le texte de l'IGEN de mathématiques sur les compétences mathématiques au lycée ou bien les nouveaux programmes de collège. Toutefois certains candidats s'obligent à citer les six compétences de l'activité mathématique, parfois un peu à tort et à travers, alors même que deux ou trois d'entre elles sont plus pertinentes que les autres sur le cas étudié, voire une seule.

De nombreux candidats savent dépasser le modèle « correct / incorrect » mais il faut bien lire la question posée, tous les dossiers ne demandant pas la même démarche d'analyse. Il conviendrait également d'avoir des idées de pistes de remédiation à proposer en regard de certaines « erreurs » d'élèves ou du manque de maitrise de certaines compétences. D'ailleurs, certains dossiers demandent explicitement de proposer des pistes pour aider les élèves à remédier à leurs erreurs ou à progresser sur les éléments travaillés dans l'exercice.

La correction d'une partie de l'exercice proposé pose aux candidats des difficultés dont ils n'ont pas toujours conscience, notamment en termes de rédaction ou de qualité des justifications : il ne s'agit pas de proposer une « solution d'élève ». De plus, il convient de réfléchir à la présentation d'une correction « comme devant une classe ». On attend alors clairement des traces écrites analogues à celles qu'un professeur présenterait à ses élèves, accompagnées de toutes les justifications ou précisions nécessaires ; on s'appuiera bien sur les hypothèses ou sur telle ou telle propriété justifiant un « pas déductif » ; on utilisera correctement les connecteurs logiques. Il ne s'agit pas de présenter le « brouillon du professeur », issu directement de ses notes personnelles ou un tableau d'élève ou d'étudiant.

Notons que de nombreux candidats utilisent très bien les logiciels pour illustrer la mise en place des conjectures.

Dans la proposition d'un choix d'exercices, le candidat peut se mettre en valeur en présentant des justifications claires d'ordre didactique ou pédagogique, souvent demandées explicitement par le sujet. Le choix proposé est souvent trop pauvre, parfois trop proche de l'exercice du dossier, même s'il peut être intéressant de proposer un exercice de « remédiation » à l'éclairage de difficultés rencontrées dans les productions d'élèves. Cela ne saurait suffire toutefois pour l'illustration d'un thème dans sa généralité. Si les exercices proposés sont souvent pertinents dans leur thématique, le jury regrette le manque de recul des candidats vis-à-vis des manuels utilisés : les exercices sont parfois d'une longueur démesurée et seules une ou deux questions seraient vraiment intéressantes, ou bien en résolvant l'exercice à l'énoncé semblant attrayant, on s'aperçoit qu'il est en fait un peu vide de sens, etc. Notons que les modifications d'énoncés, par exemple en présentant une forme « fermée » puis « ouverte », sont appréciées.

De façon générale, il est important de montrer une posture de professeur capable d'animer des séances d'apprentissages préalablement construites. Pour cela, il est important de montrer l'envie de communiquer et de favoriser les interactions avec son public. La prestation d'un candidat regardant essentiellement le tableau ou les murs de la salle, et pas le jury à qui il est censé s'adresser, ne pourra évidemment être valorisée.

Par ailleurs, on dynamisera sa présentation par un langage clair et compréhensible de tous les élèves et en l'accompagnant de supports intelligibles et lisibles.

En guise de conseils de préparation

Dans un premier temps, il est bon de bien connaître le format de l'épreuve pour ne pas le découvrir le jour du passage devant le jury. Gérer de façon efficiente les vingt minutes à disposition du candidat pour présenter ses réponses aux questions posées par le sujet demande un minimum de réflexion et d'entraînement, notamment à alterner les phases écrites et orales.

On ne peut qu'encourager les candidats à assister à quelques oraux du concours lorsque cela est possible, et bien sûr à étudier les rapports de jury des sessions précédentes.

S'entrainer à bien gérer le tableau, de façon claire et pédagogique, en alternance ou pas avec des documents vidéo projetés, apprendre à utiliser les manuels numériques, étudier les textes sur les compétences relatives aux mathématiques et les documents ressources en général, représentent bien sûr un atout indéniable pour une bonne préparation.

En amont du concours, s'entraîner régulièrement à résoudre des exercices de tous niveaux dans le cadre des programmes et des thèmes proposés les années précédentes, réfléchir ensuite de façon plus approfondie à quelques exercices par thème, constituent bien sûr un plus indéniable. Pour ces derniers exercices, il s'agit de savoir les résoudre bien évidemment, mais également d'avoir réfléchi aux objectifs didactiques et pédagogiques de leur utilisation avec les élèves, à différentes versions possibles suivant l'objectif visé, etc. Il est à noter que les manuels ne constituent pas la seule source d'inspiration possible ; les documents d'accompagnement des programmes, les autres ressources disponibles sur le site EDUSCOL, voire les exercices de dossiers proposés les années précédentes peuvent donner bien des idées intéressantes. Se contenter de proposer des captures d'écran de pages d'exercices de manuels numériques sans avoir réfléchi aux contenus de ces exercices est bien évidemment contre-productif.

La mise en valeur de l'expérience professionnelle

Certains candidats ont bien réfléchi à cette problématique et cela se remarque ; d'autres pas du tout et cela se remarque aussi. Certains candidats arrivent à bien mettre en perspective leur expérience professionnelle en rapport avec les métiers de l'enseignement. Ils n'hésitent pas à mettre en avant leur parcours, parfois atypique, comme une qualité potentielle pour l'enseignement.

La mise en avant de l'expérience professionnelle pourrait être mieux préparée en amont, pour analyser les rapprochements possibles avec les métiers de l'enseignement. Le jury attend plus que la simple mention d'un métier. À ce propos, la connaissance des « missions d'un professeur » semble un préalable indispensable. On pourra à ce propos consulter avec profit le BO du 25/07 2013 (référentiel de compétences des métiers du professorat et de l'éducation).

4 Annexe : ressources diverses

Les sujets des épreuves écrites sont disponibles sur le serveur SIAC2 et sur le site du concours.

La liste des sujets de l'épreuve de mise en situation professionnelle est publiée chaque année, bien avant la tenue des épreuves. Cette liste est disponible sur le site du concours, dans la rubrique épreuves orales, puis dans la rubrique archives.

Les sujets de l'épreuve sur dossier ne sont publiés sur le site du concours qu'après la session, en page d'accueil, puis dans la rubrique archives du concours.

Pendant le temps de préparation de chaque épreuve orale, les candidats ont à leur disposition des ressources numériques de diverses natures : textes réglementaires, ressources d'accompagnement des programmes, logiciels, manuels numériques. On trouvera la liste de toutes ces ressources sur le site du concours, rubrique des épreuves orales.

Cette épreuve est constituée de deux problèmes indépendants.

Problème n° 1

Notations.
$\mathbb{N}$ désigne l'ensemble des entiers naturels.
Pour m et n deux entiers naturels, $[\![m, n]\!]$ désigne l'ensemble des entiers naturels k tels que $m \leqslant k \leqslant n$.

On souhaite crypter des messages, lettre à lettre. Pour écrire ces messages, on utilise 29 caractères différents : les 26 lettres de l'alphabet et les trois symboles espace, virgule et point. Pour faciliter le travail de cryptage, on code chacun de ces 29 caractères par un entier :

.	␣	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	,
15	16	17	18	19	20	21	22	23	24	25	26	27	28

On note R l'ensemble des entiers utilisés dans ce cryptage, c'est-à-dire l'ensemble $[\![0, 28]\!]$. Pour tout entier naturel k non nul, on note f_k l'application de R dans R qui à tout x de R associe le reste de la division euclidienne de x^k par 29.

Ces fonctions f_k, appelées *fonctions de cryptage*, sont utilisées pour crypter des messages.

Partie A : premiers essais

Albert souhaite utiliser comme fonction de cryptage l'application f_3. Benoît propose d'utiliser f_7. Camille choisit d'utiliser f_{19}.

I. Que devient la lettre E par la méthode de cryptage d'Albert ?

$6^3 = 216 = 7 \times 29 + 13$. Donc E devient L.

II. Montrer que, quelle que soit la fonction de cryptage f_k choisie, les symboles espace et point sont inchangés.

Le symbole point correspond à 0 et le symbole point à 1. Pour tout $k \geqslant 1$, comme $0^k = 0$ et $1^k = 1$, $f_k(0) = 0$ et $f_k(1) = 1$, donc les symboles points et espaces sont inchangés.

III. Un élève de troisième propose d'utiliser un tableur pour calculer les valeurs de f_k. Il prépare la feuille de calcul suivante :

	A	B	C	D	E	...	AC	AD	AE
1		.	␣	A	B	...	Z	,	
2	x	0	1	2	3	...	27	28	Exposant k
3	$f_k(x)$	0	1						3

Dans la cellule D3, il entre la formule =MOD(D2^AE3 ;29). Comment modifier cette formule afin de pouvoir la dupliquer en utilisant la poignée de recopie, sachant que le tableau doit rester correct lorsque le contenu de la cellule AE3 est modifié ?
On rappelle que MOD(a ;b) renvoie le reste de la division euclidienne de a par b.

Il doit entrer en D3 la formule =MOD(D21^AE3 ;29).

IV. Benoît utilise la feuille de calcul précédente pour son cryptage avec f_7. Il obtient le tableau suivant :

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f_k(x)$	0	1	12	12	28	28	28	1	17	28	17	12	17	28	12

x	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$f_k(x)$	17	1	12	17	12	1	12	28	1	1	1	17	17	28

Crypter les mots CLE et LUC. Que constate t-on ?

CLE correspond à 4–13–6 donc est crypté par 28–28–28, soit « , , , ». LUC correspond à 13–22–4 donc est crypté par 28–28–28, soit « , , , ». Ces deux mots distincts sont cryptés de la même façon.

V. Quelle propriété doit vérifier la fonction f_k pour assurer le décryptage ?

Pour pouvoir décrypter les messages, il est nécessaire que deux lettres distinctes soient envoyées sur deux lettres distinctes, pour éviter ce qu'il se passe à la question IV. Autrement dit, la fonction f_k doit être injective. Comme f_k va d'un ensemble fini dans lui-même, l'injectivité de f_k est équivalente à sa bijectivité.

VI. Camille utilise la feuille de calcul de la question **III.** avec $k = 19$. Dans les cellules allant de E3 à AD3, il s'affiche ♯NOMBRE !. Comment expliquer ce résultat ? On verra dans la partie C comment contourner ce problème.

Pour calculer $f_k(3)$, le tableur calcule d'abord 3^{19} à l'aide de nombres flottants. La représentation de ce nombre en mémoire n'est plus exacte, ce nombre étant trop élevé. En conséquence, le tableur n'est pas capable de calculer son reste modulo 29.

Partie B : choix de la fonction de cryptage

On se propose dans cette partie de déterminer les valeurs de k pour lesquelles la fonction de cryptage f_k permet d'assurer le décryptage.

VII. On fixe un nombre premier p. Soit a un entier (relatif) tel que p ne divise pas a. Le but de cette question est de **démontrer** l'égalité suivante, connue sous le nom de petit théorème de Fermat :

$$a^{p-1} \equiv 1[p].$$

On désigne par A l'ensemble $\{a, 2a, 3a, \ldots, (p-1)a\}$.

1. Soit k un entier relatif. Montrer que p divise ka si, et seulement si, p divise k. En déduire que p ne divise aucun élément de A.

Supposons que p divise ka. Par le lemme de Gauss, p divise k ou p divise a. Comme p ne divise pas a, p divise k.

Supposons que p divise k. Comme k divise ka, par transitivité p divise ka.

Par contraposée, comme p ne divise pas k si $k \in [\![1, p-1]\!]$, p ne divise pas ka. Donc p ne divise aucun élément de A.

2. Pour $i \in [\![1, p-1]\!]$, on note α_i le reste modulo p de l'entier ia.

a. Établir que ces restes sont tous non nuls et deux à deux distincts.

Soient $i, j \in [\![1, p-1]\!]$ tels que $\alpha_i = \alpha_j$. Comme p divise $ia - \alpha_i$ et $ja - \alpha_j$, p divise $ja - \alpha_j - (ia - \alpha_i) = ja - ia = (j-i)a$. D'après la question VII.1, p divise $j-i$. De plus, $-(p-2) \leqslant j-i \leqslant p-2$, donc $j-i = 0$ et $j = i$. Les restes α_i sont donc deux-à-deux distincts. De plus, pout tout $i \in [\![1, p-1]\!]$, $\alpha_i \neq 0$ car p ne divise pas ia d'après la question VII. 1.

b. En déduire que $\{\alpha_i, i \in [\![1, p-1]\!]\} = [\![1, p-1]\!]$.

On a donc une application $f : [\![1, p-1]\!] \longrightarrow [\![1, p-1]\!]$ envoyant i sur α_i. Elle est injective d'après la question VII.2.a, donc bijective. Par suite, $\{\alpha_i, i \in [\![1, p-1]\!]\} = [\![1, p-1]\!]$.

3. On appelle P le produit de tous les éléments de A. Établir que $P = a^{p-1}(p-1)!$ et que $P \equiv (p-1)![p]$.

D'une part :

$$P = \prod_{i=1}^{p-1} ai = a^{p-1}(p-1)!.$$

D'autre part, pour tout i, ia est congru à α_i modulo p donc :

$$P \equiv \prod_{i=1}^{p-1} \alpha_i [p].$$

D'après la question VII.3.b. :

$$P \equiv \prod_{i=1}^{p-1} i \equiv (p-1)![p].$$

4. En déduire que pour tout entier relatif a premier avec p , $a^{p-1} \equiv 1[p]$.

On en déduit que p divise $a^{p-1}(p-1)! - (p-1)! = (a^{p-1}-1)(p-1)!$. Par le lemme de Gauss, p divise l'un des facteurs de ce produit. Aucun des facteurs $1, \ldots, p-1$ de $(p-1)!$ n'est divisible par p, donc $a^{p-1}-1$ est divisible par p. Par suite, $a^{p-1} \equiv 1[p]$.

5. Que peut-on en déduire pour f_{28} et f_{29} ?

Soit $i \in R$. Si $i = 0$ alors $f_{28}(i) = f_{29}(i) = 0$ d'après la question II. Sinon, p ne divise pas a. D'après la question VII. 4, comme 29 est un nombre premier, $a^{28} \equiv 1[29]$ et donc $a^{29} = a^{28} \times a \equiv a[p]$. Autrement dit, $f_{28}(a) = 1$ et $f_{29}(a) = a$. Par suite, $f_{29} = Id_R$ et pour tout $a \in R$:

$$f_{28}(a) = \begin{cases} 0 \text{ si } a = 0, \\ 1 \text{ sinon.} \end{cases}$$

6. Soit k et l deux entiers naturels non nuls. Montrer que si $k \equiv l[28]$, alors $f_k = f_l$.

quitte à permuter k et l, on peut supposer $l \geqslant k$. Alors $l = 28q + l$, avec $q \in \mathbb{N}$. Soit $i \in R$. Si $i = 0$, d'après la question II, $f_k(i) = f_l(i) = 0$. Sinon :

$$f_l(i) \equiv i^{28q+k} \equiv (i^{28})^q i^k \equiv 1^q i^k \equiv i^k \equiv f_k(i)[29],$$

donc $f_l(i) = f_k(i)$. En conséquence, $f_k = f_l$.

VIII. Dans cette question x désigne un entier naturel premier avec 29 .

1. Montrer qu'il existe un plus petit entier naturel non nul k tel que $x^k \equiv 1[29]$, et que cet entier k est inférieur ou égal à 28. Cet entier k est appelé *ordre de* x et est noté $o(x)$.

Soit $E = \{k \in \mathbb{N}^*, x^k \equiv 1[29]\}$. D'après VII.4, cet ensemble est non vide car il contient 28. Par suite, il contient un plus petit élément k, qui est donc inférieur ou égal à 28.

Définition. Soit x un entier premier avec 29.
On dit que x est primitif modulo 29 si $o(x) = 28$.

2. Soit k un entier naturel. Montrer que $x^k \equiv 1[29]$ si et seulement si $o(x)$ divise k.

Supposons que $o(x)$ divise k. Posons $k = o(x)q$, avec $q \in \mathbb{N}^*$. Alors :

$$x^k = (x^{o(x)})^q \equiv 1^q \equiv 1[29].$$

Supposons que $x^k \equiv 1[29]$. Soit $k = o(x)q + r$ la division euclidienne de k par $o(x)$, avec $0 \leqslant r \leqslant o(x)$ et $q \in \mathbb{N}$. Alors :

$$x^k = (x^{o(x)})^q x^r \equiv 1^q x^r \equiv x^r \equiv 1[29].$$

Si $r \neq 0$, ceci contredit la minimalité de $o(x)$. Donc $r = 0$ et $o(x)$ divise k.

3. En déduire que $o(x)$ est un diviseur de 28.

Comme $x^{28} \equiv 1[29]$, $o(x)$ divise 28.

4. Écrire un algorithme permettant de calculer l'ordre d'un nombre entier x premier avec 29.

```
o ← 1
N ← x mod 29
Tant que (N ≠ 1) faire
    | N ← N × x mod 29
    | o ← o + 1
Fin Tant que
Rendre o
```

5. a. Déterminer l'ensemble des diviseurs de 28.

La décomposition en nombres premiers de 28 est $28 = 2^2 \times 7$. Ses diviseurs sont donc les nombres de la forme $2^a \times 7^b$, avec $0 \leqslant a \leqslant 2$ et $0 \leqslant b \leqslant 1$. Il s'agit donc de 1, 2, 4, 7, 14, 28.

b. Montrer que si $x^{14} \equiv 1[29]$ ou $x^4 \equiv 1[29]$, alors l'ordre $o(x)$ ne peut pas valoir 28.

Si $x^{14} \equiv 1[29]$ ou $x^4 \equiv 1[29]$, d'après VIII.2, $o(x)$ divise 14 ou $o(x)$ divise 4, donc $o(x) \neq 28$.

c. Montrer que si $x^{14} \not\equiv 1[29]$ et $x^4 \not\equiv 1[29]$, alors $o(x) = 28$.

Comme $o(x)$ divise 28, $o(x) \in \{1, 2, 4, 7, 14, 28\}$. Supposons $x^{14} \not\equiv 1[29]$ et $x^4 \not\equiv 1[29]$. D'après VIII.2, $o(x)$ ne divise pas 14, donc est différent de 1, 2, 7 et 14. Par suite, $o(x) \in \{4, 28\}$. D'après VIII.2, $o(x)$ ne divise par 4, donc $o(x) = 28$.

d. En déduire que 2 est primitif modulo 29.

Par multiplication successives par 2 :

$$2^4 = 16 \equiv 16[29], \qquad 2^5 \equiv 32 \equiv 3[29],$$
$$2^6 \equiv 6[29], \qquad 2^7 \equiv 12[29].$$

En élevant au carré, $2^{14} \equiv 144 \equiv 28[29]$. D'après la question VIII.5.c, $o(2) = 28$.

IX. On rappelle que si p est un nombre premier, l'ensemble $\{\overline{x} \in \mathbb{Z}/p\mathbb{Z} \mid \overline{x} \neq \overline{0}\}$ muni de la loi $\overline{\times}$ induite par la multiplication de $\mathbb{Z}$ est un groupe. En utilisant les résultats de la question **VIII.**, vérifier que, pour $p = 29$, ce groupe est cyclique et donner un générateur de ce groupe.

Considérons $E = \{\overline{2}^k, k \in [\![1, 28]\!]\} \subseteq \{\overline{x} \in \mathbb{Z}/29\mathbb{Z} \mid \overline{x} \neq \overline{0}\}$. Soient $k, l \in [\![1, 28]\!]$ tels que $\overline{2}^k = \overline{2}^l$. Supposons par exemple $l \geqslant l$. Alors $\overline{2}^{l-k} = \overline{1}$, donc $o(2) = 28$ divise $l - k$. Comme $0 \leqslant l - k \leqslant 27$, $l - k = 0$ et $l = k$. Par suite, E comprend 28 éléments, donc est égal à $\{\overline{x} \in \mathbb{Z}/29\mathbb{Z} \mid \overline{x} \neq \overline{0}\}$. Ce groupe est donc cyclique, engendré par $\overline{2}$.

X. On considère l'application φ définie sur $S = [\![1, 28]\!]$ et à valeurs dans S qui à tout entier $k \in S$ associe $\varphi(k) = \beta_k$, où β_k désigne le reste de la division euclidienne de 2^k par 29.

1. Justifier que φ est bien définie.

Pour tout $k \in \mathbb{N}$, 29 ne divise pas 2^k, car 29 ne divise pas 2. Par suite, pour tout $k \in S$, $\beta_k \neq 0$ et donc $\beta_k \in S$.

2. Soient $k \leqslant k'$ deux éléments de S. Établir que $\varphi(k) = \varphi(k')$ si et seulement si 29 divise $2^{k'-k} - 1$.

$$\begin{aligned}\varphi(k) = \varphi(k') &\iff 2^k \equiv 2^{k'}[29] \\ &\iff (2^{k'-k} - 1)2^k \equiv 0[29] \\ &\iff 29 \mid (2^{k'-k} - 1)2^k.\end{aligned}$$

Comme 29 ne divise pas 2, par le lemme de Gauss :

$$\varphi(k) = \varphi(k') \Longleftrightarrow 29 \mid 2^{k'-k} - 1.$$

3. En déduire que φ est injective, puis que φ est bijective.

Soient k, k' deux éléments de S. On suppose par exemple que $k' \geqslant k$.

$$\begin{aligned}\varphi(k) = \varphi(k') &\Longleftrightarrow 29 \mid 2^{k'-k} - 1\\ &\Longleftrightarrow 2^{k'-k} \equiv 1[29]\\ &\Longleftrightarrow o(2) = 28 \mid k' - k\\ &\Longleftarrow k' = k,\end{aligned}$$

car $0 \leqslant k' - k \leqslant 27$. Par suite, φ est injective. Comme S est de cardinal fini, φ est bijective.

4. En déduire que, pour tout élément de $y \in S$, il existe un unique $x \in S$ tel que $y \equiv 2^x[29]$.

Soit $y \in S$. Comme φ est bijective, il existe un unique $x \in S$ tel que $\varphi(x) = y$, c'est-à-dire qu'il existe un unique $x \in S$ tel que $2^x \equiv y[29]$.

XI. Soit k un entier naturel non nul fixé. Étant donné $y \in S$, on cherche à trouver $z \in R$ tel que $z^k \equiv y[29]$.

1. Établir que 29 ne peut diviser z et que l'on peut se ramener à chercher z dans S.

Si 29 divise z, alors $z^k \equiv 0[29]$ et donc $z^k \neq y[29]$, car $y \in S$. Donc 29 ne divise pas z. Par suite, si $z \in R$ vérifie $z^k \equiv y[29]$, $z \neq 0$ et donc $z \in S$: on peut se ramener à chercher z dans S.

2. Soit z un élément de S et t (respectivement x) l'unique élément de S tel que $z \equiv 2^t\,[29]$ (respectivement $y \equiv 2^x\,[29]$). Démontrer que $z^k \equiv y\,[29]$ si et seulement si $kt - x$ est divisible par 28.

D'après X.2 :

$$z^k \equiv y[29] \Longleftrightarrow 2^{tk} \equiv 2^x[29] \Longleftrightarrow 28 \mid tk - x.$$

3. On considère l'équation diophantienne $(*)$ $ak + 28b = 1$, où les inconnues a et b sont des entiers relatifs.

a. Donner une condition nécessaire et suffisante (C) pour que $(*)$ admette des solutions.

$(*)$ admet des solutions si, et seulement si, a et 28 sont premiers entre eux.

b. On suppose cette condition (C) satisfaite. À partir d'une solution particulière (a_0, b_0), donner alors toutes les solutions de $(*)$.

Let solutions de $(*)$ sont les couples $(a_0 + 28n, b_0 - bn)$, où $n \in \mathbb{Z}$.

c. On suppose cette condition (C) satisfaite. Établir que $(*)$ a une unique solution (a_1, b_1) pour laquelle $a_1 \in S$.

Soit $a_0 = 28q + a_1$ la division euclidienne de a_0 par 28. Alors $a_1 \in S$ et de plus $(a_1, b_0 + qk)$ est une solution de $(*)$, ce qui prouve l'existence d'une telle solution.
Soit (a_2, b_2) une solution de $(*)$ avec $a_2 \in S$. Alors il existe $n \in \mathbb{Z}$ tel que $a_2 = a_0 + 28n$ et $b_2 = b_0 - bn$. Donc $a_2 = a_1 + 28(q + n)$.
Comme $-27 \leqslant a_2 - a_1 \leqslant 27$, nécessairement $a_2 = a_1$ et donc $n - q$. Par suite, $(a_2, b_2) = (a_1, b_1)$, ce qui prouve l'unicité d'une telle solution.

4. En déduire que si k et 28 sont premiers entre eux alors $f_{a_1} \circ f_k(w) = f_k \circ f_{a_1}(w) = w$ pour tout $w \in R$.

Si $w = 0$, alors $f_{a_1} \circ f_k(w) = f_k \circ f_{a_1}(w) = 0 = w$ d'après la question II. Si $w \in S$, il existe un unique $x \in S$ tel que $w \equiv 2^x [29]$. Comme 28 divise $ka_1x - x$, d'après XI.2 :

$$f_{a_1} \circ f_k(w) \equiv 2^{a_1 kx} \equiv 2^x \equiv w [29],$$

donc $f_{a_1} \circ f_k(w) = w$. De même, $f_k \circ f_{a_1}(w) = w$.

5. Que conclure pour f_k ?

f_k est donc bijective, d'inverse f_{a_1}.

XII. Montrer que tout message crypté par la fonction f_3 peut être décrypté à l'aide de la fonction f_{19}.

Une solution particulière de $(*)$: $3a + 28b = 1$ est donnée par $(-9, 1)$. Les solutions de $(*)$ sont donc les couples $(-9 + 28n, 1 - 3n)$, où $n \in \mathbb{Z}$. L'unique solution (a_1, b_1) avec $a_1 \in S$ est donnée pour $n = 1$, ce qui donne $(19, -2)$ Donc $f_{19} \circ f_3(w) = w$ pour tout $w \in S$: f_{19} permet donc de décrypter les messages cryptés par f_3.

XIII. Quelles sont les valeurs de k permettant le décryptage de tout message ayant été crypté par f_k ? Justifier votre réponse.

Le décryptage des messages cryptés par f_k est possible si, et seulement si, 28 et k sont premiers entre eux.
$\Longleftarrow$. D'après XI.3, dans ce cas, f_k est bijective, d'inverse f_{a_1}.
$\Longrightarrow$. Si 28 et k ne sont pas premiers entre eux, $(*)$ n'a pas de solution. D'après la question XI.2, il n'existe donc aucun $z \in R$ tel que $f_k(z) = 2$ (pour $t = 1$). Donc f_k n'est pas surjective et donc pas bijective.

Partie C : différents procédés de calcul de f_{19}

On décrit dans cette partie trois méthodes pour calculer f_{19} à l'aide d'un tableur.

XIV. Première méthode. On souhaite compléter la feuille de calcul suivante :

	A	B	C	D	E	...	AC	AD
1		.		A	B	...	Z	,
2	x	0	1	2	3	...	27	28
3	$f_2(x)$	0	1					
4	$f_3(x)$	0	1					
⋮	⋮	⋮	⋮					
20	$f_{19}(x)$	0	1					

1. Quelle formule doit-on écrire en D3 pour remplir le tableau en utilisant la poignée de recopie ?

=MOD(D2*D$2 ;29)

2. Pour remplir chaque colonne, combien de multiplications et combien de divisions euclidiennes par 29 sont-elles effectuées ?

On effectue 18 multiplications et 18 divisions euclidiennes par 29.

XV. Seconde méthode. On souhaite compléter la feuille de calcul suivante :

	A	B	C	D	E	...	AC	AD
1		.		A	B	...	Z	,
2	x	0	1	2	3	...	27	28
3	$f_2(x)$	0	1					
4	$(f_2 \circ f_2)(x)$	0	1					
5	$(f_2 \circ f_2 \circ f_2)(x)$	0	1					
6	$(f_2 \circ f_2 \circ f_2 \circ f_2)(x)$	0	1					
7								

1. Quelle formule doit-on écrire en D3 pour remplir le tableau en utilisant la poignée de recopie ?

=MOD(D2^ 2 ;29)

2. En constatant que $19 = 2^4 + 2^1 + 2^0$, montrer que pour tout $x \in R$,

$$f_{19}(x) \equiv (f_2 \circ f_2 \circ f_2 \circ f_2)(x) \times f_2(x) \times x \,[29].$$

$2^4 + 2^1 + 2^0 = 16 + 2 + 1 = 19$. Donc, si $x \in R$:

$$\begin{aligned} f_{19}(x) &\equiv x^{2^4+2+1} \equiv (((x^2)^2)^2)^2 x^2 x[29] \\ &= (f_2 \circ f_2 \circ f_2 \circ f_2)(x) \times f_2(x) \times x \,[29] \end{aligned}$$

3. Quelle formule doit-on écrire en D7 pour remplir la ligne 7 en utilisant la poignée de recopie et obtenir ainsi f_{19} ?

=MOD(D4*D4*D2 ;29)

4. Pour remplir chaque colonne, combien de multiplications et combien de divisions euclidiennes par 29 sont-elles effectuées ?

On effectue $4 + 2 = 6$ multiplications et 5 divisions euclidiennes pas 29.

XVI. Troisième méthode. On souhaite compléter la feuille de calcul suivante :

	A	B	C	D	E	...	AC	AD
1		.		A	B	...	Z	,
2	x	0	1	2	3	...	27	28
3	$f_3(x)$	0	1					
4	$(f_3 \circ f_3)(x)$	0	1					
5								

1. Quelle formule doit-on écrire en D3 pour remplir le tableau en utilisant la poignée de recopie ?

=MOD(D2^ 3 ;29)

2. En constatant que $19 = 2 \times 3^2 + 3^0$, donner une formule permettant de calculer $f_{19}(x)$ à partir de la feuille de calcul précédente.

$2 \times 3^2 + 3^0 = 18 + 1 = 19$. Pour tout $x \in R$:

$$f_{19}(x) \equiv ((x^3)^3)^2 x \equiv f_3 \circ f_3(x)^2 \times x[29].$$

3. Quelle formule doit-on écrire en D5 pour remplir la ligne 5 en utilisant la poignée de recopie et obtenir ainsi f_{19} ?

=MOD(D4^ 2*D2 ;29)

4. Pour remplir chaque colonne, combien de multiplications et combien de divisions euclidiennes par 29 sont-elles effectuées ?

On effectue $2 + 2 + 3 = 7$ multiplications et 3 divisions euclidiennes par 29.

XVII. Laquelle de ces trois méthodes vous semble la plus performante ?

La première méthode nécessite le plus d'opérations : c'est la moins performante des trois. Soit m le temps nécessaire pour une multiplication et d le temps nécessaire pour une division euclidienne par 29. Le temps mis pour calculer une colonne est $6m + 5d$ avec la deuxième méthode et $7m + 3d$ avec la troisième méthode.

$$6m + 5d \leqslant 7m + 3d \iff 2d \leqslant m.$$

Par suite, si $2d < m$, la deuxième méthode est la plus performante ; si $2d > m$, la troisième méthode est la plus performante ; si $2d = m$, ces deux méthodes sont aussi performantes l'une que l'autre.

Problème n° 2

Notations.
$\mathbb{N}$ désigne l'ensemble des entiers naturels.
$\mathbb{C}$ désigne l'ensemble des nombres complexes.
Pour m et n deux entiers naturels, $[\![m, n]\!]$ désigne l'ensemble des entiers k tels que $m \leqslant k \leqslant n$.

Si z est un nombre complexe, son conjugué est noté $\overline{z}$.

Partie A : constructions à la règle et au compas

On se place dans un plan euclidien $\mathcal{P}$ muni d'un repère orthonormé (O, I, J), qu'on identifie avec le plan complexe $\mathbb{C}$. On construit des points de $\mathcal{P}$ à l'aide d'une règle non graduée et d'un compas de la façon suivante :

— au départ, seuls O, I et J sont construits ;
— à chaque étape, on peut :

- construire le cercle de centre A et de rayon BC si A, B et C sont des points déjà construits ;
- construire la droite (AB) si A et B sont des points déjà construits.

On obtient ainsi de nouveaux points, intersections des cercles et des droites qui ont été construits. Ces points pourront être utilisés aux étapes suivantes. Les droites, cercles et points ainsi obtenus sont dits *constructibles à la règle et au compas*.

Soit x un nombre réel. On dit que x est un nombre *constructible* s'il est l'abscisse dans le repère (O, I, J) d'un point constructible.

I. Dans toutes les questions qui suivent, on attend à la fois la représentation d'une construction à la règle et au compas laissant apparaître les traits de construction et la rédaction d'un programme de construction tel qu'il figurerait comme trace écrite dans les cahiers des élèves.

1. On suppose que A et B sont deux points distincts constructibles à la règle et au compas. Montrer que la médiatrice de $[AB]$ et le milieu de $[AB]$ sont constructibles à la règle et au compas.

(La figure est laissée au lecteur). Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ les cercles de centres respectifs A et B et de rayon AB. Comme A et B sont constructibles, $\mathcal{C}1$ et $\mathcal{C}_2$ sont des cercles constructibles, donc leurs deux points d'intersection I et J sont constructibles. De plus, $IA = IB = AB$ et $JA = JB = AB$, donc I et J sont sur la médiatrice $\mathcal{D}$ de $[AB]$. En conséquence, $\mathcal{D}$ est constructible. Le point d'intersection de $\mathcal{D}$ et de (AB) est donc lui aussi constructible : c'est le milieu de $[AB]$.

2. On suppose que A, B et C sont trois points constructibles à la règle et au compas, avec $A \neq B$. Montrer que la droite perpendiculaire à (AB) passant par C est constructible à la règle et au compas.

(La figure est laissée au lecteur). Soit $\mathcal{C}$ le cercle de centre C et de rayon AC. Comme A et C sont constructibles, $\mathcal{C}$ est constructible. Ce cercle coupe la droite (AB) en A. Deux cas se présentent :

— Si A est le seul point d'intersection de $\mathcal{C}$ et (AB), alors (AB) et $\mathcal{C}$ sont tangents en A. Par suite, (AC) est perpendiculaire à (AB). La perpendiculaire à (AB) passant par C est donc (AC), qui est constructible.
— Sinon, $\mathcal{C}$ coupe (AB) en un second point D. Alors $CA = CD$, donc C est sur la médiatrice à $[AD]$. En conséquence, la perpendiculaire à (AB) passant par C est la médiatrice de $[AD]$. D'après la question I.1, cette droite est constructible.

3. On suppose que A, B et C sont trois points constructibles à la règle et au compas, avec $A \neq B$. Montrer que la droite parallèle à (AB) passant par C est constructible à la règle et au compas.

(La figure est laissée au lecteur). D'après la question I.2, la perpendiculaire $\mathcal{D}$ à (AB) passant par C est constructible. On considère le cercle $\mathcal{C}$ de centre C et de rayon AB : ce cercle est constructible et coupe $\mathcal{D}$ en deux points constructibles D et E, de sorte que $\mathcal{D} = (DE)$. La droite recherchée est la perpendiculaire à (DE) passant par C : en effet, cette droite passe par C et est parallèle à (AB) car (DE) est perpendiculaire à (AB). D'après la question I.2, cette droite est constructible.

4. Soient $\mathcal{D}$ et $\mathcal{D}'$ deux droites constructibles à la règle et au compas, sécantes en un point A. Montrer que les bissectrices de ces deux droites sont constructibles à la règle et au compas.

(La figure est laissée au lecteur). Comme $\mathcal{D}$ est constructible, elle contient un point I constructible différent de A. Le cercle $\mathcal{C}$ de centre A et de rayon AI est constructible et coupe $\mathcal{D}$ en un autre point J et $\mathcal{D}'$ en deux point I' et J'. Par construction, I', J et J' sont constructibles. Le triangle AII' est isocèle en A, donc la bissectrice Γ issue de A est aussi la médiatrice du segment $[II']$: d'après la question I.1, Γ est constructible. On obtient ainsi l'une des bissectrices des droites $\mathcal{D}$ et $\mathcal{D}'$. On obtient la seconde en considérant le triangle AIJ'.

On pourra désormais utiliser ces constructions sans en préciser tous les détails.

II. Soit M un point constructible à la règle et au compas. On note $(x; y)$ ses coordonnées dans le repère (O, I, J). Montrer que x et y sont des nombres constructibles.

Par définition, x est un nombre constructible. La perpendiculaire à (OI) passant par M est constructible, donc le point d'intersection $N(x; 0)$ de cette droite avec (OI) est constructible. Le cercle $\mathcal{C}$ de centre O et de rayon $MN = |y|$ coupe la droite (OI) en les points de coordonnées $(-y; 0)$ et $(y; 0)$, qui sont donc constructibles. Par suite, y (ainsi que $-y$) est un nombre constructible.

III. Soit x un nombre réel constructible. Montrer que les points de coordonnées $(x; 0)$ et $(0; x)$ dans le repère (O, I, J) sont constructibles à la règle et au compas.

Par définition, O et I sont constructibles. La perpendiculaire à (OI) passant par M est donc elle aussi constructible et le point d'intersection N de cette droite avec (OI) est constructible : il s'agit du point de coordonnées $(x; 0)$, qui est donc constructible. En utilisant la perpendiculaire à (OJ) passant par M, on obtient de même que le point $P(0; y)$ est constructible. Le cercle $\mathcal{C}$ de centre O et de rayon OP est constructible et coupe la droite (OI) en les points de coordonnées $(-y; 0)$ et $(0; y)$, qui sont donc constructibles.

IV. Soient x et y deux nombres réels constructibles strictement positifs.

1. Montrer que $-x$ est un nombre réel constructible. La réponse à cette question doit être rédigée telle que vous la présenteriez à une classe de collège.

D'après la question III, le point $M(x;0)$ est constructible. Le cercle de centre O et de rayon OM est donc constructible. Il coupe la droite (OI) en M et en le point de coordonnées $(-x;0)$, qui est donc constructible. Par suite, $-x$ est un nombre constructible.

2. Montrer que $x+y$ et $x-y$ sont constructibles. La réponse à cette question doit être rédigée telle que vous la présenteriez à une classe de collège.

D'après III, les points $M(x;0)$ et $N(y;0)$ sont constructibles. Le cercle $\mathcal{C}$ de centre M et de rayon $ON = y$ est donc constructibles. Il coupe (OI) en les points de coordonnées $(x-y;0)$ et $(x+y;0)$, qui sont donc constructibles. Par suite, $x-y$ et $x+y$ sont des nombres constructibles.

3. En utilisant les points J, $A(x;0)$ et $B(0;y)$ et la droite parallèle à (AJ) passant par B, montrer que xy est constructible. La réponse à cette question doit être rédigée telle que vous la présenteriez à une classe de collège.

D'après la question III, A et B sont constructibles. D'après la question I.3, la parallèle à (AJ) passant par B est constructible. L'intersection de cette droite avec (OI) est un point constructible C, de coordonnées $(z;0)$. D'après le théorème de Thalès, comme (AJ) est parallèle à (BC), $\frac{x}{z} = \frac{1}{y}$, donc $z = xy$ et z est un nombre constructible.

4. Montrer que $\dfrac{x}{y}$ est constructible.

Soit $\mathcal{D}$ la parallèle à (AB) passant par J : cette droite est constructible d'après I.3. Son intersection avec (OI) est un point C constructible, de coordonnées $(z;0)$. D'après le théorème de Thalès, comme (JD) est parallèle à (AB), $\frac{z}{x} = \frac{1}{y}$, donc $z = \frac{x}{y}$ et z est constructible.

V. Montrer que si x et y sont des nombres réels constructibles, alors $x+y$, $x-y$, xy et, si y est non nul, $\dfrac{x}{y}$ sont des nombres constructibles.

Le résultat est évident si $x = 0$ ou $y = 0$. On suppose donc x et y non nuls. D'après la question IV.1, x, y, $-x$ et $-y$ sont constructibles, donc $|x|$ et $|y|$ sont constructibles. D'après la question IV, $|x|+|y|$, $|x|-|y|$, $|y|-|x|$, $-|x|-|y|$, $|x||y|$, $-|x||y|$, $\frac{|x|}{|y|}$ et $-\frac{|x|}{|y|}$ sont constructibles. Donc $x+y$, $x-y$, xy et $\frac{x}{y}$ sont constructibles.

VI. Soit x un nombre réel constructible strictement positif.

1. Montrer que le point $A(1+x;0)$ est constructible à la règle et au compas.

1 et x sont constructibles, donc $1+x$ aussi d'après la question VI.1. D'après la question III, A est constructible.

2. Montrer que le cercle $\mathcal{C}$ de diamètre $[OA]$ est constructible à la règle et au compas.

D'après $I.1$, le milieu de K de $[OA]$ est constructible. Alors $\mathcal{C}$ est le cercle de centre K et de rayon OK, donc est constructible.

3. Soit B le point d'intersection d'ordonnée positive de $\mathcal{C}$ et de la droite $\mathcal{D}$ perpendiculaire à (OI) passant par I. Montrer que B est constructible à la règle et au compas.

D'après a question I.2, $\mathcal{D}$ est constructible. Comme $\mathcal{C}$ est constructible, les points d'intersection de $\mathcal{C}$ et $\mathcal{D}$ sont constructibles. En particulier, B est constructible.

4. Soit $\theta = (\widehat{\overrightarrow{OI}, \overrightarrow{OB}})$. Exprimer $\tan(\theta)$ et $\tan\left(\frac{\pi}{2} - \theta\right)$ en fonction de BI et de x. En déduire BI.

$\tan(\theta) = \frac{IB}{OI} = IB$. Comme B est sur le cercle de diamètre OA, OAB est rectangle en B, donc $(\widehat{\overrightarrow{AB}, \overrightarrow{AI}}) = \frac{\pi}{2} - \theta$. On a donc :

$$\tan\left(\frac{\pi}{2} - \theta\right) = \frac{IB}{AI} = \frac{IB}{x}.$$

De plus :

$$\tan\left(\frac{\pi}{2} - \theta\right) = \frac{\sin\left(\frac{\pi}{2} - \theta\right)}{\cos\left(\frac{\pi}{2} - \theta\right)} = \frac{\cos(\theta)}{\sin(\theta)} = \frac{1}{\tan(\theta)}.$$

Donc :

$$BI = \tan(\theta) = \frac{x}{\tan(\theta)}.$$

On obtient $x = \tan(\theta)^2$, donc $BI = \tan(\theta) = \sqrt{x}$.

5. Montrer que $\sqrt{x}$ est un nombre constructible.

Comme $B(1; \sqrt{x})$ est constructible, $\sqrt{x}$ est un nombre constructible d'après II.

VII. Montrer que tous les nombres rationnels sont constructibles.

0 et 1 sont constructibles. Supposons n constructible, pour un certain $n \in \mathbb{N}$. D'après V., $n + 1$ est constructible. Par le principe de récurrence, tous les entiers naturels sont constructibles. D'après V, leurs opposés aussi, donc tous les entiers relatifs sont constructibles. Par suite, si $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, non nul, d'après V., a/b est constructible. Donc les nombres rationnels sont constructibles.

VIII. Montrer que $\sqrt{2}$ et $\sqrt[4]{2}$ sont des nombres constructibles. Proposer une construction à la règle et au compas des points de coordonnées $(\sqrt{2}; 0)$ et $(\sqrt[4]{2}; 0)$.

D'après VII., 2 est constructible. D'après VI.5, $\sqrt{2}$ est constructible et $\sqrt{\sqrt{2}} =^4 \sqrt{2}$ est constructible.
On trace la perpendiculaire à (OI) passant par I et la perpendiculaire à (OJ) passant par J : ces deux droites se coupent en le point K de coordonnées $(1; 1)$, et $OK = \sqrt{2}$. Le cercle de centre O er de rayon OK coupe la droite (OI) en les points de coordonnées $A = (\sqrt{2}; 0)$ et $(-\sqrt{2}; 0)$. À l'aide de la construction de la question VI.4, on trace le point de coordonnées $(1; \sqrt[4]{2})$ puis le point de coordonnées $(\sqrt[4]{2}; 0)$.

Partie B : polygones réguliers

Dans toute cette partie, n est un entier naturel supérieur ou égal à 3.

Soit $M_0 \dots M_{n-1}$ un polygone. On dit qu'il est régulier s'il existe un point O, appelé le centre du polygone, tel que

$$OM_0 = OM_1 = \dots = OM_{n-1},$$
$$(\widehat{\overrightarrow{OM_0}, \overrightarrow{OM_1}}) = (\widehat{\overrightarrow{OM_1}, \overrightarrow{OM_2}}) = \dots = (\widehat{\overrightarrow{OM_{n-2}}, \overrightarrow{OM_{n-1}}}) = (\widehat{\overrightarrow{OM_{n-1}}, \overrightarrow{OM_0}}).$$

IX. 1. Résoudre dans $\mathbb{C}$ l'équation $z^n = 1$.

Si $z^n = 1$, alors $z \neq 0$. Soit z un complexe non nul. On note r son module et soit θ un argument de z.

$$\begin{aligned} z^n = 1 &\iff r^n e^{in\theta} = 1 \\ &\iff \begin{cases} r = 1, \\ n\theta \equiv 0[2\pi], \end{cases} \\ &\iff \begin{cases} r = 1, \\ \theta \equiv 0\left[\frac{2\pi}{n}\right], \end{cases} \\ &\iff \exists k \in \mathbb{Z},\ z = e^{\frac{2i\pi k}{n}}. \end{aligned}$$

Comme $e^{2i\pi} = 1$, les solutions de $z^n = 1$ sont donc les nombres complexes $e^{\frac{2i\pi k}{n}}$, avec $0 \leqslant k < n$.

2. Montrer que les points d'affixe les solutions de l'équation $z^n = 1$ forment un polygone régulier.

Pour tout $k \in [\![0, n-1]\!]$, sont M_k le point d'affixe $e^{\frac{2i\pi k}{n}}$. Pour simplifier la rédaction, on pose aussi $M_n = M_0$, point d'affixe $e^{\frac{2i\pi n}{n}} = 1$. Pour tout $k \in [\![0, n-1]\!]$, $OM_k = |e^{\frac{2i\pi k}{n}}| = 1$. De plus, $(\widehat{\overrightarrow{OM_k}, \overrightarrow{OM_{k+1}}})$ est un argument du nombre complexe

$$\frac{e^{\frac{2i\pi(k+1)}{n}}}{e^{\frac{2i\pi k}{n}}} = e^{\frac{2i\pi}{n}},$$

donc est égal à $\frac{2\pi}{n}$.

X. Pour tout $k \in [\![0, n-1]\!]$, on note M_k le point d'affixe $e^{\frac{2i\pi k}{n}}$. En particulier, $M_0 = I$. Soit B le point d'affixe $\cos\left(\frac{2\pi}{n}\right)$.

1. Montrer que si M_1 est constructible à la règle et au compas, alors B est constructible à la règle et au compas.

M_1 a pour abscisse $\cos\left(\frac{2\pi}{n}\right)$. D'après III, B est constructible car M_1 est constructible.

2. Montrer que si B est constructible à la règle et au compas, alors M_1 est constructible à la règle et au compas.

Soit $\mathcal{D}$ la perpendiculaire à (OI) passant par B : cette droite est constructible. Elle coupe le cercle de centre O et de rayon OI en les points M_1 et M_{n-1}, qui sont donc constructibles.

XI. Montrer que $M_0, \ldots, M_{n-1}$ sont constructibles à la règle et au compas si, et seulement si, B est constructible à la règle et au compas.

Supposons $M_0, \ldots, M_{n-1}$ constructibles. D'après X.1, B est constructible.

Supposons B constructible. $M_0 = I$ est constructible. D'après X.2, M_1 est constructible. Les deux cercles $\mathcal{C}$ et $\mathcal{C}_1$ (constructibles) de centre respectifs O et M_1 et de rayons respectifs OI et M_0M_1 se coupent en M_0 et M_2, qui est donc constructibles. En utilisant les cercles $\mathcal{C}_i$ de centre M_i et de rayon M_0M_1, on obtient successivement $M_2, \ldots, M_{n-1}$, qui sont donc tous constructibles.

XII. En utilisant le point B, montrer que $M_0, \ldots, M_{n-1}$ sont constructibles à la règle et au compas lorsque $n = 3$, $n = 4$ ou $n = 6$. Dans chacun de ces cas, on proposera une construction des points $M_0, \ldots, M_{n-1}$.

Pour $n = 3$: $B(-\frac{1}{2}; 0)$. À l'aide du cercle unité, on obtient le point $I'(-1; 0)$. Alors B est le milieu de $[I'O]$ et on l'obtient par la construction de I.1. On construit la perpendiculaire à (OI) passant par B. L'intersection de cette droite et du cercle unité donne M_1 et M_2.

Pour $n = 4$: $B = O$ L'intersection du cercle unité avec les axes (OI) et (OJ) détermine les points $M_0 = I$, $M_1 = J$, $M_2 = I'$ et $M_3 = J'$.

Pour $n = 6$: $B(\frac{1}{2}; 0)$, donc B est le milieu de $[OI]$. On construit alors la perpendiculaire à (OI) passant par B et l'intersection de cette droite avec le cercle unité donne M_1 et M_5. À l'aide de cercles de rayon M_1I, on obtient M_2, puis M_3, puis M_4.

XIII. On suppose maintenant $n = 5$. On pose $\omega = e^{\frac{2i\pi}{5}}$, et on note $\alpha = \omega + \overline{\omega}$.

1. Justifier que $\alpha = 2\cos\left(\dfrac{2\pi}{5}\right)$.

$$\alpha + \overline{\alpha} = 2Re(\alpha) = 2\cos\left(\frac{2\pi}{5}\right).$$

2. Montrer que $1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$.

Comme $\omega \neq 1$ et $\omega^5 = 1$:

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 = \frac{1 - \omega^5}{1 - \omega} = 0.$$

3. Montrer que $\alpha = \omega + \omega^4$ et que $\alpha^2 = \omega^2 + \omega^3 + 2$.

$$\overline{\omega} = e^{-\frac{2i\pi}{5}} = e^{-\frac{2i\pi}{5} + 2i\pi} = e^{\frac{8i\pi}{5}} = \omega^4,$$

donc $\alpha = \omega + \omega^4$. Par suite :

$$\alpha^2 = \omega^2 + 2\omega^5 + \omega^8 = \omega^2 + 2 + \omega^3.$$

4. En déduire que $-1+\alpha+\alpha^2=0$ puis que

$$\cos\left(\frac{2\pi}{5}\right)=\frac{-1+\sqrt{5}}{4}.$$

$$0=1+\omega+\omega^2+\omega^3+\omega^4=1+\alpha+\alpha^2-2=-1+\alpha+\alpha^2.$$

Donc $\alpha=\frac{-1+\sqrt{5}}{2}$ ou $\alpha=\frac{-1-\sqrt{5}}{2}$. Comme $\alpha>0$, $\alpha=\frac{-1+\sqrt{5}}{2}$. On obtient :

$$\cos\left(\frac{2\pi}{5}\right)=\frac{\alpha}{2}=\frac{-1+\sqrt{5}}{4}.$$

5. En déduire que $M_0,\dots,M_4$ sont des points constructibles.

D'après VII., 1, 5 et 4 sont des nombres constructibles. D'après VI.5, $\sqrt{5}$ est constructible. D'après V., $\frac{-1+\sqrt{5}}{4}$ est constructible. D'après III., B est constructible. D'après XII., $M_0,\dots,M_4$ sont constructibles.

XIV. On considère la construction suivante.

— Tracer le cercle $\mathbb{U}$ de centre O et de rayon 1. Soit K le point d'affixe -1.
— Construire le milieu B de $[KO]$ et tracer le cercle Γ de centre B et de rayon BJ. On note C le point intersection de Γ et de $[OI]$.
— Construire le milieu de D de $[OC]$.

1. Calculer l'affixe de D.

$$JB=\sqrt{\frac{1}{4}+1}=\frac{\sqrt{5}}{2}.$$

Donc l'affixe de D est $\frac{-1+\sqrt{5}}{4}=\cos\left(\frac{2\pi}{5}\right)$.

2. En déduire une construction du pentagone $M_0M_1M_2M_3M_4$ à la règle et au compas.

En traçant la perpendiculaire à (OI) passant par D, on obtient M_1 et M_4. En traçant les cercles de centre M_1 et M_4 et de rayon IM_1, on obtient M_2 et M_3 par intersection avec le cercle unité.

Thème : fonction

L'exercice

Une entreprise fabrique des cartons d'emballage. La production, exprimée en tonnes varie entre 0 et 10. Pour l'entreprise, le coût correspondant à la production de x tonnes de cartons, exprimé en milliers d'euros, est modélisé par :

$$C(x) = 0,5x^3 - 3x^2 + 5,5x - 2.$$

On appelle coût moyen la fonction C_M définie sur l'intervalle $]0;10]$ par : $C_M(x) = \dfrac{C(x)}{x}$.
L'entreprise vend ses cartons au prix de 40 milliers d'euros la tonne.
Que pensez-vous de l'affirmation « Le bénéfice est maximal lorsque le coût moyen est minimal » ? Justifiez la réponse.

d'après Tle STMG collection algomaths Delagrave

Les réponses de deux élèves de terminale STMG

Élève 1

J'ai tracé sur l'écran de ma calculatrice la courbe de chacune des deux fonctions. Le coût moyen est minimal pour 3 tonnes de cartons et le bénéfice est maximal pour 7 tonnes de cartons donc l'affirmation est incorrecte.

Élève 2

$C'_M(x) = x - 3 + \dfrac{2}{x^2} = \dfrac{x^3 - 3x^2 + 2}{x^2} = \dfrac{(x-1)(x^2 - 2x - 2)}{x^2}$.

$\Delta = 2^2 - 4 \times 1 \times (-2) = 12$ *donc il y a deux solutions :* $x_1 = \dfrac{2 - \sqrt{12}}{2 \times 1} \approx -0,73$ *et* $x_2 = \dfrac{2 + \sqrt{12}}{2 \times 1} \approx 2,73$.

Le coût moyen est donc minimal pour 2,73 tonnes de cartons mais je ne sais pas calculer le bénéfice.

Le travail à exposer devant le jury

1 – Analysez les productions de ces deux élèves en mettant en évidence leurs réussites et leurs éventuelles erreurs ainsi que l'accompagnement que vous pourriez leur proposer pour les aider.

2 – Exposez une correction de l'exercice telle que vous la présenteriez devant une classe de terminale STMG.

3 – Proposez deux exercices sur le thème *fonction* l'un au niveau collège, l'autre au niveau lycée permettant de développer la compétence « modéliser ».

Thème : grandeurs et mesures

L'exercice

Lors d'une promenade à bicyclette, Lucie utilise une application de son smartphone pour évaluer sa vitesse sur chacun des quatre tronçons du trajet.

Longueur du tronçon	5km	5km	5km	5km
Vitesse	18,4 km/h	17,3 km/h	21,2 km/h	16,8 km/h

Estimer la durée totale de son trajet ainsi que sa vitesse moyenne au cours de ce trajet.

Les productions de deux élèves de troisième

Élève 1

Comme toutes les distances sont identiques il suffit de faire la moyenne des vitesses :
$(18,4+17,3+21,2+16,8)/4 = 18,4$ *donc* $18,4$ *km/h.*
Par conséquent Lucie a mis un peu plus d'une heure.

Élève 2

J'ai utilisé un tableur :

	A	B	C	D	E	F
1	*distance*	*5*	*5*	*5*	*5*	*20*
2	*vitesse*	*18,4*	*17,3*	*21,2*	*16,8*	
3	*temps*	*3,68*	*3,46*	*4,24*	*3,36*	*14,74*
4						*1,356852103*

Je trouve un temps total de $14,74h$ *et une vitesse moyenne de* $1,35km/h$*, mais j'ai dû me tromper.*

Le travail à exposer devant le jury

1 – Analysez les productions de ces deux élèves en mettant en valeur leurs réussites et en précisant leurs erreurs. Vous indiquerez les conseils à leur apporter.

2 – Présentez une correction de l'exercice telle que vous l'exposeriez devant une classe de troisième.

3 – Proposez deux exercices (l'un au niveau du collège, l'autre au niveau du lycée) sur le thème *grandeurs et mesures* permettant notamment de développer les compétences « modéliser » et « calculer ».

Thème : conjecture et démonstration

L'exercice

Soit LEO un triangle rectangle en L tel que OE = 4 cm et OL = 2 cm. OLGA est un losange tel que E, O et A sont alignés dans cet ordre.

1. Réaliser une figure.
2. Conjecturer et démontrer une propriété sur les longueurs LE et LA.

D'après les fiches de tonton Lulu, vol.1 diffusion Tangente

La réponse de deux élèves de cycle 4 à la question 2

Élève 1

2. Je conjecture que LE = LA.
J'appelle I *le milieu du segment* [EO].
Je vois que le triangle OIL *est équilatéral et que les triangles* EIL *et* OLA *sont égaux.*
Par conséquent LE = LA.

Élève 2

2. Sur mon dessin je pense que LA est plus grand que LE.
Dans le triangle LEO *rectangle en* L *je peux calculer la longueur* [EL] *avec le théorème de Pythagore :* $EL^2 + LO^2 = EO^2$ *donc* $EL = \sqrt{12}$.
Ensuite j'ai appelé C *le centre du losange et je voulais montrer que la longueur* CL *est* $\frac{\sqrt{12}}{2}$ *mais je n'y suis pas arrivé car il me manque une longueur dans le triangle rectangle* OCL.

Le travail à exposer devant le jury

1 – Analysez ces productions d'élèves en mettant en évidence leurs réussites et leurs éventuelles erreurs. Vous préciserez l'aide que vous pouvez leur apporter.

2 – Présentez une correction de l'exercice telle que vous l'exposeriez devant une classe de collège de cycle 4.

3 – Proposez deux exercices sur le thème *conjecture et démonstration*, l'un au niveau collège, l'autre au niveau lycée. L'un au moins des exercices devra permettre de développer la compétence « raisonner ».

Thème : fonctions

L'exercice

Dans un magasin de reprographie, il existe deux types de photocopieurs.

Le prix des photocopies effectuées en utilisant le **photocopieur de type A** est obtenu à l'aide de la fonction `prixtotal` programmée ci-contre en langage Python.

```
def prixtotal(n):
    if n<=50:
        prix=n*0.1
    if 50<n and n<=200 :
        prix=5+(n-50)*0.05
    if n>200:
        prix=12.5+(n-200)*0.02
    return prix
```

Le **photocopieur de type B** fonctionne à l'aide d'une carte vendue 15 €. Cette carte permet d'effectuer 200 photocopies puis à partir de la 201e, la photocopie est facturée 0,01 €.

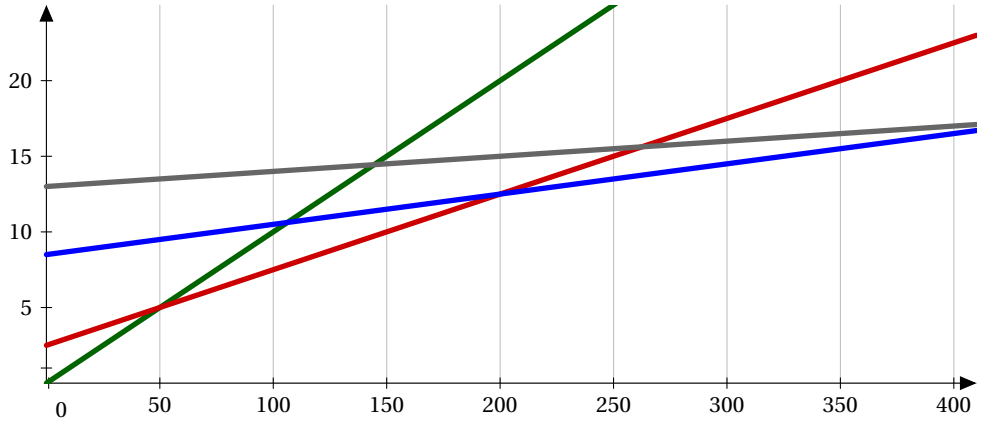
Déterminer en fonction du nombre de photocopies réalisées, le type de photocopieur à utiliser.

Les réponses de trois élèves de seconde

Élève 1

J'ai créé une fonction « affichage B » puis j'ai fait des tests. J'ai trouvé qu'il est préférable de choisir le photocopieur A pour un nombre de photocopies inférieur ou égal à 450.

Élève 2



À l'aide d'un logiciel de géométrie dynamique, j'ai tracé les 4 fonctions affines. Après je ne sais pas comment faire.

Élève 3

x est le nombre de photocopies à réaliser. Je résous alors : $12,5+(x-200)\times 0,02<15+0,01x$.
Soit $0,01x<6,5$. *Soit* $x<650$. *Il est préférable de choisir le photocopieur A pour* $x<650$.

Le travail à exposer devant le jury

1 – Analysez les productions de ces trois élèves en mettant en évidence leurs réussites et leurs éventuelles erreurs, ainsi que l'aide que vous pourriez leur proposer.

2 – Présentez une correction de l'exercice telle que vous l'exposeriez devant une classe de seconde.

3 – Proposez deux exercices sur le thème *fonctions* permettant de développer les compétences « modéliser » et « représenter ».