LMAT2440

2014-2015

Théorie des nombres

5.0 crédits	30.0 h + 15.0 h	1q

Enseignants:	Pereira Olivier ; Tignol Jean-Pierre ;
Langue d'enseignement:	Français
Lieu du cours	Louvain-la-Neuve
Ressources en ligne:	<!--{cke_protected}{C}%3C!%2D%2D%0A%20%2F*%20Font%20Definitions%20*%2F%0A%40font-face%0A%09%7Bfont-family%3A%22Cambria%20Math%22%3B%0A%09panose-1%3A2%204%205%203%205%204%206%203%202%204%3B%0A%09mso-font-charset%3A1%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-format%3Aother%3B%0A%09mso-font-pitch%3Avariable%3B%0A%09mso-font-signature%3A0%200%200%200%200%200%3B%7D%0A%40font-face%0A%09%7Bfont-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-font-charset%3A0%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-pitch%3Aauto%3B%0A%09mso-font-signature%3A0%200%200%200%200%200%3B%7D%0A%20%2F*%20Style%20Definitions%20*%2F%0Ap.MsoNormal%2C%20li.MsoNormal%2C%20div.MsoNormal%0A%09%7Bmso-style-unhide%3Ano%3B%0A%09mso-style-qformat%3Ayes%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-fareast-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-ansi-language%3AEN-US%3B%0A%09mso-fareast-language%3AEN-US%3B%7D%0Ap.Corps%2C%20li.Corps%2C%20div.Corps%0A%09%7Bmso-style-name%3ACorps%3B%0A%09mso-style-unhide%3Ano%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%0A%09font-family%3AHelvetica%3B%0A%09mso-fareast-font-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09color%3Ablack%3B%0A%09mso-ansi-language%3AFR%3B%7D%0A.MsoChpDefault%0A%09%7Bmso-style-type%3Aexport-only%3B%0A%09mso-default-props%3Ayes%3B%0A%09font-size%3A10.0pt%3B%0A%09mso-ansi-font-size%3A10.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%7D%0A%40page%20WordSection1%0A%09%7Bsize%3A612.0pt%20792.0pt%3B%0A%09margin%3A70.85pt%2070.85pt%2070.85pt%2070.85pt%3B%0A%09mso-header-margin%3A36.0pt%3B%0A%09mso-footer-margin%3A36.0pt%3B%0A%09mso-paper-source%3A0%3B%7D%0Adiv.WordSection1%0A%09%7Bpage%3AWordSection1%3B%7D%0A%2D%2D%3E--> Site iCampus (> http://icampus.uclouvain.be/).
Préalables :	& t;!--{cke_protected}{C}%3C!%2D%2D%0A%20%2F*%20Font%20Definitions%20*%2F%0A%40font-face%0A%09%7Bfont-family%3A%22Cambria%20Math%22%3B%0A%09panose-1%3A2%204%205%203%205%204%206%203%202%204%3B%0A%09mso-font-charset%3A1%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-format%3Aother%3B%0A%09mso-font-pitch%3Avariable%3B%0A%09mso-font-signature%3A0%200%200%200%200%200%3B%7D%0A%40font-face%0A%09%7Bfont-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-font-charset%3A0%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-pitch%3Aauto%3B%0A%09mso-font-signature%3A0%200%200%200%200%200%3B%7D%0A%20%2F*%20Style%20Definitions%20*%2F%0Ap.MsoNormal%2C%20li.MsoNormal%2C%20div.MsoNormal%0A%09%7Bmso-style-unhide%3Ano%3B%0A%09mso-style-qformat%3Ayes%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-fareast-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-ansi-language%3AEN-US%3B%0A%09mso-fareast-language%3AEN-US%3B%7D%0Ap.Corps%2C%20li.Corps%2C%20div.Corps%0A%09%7Bmso-style-name%3ACorps%3B%0A%09mso-style-unhide%3Ano%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%0A%09font-family%3AHelvetica%3B%0A%09mso-fareast-font-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09color%3Ablack%3B%0A%09mso-ansi-language%3AFR%3B%7D%0A.MsoChpDefault%0A%09%7Bmso-style-type%3Aexport-only%3B%0A%09mso-default-props%3Ayes%3B%0A%09font-size%3A10.0pt%3B%0A%09mso-ansi-font-size%3A10.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%7D%0A%40page%20WordSection1%0A%09%7Bsize%3A612.0pt%20792.0pt%3B%0A%09margin%3A70.85pt%2070.85pt%2070.85pt%2070.85pt%3B%0A%09mso-header-margin%3A36.0pt%3B%0A%09mso-footer-margin%3A36.0pt%3B%0A%09mso-paper-source%3A0%3B%7D%0Adiv.WordSection1%0A%09%7Bpage%3AWordSection1%3B%7D%0A%2D%2D%3E--& t; LMAT1131 - algèbre linéaire (première année de bachelier en sciences mathématiques) ou cours équivalent.
Thèmes abordés :	& t;!--{cke_protected}{C}%3C!%2D%2D%0A%20%2F*%20Font%20Definitions%20*%2F%0A%40font-face%0A%09%7Bfont-family%3A%22Cambria%20Math%22%3B%0A%09panose-1%3A2%204%205%203%205%204%206%203%202%204%3B%0A

	%09mso-font-charset%3A1%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-format%3Aother%3B%0A%09mso-font-pitch%3Avariable%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%40font-face%0A%09%7Bfont-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-font-charset%3A0%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-pitch%3Aauto%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%20%2F*%20Style%20Definitions%20*%2F%0Ap.MsoNormal%2C%20li.MsoNormal%2C%20div.MsoNormal%0A%09%7Bmso-style-unhide%3Ano%3B%0A%09mso-style-qformat%3Ayes%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-fareast-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-ansi-language%3AEN-US%3B%0A%09mso-fareast-language%3AEN-US%3B%7D%0Ap.Corps%2C%20li.Corps%2C%20div.Corps%0A%09%7Bmso-style-name%3ACorps%3B%0A%09mso-style-unhide%3Ano%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%0A%09font-family%3AHelvetica%3B%0A%09mso-fareast-font-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09color%3Ablack%3B%0A%09mso-ansi-language%3AFR%3B%7D%0A.MsoChpDefault%0A%09%7Bmso-style-type%3Aexport-only%3B%0A%09mso-default-props%3Ayes%3B%0A%09font-size%3A10.0pt%3B%0A%09mso-ansi-font-size%3A10.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%7D%0A%40page%20WordSection1%0A%09%7Bsize%3A612.0pt%20792.0pt%3B%0A%09margin%3A70.85pt%2070.85pt%2070.85pt%2070.85pt%3B%0A%09mso-header-margin%3A36.0pt%3B%0A%09mso-footer-margin%3A36.0pt%3B%0A%09mso-paper-source%3A0%3B%7D%0Adiv.WordSection1%0A%09%7Bpage%3AWordSection1%3B%7D%0A%2D%2D%3E--& t; Initiation à divers aspects de la théorie des nombres et de ses méthodes, en particulier en vue de ses applications à la cryptographie mathématique.
Acquis d'apprentissage	Contribution du cours aux acquis d'apprentissage du programme de master en mathématique. A la fin de cette activité, l'étudiant aura progressé dans sa capacité à: - Connaître et comprendre un socle fondamental des mathématiques. Il aura notamment développé sa capacité à: -- Choisir et utiliser les méthodes et les outils fondamentaux de calcul. -- Reconnaître les concepts fondamentaux d'importantes théories mathématiques actuelles. -- Etablir les liens principaux entre ces théories. - Faire preuve d'abstraction, de raisonnement et d'esprit critique. Il aura notamment développé sa capacité à: -- Dégager les aspects unificateurs de situations et expériences différentes. -- Raisonner dans le cadre de la méthode axiomatique. -- Construire et rédiger une démonstration de façon autonome, claire et rigoureuse. - Analyser un problème mathématique et proposer des outils adéquats pour l'étudier de façon autonome. Acquis d'apprentissage spécifiques au cours. A la fin de cette activité, l'étudiant sera capable de: - résoudre des équations dans des anneaux d'entiers modulaires; - déterminer des conditions d'existence de solutions de certaines équations diophantiennes; - appliquer des résultats d'analyse mathématique à l'étude des nombres premiers; - appliquer des résultats d'arithmétique modulaire à la construction d'algorithmes utilisés en cryptographie. Mode d'évaluation des acquis des étudiants L'évaluation se fait sur base d'un examen écrit. On y teste la connaissance et la compréhension des notions, des exemples et des résultats fondamentaux, la capacité de construire un raisonnement cohérent, la maîtrise des techniques de démonstration introduites pendant le cours. *La contribution de cette UE au développement et à la maîtrise des compétences et acquis du (des) programme(s) est accessible à la fin de cette fiche, dans la partie « Programmes/formations proposant cette unité d'enseignement (UE) ».*

Modes d'évaluation des acquis des étudiants :	& mp;lt;!--{cke_protected}{C}%3C!%2D%2D%0A%20%2F*%20Font%20Definitions%20*%2F%0A%40font-face%0A%09%7Bfont-family%3A%22Cambria%20Math%22%3B%0A%09panose-1%3A2%204%205%203%205%204%206%203%202%204%3B%0A%09mso-font-charset%3A1%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-format%3Aother%3B%0A%09mso-font-pitch%3Avariable%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%40font-face%0A%09%7Bfont-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-font-charset%3A0%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-pitch%3Aauto%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%20%2F*%20Style%20Definitions%20*%2F%0Ap.MsoNormal%2C%20li.MsoNormal%2C%20div.MsoNormal%0A%09%7Bmso-style-unhide%3Ano%3B%0A%09mso-style-qformat%3Ayes%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-fareast-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-ansi-language%3AEN-US%3B%0A%09mso-fareast-language%3AEN-US%3B%7D%0Ap.Corps%2C%20li.Corps%2C%20div.Corps%0A%09%7Bmso-style-name%3ACorps%3B%0A%09mso-style-unhide%3Ano%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%0A%09font-family%3AHelvetica%3B%0A%09mso-fareast-font-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09color%3Ablack%3B%0A%09mso-ansi-language%3AFR%3B%7D%0A.MsoChpDefault%0A%09%7Bmso-style-type%3Aexport-only%3B%0A%09mso-default-props%3Ayes%3B%0A%09font-size%3A10.0pt%3B%0A%09mso-ansi-font-size%3A10.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%7D%0A%40page%20WordSection1%0A%09%7Bsize%3A612.0pt%20792.0pt%3B%0A%09margin%3A70.85pt%2070.85pt%2070.85pt%2070.85pt%3B%0A%09mso-header-margin%3A36.0pt%3B%0A%09mso-footer-margin%3A36.0pt%3B%0A%09mso-paper-source%3A0%3B%7D%0Adiv.WordSection1%0A%09%7Bpage%3AWordSection1%3B%7D%0A%2D%2D%3E--& mp;gt; L'évaluation se fait sur base d'un examen écrit. On y teste la connaissance et la compréhension des notions, des exemples et des résultats fondamentaux, la capacité de construire un raisonnement cohérent, la maîtrise des techniques de démonstration introduites pendant le cours.
Méthodes d'enseignement :	& mp;lt;!--{cke_protected}{C}%3C!%2D%2D%0A%20%2F*%20Font%20Definitions%20*%2F%0A%40font-face%0A%09%7Bfont-family%3A%22Cambria%20Math%22%3B%0A%09panose-1%3A2%204%205%203%205%204%206%203%202%204%3B%0A%09mso-font-charset%3A1%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-format%3Aother%3B%0A%09mso-font-pitch%3Avariable%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%40font-face%0A%09%7Bfont-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-font-charset%3A0%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-pitch%3Aauto%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%20%2F*%20Style%20Definitions%20*%2F%0Ap.MsoNormal%2C%20li.MsoNormal%2C%20div.MsoNormal%0A%09%7Bmso-style-unhide%3Ano%3B%0A%09mso-style-qformat%3Ayes%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-fareast-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-ansi-language%3AEN-US%3B%0A%09mso-fareast-language%3AEN-US%3B%7D%0Ap.Corps%2C%20li.Corps%2C%20div.Corps%0A%09%7Bmso-style-name%3ACorps%3B%0A%09mso-style-unhide%3Ano%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%0A%09font-family%3AHelvetica%3B%0A%09mso-fareast-font-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09color%3Ablack%3B%0A%09mso-ansi-language%3AFR%3B%7D%0A.MsoChpDefault%0A%09%7Bmso-style-type%3Aexport-only%3B%0A%09mso-default-props%3Ayes%3B%0A%09font-size%3A10.0pt%3B%0A%09mso-ansi-font-size%3A10.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%7D%0A%40page%20WordSection1%0A%09%7Bsize%3A612.0pt%20792.0pt%3B%0A%09margin%3A70.85pt%2070.85pt%2070.85pt%2070.85pt%3B%0A%09mso-header-margin%3A36.0pt%3B%0A%09mso-footer-margin%3A36.0pt%3B%0A%09mso-paper-source%3A0%3B%7D%0Adiv.WordSection1%0A%09%7Bpage%3AWordSection1%3B%7D%0A%2D%2D%3E--& mp;gt; Le cours est donné sous forme de cours magistraux et de séances de travaux pratiques. Pendant les séances, les étudiants sont appelés à faire des suggestions et formuler des idées pour faire avancer le cours en se basant sur leurs connaissances préalables.
Contenu :	& mp;lt;!--{cke_protected}{C}%3C!%2D%2D%0A%20%2F*%20Font%20Definitions%20*%2F%0A%40font-face%0A%09%7Bfont-family%3A%22Cambria%20Math%22%3B%0A%09panose-1%3A2%204%205%203%205%204%206%203%202%204%3B%0A%09mso-font-charset%3A1%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-format%3Aother%3B%0A%09mso-font-pitch%3Avariable%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%40font-face%0A%09%7Bfont-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-font-charset%3A0%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-pitch%3Aauto%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%20%2F*%20Style%20Definitions%20*%2F%0Ap.MsoNormal%2C%20li.MsoNormal%2C%20div.MsoNormal%0A%09%7Bmso-style-unhide%3Ano%3B%0A%09mso-style-qformat%3Ayes%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-fareast-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-ansi-language%3AEN-US%3B%0A%09mso-fareast-language%3AEN-US%3B%7D%0Ap.Corps%2C%20li.Corps%2C%20div.Corps%0A%09%7Bmso-style-name%3ACorps%3B%0A%09mso-style-unhide%3Ano%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%0A%09font-family%3AHelvetica%3B%0A%09mso-fareast-font-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09color%3Ablack%3B%0A%09mso-ansi-language%3AFR%3B%7D%0A.MsoChpDefault%0A%09%7Bmso-style-type%3Aexport-only%3B%0A%09mso-default-props%3Ayes%3B%0A

	%09font-size%3A10.0pt%3B%0A%09mso-ansi-font-size%3A10.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%7D%0A%40page%20WordSection1%0A%09%7Bsize%3A612.0pt%20792.0pt%3B%0A%09margin%3A70.85pt%2070.85pt%2070.85pt%2070.85pt%3B%0A%09mso-header-margin%3A36.0pt%3B%0A%09mso-footer-margin%3A36.0pt%3B%0A%09mso-paper-source%3A0%3B%7D%0Adiv.WordSection1%0A%09%7Bpage%3AWordSection1%3B%7D%0A%2D%2D%3E--& mp;gt; Cette activité consiste à illustrer divers aspects de la théorie des nombres, en particulier ceux qui sont applicables à la cryptographie. Les contenus suivants sont abordés dans le cadre du cours. - Arithmétique modulaire : théorème chinois des restes et loi de réciprocité quadratique. - Formes quadratiques rationnelles : corps de nombres p-adiques et principe local-global. - Méthodes analytiques : fonction zêta et théorème de Dirichlet. - Cubiques projectives : propriétés arithmétiques des courbes elliptiques. - Théorie algorithmique des nombres: tests de primalité, factorisation. - Construction d'objets utiles en cryptographie: courbes elliptiques, systèmes de chiffrement. L'équilibre entre les différentes parties et les détails du programme ci-dessus sont susceptibles de varier d'année en année.
Bibliographie :	& mp;lt;!--{cke_protected}{C}%3C!%2D%2D%0A%20%2F*%20Font%20Definitions%20*%2F%0A%40font-face%0A%09%7Bfont-family%3A%22Cambria%20Math%22%3B%0A%09panose-1%3A2%204%205%203%205%204%206%203%202%204%3B%0A%09mso-font-charset%3A1%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-format%3Aother%3B%0A%09mso-font-pitch%3Avariable%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%40font-face%0A%09%7Bfont-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-font-charset%3A0%3B%0A%09mso-generic-font-family%3Aroman%3B%0A%09mso-font-pitch%3Aauto%3B%0A%09mso-font-signature%3A0%200%200%200%200%3B%7D%0A%20%2F*%20Style%20Definitions%20*%2F%0Ap.MsoNormal%2C%20li.MsoNormal%2C%20div.MsoNormal%0A%09%7Bmso-style-unhide%3Ano%3B%0A%09mso-style-qformat%3Ayes%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-fareast-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09mso-ansi-language%3AEN-US%3B%0A%09mso-fareast-language%3AEN-US%3B%7D%0Ap.Corps%2C%20li.Corps%2C%20div.Corps%0A%09%7Bmso-style-name%3ACorps%3B%0A%09mso-style-unhide%3Ano%3B%0A%09mso-style-parent%3A%22%22%3B%0A%09margin%3A0cm%3B%0A%09margin-bottom%3A.0001pt%3B%0A%09mso-pagination%3Awidow-orphan%3B%0A%09font-size%3A12.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%0A%09font-family%3AHelvetica%3B%0A%09mso-fareast-font-family%3A%22%E3%83%92%E3%83%A9%E3%82%AE%E3%83%8E%E8%A7%92%E3%82%B4%20Pro%20W3%22%3B%0A%09mso-bidi-font-family%3A%22Times%20New%20Roman%22%3B%0A%09color%3Ablack%3B%0A%09mso-ansi-language%3AFR%3B%7D%0A.MsoChpDefault%0A%09%7Bmso-style-type%3Aexport-only%3B%0A%09mso-default-props%3Ayes%3B%0A%09font-size%3A10.0pt%3B%0A%09mso-ansi-font-size%3A10.0pt%3B%0A%09mso-bidi-font-size%3A10.0pt%3B%7D%0A%40page%20WordSection1%0A%09%7Bsize%3A612.0pt%20792.0pt%3B%0A%09margin%3A70.85pt%2070.85pt%2070.85pt%2070.85pt%3B%0A%09mso-header-margin%3A36.0pt%3B%0A%09mso-footer-margin%3A36.0pt%3B%0A%09mso-paper-source%3A0%3B%7D%0Adiv.WordSection1%0A%09%7Bpage%3AWordSection1%3B%7D%0A%2D%2D%3E--& mp;gt; R. Crandall, C.B. Pomerance : Prime Numbers: A Computational Perspective, Springer,2005. K. Ireland, M. Rosen : A classical introduction to modern number theory, Springer, 2d edition, 1991. N. Koblitz: A Course in Number Theory and Cryptography, Springer, 2nd edition, 1994. J.P. Serre: Cours d'arithmétique, PUF, 1970.
Cycle et année d'étude: :	> Master [120] en sciences mathématiques > Bachelier en sciences mathématiques > Master [120] : ingénieur civil en informatique > Master [120] : ingénieur civil électricien > Master [120] : ingénieur civil en mathématiques appliquées
Faculté ou entité en charge:	MATH