女子中高生夏の学校 2017
ポスターセッション 「暗号と数学」

愛知工業大学基礎教育センター
大島　和幸

1　はじめに

2017 年 8 月 5 日から 7 日まで埼玉県比企郡嵐山町にある国立女性教育会館において「女子中高生夏の学校 2017 〜科学・技術・人との出会い〜」が開催されました.

この夏の学校では，女子中高生に理系の進路にはいろいろな選択肢があることを知ってもらうため，2 日目にサイエンスアドベンチャー I ・ II というプログラムが組まれています．午前中のサイエンスアドベンチャー I では「ミニ科学者になろう」というテーマで，理系のいろいろな分野の実験・実習を体験してもらいます．日本数学会からは「組みひもの数学で遊んで占おう」というタイトルで出展がありました．組みひもで占う？と不思議に思われた方は，是非，船越紫先生のご報告をご覧ください.

午後のサイエンスアドベンチャー II では「研究者・技術者と話そう」というテーマで，いろいろな学会・団体が出展するポスターを自由に見て回ります．日本数学会からは「暗号と数学」というタイトルで出展しました．この稿ではそのポスターの内容をご報告いたします.

2 節にポスターの内容を再現しました．3 節はポスターの中の問題の答えや定理の証明ですが，当日はポスターをプリントしたものを希望者に手渡しました.

2　ポスター「暗号と数学」

暗号と言うとスパイ映画のような怪しい響きがありますが，私たちの日常生活にも活用されています．例えば，インターネットで買い物をするときなど，クレジットカード番号やパスワードなど大切な情報を第三者に知られないように暗号化して送る必要があります．でも，スパイ同士ならあらかじめ暗号化の仕方を打ち合わせして通信しあえばよいのですが，あらかじめ打ち合わせできないお店や人と暗号で通信するにはどうすればいいのでしょうか？ このようなとき，現在広く使われているものとして **公開鍵暗号** があります．この暗号の仕組みをご紹介しましょう.

まず，インターネットで情報をやり取りするときは，情報を全て数字にしてやり取りをします．したがって，以下に「メッセージ M」とありますが，M は文字列ではなく数字であることを注意しておきます.

まずは，そもそも…

Question

公開鍵暗号って何？

Answer

公開鍵暗号は，その名の通りメッセージを受け取る側が暗号化する鍵と手順を公開している暗号です．具体的に言うと「2つの自然数 e と n が暗号化の鍵です．メッセージ M を e 乗して n で割った余り C を暗号文として送ってください」というように暗号化の鍵と手順を公開しています．

そこで，疑問に思うことは次のことかと思います．

Question

暗号文 C を他人に知られても大丈夫なの？

Answer

暗号文 C を第三者が傍受したとしても，分かっている e, n, C から元のメッセージ M を復元するのは容易ではありません．

分かっている e, n, C から元のメッセージ M を復元するには $M^e = nQ + C$ （Q は商）という方程式を解いて M を求めなければいけませんが，例えば次の問題を考えてみてください．

問題

ある数を 35 乗して 221 で割った余りが 70 です．ある数を求めてください．

これを解くにはある数を x とおいて $x^{35} = 221Q + 70$ （Q は商）という方程式を解くことになります．なかなか難しいことが分かるかと思います[1]．

そうなると，次に疑問なのは…

Question

暗号文 C を受け取った相手はどうやって元のメッセージ M を復元しているの？

Answer

実はメッセージを受け取る側は復元するための秘密の鍵 d を持っています．この d を使うと C^d を n で割ったものが元のメッセージ M になります．

[1]実は，この問題の答えは 8 なので，1 から順に調べていけばすぐに答えが求まってしまうのですが，実際には，総当たりの計算では計算しきれないような，大きな空間を用います．

以下，ここのところの仕組みを少し詳しく説明します．実は，**メッセージを受け取る側は公開する鍵 e，n と同時に秘密の鍵 d を作っておいているのです．**したがって e と n は何でもいいわけではなく，次のように巧妙に選ばれています．まず

$$n \text{ は } 2 \text{ つの大きな素数 } p, q \text{ の積 } n = pq$$

とします．そして，

$$\varphi(n) = n \text{ 以下の自然数で } n \text{ と互いに素なものの個数}$$

というものを考え（これを **オイラー関数** と言います），

$$e \text{ は } \varphi(n) \text{ と互いに素な自然数}$$

と選びます．さらに，復元のための秘密の鍵 d を

$$d \text{ は } ed \text{ を } \varphi(n) \text{ で割った余りが } 1 \text{ となるような自然数}$$

と選んでおきます．そこで，大切なのは次の定理です．

オイラーの定理
M, n が互いに素な自然数なら，$M^{\varphi(n)}$ を n で割った余りは 1.

さて，$M^e = nQ + C$ から $C = M^e - nQ$ です．e や d を以上のように選んでおきますと，$C^d = (M^e - nQ)^d$ は

$$\begin{aligned} C^d &= (M^e - nQ)^d \\ &\quad \text{（二項展開します．展開の 2 項目以降は全部 } n \text{ がかかるのでくくります.）} \\ &= M^{ed} + n \times (\text{自然数}) \\ &\quad (ed \text{ は } \varphi(n) \text{ で割って 1 余る数です．そのときの商を } q \text{ とおきます.）} \\ &= M^{1+q\varphi(n)} + n \times (\text{自然数}) \\ &= M \cdot (M^{\varphi(n)})^q + n \times (\text{自然数}) \end{aligned}$$

と変形できますが， オイラーの定理から $M^{\varphi(n)}$ を n で割った余りは 1 でしたから [2]，C^d を n で割った余りを計算すれば，めでたく元のメッセージ M が得られます！

最後に心配なのは…

[2]オイラーの定理を使うためには M と n が互いに素という条件が必要ですが，n が十分大きい素数 2 つの積である場合には M と n が共通因数をもつ確率はほとんどないと考えられます.

Question

他人が秘密の鍵 d を求めることはできないの？

Answer

秘密の鍵 d はその作り方からまず $\varphi(n)$ を求めなければならず，$\varphi(n)$ を求めるには n を因数分解する必要があります．n がすごく大きいとき，この因数分解がとても難しいので，第三者が d を求めることは難しいと考えられています．

以上の話をまとめると次のようになります．

まとめ

公開鍵暗号はメッセージを受け取る側が暗号化するための鍵と手順を公開している暗号です．
公開された鍵 e, n と暗号文 C から元のメッセージ M を復元することは $M^e = n$ Q $+ C$ と言う M と Q が未知数の方程式を解くことになり難しく，復元のための秘密の鍵 d を求めることも大きな自然数 n を素因数分解しなければならないことから困難です．この難しさによって安全性が保証されている暗号です．

3 参考

3.1 問題の答え

先ほどの問題くらいなら $n = 221$ はすぐ因数分解できてしまいますので，秘密の鍵 d は次のように求められます．まず，

$$221 = 13 \times 17$$

です．すると $\varphi(221)$ は 13 とも 17 とも互いに素なものの個数ですから 1 から 221 までの自然数のうち，13 の倍数（17 個あります）と 17 の倍数（13 個あります）を除いた自然数の個数になります．221 は 13 の倍数でも 17 の倍数でもあることに注意して

$$\varphi(221) = 221 - (13 + 17) + 1 = 192$$

となります．そうすると，d は $ed = 35d$ を $\varphi(221) = 192$ で割った余りが 1 となるように選ぶのですから，

$$35d = 192k + 1$$

という不定方程式を解けばＯＫです．ユークリッドの互除法を用いて

$$192 = 35 \times 5 + 17$$

$$35 = 17 \times 2 + 1$$

より

$$1 = 35 - 17 \times 2 = 35 - (192 - 35 \times 5) \times 2 = 35 \times 11 + 192 \times (-2).$$

したがって,

$$35 \times 11 = 192 \times 2 + 1$$

となり $d = 11$ と求まります.

そうすると後は 70^{11} を 221 で割った余りを計算すればよく, ある数は 8 と分かります.

3.2 オイラーの定理の証明

n 以下で n と互いに素な自然数全体の集合を

$$\{x_1, x_2, \cdots, x_{\varphi(n)}\}$$

とおきます. この各要素を一斉に M 倍し, それらを n で割った余りとして得られる集合はもとの集合 $\{x_1, x_2, \cdots, x_{\varphi(n)}\}$ に等しくなります.

(実際, Mx_i を n で割った余りは, M も x_i も n と互いに素ですから, 再び x_1 から $x_{\varphi(n)}$ のどれかになります. また, もし $i \neq j$ で Mx_i と Mx_j の n で割った余りが等しくなってしまったとすると $M(x_i - x_j)$ は n で割り切れることになりますが, M と n は互いに素でしたので, $x_i - x_j$ が n で割り切れることになってしまいます. ということは $x_i = x_j$ でなければならなくなりおかしいですね. というわけで Mx_i を n で割った余りは x_1 から $x_{\varphi(n)}$ のどれかになって, 重なりがないわけですので, 集合として同じものになります.)

したがって, $x_1x_2\cdots x_{\varphi(n)}$ と $(Mx_1)(Mx_2)\cdots(Mx_{\varphi(n)})$ は n で割った余りが同じになりますから

$$(Mx_1)(Mx_2)\cdots(Mx_{\varphi(n)}) - x_1x_2\cdots x_{\varphi(n)} = (M^{\varphi(n)} - 1)x_1x_2\cdots x_{\varphi(n)}$$

は n で割り切れますが, $x_1x_2\cdots x_{\varphi(n)}$ は n で割り切れませんので, $M^{\varphi(n)} - 1$ が n で割り切れなければいけません. したがって, $M^{\varphi(n)}$ を n で割った余りは 1 になります. (証明終わり)

4 おわりに

インターネットショッピングのような日常の中にも, 秘かに数学が使われているということ知ってもらえたらと思い公開鍵暗号をテーマに選びました. 予想以上に興味を持ってもらえたようで, ポスター展示には生徒さんが絶え間なく訪れてくれるような状況でした. 内容については, やはり, オイラーの定理あたりは難しいと感じる生徒さんが多

かったようですが，うまく作られているんだなぁという感想はもってもらえたように思います．

ポスターを作るにあたって，柏原賢二先生（東京大学），清水理佳先生（群馬工業高等専門学校），大山口菜都美先生（秀明大学），船越紫先生（奈良女子大学），久野恵理香さん（東京工業大学）に大変お世話になりました．筆者はポスターの下書きだけして会場に持って行ったのですが，夏の学校１日目の夜に皆さんで，とてもカラフルで立体的なポスターに変えていただきました．その結果，生徒さんの目を惹く魅力的なものになったと思います[3]．発表の際にも，説明を補足する寸劇など，いろいろと協力をしていただきました．本当にありがとうございました．

また，夏の学校の期間中，日本数式処理学会から参加されていた照井章先生（筑波大学）と藤村雅代先生（防衛大学）にはキャリア相談などでご一緒させていただき大変お世話になりました．ありがとうございます．

柏原先生や藤村先生には，この稿に関してさまざまな誤りをご指摘いただきました．ありがとうございました．

最後になりましたが，このような報告を書く機会を与えていただいた「数学通信」編集部，並びに男女共同参画社会推進委員会委員長の杉山由恵先生（九州大学），担当理事の清水扇丈先生（京都大学）に厚く御礼申し上げます．

参考文献

[1] 「暗号の整数論」　金子昌信・堺隆一　共著　講談社サイエンティフィック

[2] 「暗号解読　上・下」　サイモン・シン（青木薫訳）　新潮文庫

[3]夜にロビーでワイワイガヤガヤとポスターに飾りつけをしている集団も目を惹いたと思いますが….