## 教科目名 数論 (Number Theory)

**専攻名・学年** : 全専攻 1年 (教育プログラム 第3学年 ○科目) **単位数など** : 選択 2単位 (後期1コマ,授業時間23.25時間)

担 当 教 員 : 髙妻倫太郎

## 授業の概要

イギリスが生んだ20世紀初期最高の数学者の1人,G.H.ハーディは誇り高くこう述べた.

「真の数学は実用とは無縁である.数論を実用化する方法は、いまだかつて誰も見出していないのだ」

しかし 1970 年代,数論が暗号理論に実用化できることが発見されたのは,数論の位置付けを実社会にまで広げる 20世紀最大の快挙の1つであった.以降,数に関する根本原理の解明は,社会的応用面からも重要性を増し続けている.本講義は,数論における数の初等的取り扱いについて,関わる歴史や人物に触れつつ,以下5段階の発見的方法を踏みながら吟味していく.予備知識は本科1年次程度を仮定する.

- 1. データを集める.
- 2. データを調べてパターンや関係性を見出す.
- 3. パターンや関係性を説明できるような予想を式に立てる(推測する).
- 4. さらにデータを集めることによって予想を確かめる. そして新たなデータも予想に合うことを確かめる.
- 5. 予想が正しいことを示す根拠を考え出す(証明する).

## 達成目標と評価方法

## 大分高専目標(B1), JABEE 目標(c)(g)

- (1) 数の諸性質を理解し、その取り扱いに慣れる. (定期試験と課題)
- (2) 数学的に考える習慣を身につける. (定期試験と課題)
- (3) 問題解決の意欲を高め、自主的・継続的な学習習慣を身につける. (課題)

□ 数論とは何ものでしょう?     ○ 数論における諸問題を具体的に紹介する。     ○ ピタゴラスの定理を幾何的に分析し、その高次化を考える。     ○ ユーツリッドの互除法を理解し、一次方程式と最大公約数    ○ ユーツリッドの互除法を理解し、一次方程式に応用する。     ○ 数の合同概念を理解する。     ○ 数の合同概念を理解する。     ○ 数の合同概念を理解する。     ○ 数の原子一素数    ○ 中国式創会定理(係子の定理)を理解する。     ○ 素数が無数に存在することを証明し、その一般化であるオイラーの完全数定理を証明する。     ○ 本イラー関数と中国の剩余定理     ○ 本イラーの完全数定理を証明する。     ○ 本のに表表を理解を述べる。     ○ 本のにも表表を対し、その一般化であるディリッと質符定理を述べる。     ○ 本のに表表を理解を対し、その一般化であるディリッと質符定理を述べる。     ○ 本のに表表を理解を対し、その一般化であるディリッと質符定理を述べる。     ○ 本のによる利用して公開鍵暗号(RSA 暗号)を実現する。     ○ 合同概念の取り扱いに慣れる。     ○ 合同概念の取り扱いに慣れる。     ○ 合同概念の取り扱いに慣れる。     ○ 合同概念の取り扱いに関れる。     ○ 合同概念の取り扱いに関れる。     ○ 合同表を利用して公開鍵暗号(RSA 暗号)を実現する。     ○ フェルマーの最終定理について観説する。     ○ 信託的の解答と解説    ○ 「議稿」に辿り着くまで、また講義の概書は英語もしくは日本語。    ジョセフ・リ・ン・グェン・オーカン・ガーンを表、第本が第、訳 「信はしいて知道、「総合達成度】     ○ 本のに関連を対していると、または、対しのに講義の際必ず提出すること。事前に数料書を読んでくること     □ 本のに対しに対していて別まま、新潮文庫     □ 学上の注意    ○ 定田原(1) ~ (4) について別まま、映画のに、、、次回の講義の際必ず提出すること。事前に数料書を読んでくること。    ② 定田原(1) ~ (4) について別まま、映画のに、は合き評価・カースに、との書が、のに、との書価のに、原とする場合に、ないよりによれ、表別とで合格)次の場合は再述験の受験資格はないものとする。    ② は合評価】	□		受 業 項 目	内 容	理解度の自己点検
高次化を考える。	1	数論と	は何ものでしょう?	○数論における諸問題を具体的に紹介する.	【理解の度合い】
高次化を考える。	2	べき乗	和	   ○ピタゴラスの定理を幾何的に分析し、その	
式に応用する。		2710			
5 余りを調べる一合同式	3, 4	一次方程式と最大公約数			
(	5	   余りを調べる-合同式			
1					
8 オイラー関数と中国の剰余定理 9 数の原子ー素数 ○中国式剰余定理(孫子の定理)を理解する。 ○素数が無数に存在することを証明し、その一般化であるディリクレ算術定理を述べる。 ○オイラーの完全数定理を証明する。 ○11,12 合同式のべき乗とべき乗根 ○合同概念の取り扱いに慣れる。 ○合同概念の取り扱いに慣れる。 ○合同概念の取り扱いに慣れる。 ○ 合同式を利用して公開鍵暗号(RSA 暗号)を実現する。 ○ フェルマーの最終定理について概説する。  「試験の点数」点 後期期末試験の解答と解説 「結論」に辿り着くまでの「過程」を重視するので、課題レポートは十分な説明書きがなければ不可とする。また講義の板書は英語もしくは日本語。 ジョセフ Ⅱ、シルヴァーマン 著、鈴木治郎 訳 「はじめての数論 原著第3版一発見と証明の大航海ーピタゴラスの定理から相回線まで」、ピアソンエデュケーション。(ISBN: 978-4894714922) 参 考 図 書 サイモン シン 著、青木薫 訳、「フェルマーの最終定理」、新潮文庫、サイモン シン 著、青木薫 訳、「フェルマーの最終定理」、新潮文庫・サイモン シン 著、青木薫 訳、「アェルマーの最終定理」、新潮文庫・サイモン シン 著、青木薫 訳、「アェルマーの最終定理」、新潮文庫・サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫・サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫・サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫・サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫・サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫・「金融」、「金融」、「金融」、「金融」、「金融」、「金融」、「金融」、「金融」、	6, 7	フェルマー・オイフーの定埋		7,2 == 2 ,21,2 11,2	
一般化であるディリクレ算術定理を述べる。	8	オイラー関数と中国の剰余定理		• 1	
10	9	数の原子-素数		   ○素数が無数に存在することを証明し,その	
11, 12   合同式のべき乗とべき乗根					
13 解読不能な暗号	10	メルセンヌ神父の素数と完全数		○オイラーの完全数定理を証明する. 	
#	11, 12	合同式のべき乗とべき乗根		○合同概念の取り扱いに慣れる.	
14 楕円曲線とフェルマーの最終定理 ○フェルマーの最終定理について概説する.  15 後期期末試験 ○ 【試験の点数】 点 後期期末試験の解答と解説 「結論」に辿り着くまでの「過程」を重視するので、課題レポートは十分 な説明書きがなければ不可とする.また講義の板書は英語もしくは日本語. ジョセフ H. シルヴァーマン 著、鈴木治郎 訳 「はじめての数論 原著第3版一発見と証明の大航海ーピタゴラスの定理 から楕円曲線まで」、ピアソンエデュケーション. (ISBN: 978-4894714922)  参 考 図 書 サイモン シン 著、青木薫 訳、「フェルマーの最終定理」、新潮文庫. サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫. 毎回レポートを課すので、十分に時間をかけ、次回の講義の際必ず提出すること. 事前に教科書を読んでくること. 関連 科 目 応用数学 I、応用数学 II、数学演習 達成目標(1)~(4)について期末試験と課題で評価する. 総合評価 毎回東末試験 60%+課題 40% (総合評価 60 点以上で合格) 次の場合は再試験の受験資格はないものとする. 【総合評価】 点	13	解読不能な暗号		○合同式を利用して公開鍵暗号 (RSA 暗号)	
後期期末試験	1.4			2,7,52,7 0:	
後期期末試験の解答と解説	14	精円曲線とフェルマーの最終定理		〇ノエルマーの取於足壁について慨説する。	
<ul> <li>履修上の注意 「結論」に辿り着くまでの「過程」を重視するので、課題レポートは十分な説明書きがなければ不可とする.また講義の板書は英語もしくは日本語. ジョセフ H. シルヴァーマン 著、鈴木治郎 訳 「はじめての数論 原著第 3 版 − 発見と証明の大航海 − ピタゴラスの定理から楕円曲線まで」、ピアソンエデュケーション. (ISBN: 978-4894714922)</li> <li>参 考 図 書 サイモン シン 著、青木薫 訳、「フェルマーの最終定理」、新潮文庫.サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫.</li> <li>自学上の注意 毎回レポートを課すので、十分に時間をかけ、次回の講義の際必ず提出すること.事前に教科書を読んでくること.</li> <li>関 連 科 目 応用数学 I、応用数学 II、数学演習 達成目標(1)~(4)について期末試験と課題で評価する. 総合評価=期末試験 60%+課題 40% (総合評価 60 点以上で合格)次の場合は再試験の受験資格はないものとする.</li> <li>【総合評価】点</li> </ul>	15				【試験の点数】  点
な説明書きがなければ不可とする.また講義の板書は英語もしくは日本語. ジョセフ H. シルヴァーマン 著, 鈴木治郎 訳 「はじめての数論 原著第3版一発見と証明の大航海ーピタゴラスの定理から楕円曲線まで」, ピアソンエデュケーション. (ISBN: 978-4894714922)  参 考 図 書 サイモン シン 著, 青木薫 訳, 「フェルマーの最終定理」, 新潮文庫. サイモン シン 著, 青木薫 訳, 「暗号解読」, 新潮文庫.  自学上の注意 毎回レポートを課すので, 十分に時間をかけ, 次回の講義の際必ず提出すること. 事前に教科書を読んでくること. 関 連 科 目 応用数学 II, 数学演習 達成目標(1)~(4)について期末試験と課題で評価する. 総合評価=期末試験60%+課題40%(総合評価60点以上で合格)次の場合は再試験の受験資格はないものとする.  [総合評価]	= 4-1	「純粋」に辿り差くまでの「過程」を重視するので、理題レポートは十			
<ul> <li>教 科 書 「はじめての数論 原著第3版-発見と証明の大航海-ピタゴラスの定理から楕円曲線まで」,ピアソンエデュケーション.(ISBN: 978-4894714922)</li> <li>参 考 図 書 サイモン シン 著,青木薫 訳,「フェルマーの最終定理」,新潮文庫.サイモン シン 著,青木薫 訳,「暗号解読」,新潮文庫.</li> <li>自学上の注意 毎回レポートを課すので,十分に時間をかけ,次回の講義の際必ず提出すること.事前に教科書を読んでくること.</li> <li>関 連 科 目 応用数学 I,応用数学 II,数学演習 達成目標(1)~(4)について期末試験と課題で評価する.総合評価=期末試験60%+課題40%(総合評価60点以上で合格)次の場合は再試験の受験資格はないものとする. 【総合評価】</li> </ul>	腹修上の注意   な説明書きがなければ不可		な説明書きがなければ不可	とする.また講義の板書は英語もしくは日本語.	【総合達成度】
<ul> <li>教 科 書 から楕円曲線まで」,ピアソンエデュケーション. (ISBN: 978-4894714922)</li> <li>参 考 図 書 サイモン シン 著,青木薫 訳,「フェルマーの最終定理」,新潮文庫.サイモン シン 著,青木薫 訳,「暗号解読」,新潮文庫.</li> <li>自学上の注意 毎回レポートを課すので,十分に時間をかけ,次回の講義の際必ず提出すること.事前に教科書を読んでくること.</li> <li>関 連 科 目 応用数学 I,応用数学 II,数学演習 達成目標(1)~(4)について期末試験と課題で評価する.総合評価=期末試験 60%+課題 40%(総合評価 60 点以上で合格)次の場合は再試験の受験資格はないものとする. 【総合評価】</li> </ul>	I			***	
(ISBN: 978-4894714922)  参 考 図 書 サイモン シン 著、青木薫 訳、「フェルマーの最終定理」、新潮文庫・サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫・サイモン シン 著、青木薫 訳、「暗号解読」、新潮文庫・ 自学上の注意 毎回レポートを課すので、十分に時間をかけ、次回の講義の際必ず提出すること・事前に教科書を読んでくること・ 関 連 科 目 応用数学 I、応用数学 II、数学演習 達成目標(1)~(4)について期末試験と課題で評価する・総合評価=期末試験 60%+課題 40%(総合評価 60 点以上で合格)次の場合は再試験の受験資格はないものとする・ 【総合評価】	教科	書			
** *** *** *** *** *** *** *** *** ***					
1	参考				
関連科目       応用数学Ⅰ,応用数学Ⅱ,数学演習         達成目標(1)~(4)について期末試験と課題で評価する.         総合評価=期末試験 60%+課題 40%(総合評価 60 点以上で合格)         次の場合は再試験の受験資格はないものとする.    【総合評価】	1 日 字 E /// 江 音 l				
総合評価       達成目標(1)~(4)について期末試験と課題で評価する.         総合評価=期末試験 60%+課題 40%(総合評価 60 点以上で合格)         次の場合は再試験の受験資格はないものとする.       【総合評価】					
総合評価=期末試験 60%+課題 40%(総合評価 60 点以上で合格)         次の場合は再試験の受験資格はないものとする.       【総合評価】	第				
次の場合は再試験の受験質格はないものとする.   【総合評価】 点	<b>₩</b> Δ	=π / <del>π</del>	総合延価=期末試験 60%+課題 40% (総合延価 60 占以上で会校)		
総合評価が 50 点未満の場合,または,未提出レボートがある場合.	松 百	計 1四	2		【総合評価】 点
			総合評価が 50 点未満の場合	, または, 未提出レボートがある場合.	