科目区分：自然科学科目

授業科目名	数理科学（数論への入門）					学期	曜日	校時
英　語　名	Mathematical Science (Introduction to Number Theory)							
担　当 教　員　名	末吉　豊	単位数	2単位	必修 選択	選択	前期	木曜日	2校時

授　業　の　ね　ら　い　・　内　容　・　方　法

整数に関する話題を通して，数及び数学への理解を深め，論理的な思考力，判断力，表現力を身につけることがねらいである．「整数の性質のいくつかについて説明できること」，「関連する計算ができること」，「数学が社会の中で果たす役割について説明できること」を到達目標とする．授業の前半で講義，後半で演習問題を解く．

テ　キ　ス　ト　、　教　材　等

テキストなし．プリントを配布する．以下の書物を参考にする．
J. H. シルヴァーマン（鈴木治郎訳），はじめての数論，ピアソン・エデュケーション，2001（2001）
A. ヴェイユ（片山孝次他訳），初学者のための整数論，現代数学社，1979（1995）

対　象　学　生	成　績　評　価　の　方　法	教　員　研　究　室
全　学　部	平常点（演習・小テスト）50% 期末試験（又はレポート）50% 合計 60 点（100 点満点）以上が合格	

授　　業　　計　　画

整数，特に，素数に関する話題について講義する．そのうちのいくつかを紹介する．

メルセンヌ素数は世界最大の素数として知られる．現在 41 個知られていて，最大のものは 2004 年 5 月 15 日に見つかったもので，10 進で約 720 万桁と巨大である．現在，インターネットを通じて世界で 20 万台以上のコンピュータが参加し，日夜新しいメルセンヌ素数の探索が続けられている．1000 万桁を越える素数の発見には 10 万ドルの懸賞金が掛けられている．メルセンヌ素数が無限に存在するかどうかは未解決である．

1796 年 3 月 30 日，当時 19 歳のガウスは正十七角形の定規とコンパスによる作図法を発見した．ユークリッドの時代から，正三角形，正五角形，正十五角形等の作図法は知られていたが，ガウスは一般に，p がフェルマー素数なら，正 p 角形が定規とコンパスにより作図可能であることを証明した．フェルマー素数は現在，3, 5, 17, 257, 65537 が見つかっているが，他にはないと予想されている．

インターネット上の秘密通信や身元証明に，公開鍵暗号という新しい暗号が使われている．従来の暗号では鍵を秘密にするが，公開鍵暗号では鍵の一部を公開する．公開鍵暗号の構成に，150 桁以上の素数を用いる．暗号を作るため，素数を見つけるため，素数の様々な性質が利用されている．講義では，その一端を紹介する．

１回目　数論で扱う問題（イントロダクション）
２回目　素数の無限性（2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ･･･）
３回目　メルセンヌ素数探索計画（2^p – 1）
４回目　完全数（1 + 4 + 7 + 14 = 28）
５回目　フェルマー素数（2^(2^n) + 1）
６回目　作図問題（ギリシャ数学とガウス，ガロアの功績）
７回目　ユークリッドの互除法（最大公約数）
８回目　ガウスの整数（素数を分解する）
９回目　ピタゴラス数（x^2 + y^2 = z^2）
１０回目　フェルマーの最終定理（x^n + y^n = z^n）
１１回目　合同式（余りで作る新しい数）
１２回目　RSA 暗号（鍵配送と電子署名）
１３回目　素数判定（300 桁の素数）
１４回目　カーマイケル数（素数判定をすり抜ける）
１５回目　期末試験（又はレポート）

○オフィスアワー（質問受付時間）：月曜日，水曜日 16:10～17:40　教員研究室