

# 数学は

# こんなに面白い！ 9

特別編

## 1月のテーマ Sageで行う楕円曲線の計算

整数論で扱う三次曲線の一つに、楕円曲線と呼ばれる曲線があります。

楕円曲線は面白い性質を持っていて、有理点の有無や加算などを利用して、暗号化などにも利用されています。ただ、楕円曲線に対する演算は複雑なのと、加算などでは有理数の桁数が急速に増大するので、手計算やパソコンを利用しても、一般の言語では計算結果を求めるのはちょっと困難な作業となります。

楕円曲線の演算を簡単に行うことができる言語として、フリーで利用可能なSage(SageMath)と呼ばれる言語があります。単純な計算ならばインターネット上で公開されている「SageMathCell」にアクセスすることで、ブラウザでの手軽な利用が可能となっています。

今回は、このプログラミング言語 Sage の利用方法とSageでの楕円曲線の演算方法を紹介します。

**1月 10日 (木) 午前10時～11時30分**

講師 / 小林 一章 東京女子大学名誉教授

ゲスト講師 / 濱中 由典 ハマフ(株)代表取締役

定員 / 30人 (先着制) 受講料 / 500円

会場 / 三鷹ネットワーク大学

お申し込み・お問い合わせ

三鷹ネットワーク大学推進機構

FAX 0422-40-0314 お問い合わせ 0422-40-0313

URL <http://www.mitaka-univ.org/>

申込開始 ▶ 12月4日(火) 午前9時30分～

〒181-0013 三鷹市下連雀3-24-3 三鷹駅前協同ビル3階

文化・教養	東京女子大学寄付講座 <b>数学はこんなに面白い！9 特別編</b> 1月のテーマ Sageで行う楕円曲線の計算	D185 5300
-------	----------------------------------------------------------------	--------------

講座趣旨	講座開催概要																		
<p>現代数学は抽象化が進み、一見どのように発生し、どのように使われるかが見えにくくなっていますが、実は生活の中や他の自然科学の中に、その源を持ち、思いもよらない応用を持っていたりします。それらの源を訪ね、どうして、その応用を持つに至ったかを明らかにしたいと思います。</p> <p>月1回ずつ、幅広くテーマを選んでお話ししていきます。出来るだけ予備知識を必要としないように、必要な知識は講座の中で説明していく予定です。</p> <p>数学が好きな方、数学で語り合う仲間を見つけたい方、久しぶりに勉強したい方、数学には興味があるけど難しそうだなと思う方、ぜひこの機会にお集まりください。2018年度も4月から毎月1回開催をしていきます。</p> <p>1月のテーマは「Sageで行う楕円曲線の計算」です。</p> <p>今回は趣向をかえて、ハマフ(株)代表取締役、濱中由典さんと小林一章先生のお二人で講義を行います。</p>	<table border="1"> <tr> <td>日 程</td> <td>平成31年1月10日 木曜日</td> </tr> <tr> <td>時 間</td> <td>午前10時～11時30分</td> </tr> <tr> <td>定 員</td> <td>30人(先着制)</td> </tr> <tr> <td>回 数</td> <td>全1回</td> </tr> <tr> <td>受講料</td> <td>500円</td> </tr> <tr> <td>教 材</td> <td>レジュメ資料 ほか</td> </tr> <tr> <td>難易度</td> <td>★★☆</td> </tr> <tr> <td>会 場</td> <td>三鷹ネットワーク大学</td> </tr> <tr> <td>申し込み</td> <td>ネット申込可 申込受付:12月4日(火) 午前9時30分～</td> </tr> </table>	日 程	平成31年1月10日 木曜日	時 間	午前10時～11時30分	定 員	30人(先着制)	回 数	全1回	受講料	500円	教 材	レジュメ資料 ほか	難易度	★★☆	会 場	三鷹ネットワーク大学	申し込み	ネット申込可 申込受付:12月4日(火) 午前9時30分～
	日 程	平成31年1月10日 木曜日																	
	時 間	午前10時～11時30分																	
	定 員	30人(先着制)																	
	回 数	全1回																	
	受講料	500円																	
	教 材	レジュメ資料 ほか																	
	難易度	★★☆																	
	会 場	三鷹ネットワーク大学																	
申し込み	ネット申込可 申込受付:12月4日(火) 午前9時30分～																		

Sageで行う楕円曲線の計算	
1月10日	<p>整数論で扱う三次曲線の一つに、楕円曲線と呼ばれる曲線があります。</p> <p>楕円曲線は面白い性質を持っていて、有理点の有無や加算などを利用して、暗号化などにも利用されています。ただ、楕円曲線に対する演算は複雑なものと、加算などでは有理数の桁数が急速に増大するので、手計算やパソコンを利用しても、一般の言語では計算結果を求めるのはちょっと困難な作業となります。</p> <p>楕円曲線の演算を簡単に行うことができる言語として、フリーで利用可能な Sage(SageMath)と呼ばれる言語があります。単純な計算ならばインターネット上で公開されている「SageMathCell」にアクセスすることで、ブラウザーでの手軽な利用が可能となっています。</p> <p>今回は、このプログラミング言語 Sage の利用方法と Sage での楕円曲線の演算方法を紹介したいと思います。</p>

講師紹介（敬称略）	
<p><b>小林 一章（こばやし かずあき） 東京女子大学名誉教授</b></p> <p>1940年東京生まれ。早稲田大学理工学研究科卒業。神戸大学、北海道大学を経て、84年から東京女子大学文理学部数理学科教授。2009年より同大学名誉教授。専門は位相幾何学で80年代後半より結び目の研究を始め、その後空間グラフの研究に重心を移す。著書に「曲面と結び目のトポロジー」（朝倉書店）、「空間グラフの理論」（培風館）など。（公財）数学オリンピック財団前理事長。</p>	
<p><b>濱中 由典（はまなか よしのり） ハマフ(株)代表取締役</b></p> <p>1956年生まれ広島県出身。愛媛大学理学部物理学科卒業。79年からコンピュータソフトウェア開発会社に勤務、87年特種情報処理技術者、01年 RIMS 認定プロジェクトマネージャー(PM)資格を取得。金融機関や商社などの業務システムや政府関係の電子システム開発に携わる。98年の中央省庁向け電子申請、電子入札システムの開発以降、Java をベースにした Web システム開発のプロジェクトに携わっている。2012年に会社を設立し現在に至る。</p>	

## 三鷹ネットワーク大学 受講者登録用紙

\*すでに受講者登録を済まされている方は必要ありません。インターネットでもご登録ができます。

※太枠内の項目は必須事項です。

登録日： 平成 年 月 日

<b>お名前</b>	フリガナ	<b>性別</b>	男・女	<b>生年月日</b>	西暦 年 月 日
<b>受講者区分</b> ※該当する番号を1つ選んで○をつけてください。	(1)【市民】三鷹市にお住まいの方(学生は除く) (2)【市民(在勤・在学)】三鷹市外にお住まいで、三鷹市内の職場・学校に通われている方 (3)【市民学生】三鷹市にお住まいの学生の方 (4)【会員】勤務先、学校等が三鷹ネットワーク大学の正会員または賛助会員の方 (5)【一般】三鷹市外にお住まいの方				

<b>Eメール</b>					
<b>緊急連絡先</b>	携帯電話番号：		携帯Eメール：		

《郵便物の送付先※振込用紙や受講証等のお送り先を、下記から選んでください。》

<b>郵便物送付先</b>	ご自宅	勤務先
---------------	-----	-----

《ご自宅》

<b>ご住所</b>	〒 —				
<b>電話番号</b>		F A X			

《勤務先・学校名等》

<b>勤務先名称</b>	※学生の場合は学校名と学部・学科名				
<b>勤務先部署名</b>	※学生の場合は学籍番号			<b>役職名</b>	
<b>ご住所</b>	〒 —				
<b>電話番号</b>		F A X			

《ご職業等》※職種・業種について該当するものにそれぞれ○をつけてください。

<b>勤務先業種</b>	①官公庁 ②団体 ③教育 ④宗教 ⑤医療 ⑥建設 ⑦金融・保険 ⑧製造 ⑨運輸・通信 ⑩農林水産 ⑪電気・水道 ⑫不動産 ⑬卸・小売 ⑭飲食 ⑮IT・ソフト ⑯その他
<b>職業(職種)</b>	①経営者 ②役員・管理職 ③一般事務 ④営業 ⑤販売・サービス ⑥生産管理 ⑦研究開発 ⑧専門職(医師・弁護士等) ⑨教職 ⑩自由業 ⑪専業主婦 ⑫無職 ⑬その他

《三鷹ネットワーク大学からの情報提供ご希望の有無》

<b>情報提供</b>	希望する	希望しない
-------------	------	-------

《興味をお持ちの分野》※3つまでお選びください。

1 経営・経済学	2 歴史学	3 法学	4 文学	5 工学	6 教育学	7 福祉・医療	8 介護・看護
9 コンピューターサイエンス	10 アジア・アフリカ系言語	11 総合政策	12 国際関係論	13 政治学	14 天文学	15 農学	16 臨床心理学
17 カウンセリング学	18 社会心理学	19 国際コミュニケーション学	20 スポーツ医学	21 マーケティング学	22 人間環境学	23 キャリアデザイン等	24 社会福祉学
25 情報科学	26 情報コミュニケーション学	27 グローバルビジネス学	28 宗教学	29 平和学	30 生物学	31 化学	32 数学
33 教養学	34 建築学	35 その他					

◆受講者登録について \*すでに受講者登録を済まされている方は必要ありません。

三鷹ネットワーク大学で受講される場合は、受講者登録の手続きが必要です。講座のお申し込みをする前に（講座のお申し込みと同時に）、必ず受講者登録を済ませてください。ご登録をしていただくことにより、今後お申し込みされる際に、ご住所等、個人情報を記入する手間がなくなります。またインターネットからのお申し込みも可能となります。

◆個人情報について

ご記入いただいたお客様の個人情報は、個人情報保護法に基づいて適切に管理するとともに、受講決定通知および講座のご案内目的のために使用します。

D53

東京女子大学寄付講座

[D1855300]

数学はこんなに面白い！9

1月のテーマ Sageで行う楕円曲線の計算

申込用紙

受講者 番号	E .... .... .... ....	申込日	平成	年	月	日
名前	フリガナ	電話番号				

※申込欄に○をご記入ください。

申込欄	講座日程・講座タイトル・講師・受講料	領収印
	平成31年1月10日 木曜日 午前10時～11時30分 東京女子大学寄付講座 数学はこんなに面白い！9 1月のテーマ Sageで行う楕円曲線の計算 講師：小林 一章 東京女子大学名誉教授 ゲスト講師：濱中 由典 ハマフ(株)代表取締役 受講料：500円	文化・教養

※ファックスでお送りいただく場合には、着信確認のためのお電話をお願いいたします。

電話：0422(40)0313 ファックス：0422(40)0314

[郵送での申込]〒181-0013 三鷹市下連雀3-24-3 三鷹駅前協同ビル3階 三鷹ネットワーク大学事務局

この講座をどこでお知りになりましたか？（該当するものに○を1つだけご記入ください）

- |                     |                |                      |
|---------------------|----------------|----------------------|
| 1. 三鷹ネットワーク大学ホームページ | 5. 学内ポスター・チラシ  | 9. その他（            ） |
| 2. ダイレクトメール         | 6. 講師・教職員よりの紹介 |                      |
| 3. 三鷹市広報            | 7. 友人・知人よりの紹介  |                      |
| 4. ポスター / チラシ       | 8. 新聞記事等       |                      |

## 【ご受講について】

## ●受講料のお支払いについて

受講予定者の方には、受講料のお支払い方法についてのご案内をお送りします。郵便振替、現金等、書類に記載されている方法で、お支払いいただきますようお願いいたします。受講予定者としてご通知した方からの受講料のお支払いを事務局が確認できた時点で、受講が確定します。期日までに受講料をお支払いいただけない場合には、お申し込みを取り消す場合がありますのでご注意ください。※お支払い方法は、講座によって異なる場合がありますので、詳しくはお送りする書類をご確認ください。

## ●受講のキャンセルについて

- 講座申し込み後にお客様の事情により受講をキャンセルする場合は、至急事務局まで電話でご連絡ください。
- 一度申し込んだ講座を別の講座に変更することはできません。申し込み済みの講座のキャンセルをしてから、再度希望の講座にお申し込みください。ただし、講座申込期間内のみ受け付けます。
- 受講料入金後のキャンセルについて

## 1. 講座前日（連続講座の場合は第一回講座前日）までに申し出があった場合

キャンセルの申し出があった日から2週間以内に事務局まで受け取りに来ていただければ、全額返金します。なお、2週間を過ぎても受け取りに来ていただけなかった場合は500円の手数料を差し引いた残額を郵便小為替で送付します。この場合、受講料500円以下の講座については返金はいたしません。

## 2. 講座当日（連続講座の場合は第一回講座当日）、講座開始時刻前に申し出があった場合

講座当日（連続講座の場合は第一回講座当日）から2週間以内に事務局まで受け取りに来ていただければ、500円の手数料を差し引いた残額を返金します。なお、2週間を過ぎても受け取りに来ていただけなかった場合は500円の手数料を差し引いた残額を郵便小為替で送付します。この場合、受講料500円以下の講座については返金はいたしません。

## 3. 1, 2以外のキャンセルの場合

受講料の返金はいたしません。

## ●受講資格について

受講は原則としてお申し込みされた本人のみとさせていただきます。受講資格を他の人に譲渡することはできません。