

Séances	Enseignement	Objectif pédagogique
1 et 2	Calcul propositionnel (principe du tiers exclu, principe de contraposition) ; manipulations des formules avec quantificateurs	Savoir nier une formule quantifiée ; savoir nier une implication, énoncer une implication réciproque, contraposée. . .
3 et 4	Exemples de démonstrations par contraposée, absurde. La preuve par récurrence. Suites (arithmétiques, géométriques et définies par récurrence simple)	Savoir rédiger de telles démonstrations.
5 et 6	Opérations sur les ensembles (inclusion, intersection, réunion, produit cartésien). Ensemble des parties d'un ensemble.	Savoir rédiger une preuve en utilisant les éléments.
7 et 8	Applications d'ensembles. Composition d'applications. Injectivité, surjectivité, bijectivité. Applications réciproques. Equipotence. Images inverses et directes de parties.	Savoir utiliser la formule de l'injectivité, de la surjectivité et leurs négations. Savoir reconnaître de telles applications. Savoir manipuler les images inverses et directes de parties.
9 et 10	Ensembles finis. Principe des bergers, d'inclusion-exclusion, des tiroirs.	Savoir utiliser ces principes dans des raisonnements simples.
11 et 12	Dénombrement élémentaire. Combinaisons, arrangements, triangle de Pascal, binôme de Newton.	Savoir résoudre des exercices de dénombrement simples.
13 et 14	Division euclidienne. Application 2 écriture d'un entier en base b .	Savoir effectuer la division euclidienne.
15 et 16	Divisibilité, congruences. Opérations sur les classes de congruences.	Savoir manipuler les opérations sur les classes de congruences.
17 et 18	Plus grand commun diviseur. Algorithme d'Euclide. Théorème de Bézout. Lemme de Gauss.	Savoir mettre en œuvre l'algorithme d'Euclide.
19	Plus petit commun multiple. Pgcd et ppcm d'un nombre d'entiers supérieur à 3.	
21 et 22	Nombres premiers. Crible d'Ératostène. Lemme d'Euclide. Infinitude de l'ensemble des nombres premiers. Décomposition d'un entier non nul en facteurs premiers. Application aux calculs de pgcd et ppcm. Petit théorème de Fermat	Savoir décomposer un entier en facteur premier. Calculs de pgcd et ppcm.
23 et 24	Inverse modulo n . Résolution d'une équation aux congruences linéaire. Résolution d'un système d'équations aux congruences linéaires, théorème des restes chinois.	Savoir résoudre les équations et système d'équations aux congruences linéaires
	Indicatrice d'Euler, propriétés et calcul en termes de la décomposition en facteurs premiers. Théorème d'Euler. Le système de cryptage RSA.	