2015.6.27

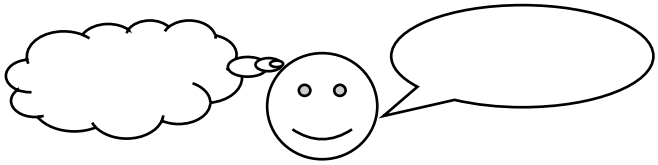
岐阜大学公開講座

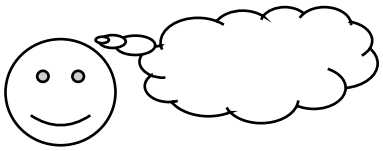
視る・考える・創る「数と形」の教室―キミは数学イノベーター！―

暗号の数学

岐阜高等学校　栗田 和輝

１．暗号とは何だろう？？





２．数あてマジック

★数あてマジックの仕組みを解き明かそう。

★数あてマジックを考えて、みんなをアッと言わせよう。

※「相手への指示」と、「数の変換」の仕組みは違うものにできるとベスト！！

３．コンピュータの世界で使われている暗号

★１～９を何度もかけ算して、１の位の数字を調べてみよう。

□×□　　□×□×□

数字	１回	２回	３回	４回	５回	６回	７回	８回	９回
１									
２									
３									
４									
５									
６									
７									
８									
９									

＜気づいたことをまとめよう＞

⇒上の規則から、数あてマジックの仕組みを考えよう

わたし「　　回かけ算して、１の位の数字を教えてください。」

相　手「　７　です　」

⇒わたし（　“7”を　　回かけ算し、１の位の数字を調べて）

「あなたの考えた数は　　ですね！」

拍手～♪

★レベルアップ１～20 を何度もかけ算して、21 で割った余りを調べてみよう。

□×□　　□×□×□

数字	１回	２回	３回	４回	５回	６回	７回	８回	９回
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									

回ごとに同じ数字が表れる！

２１＝　　×
と　　の＿＿＿＿＿

★数あてマジック（暗号）の仕組み

わたし「　　回かけ算して、21 で割った余りを教えてください。」

相　手「　18　です　」

⇒わたし（　“18”を　　回かけ算し、21 で割った余りを調べて）

「あなたの考えた数は　　ですね！」拍手～♪

★資料ＲＳＡ暗号の仕組み（上級生・大人向け）

ＲＳＡ暗号は、２つの素数を使った暗号の仕組みで、現代暗号のひとつです。

① ２つの素数の積ａ×ｂを決める。【前ページではａ＝３、ｂ＝７】
→積ａ×ｂより小さい自然数が暗号化できる数字。【１～20】

② 数をかけ合わせて（累乗して）ａ×ｂで割った余りを考えたときに、元の数に戻る回数（ａ－1 とｂ－1 の最小公倍数）を求める。
【２と６の最小公倍数は６　→　６回ごとに元に戻る】
→６の倍数＋１回かけ合わせると元の数字と同じ。

③ 数が元に戻る回数の中で、２つの数の積になるものを探して、相手への指示（暗号鍵）と数あてトリック（復号鍵）とする。
→1、7、13、19、25（＝５×５）、31、37、43、49（＝７×７）、･･･
と考えると、暗号「５回かけ算」→復号「５回かけ算」
暗号「７回かけ算」→復号「７回かけ算」
などが見つかる。

④ 積ａ×ｂと相手への指示「〇回かけ算」を伝える（公表する）。

積ａ×ｂを公表すると、復号の仕組み「△回かけ算」がわかってしまうような気がします。しかし、実際に使われる積はとても大きな数で、それを２つの素数の積に分けることが非常に困難なため、解読の危険性が低いとされています。

例えば、２つの２ケタの素数の積 247 は、電卓を使えば、２つの素数を見つけることはできると思いますが、２つの３ケタの素数の積 201379 は、かなり時間がかかると思います。実際は 300～1000 ケタくらいの積を用いることが推奨されているようです。