平成１８年度　千葉大学理学部公開講座

「IT 社会を支える現代数学」

－符号・暗号の世界－

平成１８年１１月２５日（土）

１２月　２日（土）

千葉大学理学部２号館

主　催　　**千葉大学理学部**

後　援　　**千葉市教育委員会**

「ＩＴ 社会を支える現代数学」
－符号・暗号の世界－

１．講座の趣旨

千葉大学理学部では、「IT 社会を支える現代数学－符号・暗号の世界－」と題した公開講座を開催します。主に高校生ならびに一般の方を対象にした講義です。

符号・暗号技術は、IT 社会が成立するのに必須の技術と言われ、その基盤として現代数学が大きな役割を果たしています。

本公開講座は、ガロア理論入門から始まり、群論、整数論、有限体論、代数幾何、楕円曲線論、関数解析等々の数学が、誤り訂正符号、配置問題、擬似乱数列、公開鍵暗号、デジタル署名、量子暗号、量子コンピュータ等々の情報科学の基礎として如何に関わっているか、数学的厳密性はある程度抜きにしても概観できるように易しく解説し、現代における数学の重要性および楽しさを伝えようとするものです。

２．日程・講義題目等

期　日	時　間	講　義　題　目	講　師
11 月 25 日（土）	9:30～10:00	受付	
	10:00～10:05	開講の挨拶	理学部長 廣井美邦
	10:05～10:25	「公開講座『IT 社会を支える現代数学』開催の趣旨」	理学部 教授 中村勝洋
	10:30～12:00	「ガロア理論入門－群と構造－現代数学事始」	理学部 教授 野澤宗平
	12:00～13:00	昼休み	
	13:00～14:30	「配置問題、符号デザインと群論」	理学部 教授 北詰正顕
	14:30～16:00	「誤り訂正符号、擬似乱数列と有限体」	理学部 教授 中村勝洋
	16:00～17:30	「誤り訂正符号、線形符号と代数幾何学」	理学部 助教授 杉山健一
12 月 2 日（土）	10:30～12:00	「公開鍵暗号、デジタル署名と整数論」	総合メディア基盤センター 助教授 多田充
	12:00～13:00	昼休み	
	13:00～14:30	「暗号と楕円曲線論」	理学部 助教授 松田茂樹
	14:30～16:00	「量子暗号、量子コンピュータと関数解析」	理学部 教授 渚勝
	16:00～	閉講の挨拶 修了証書授与	理学部 教授 種村秀紀

３．受講対象者　　一般および高校生

４．募 集 人 員　　５０名

５．受　講　料　　無　料

６．受 付 期 間　　平成１８年　９月２５日（月）～１１月１０日（金）
ただし、定員になり次第締め切らせていただきます。

７．申 込 方 法　　“**千葉大学理学部公開講座受講希望**”と記し、氏名（ふりがな）・年齢・性別・職業または学年・連絡先（住所・電話番号）を明記のうえ、以下【申込先】へお送りください。

【申　込　先】

はがきの場合（往復はがきにてお申し込みください）
〒263-8522　千葉市稲毛区弥生町 1-33
千葉大学理学部学務係　宛

FAX 場合　　FAX 番号:　　043-290-2874
千葉大学理学部学務係　宛

電子メールの場合　E-mail アドレス: iad2880@office.chiba-u.jp

※申込みの際に記載いただいた個人情報は本公開講座業務以外には使用しません。

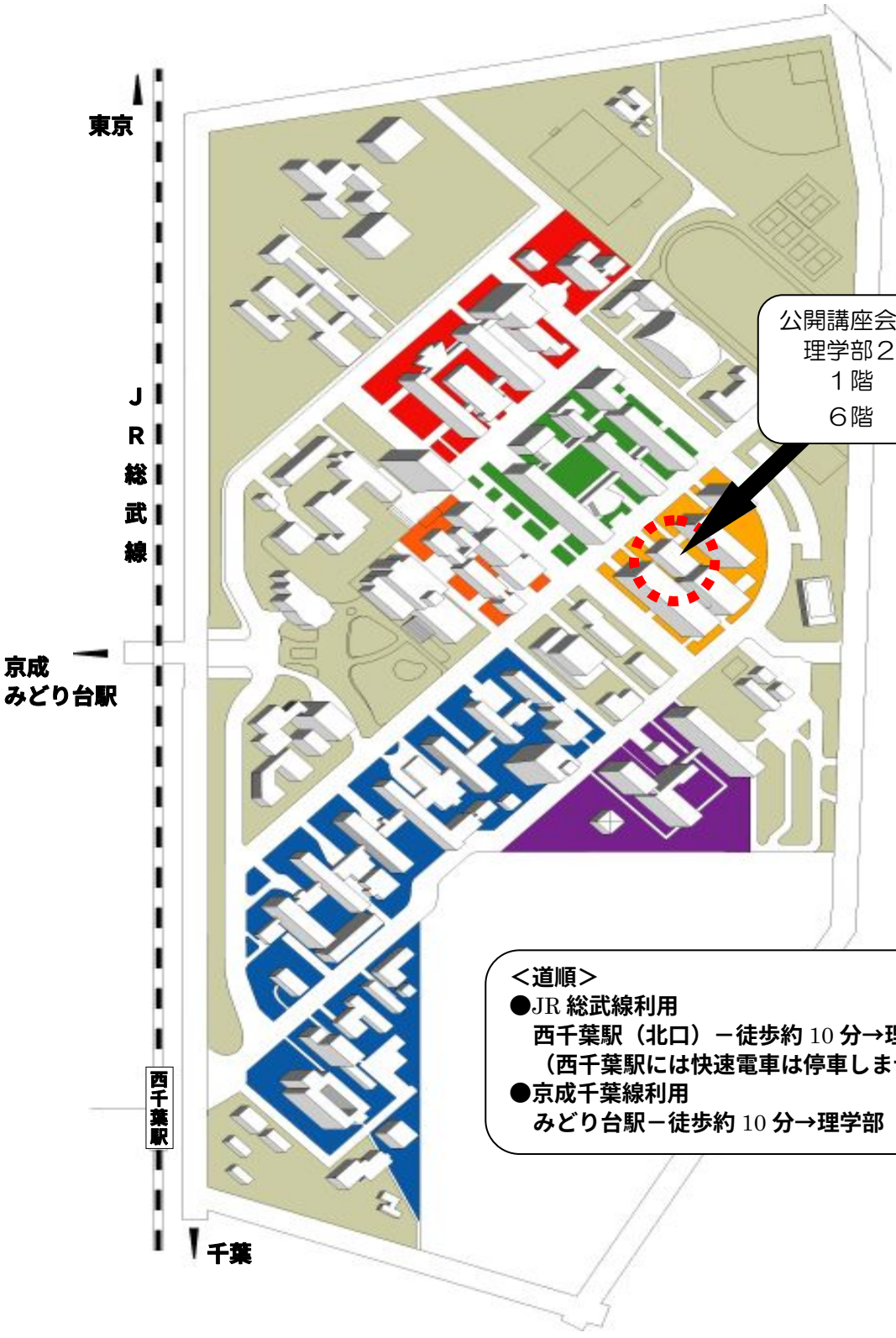
８．決 定 通 知　　申込順により受講者を決定し、「受講決定通知」等を送付します。
募集人員を超えたため受講できない方についてもその旨通知します。

９．修 了 証 書　　２日間全てを受講すると、修了証書が交付されます。

１０．そ　の　他　　お車での来学はご遠慮願います。

問い合わせ先
千葉大学理学部学務係
〒263-8522　千葉市稲毛区弥生町 1-33
TEL:　043-290-2881
FAX:　043-290-2874
E-mail:　iad2880@office.chiba-u.jp

会　場　案　内　図



※お車での来学はご遠慮願います

平成１８年度　千葉大学理学部公開講座
「IT 社会を支える現代数学」－符号・暗号の世界－
要　　旨

１日目　平成１８年１１月２５日（土）

１．「公開講座『IT 社会を支える現代数学』開催の趣旨」　　中　村　勝　洋　　教　授

本公開講座の開講にあたって、その開催趣旨・目的について簡単な紹介を行います。

２．「ガロア理論入門－群と構造－現代数学事始」　　野　澤　宗　平　　教　授

符号・暗号系を代数的に記述するためには、群・環・体といった代数の基本概念が不可欠です。ここでは、作図問題と高次方程式の解法という２つの主題から発展したガロア理論を解説し、群と体の間の１対１対応を与えるガロアの基本定理を通して、群と有限体について学ぶことで、符号・暗号理論への序論とします。

３．「配置問題、符号デザインと群論」　　北　詰　正　顕　　教　授

符号は、情報通信の理論のみならず、数学の諸分野でも大きな役割を果たしています。ここでは、群論・組合せ論・実験計画法（デザインの理論）における符号の役割について、実例を中心に解説します。

４．「誤り訂正符号、擬似乱数列と有限体」　　中　村　勝　洋　　教　授

有限個の要素からなる集合でそこに加減乗除が定義されている集合、つまり有限体は、デジタル情報通信技術を捕らえる上で重要です。中でも、誤り訂正符号技術は、信頼性の高い情報通信を行うために必要不可欠な技術であり、衛星通信、地上通信、あるいは CD を始めとする各種記憶媒体で活用されてきています。そこで使われている符号の大部分は、数学的には、有限体の要素からなるベクトル空間の、所定の距離構造を満たした線形部分空間として構成されています。この研究領域は、有限体自身の持つ美しい性質から、研究者にとっては大変楽しい、数学と技術のはざ間にある領域でもあり、いつまでも追いかけたくなる領域でもあります。また擬似乱数列も情報通信機器の設計において、また計算機シミュレーション等において広く使われており、有限体や符号との関連も深いものがあります。本講演ではこれらの一端を分かりやすくお伝えできれと考えています。

５．「誤り訂正符号、線形符号と代数幾何学」　　杉　山　健　一　　助教授

この講演では、有限体上定義された代数曲線を用いて線型符号を構成する方法について解説します。まず、代数曲線の基本的な概念を説明し、そこに現れる様々な定理や公式を、有理曲線や楕円曲線などの具体的な曲線で確認します。次に、代数曲線を用いて線型符号を構成する一般的な方法を説明した後、その方法を具体的な曲線に対して適用して実際に線型符号を構成し、その性質を調べます。また、時間が許すのであれば、代数曲線の有理点の個数を上から評価する、いわゆる Weil bound についても言及したいと思います。これらの事柄を説明するにあたり、抽象的な表現はなるべく避けて、具体的に話を進める予定です。

平成１８年度　千葉大学理学部公開講座
「IT 社会を支える現代数学」－符号・暗号の世界－
要　　旨

２日目　平成１８年１２月　２日（土）

１．「公開鍵暗号、デジタル署名と整数論」　　多　田　　充　　助教授

19 世紀を代表する大数学者ガウスは、整数論のことを「数学の女王」と呼びました。最も高貴で最も美しい理論であると同時に他の分野の成果を利用するが、整数論の成果は他の分野では利用されない（女王は家来を使うが自分は使われない）のが理由であろうと言われていました。しかし、その整数論も 1977 年ディフィーとヘルマンによって公開鍵暗号の概念が提唱されると、その状況は一変しました。公開鍵暗号系は、整数論の応用であり、それにより、インターネットのような公開ネットワーク上でも安全に情報のやりとりを行うことができるようになりました。このように、公開鍵暗号系は安全で健全なＩＴ社会のために不可欠な要素となっています。

本講演では、公開鍵暗号およびその応用であるデジタル署名の概念、その具体例としてＲＳＡ暗号系の概略について述べます。

２．「暗号と楕円曲線論」　　松　田　茂　樹　　助教授

ガロア理論が生まれた時代、楕円関数論も大きな発展を遂げました。楕円の弧長を求める逆関数を楕円関数と呼びます。5 次以上の代数方程式が必ずしも代数的に解けないことを初めて厳密に証明し、ガロア理論にも大きな影響を与えたアーベル、その良きライバルであったヤコビは、楕円関数を複素関数とみなすと 2 重周期を持つ有理型関数であることを発見しました。これは、楕円関数が 1 次元複素トーラスと呼ばれる群構造を持ったリーマン面の上の関数であることを意味します。更に楕円関数を用いることで、1 次元複素トーラスが $y^2=4x^3-ax-b$ という 3 次方程式の解に無限遠点を加えてできる代数曲線と同一視できます。

このように $y^2=4x^3-ax-b$ の解全体に無限遠点を加えた形をした曲線を楕円曲線と呼びます。複素トーラスと同一視できることからこの曲線にはアーベル群の構造が入りますが、この構造は代数的であり、係数体を複素数体ではなく有限体で取り換えてもやはり群構造を持つことがわかります。本講演では、この群構造を持つ有限体上の代数曲線が現代の公開鍵暗号にどのように応用されているのかについて解説します。

３．「量子暗号、量子コンピュータと関数解析学」　　渚　　勝　　教　授

量子力学は強力な道具ですが、その道を拓いたアインシュタインでさえ頭を悩ませた現象が起こります。EPR(E は Einstein)パラドックスと呼ばれる現象は、多くの論争を呼び起こしましたが､現在では量子縺れの状態として認められ､量子情報理論の興味ある理論のすべてにとってキーポイントとなっています。これらの議論はとてつもなく難しいことのように見えますが、量子力学の考え方を認めてしまうと、数学的にはベクトルとその内積によって記述することができます（高校でも出てくるベクトルの長さとその間の角度というものです。）。これによって高速通信ができることや、量子通信が自然に暗号の効果を持つことなどを解説します。