豊田工業高等専門学校	開講年度	平成31年度 (2019年度)	授業科目	初等代数

科目基礎情報

科目番号	91021	科目区分	一般 / 選択
授業形態	講義	単位の種別と単位数	学修単位: 2
開設学科	情報科学専攻	対象学年	専2
開設期	前期	週時間数	2
教科書/教材	特に指定しない		
担当教員	米澤 佳己		

到達目標

(ア)数学的な基本的記号の意味を理解できる。簡単な証明ができる。
(イ)最大公約数, 最小公倍数一次合同式に関する基本的な計算ができる。
(ウ)オイラーの定理、RSA 暗号の仕組みを理解し、簡単な例の計算が行える。

ルーブリック

	理想的な到達レベルの目安	標準的な到達レベルの目安	未到達レベルの目安
評価項目(ア)	数学的な基本的記号の意味を理解でき、簡単な証明をすることができる。	数学的な基本的記号の意味を理解できる。	数学的な基本的記号の意味を理解できない。
評価項目(イ)	最大公約数, 最小公倍数、１次合同式、不定方程式を理解でき、簡単な計算をすることができる。	最大公約数, 最小公倍数、１次合同式、不定方程式を理解できる。	最大公約数, 最小公倍数、１次合同式、不定方程式を理解できない。
評価項目(ウ)	オイラーの定理、RSA 暗号の仕組みを理解し、簡単な例の計算が行える。	オイラーの定理、RSA 暗号の仕組みを理解できる。	オイラーの定理、RSA 暗号の仕組みを理解できない。

学科の到達目標項目との関係

学習・教育到達度目標 A4 現実の問題や未知の問題に対して，問題の本質を数理的に捉え，コンピュータシステムを応用した問題解決方法を多角的視野から検討することができる.
JABEE c 数学及び自然科学に関する知識とそれらを応用する能力
本校教育目標 ② 基礎学力

教育方法等

概要	この講義では自然数及び整数の性質について考察する。整数には最大公約数、最小公倍数などの実数には無い概念を導入することにより様々な応用が与えられる。中でも現在では計算機によるネットワークの利用における暗号の取り扱いにおいて整数の性質が重要な論理的基礎をになっている。本講義においては、整数の性質を基本から解説し、その応用として現在の暗号の理論の初歩を述べる。
授業の進め方・方法	
注意点	授業内容に関連する課題を毎回出題するので、必ず提出すること。

選択必修の種別・旧カリ科目名

授業計画

		週	授業内容	週ごとの到達目標
前期	1stQ	1週	数学の基本的記号の使い方と基本的性質	数学の基本的記号の使い方と基本的性質を理解する。
		2週	数学的帰納法の復習	簡単な数学的帰納法の証明をすることができる。
		3週	背理法による証明法	背理法を用いた簡単な証明をすることができる。
		4週	整数に関する基本的定義と基本的性質	整数に関する基本的定義と基本的性質を理解する。
		5週	ユークリッドの互除法とその応用	ユークリッドの互除法を理解し、とその応用を計算できる。
		6週	最大公約数・最小公倍数に関する性質	最大公約数・最小公倍数に関する性質を理解する。
		7週	素因数分解の可能性と一意性	素因数分解の可能性と一意性を理解する。
		8週	一次合同式の定義と基本的性質	一次合同式の定義と基本的性質を理解する。
	2ndQ	9週	合同方程式, 不定方程式	簡単な合同方程式, 不定方程式の性質を理解し、解くことができる。
		10週	剰余に関する定理	剰余に関する定理を理解する。
		11週	オイラー関数の定義	オイラー関数の定義を理解し、基本的な性質を利用できる。
		12週	オイラーの定理, フェルマーの定理	オイラーの定理, フェルマーの定理を理解する。
		13週	公開鍵暗号の仕組み	公開鍵暗号の仕組みを理解する。
		14週	公開鍵暗号の例としての RSA暗号	公開鍵暗号の例としての RSA暗号を理解する。
		15週	電子署名の仕組みとRSA暗号におけるその実現法	電子署名の仕組みとRSA暗号におけるその実現法を理解する。
		16週		

モデルコアカリキュラムの学習内容と到達目標

分類	分野	学習内容	学習内容の到達目標	到達レベル	授業週

評価割合

	定期試験	課題	合計
総合評価割合	50	50	100
分野横断的能力	50	50	100