これは楽しい数学マジック！

―第1回―

数学の力　～婚活方法からギャンブル必勝術まで～

神戸新聞文化センター

2013年1月27日

森井昌克

morii@eedept.kobe-u.ac.jp

（神戸大学大学院　工学研究科）

神戸新聞文化センター
2013年1月27日
森井昌克
mmorii@kobe-u.ac.jp
（神戸大学大学院　工学研究科）

自己紹介（森井昌克）

- 神戸大学大学院　教授
  - 電気電子工学専攻
- 情報通信工学
  - 簡単に言うと、インターネットや携帯電話（スマホ）の研究
  - 最初に書いた論文（大学生の際に）
    - A Theorem that GF (2^{4m}) has no Self-Complementary Normal Bases over GF (2) for Odd *m*（1984）

数学を使って

これは楽しい数学マジック！

―第1回―

数学の力　～婚活方法からギャンブル必勝術まで～

神戸新聞文化センター

2013年1月27日

森井昌克

morii@eedept.kobe-u.ac.jp

（**神戸大学大学院　工学研究科**）

これは楽しい数学マジック！

数学の力　～婚活方法からギャンブル必勝術まで～

- 本日の主題
  - 本日は導入を含めて、次の2テーマで。
  - 数の感覚
    - 大きな数、小さな数
    - 数の増え方
  - アルゴリズム
    - 解き方（算法）

人間が扱える数はごく小さい？

- ５＋７＝１３
  - 一桁、二桁、三桁、…
  - 日本の国家予算
    - １００兆円（一般会計、H23年度）
      - GDP 500兆円
    - たかだか、１４桁の数

スーパーコンピュータ　京

どんな数でも扱えるのか？
　　１秒間に京回、計算出来る！

大きな数の計算

- 素因数分解
  - 言葉は難しいが、考え方は簡単！
  - 素数
    - それ以外の数で割り切れない数
      - 3、5、7、11、13。…
    - どんな自然数も一意に素数の積に分解出来る。
      - 「一意に」という用語は「ただ一通りに」という意味

15＝？　　3x5

35＝？　　5X7

素因数分解の方法

- 一番簡単な方法
  - 小さい数で割って行く
- スーパーコンピュータ京を使って何桁の数が素因数分解出来るか。
  - １０桁の数を素因数分解するためには５桁以下のすべての数で割って行けば良い。

$$\sqrt{n}$$

素因数分解の方法(2)

- 京は一秒間に京回、計算出来る。
  - 京＝10^{16}
    - つまり16桁の全ての数で割り算出来る(ようなもの)
  - 1秒間で32桁のどのような数でも素因数分解出来る。
  - では1年では？　100年では？　さらに

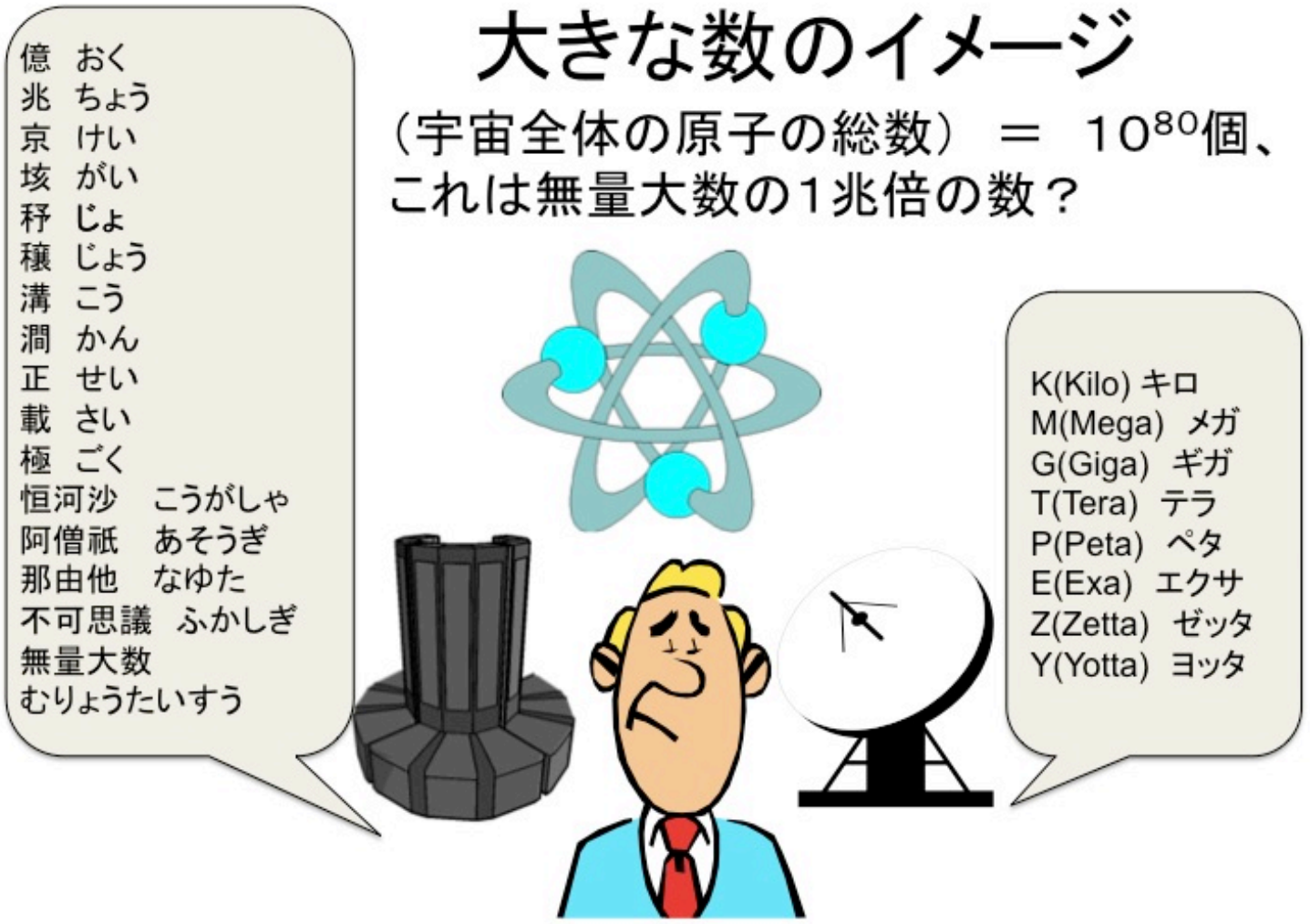
素因数分解の方法(3)

- 1分は60秒、1時間は3，600秒、さらに
- 一日は86，400秒
  - 面倒なの一日は約10万秒、つまり10^5秒
- 1年は365日なので、3,153,600秒
  - 面倒なので、(余裕を持って)10,000,000秒　10^7秒
- つまり京であれば、1年で10^{16}x10^7＝10^{23}つまり、すべての23桁以下の数で割り算出来る。よって、46桁の素因数分解は可能。100年だと48桁。

素因数分解の方法(4)

- スーパーコンピュータ京を持ってしても、100年計算したとしても、48桁の数の素因数分解しか出来ない！？
  - しか？
    - 123456789012345678901234567890123456789012345678 こんな数？
  - 本当は？　230桁程度の数の素因数分解は京で数カ月で可能。なぜ？
  - **アルゴリズムの力！**

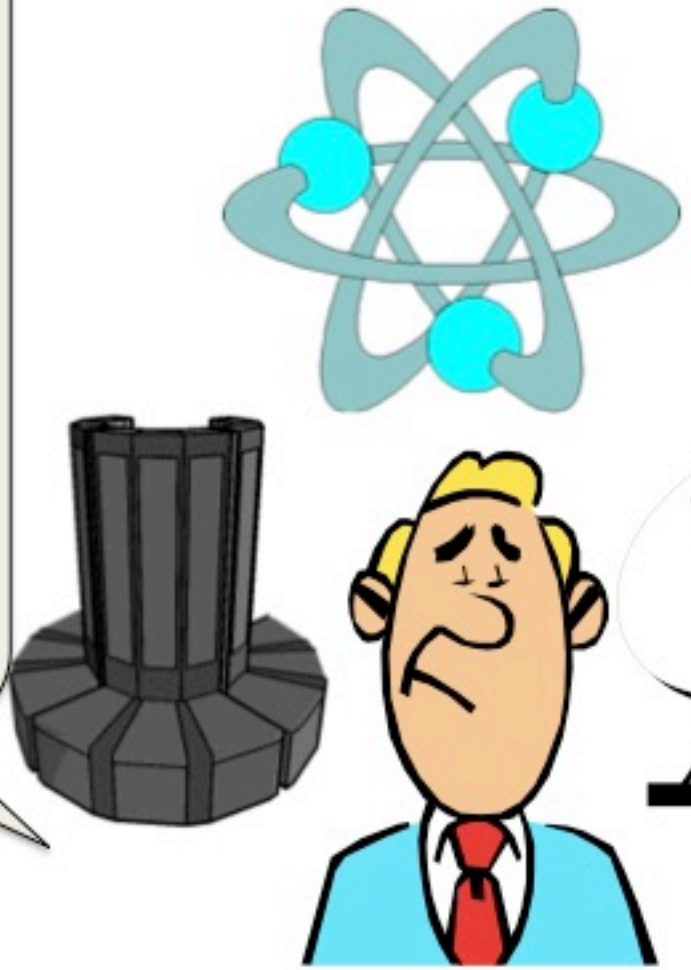
大きな数


大きな数のイメージ
（宇宙全体の原子の総数）＝ 10^{80}個、
これは無量大数の1兆倍の数？
億　おく
兆　ちょう
京　けい
垓　がい
秭　じょ
穣　じょう
溝　こう
澗　かん
正　せい
載　さい
極　ごく
恒河沙　こうがしゃ
阿僧祇　あそうぎ
那由他　なゆた
不可思議　ふかしぎ
無量大数
むりょうたいすう
K(Kilo) キロ
M(Mega)　メガ
G(Giga)　ギガ
T(Tera)　テラ
P(Peta)　ペタ
E(Exa)　エクサ
Z(Zetta)　ゼッタ
Y(Yotta)　ヨッタ

大きな数のイメージ

（宇宙全体の原子の総数）＝ 10^{80}個、
これは無量大数の1兆倍の数？

億　おく
兆　ちょう
京　けい
垓　がい
秭　じょ
穣　じょう
溝　こう
澗　かん
正　せい
載　さい
極　ごく
恒河沙　こうがしゃ
阿僧祇　あそうぎ
那由他　なゆた
不可思議　ふかしぎ
無量大数
むりょうたいすう



K(Kilo) キロ
M(Mega)　メガ
G(Giga)　ギガ
T(Tera)　テラ
P(Peta)　ペタ
E(Exa)　エクサ
Z(Zetta)　ゼッタ
Y(Yotta)　ヨッタ

大きな数

- K(キロ)、M(メガ)、G(ギガ)、T(テラ)、P(ペタ)、…
- メガピクセル携帯(カメラ)
- テラバイト・ハードディスクレコーダー

HDD容量:1TB 録画可能メディア:BD-R/BD-R DL/BD-R XL/BD-RE/BD-RE DL/BD-RE XL/DVD-R/DVD-RW/DVD-RAM/DVD-R DL デジタルチューナー:地上デジタル/BSデジタル/110度CSデジタル

大きな数

- 京という単位は上記のように10進数で0（ゼロ）が16個も並ぶ大きな数です。一般の人が耳にする最大の単位は国家予算の単位である兆程度でしょう。コンピューターの世界でも大きな単位が幅を利かせるようになりました。K（キロ）、M（メガ）、G（ギガ）が大きな単位であった時代は過ぎ去り、T（テラ）、P（ペタ）が聞かれるようになったのです。2TB（バイト）のハードディスクが1万円を切る時代に突入したのです。さらにその上の単位も聞かれるようになりました。世界中で1年間にインターネットに流れるデータ量が約400E（エクサ）Bなのです。Tの1,000倍がP、Pの1,000倍がEです。しかもこれはグローバルIPと呼ばれる、いわゆるインターネットの大通り、もしくは高速道路を流れる量であって、社内や家庭内を会わせればその何十倍、何百倍もの量になります。Eの1,000倍であるZ（ゼタ）,そしてZの1,000倍であるY(ヨッタ)も現実の単位になってきました。

情報の量について

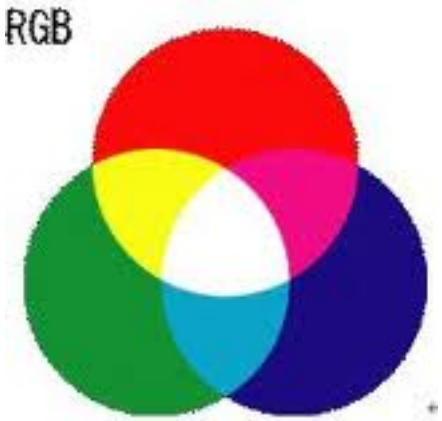
- 情報の量について考えてみましょう.
  - ビットとバイト
  - 1ビットは2択問題（YES/NO)
    - １文字は1バイト（8ビット）で表せる
      - アルファベットは26文字，英数記号合わせても100文字程度
    - でも，漢字は2バイト
      - 使う文字だけでも3，000文字以上

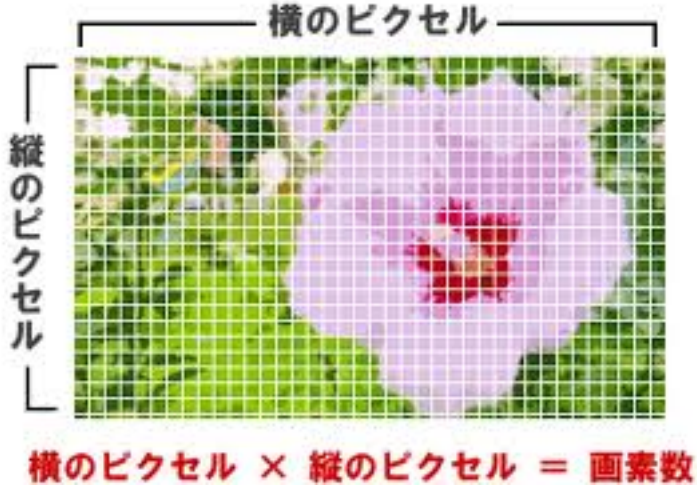
情報の量について

- 情報の量について考えてみましょう.
  - 新聞一日分は
    - たかだか100KB
      - K(キロ)　→M(メガ)→G(ギガ)→T(テラ)→P(ペタ)
    - 1年でも30MB(ホントはもっと小さい)
  - では，画像は
    - デジタルカメラ
      - 10MBぐらい
      - 圧縮して　100KBぐらい

画像（メガピクセル携帯カメラ）

- ピクセル
  - RGB（光の三原色）
  - それぞれを256段階で調節
    - 256階超
  - 1,600x1,200ピクセル
    - 1,920,000-
    - 1.9メガピクセル





情報の量について

- 情報の量について考えてみましょう.
  - 音楽は
    - CDに70分ぐらいの音楽
    - CDは700MBぐらい
    - でも，1GBのiPodで1,000分以上，なぜ？
  - 映像は
    - DVDに2時間のきれいな映像
    - DVDは4GB

人間が一生に見聞きする情報量はどれぐらいでしょうか？

- 見たり聞いたりするデータを映像にすべて残したとする
- 人間は生きている時間は，１００年x３６５日x２４時間x60分x60秒
- 人間は，約3．15x10^9秒（8．76x10^5時間）生きている
- 1秒間の映像は100KBあれば十分．1時間であれば100MBあれば十分．
- つまり，一生の映像は10^7MBあれば十分
- 10^7MBは10Tバイト

1TBのHDの実勢価格は1万円以下？！

ねずみがゾウを超える日？

- 和算家の吉田光由による塵劫記
  - 江戸時代初期のベストセラー
- 問題
  - 正月にネズミの夫婦が子供を12匹生むとする．翌月の2月には，この親ネズミを含めて，それぞれのつがいのネズミがまた12匹生むとする．するとネズミは総計98匹となる．このように毎月生み続けると年末の12月には総計何匹になるか

答えは276億8257万4402匹

米粒の問題（塵劫記が発祥）

- 一か月後に，３俵（１年分の米，約１８０Kg）もらうのと，今日から米粒１粒，明日は2粒，明後日は4粒というように2倍ずつ一か月にわたってもらうのとどちらが得か．

３００俵（２０トン）以上、１００年分以上の米

では、もう一つ

- 神戸新聞に関わる問題？
  - 神戸新聞を2つにきれいに折りましょう．そしてそれをさらに2つに折ります．さらに2つ，と次々に折っていきます．１０回も折ると，現実には折ることができなくなってしまいますが，ずっと折り続けることができたとして，４５回折るとどれぐらいの厚さになるでしょうか．

神戸新聞問題の回答

- 新聞紙１枚が０．０３ｍｍとすると，驚くことに約１００万Ｋｍにもなります．地球と月の距離約３８万Ｋｍよりも離れてしまうのです．
  - １回折って重ねると０．０６ミリになります。さらに折って重ねると、０．１２ミリ、これを４５回続ければ１００万キロメートルを超えるということです。
    - $0.03 \times 2^{45} = 1.06 \times 10^{6}$ Km

ねずみ算？？？

- 何の役に立つのでしょう？？
  - 貯金（預金）、あるいは借金の見積もりに関係するのです。
  - 100万円を1%で100年預ければ、いくらになる？

$$100\text{万円} \times (1.01)^{100} = 270\text{万円}$$

余興をひとつ(^^;)

- 皆さん、1から9までの数字を使って、2桁の数を3つ思い浮かべて下さい。
- 次に、その3つを誰にも見れないように紙に大きく書いて下さい。
- さて、その数字を関して…

誕生日の問題

- 40人学級で同じ誕生日の人はいるか？
  - 確率9割でいる！

誕生日の問題

n人集まると、互いに同じ誕生日の人がいる確率pは？

$$p = 1 - \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\cdots\left(1 - \frac{n-1}{365}\right)$$

40人だと、確率は 0.89

20人だと、確率は 0.42

誕生日の問題

- n人の中で同じ誕生日の人が少なくとも2人いる場合の確率を計算する。閏年や双子は考えないものとし、誕生日は365日とも等確率であるとする。まずは、n人の誕生日が全て異なる場合の確率 p1 を計算する。2人目が1人目と異なっている誕生日である確率は、364/365 である。次に、3人目が1人目2人目と異なる誕生日である確率は 363/365 である。同様に4人目は362/365、…、n人目は (365-n+1)/365 となる。つまり、n人の誕生日が全て異なる確率は次のようになる。

誕生日の問題

$$= \frac{364}{365} \cdot \frac{363}{365} \cdot \frac{362}{365} \cdots\cdots \frac{365-n+1}{365} = \frac{365!}{365^n(365-n)!}$$

、の中で同じ誕生日の人が少なくとも2人いる場合の確率 p_2 は、

$$= 1 - \frac{365!}{365^n(365-n)!}$$

= 23 のとき、$p_2 = 0.507\cdots$ となる。

どの、n人の部屋に"あなた"が入ったときに、あなたと同じ誕生日の人がいる確

$$= 1 - \left(\frac{364}{365}\right)^n$$

= 23 ならば、$p_3 = 0.0611\cdots$ である。n が 253 のときに初めて p_3 が 0.5

アルゴリズム

- 計算量の爆発
- スーパーコンピュータ京でも計算出来ない！

素因数分解の方法(4)

- スーパーコンピュータ京を持ってしても、100年計算したとしても、48桁の数の素因数分解しか出来ない！？
  - しか？
    - 123456789012345678901234567890123456789012345678 こんな数？
  - 本当は？　230桁程度の数の素因数分解は京で数カ月で可能。なぜ？
  - **アルゴリズムの力！**

アルゴリズム

- 算法
- 問題の見方を変えれば、易しくなる！？
  - １から１０を全て足す問題
    - １＋２＋３＋４＋５＋６＋７＋８＋９＋１０＝？

１ + ２ + ３ + ４ + ５
10+ ９ + ８ + ７ + ６ = 55

アルゴリズム

1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1

素因数分解

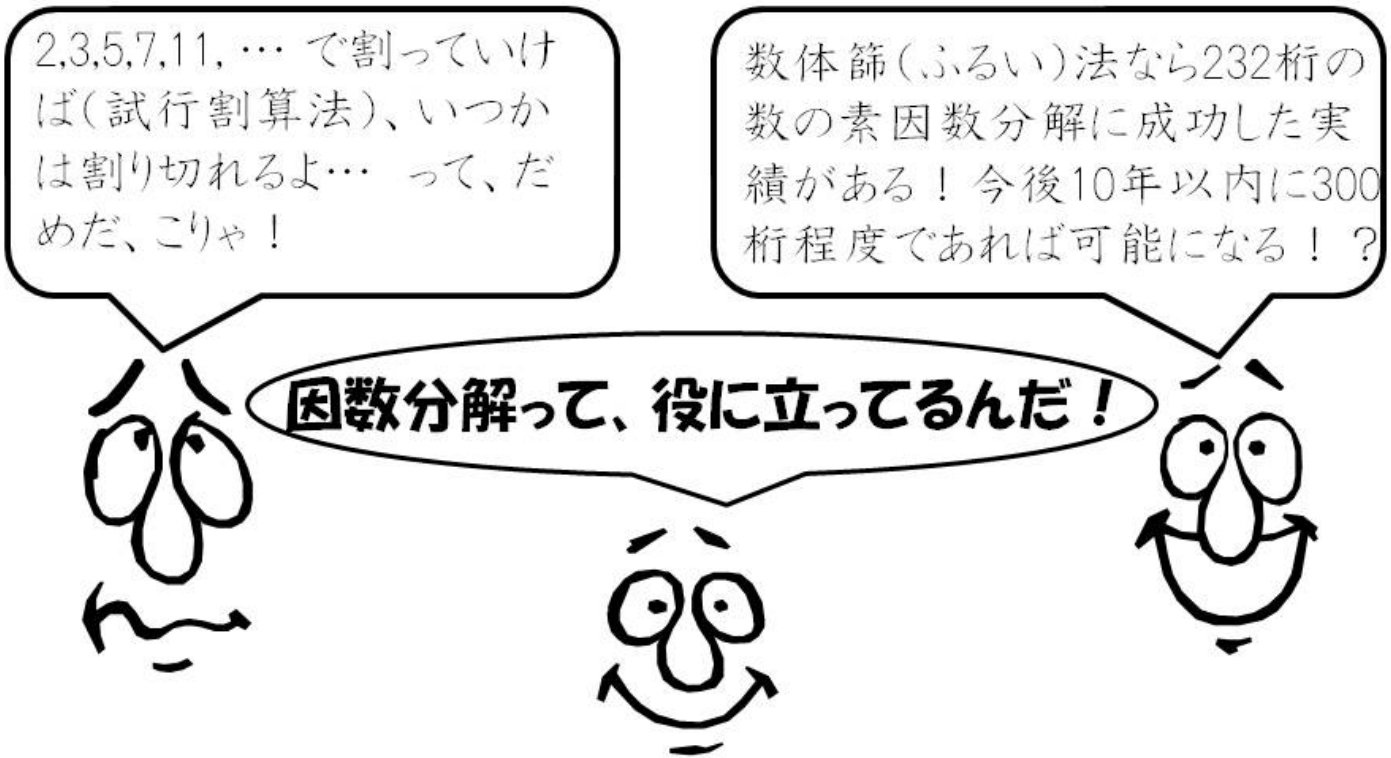
- 大きな数の素因数分解は難しい？
  - 任意の500桁の数を素因数分解するのは難しい
    - 難しいということは出来ないという事
    - とはいえ、230桁であれば可能。
      - 京で数ヶ月？

素因数分解アルゴリズム

素因数分解

すべての数は素数の積に一意に分解される

大きな数、たとえば500桁の素因数分解は難しい！



素因数分解アルゴリズム(篩法）

素因数分解を行おうとする数をnとしたとき，

$$x^2 \equiv y^2 \mod n$$

が満たされるxとyを求めます．これはy^2をnで割った余りと、x^2をnで割った余りに等しいことを表しています．$x = \pm y$以外であれば，nの素因数が求められる可能性が高いのです．なぜならば，

$$x^2 - y^2 \equiv 0 \mod n$$

であることから，$x^2 - y^2$はnの倍数であり，

$$x^2 - y^2 = (x-y)(x+y)$$

と因数分解されることから，$(x-y)$と$(x+y)$がnの倍数でなければnの素因数なのです．もちろん，xとyを試行割算法と同じように適当に探すのではなく，式を満たすxとyを組織的に作っていくのです．

公開鍵暗号への道

New Directions in Cryptography

Invited Paper

Whitfield Diffie and Martin E. Hellman

1976年

共通鍵暗号と公開鍵暗号

- 鍵配送の必要性
  - n人での鍵の数はn(n-1)/2個
- 高速
  - 転置･置換
- 安全性の合意が得られにくい
  - 証明が難しい
    - 新しい問題

- 鍵配送が不必要
  - 実際には、鍵の認証は必要
- 低速
  - 整数論、グラフ理論
- 安全性の合意が得られやすい
  - 数論的証明
    - 古い（歴史のある）問題

オイラーの定理

- フェルマーの小定理

$$a^{p-1} \equiv 1 \mod p$$

- オイラーの定理

$$a^{\varphi(n)} \equiv 1 \mod n$$

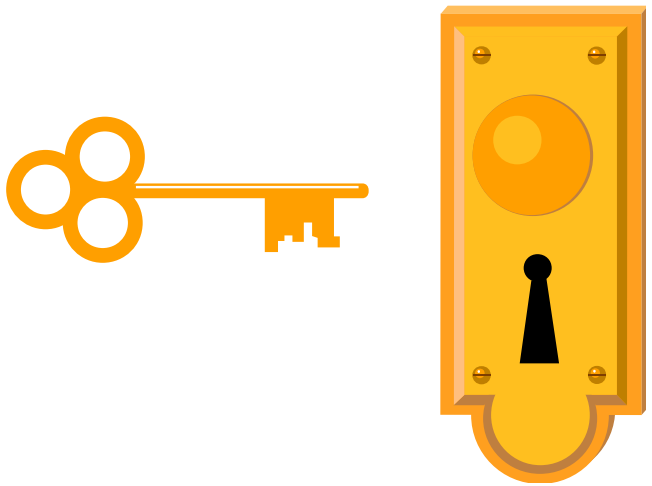
$\varphi(n)$ はオイラー関数、nと互いに素な数の個数

$n = pq$ でpとqが素数の場合

$$\varphi(pq) = (p-1)(q-1)$$

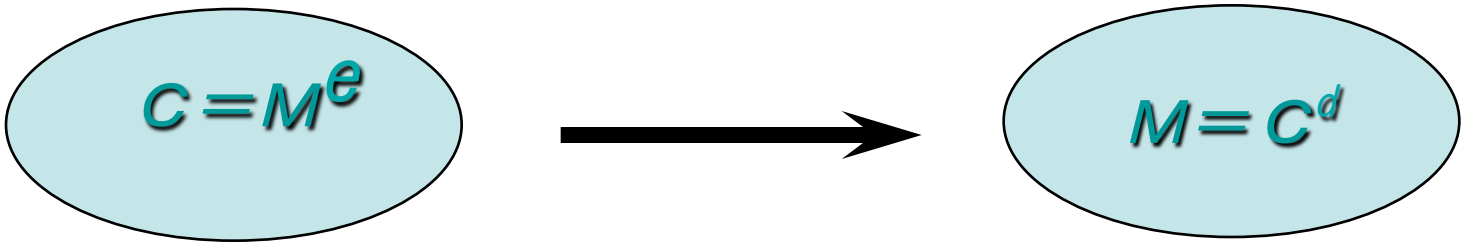
RSA暗号

- $C=M^e \bmod n$
  - n=pq
  - $ed=1 \bmod \mathrm{LCM}(p-1, q-1)$
- $M=C^d \bmod n$



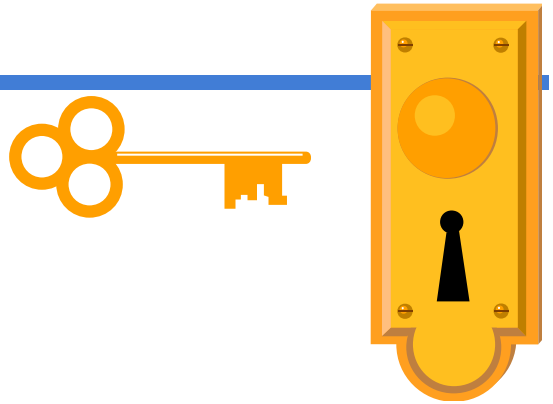
公開鍵 (e, n)

秘密鍵 (d, p, q)



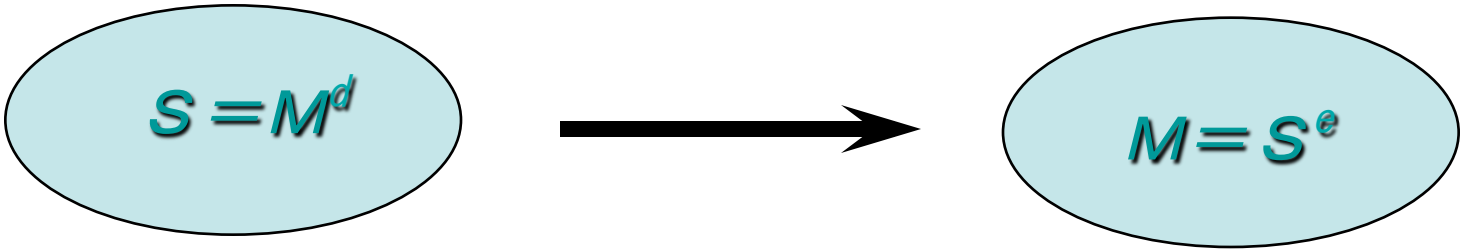
RSA暗号

- *ディジタル署名*



自分の秘密鍵 d

相手の公開鍵 e

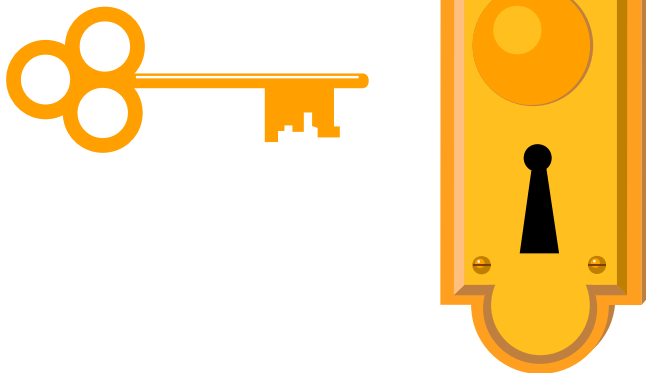


RSA暗号の解読

- RSA暗号を解くことと素因数分解を行なうことは等価と信じられている。
  - 証明はできていない。
  - 証明付きの暗号系も存在。
- 素因数分解
  - 複数多項式二次ふるい法
  - 数体ふるい法

RSA暗号

- $C=M^e \bmod n$
  - n=pq
  - $ed=1 \bmod \mathrm{LCM}(p-1, q-1)$
- $M=C^d \bmod n$



灘中学校平成24年度入学試験

5

2×2＝4 から始めて，2 つの数の間のかけ算で新しい数を作ることをくり返します。その際，2 および一度作られた数は，以降の計算に何度でも使えるという決まりにします。

例えば，2×2＝4，4×2＝8，8×2＝16 とすると，3 回のかけ算で 16 が得られますが，2×2＝4，4×4＝16 とすると，2 回のかけ算でも 16 が得られます。

このような決まりに従って，かけ算を最低 ① 回すれば 512（2 を 9 個かけた数）が得られ，かけ算を最低 ② 回すれば 32768（2 を 15 個かけた数）が得られます。

平成24年度　灘中学校入試問題

5

$2\times2=4$ から始めて，2つの数の間のかけ算で新しい数を作ることをくり返します。その際，2および一度作られた数は，以降の計算に何度でも使えるという決まりにします。

例えば，$2\times2=4, 4\times2=8, 8\times2=16$ とすると，3回のかけ算で16が得られますが，$2\times2=4, 4\times4=16$ とすると，2回のかけ算でも16が得られます。

このような決まりに従って，かけ算を最低 ① 回すれば512（2を9個かけた数）が得られ，かけ算を最低 ② 回すれば32768（2を15個かけた数）が得られます。

高速指数演算法
RSA暗号の高速計算法

今回のまとめ

数の感覚

アルゴリズムの効果