シラバス参照[2026年度／素数の魅力と暗号理論　01／高木　悟]

授業情報

開講年度	2026年度	開講箇所	グローバル・エデュケーション・センター		
科目名	素数の魅力と暗号理論　01				
担当教員	高木　悟				
学期曜日時限	春クォーター　01:無フルOD				
科目区分	数学科目（日本語）	配当年次	1年以上	単位数	1
使用教室		キャンパス			
科目キー	9S02000102	科目クラスコード	01		
授業で使用する言語	日本語				
授業方法区分	【オンライン】フルオンデマンド				
コース・コード	MATX111L				
大分野名称	数学				
中分野名称	数学				
小分野名称	代数学				
レベル	初級レベル（入門・導入）	授業形態	講義		
	オープン科目				

シラバス情報

授業概要

★ 本科目の01クラス（春クォーター設置）・03クラス（秋クォーター設置）は同一の内容です.
　1つしか履修できません.　02クラス（夏クォーター設置）・04クラス（冬クォーター設置）はありません.

★ 本科目と英語科目「Cryptography and Mathematics」の両方を履修することはできません.

本科目は，Waseda Moodle（以下「WM」と表記）によるフルオンデマンド形式の講義である.
このシラバスに記載されているすべての事項をよく読み，理解した上で履修登録すること.

本科目では，代数学の一分野である初等整数論（elementary number theory）の基礎として，整数の性質，ユークリッドの互除法，1次不定方程式，素数の性質，合同式，オイラー関数，フェルマーの小定理を順に説明し，素数を用いたRSA暗号理論を解説する.
実際に，暗号化するための鍵を作ってメッセージを暗号化したり，復号する（暗号文を元のメッセージに戻す）ための鍵を作って暗号文を復号したりすることで理解を深めるとともに，弱点を知って解読（復号する鍵を使わずに暗号文から元のメッセージを得ること）を試みることで，暗号の安全性についても考察する.
定理の証明は教科書に記載されているが，そのうち重要な定理については最終回の＃7（第7回）にまとめて証明する．ただし，これらの証明のビデオ講義については，本科目の授業期間中いつでも視聴できるように設定しておく.
まずは，定理を（証明せずに）用いて具体的な問題が解けるようになることを優先する.
予備知識としては，中学程度の数学で十分であるが，理解するのが簡単だということではない.

★ GEC数学ウェブサイト　https://www.waseda.jp/inst/gec/gec/academic/literacy/math/
　（GEC数学科目の紹介だけでなく，受講するか悩んでいるみなさんへの過去の受講生からのメッセージもあります）

★ 科目登録3次登録者は，登録結果の発表前にWMにエクスターナルユーザとして登録され受講できるようになるので，登録されたら速やかに＃1（第1回）と＃2（第2回）を受講してください．すでに授業は始まっており，＃1と＃2の試験等の解答提出期限まであまり時間がありません.
　3次登録する場合は，このことを了解の上で履修登録してください.

授業の到達目標

初等整数論の基本となる素因数分解とその一意性，ユークリッドの互除法，合同式，フェルマーの小定理を理解すること.
素数を用いたRSA暗号の仕組みを理解すること.
RSA暗号理論を用いて，公開鍵（暗号化鍵）と秘密鍵（復号鍵）を作成し，メッセージの暗号化と暗号文の復号ができること.

事前・事後学習の内容

【初回授業前】 WMの本科目・クラス内で公開している「早大GEC 暗号/群論/結び目（担当：高木）共通ガイダンス（2026）」（以下「共通ガイダンス」と表記）をよく読み，理解する.
【事前学習】 次回扱う単元について，1週間前に公開される授業プリントと教科書を読み，疑問点をまとめておく.
【事後学習】 授業で扱った単元と例題を復習し，授業プリント内の問題をもう一度解く．また，教科書の指定された問題を解く.
毎回合計で4時間程度かかると想定される.

授業計画

1: ＃1．暗号の仕組みと整数の基本性質
　まず，いろいろな暗号を紹介し，それぞれの仕組みを簡単に解説する．その後，RSA暗号理論を理解するために必要な数学を＃5まで順に解説するが，まずは整数の四則演算（加算・減算・乗算・除算）に関する基本的な性質を考察する．（教科書 7.1～7.3, 1.1節）
2: ＃2．ユークリッドの互除法
　2つ以上の整数の最大公約数を効率よく求めるアルゴリズムであるユークリッドの互除法について解説する．（教科書 1.2, 2.1節）
3: ＃3．1次不定方程式の解法と素数の基本性質
　係数も解も整数である1次不定方程式の性質を調べ，解法を考える．また，整数が素数の積にただ1通りに分解できること（素因数分解の一意性）など，素数に関する基本的な性質を紹介する．（教科書 2.2, 3.1～3.2節）
4: ＃4．合同式
　合同式の概念を導入し，時計やJR山手線など，日常にある合同式の例に触れながら，その基本的な性質を解説する．（教科書 4.1～4.4節）
5: ＃5．オイラー関数とフェルマーの小定理
　オイラー関数を導入し，その基本的な性質を解説する．また，フェルマーの小定理を解説し，具体的な応用例を紹介する．（教科書 5.1～5.3, 6.1～6.3節）
6: ＃6．RSA暗号理論
　RSA暗号の理論を解説し，実際に公開鍵（暗号化鍵）を作ってメッセージを暗号化したり，秘密鍵（復号鍵）を作って暗号文を復号したりする．また，RSA暗号の弱点を知り，解読を試みることで，RSA暗号の安全性について考察する．（教科書 7.3節）
7: ＃7．重要な定理の証明
　本科目で今までに扱った定理のうち，重要なものを証明する．（教科書 1.1～7.3節）

教科書

「整数論体験入門」 野口和範著　共立出版
　※この本を持っていることを前提に授業を進める.

授業に沿ったワークシート形式の授業プリント（PDFファイル）をWMにアップする．ワークシート形式なので，ビデオ講義を視聴しながら書き込めるようになっている．ただし，必要最小限しか記載しないので，教科書の関連する項目を適宜参照し，また教科書内の問題を解いて，理解を深めてほしい.

参考文献

(1)「初等整数論講義第2版」 高木貞治著　共立出版
(2)「整数論1　初等整数論からp進数へ」 雪江明彦著　日本評論社

成績評価方法

割合	評価基準

	試験: 36% ＃1から＃6まで毎回WMで実施する「試験」の得点（1回6点満点で合計36点満点）を成績評価に用いる. 「試験」についての補足： ・以下の「平常点評価」に記されている「理解度チェック」の類題が主であり，本科目・クラスの授業カレンダーに示された解答期間内に一度だけ受験可能である. ・制限時間は設けておらず，一時保存も可能であるが，本科目・クラスの授業カレンダーに示された解答期限までに提出する必要がある. ・得点・結果は公開しない（フルオンデマンド形式であることから，不正行為等防止のため，公開しないことにしている．各単元の復習や理解度の確認は「理解度チェック」で可能である）. ・＃7（最終回）は「試験」はない（最終試験もない）. 平常点評価: 64% ＃1から＃6まで毎回WMで実施する「理解度チェック」の得点（1回8点満点で合計48点満点）と，＃1から＃7までの「レビューシート」の提出（合計16点満点に換算）を成績評価に用いる. 「理解度チェック」についての補足： ・本科目・クラスの授業カレンダーに示された解答期間内であれば何度も受験可能で，その中の最高点を得点として採用する. ・解答直後に，各問について正解か不正解かが分かり（ただし，正答は表示されない），得点も表示されるため，間違えた箇所を復習することで，満点を取ることが可能である. ・制限時間は設けておらず，一時保存も可能であるが，本科目・クラスの授業カレンダーに示された解答期限までに提出する必要がある. ・＃7（最終回）は「理解度チェック」はない. 「レビューシート」についての補足： ・本科目・クラスの授業カレンダーに示された回答期間内であれば，何度も提出可能である. ・制限時間は設けておらず，一時保存も可能であるが，本科目・クラスの授業カレンダーに示された回答期限までに提出する必要がある. ・設問に条件（例えば，100字以上の字数制限など）があれば，それを満たす必要がある. 成績評価方法の詳細は，履修登録後に，WMの本科目・クラス内にアップしている共通ガイダンスを参照のこと.
備考・関連URL	本科目の授業スケジュールは，本学の定める当該クォーター授業開始日の 00:00 ちょうどから＃1がスタートし，当該クォーター授業終了日の 23:55 ちょうどに＃7が終了する（日時はすべて日本標準時(JST)である）. 詳しい授業スケジュールについては，下記関連資料（授業カレンダー）を参照のこと（MyWaseda にログインしないと関連資料は閲覧できない）. 本科目の2026年度・秋クォーターについては，授業終了日を（大学の定める授業終了日より1日延長して）2026年11月22日（日）とする. 従って，＃7が終了するのは 2026年11月22日（日） 23:55 である. ★ GECの数学基礎プラスシリーズとは異なるスケジュール・成績評価方法なので注意すること.
関連資料	タイトル / 掲載日時 授業カレンダー（2026年度・春クォーター） 2026/02/01 16:42:16