# 素敵な数、素数

寺杣　友秀

東京大学大学院数理科学研究科

http://gauss.ms.u-tokyo.ac.jp

**2015/1/23**

# 数理科学研究科の紹介

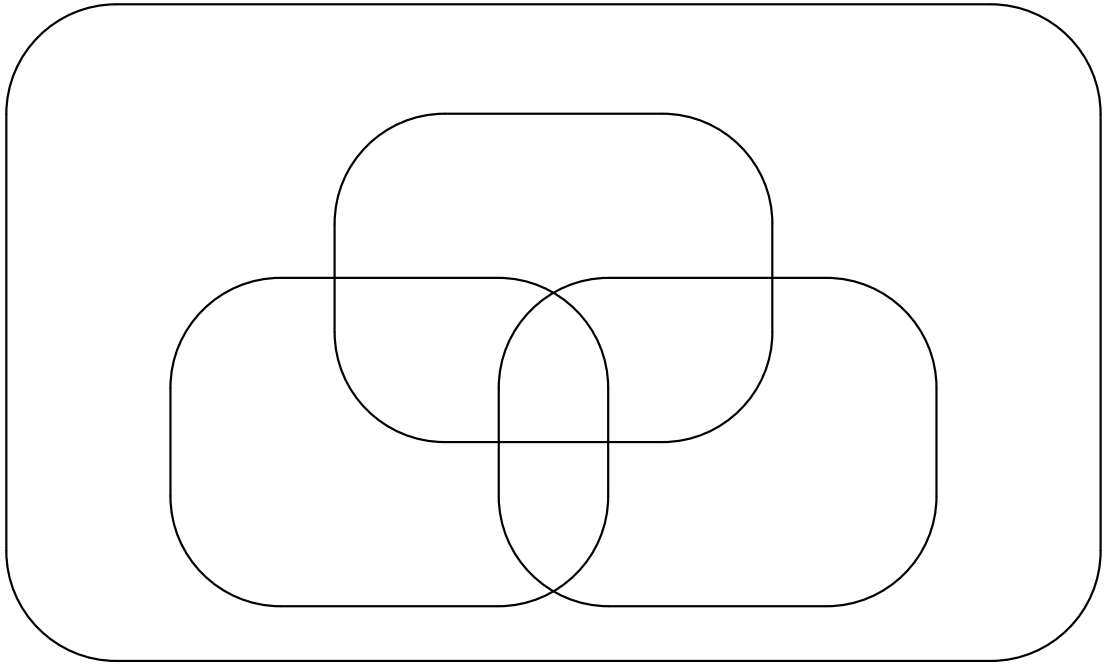
## 数学の分野

数学の分野は大きく分けて次のようになります。

# 数理科学研究科の紹介

## 数学の分野

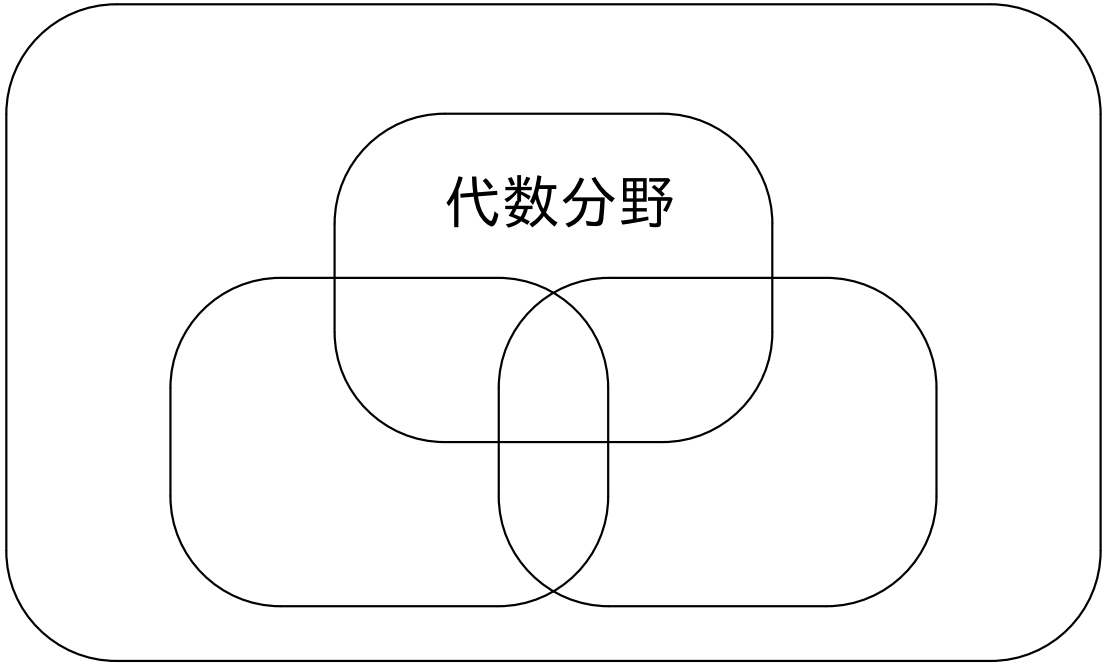
数学の分野は大きく分けて次のようになります。



# 数理科学研究科の紹介

## 数学の分野

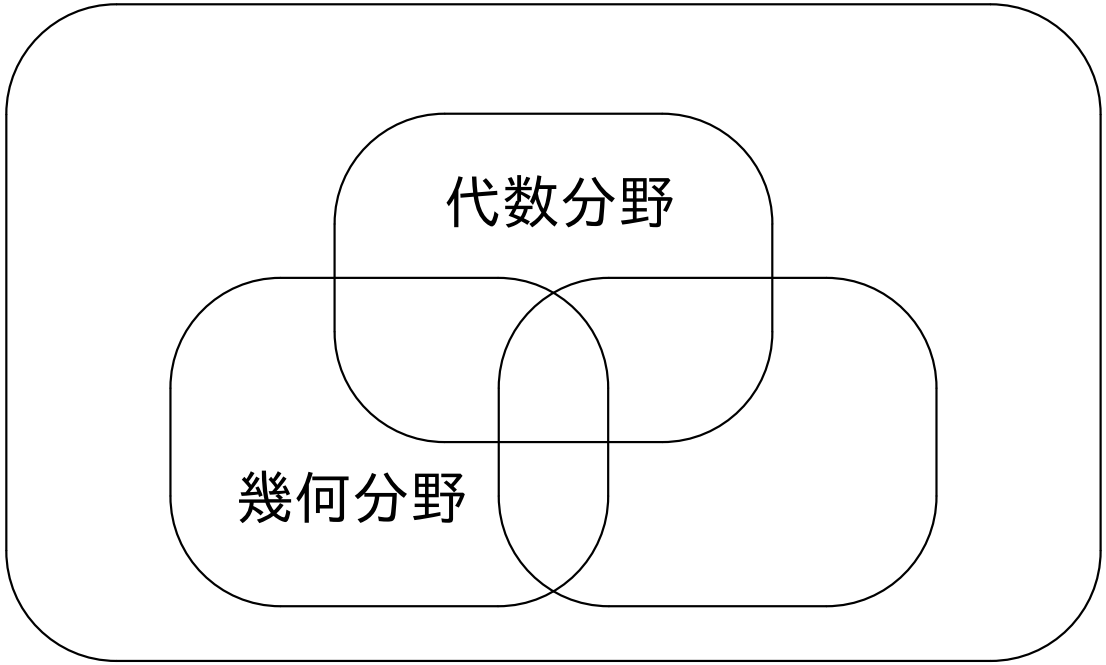
数学の分野は大きく分けて次のようになります。



# 数理科学研究科の紹介

## 数学の分野

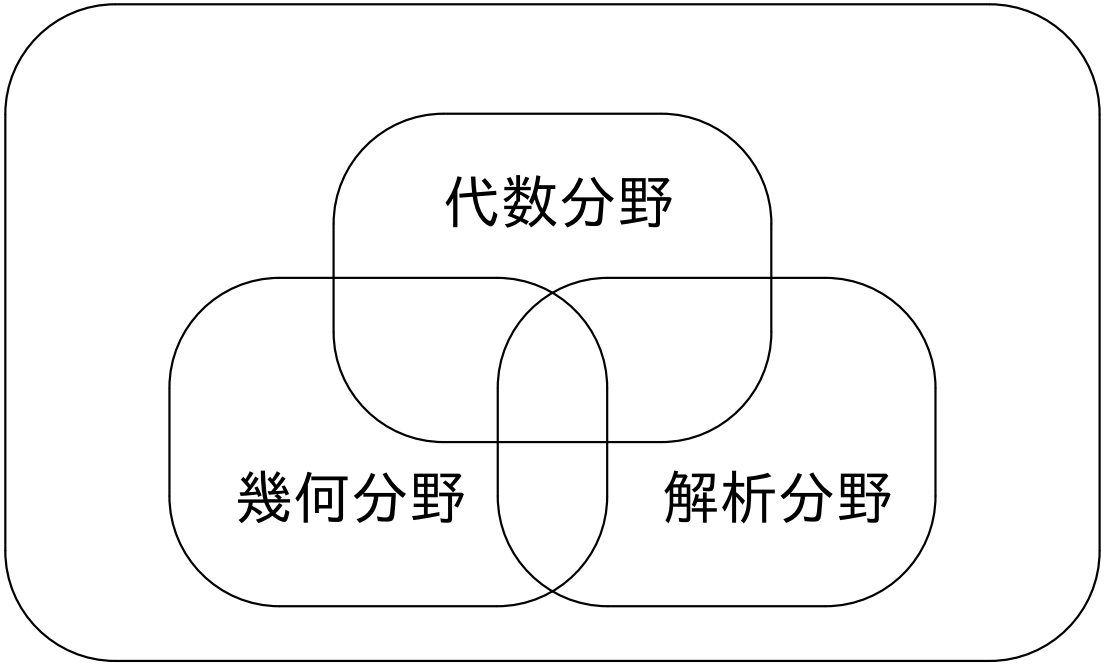
数学の分野は大きく分けて次のようになります。



# 数理科学研究科の紹介

## 数学の分野

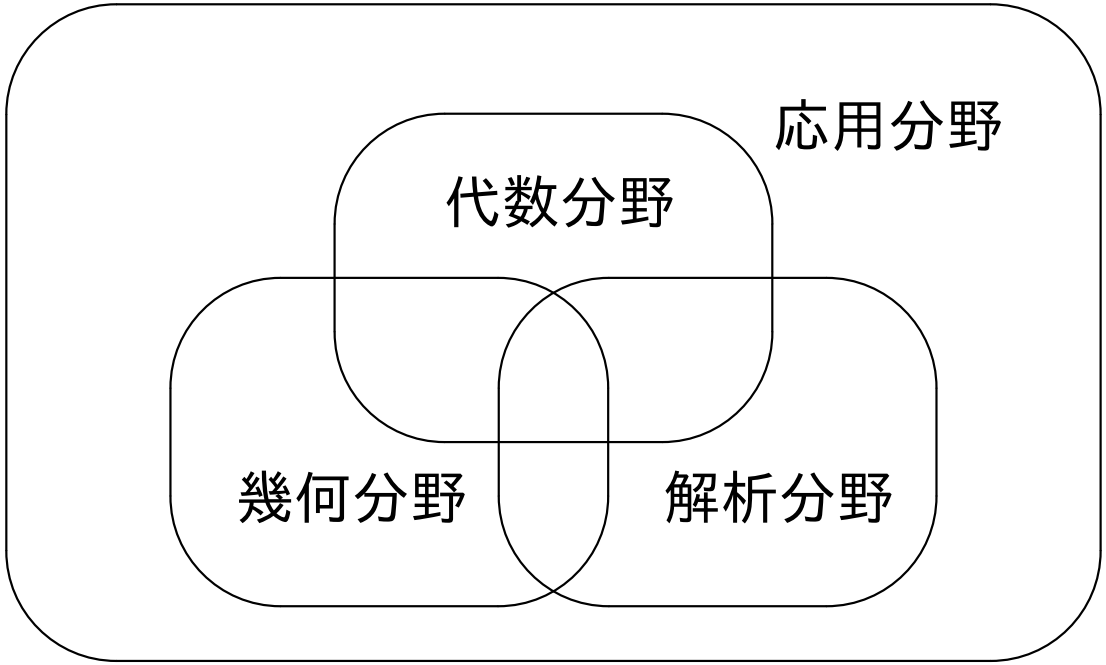
数学の分野は大きく分けて次のようになります。



# 数理科学研究科の紹介

## 数学の分野

数学の分野は大きく分けて次のようになります。



# 数理科学研究科の紹介

これらの分野についてもう少し詳しく紹介しましょう。

1. 代数学：多項式や多項式を用いた方程式、あるいは整数などの数の体系を扱う。

# 数理科学研究科の紹介

これらの分野についてもう少し詳しく紹介しましょう。

1. 代数学：多項式や多項式を用いた方程式、あるいは整数などの数の体系を扱う。 グラフなどを用いて図形などの幾何との関係を用いる手法もある。

# 数理科学研究科の紹介

これらの分野についてもう少し詳しく紹介しましょう。

1. 代数学：多項式や多項式を用いた方程式、あるいは整数などの数の体系を扱う。 グラフなどを用いて図形などの幾何との関係を用いる手法もある。
2. 幾何学：図形に関する性質をあつかう。高校における直線や２次曲線などの性質を発展させたもの。たとえば図形の曲がり方などを考えるなど。

# 数理科学研究科の紹介

これらの分野についてもう少し詳しく紹介しましょう。

1. 代数学：多項式や多項式を用いた方程式、あるいは整数などの数の体系を扱う。 グラフなどを用いて図形などの幾何との関係を用いる手法もある。
2. 幾何学：図形に関する性質をあつかう。高校における直線や２次曲線などの性質を発展させたもの。たとえば図形の曲がり方などを考えるなど。平面図形（２次元)、空間図形（３次元）だけでははく、もっと高次元のものを扱う。２次元や３次元の空間でも曲がった空間を考える。

# 数理科学研究科の紹介

3. 解析学：関数の性質を研究する。とくに自然科学に現れる重要な関数の研究。

# 数理科学研究科の紹介

3. 解析学：関数の性質を研究する。とくに自然科学に現れる重要な関数の研究。自然科学のさまざまな分野で用いられるものは主に多変数関数です。

# 数理科学研究科の紹介

3. 解析学：関数の性質を研究する。とくに自然科学に現れる重要な関数の研究。自然科学のさまざまな分野で用いられるものは主に多変数関数です。極限操作や関数の変化などを考える。高校の数学の分野では微分積分と関連が深い分野です。

# 数理科学研究科の紹介

3. 解析学：関数の性質を研究する。とくに自然科学に現れる重要な関数の研究。自然科学のさまざまな分野で用いられるものは主に多変数関数です。極限操作や関数の変化などを考える。高校の数学の分野では微分積分と関連が深い分野です。
4. これらの分野に明確な境界があるわけではない。数学以外の科学とのかかわりでは、数学以外の知識も要求される。こういったものを扱う応用分野も数理科学研究科では重要な研究課題です。

# 数理科学研究科の紹介

3. 解析学：関数の性質を研究する。とくに自然科学に現れる重要な関数の研究。自然科学のさまざまな分野で用いられるものは主に多変数関数です。極限操作や関数の変化などを考える。高校の数学の分野では微分積分と関連が深い分野です。
4. これらの分野に明確な境界があるわけではない。数学以外の科学とのかかわりでは、数学以外の知識も要求される。こういったものを扱う応用分野も数理科学研究科では重要な研究課題です。

きょうの素数の話は代数学とかかわりの深い分野ですが、解析分野の考え方も中には使われます。

# 大学での教養課程の数学

大学の１年生と２年生では理科系の学生は高校の数学を基礎として、自然科学の基礎となる数学を勉強します。これは、新しい科学の芽を育ててゆくための土壌となるものです。

# 大学での教養課程の数学

大学の１年生と２年生では理科系の学生は高校の数学を基礎として、自然科学の基礎となる数学を勉強します。これは、新しい科学の芽を育ててゆくための土壌となるものです。
また、文科系の学問でも物事を客観的に分析するためには数学が使われており、文科の学生も数学を選択することができます。

# 素数の定義

- 自然数とは $n = 1, 2, 3, \ldots$ といった数のことですが、自然数 $a, b$ に対して、和 $a + b$ および積 $ab$ を考えることができる。
- ３つの自然数 $a, b, c$ に対して $ac = b$ となる関係があるとき、$b$ は $a$ で割り切れるという。このとき、$a$ は $b$ の約数であるといい、$b$ は $a$ の倍数であるという。
- $p$ を２以上の自然数とすると、$1$ と $p$ はいつでも $p$ の約数となります。もし、$1$ と $p$ 以外の約数がなければ、その時、$p$ は素数であるという。素数を小さいほうから、列挙すると、

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

などとなります。

# 素因数分解

素数でない数を合成数といいます。

# 素因数分解

素数でない数を合成数といいます。自然数 $n$ が合成数であれば、$n$ を二つの $2$ 以上の自然数の積に書くことができます。たとえば $28$ は合成数で $4 \times 7$ とかけます。

# 素因数分解

素数でない数を合成数といいます。自然数 $n$ が合成数であれば、$n$ を二つの $2$ 以上の自然数の積に書くことができます。たとえば $28$ は合成数で $4 \times 7$ とかけます。
その積のうちに合成数があれば、さらに積に書くことを繰り返して、最終的にすべての自然数が素数の積に書けることがわかります。たとえば $4 \times 7$ は $2 \times 2 \times 7$ と書け、これ以上積の形で分けることができません。

# 素因数分解

従って

$$28 = 4 \times 7 = 2 \times 2 \times 7$$

となります。このようにして最終的にすべての $2$ 以上の自然数は素数の積の形に書くことができます。素数の積の形に書くことを素因数分解といい、そこに現れる素数を素因数といいます。

# 素因数分解

従って

$$28 = 4 \times 7 = 2 \times 2 \times 7$$

となります。このようにして最終的にすべての $2$ 以上の自然数は素数の積の形に書くことができます。素数の積の形に書くことを素因数分解といい、そこに現れる素数を素因数といいます。また別のやり方で素因数分解をすることもできます。

$$28 = 2 \times 14 = 2 \times 2 \times 7$$

実はどのようなやり方で素因数分解を求めても、（積の順番を変えれば）答えは全て等しくなります。

# 素因数分解の一意性

つまり次の定理が成り立ちます。

# 素因数分解の一意性

つまり次の定理が成り立ちます。

**定理 (素因数分解の一意性)**

素因数分解はその仕方によらない。つまり

$$n = p_1 \cdots p_n = q_1 \cdots q_m$$

と素因数分解されれば $n = m$ であり、$q_1, \ldots, q_n$ の順番を変えれば $p_1 = q_1, \ldots, p_n = q_n$ となる。

# 素因数分解の一意性

つまり次の定理が成り立ちます。

**定理 (素因数分解の一意性)**

素因数分解はその仕方によらない。つまり

$$n = p_1 \cdots p_n = q_1 \cdots q_m$$

と素因数分解されれば $n = m$ であり、$q_1, \ldots, q_n$ の順番を変えれば $p_1 = q_1, \ldots, p_n = q_n$ となる。

ここで証明はしませんが、これは自明ではなく証明しなくてはならないことです。

# 素数はたくさんあるのか

それでは問題です。

**問題**

素数はたくさんあるのでしょうか？

# 素数はたくさんあるのか

それでは問題です。

**問題**

素数はたくさんあるのでしょうか？

実は次の定理があります。

**定理**

素数は無限にある。

## 定理

素数は無限にある。

## 定理

素数は無限にある。

## 証明

## 定理

素数は無限にある。

## 証明

もし、素数が有限個しかないとすれば、素数のすべてを小さい順番に並べて $p_1 = 2, p_2 = 3, \ldots, p_n$ とおくことができる。

## 定理

素数は無限にある。

## 証明

もし、素数が有限個しかないとすれば、素数のすべてを小さい順番に並べて $p_1 = 2, p_2 = 3, \ldots, p_n$ とおくことができる。それらすべての積に 1 を加えたもの $m = p_1 p_2 \cdots p_n + 1$ を考える。

## 定理

素数は無限にある。

## 証明

もし、素数が有限個しかないとすれば、素数のすべてを小さい順番に並べて $p_1 = 2, p_2 = 3, \ldots, p_n$ とおくことができる。それらすべての積に 1 を加えたもの $m = p_1 p_2 \cdots p_n + 1$ を考える。この $m$ を $p_1$ で割った余りは 1 になるので $p_1$ では割り切れない。

## 定理

素数は無限にある。

## 証明

もし、素数が有限個しかないとすれば、素数のすべてを小さい順番に並べて $p_1 = 2, p_2 = 3, \ldots, p_n$ とおくことができる。それらすべての積に 1 を加えたもの $m = p_1 p_2 \cdots p_n + 1$ を考える。この $m$ を $p_1$ で割った余りは 1 になるので $p_1$ では割り切れない。同様にして $p_2$ で割っても $p_2, \ldots, p_n$ で割っても 1 余るので $p_1, \cdots, p_n$ で割り切れない。

## 定理

素数は無限にある。

## 証明

もし、素数が有限個しかないとすれば、素数のすべてを小さい順番に並べて $p_1 = 2, p_2 = 3, \ldots, p_n$ とおくことができる。それらすべての積に 1 を加えたもの $m = p_1 p_2 \cdots p_n + 1$ を考える。この $m$ を $p_1$ で割った余りは 1 になるので $p_1$ では割り切れない。同様にして $p_2$ で割っても $p_2, \ldots, p_n$ で割っても 1 余るので $p_1, \cdots, p_n$ で割り切れない。従って $m$ を素因数分解するとその素因子には $p_1, \ldots, p_n$ とは異なるものが存在する。

## 定理

素数は無限にある。

## 証明

もし、素数が有限個しかないとすれば、素数のすべてを小さい順番に並べて $p_1 = 2, p_2 = 3, \ldots, p_n$ とおくことができる。それらすべての積に 1 を加えたもの $m = p_1 p_2 \cdots p_n + 1$ を考える。この $m$ を $p_1$ で割った余りは 1 になるので $p_1$ では割り切れない。同様にして $p_2$ で割っても $p_2, \ldots, p_n$ で割っても 1 余るので $p_1, \cdots, p_n$ で割り切れない。従って $m$ を素因数分解するとその素因子には $p_1, \ldots, p_n$ とは異なるものが存在する。　これは素数の全体を $p_1, \ldots, p_n$ としたことに矛盾する。従って素数は無限にある。

**定理**

素数は無限にある。

**証明**

もし、素数が有限個しかないとすれば、素数のすべてを小さい順番に並べて $p_1 = 2, p_2 = 3, \ldots, p_n$ とおくことができる。それらすべての積に 1 を加えたもの $m = p_1 p_2 \cdots p_n + 1$ を考える。この $m$ を $p_1$ で割った余りは 1 になるので $p_1$ では割り切れない。同様にして $p_2$ で割っても $p_2, \ldots, p_n$ で割っても 1 余るので $p_1, \cdots, p_n$ で割り切れない。従って $m$ を素因数分解するとその素因子には $p_1, \ldots, p_n$ とは異なるものが存在する。　これは素数の全体を $p_1, \ldots, p_n$ としたことに矛盾する。従って素数は無限にある。

このように証明したい命題の否定を仮定して矛盾を導く証明法を背理法といいます。

# 素数の密度を考える

それでは素数はどれくらいたくさんあるのでしょうか？

# 素数の密度を考える

それでは素数はどれくらいたくさんあるのでしょうか？自然数の部分集合がたくさんあるか、無限にあることはあるが、それほど多くはないか、というのを比較するにはどうすればよいでしょうか？

# 素数の密度を考える

それでは素数はどれくらいたくさんあるのでしょうか？自然数の部分集合がたくさんあるか、無限にあることはあるが、それほど多くはないか、というのを比較するにはどうすればよいでしょうか？たとえば「$2$ のべきであらわされる数」

$$1, 2^2 = 4, 2^3 = 8, 2^4 = 16, \ldots$$

と、「偶数」　はどちらが多いでしょうか？

# 素数の密度を考える

それでは素数はどれくらいたくさんあるのでしょうか？自然数の部分集合がたくさんあるか、無限にあることはあるが、それほど多くはないか、というのを比較するにはどうすればよいでしょうか？たとえば「$2$ のべきであらわされる数」

$$1, 2^2 = 4, 2^3 = 8, 2^4 = 16, \ldots$$

と、「偶数」　はどちらが多いでしょうか？この場合たとえば $1$ から $100$ までのなかで比べてみると「偶数」は $50$ 個あり、「$2$ のべき」は $1, 2, 4, 8, 16, 32, 64$ の $7$ 個なので数の密度でいうと、$\dfrac{50}{100}$ と $\dfrac{7}{100}$ で $2$ のべきのほうが少ないことになります。

# 素数の密度を考える

この差は考える範囲が $\mathbf{1000, 10000}$ と増えていくとどんどん広がっていくはずです。これをもう少し正確にいうと、

$$A_N = \{N \text{ 以下の偶数 }\},$$
$$B_N = \{N \text{ 以下の数で } \mathbf{2} \text{ のべきとなるもの }\},$$

としたときに $\dfrac{B_N}{A_N}$ の $N$ が無限にいくときの極限は $\mathbf{0}$ になることが証明できます。

# 素数の密度を考える

この差は考える範囲が $\mathbf{1000, 10000}$ と増えていくとどんどん広がっていくはずです。これをもう少し正確にいうと、

$$A_N = \{N \text{ 以下の偶数 }\},$$
$$B_N = \{N \text{ 以下の数で } \mathbf{2} \text{ のべきとなるもの }\},$$

としたときに $\dfrac{B_N}{A_N}$ の $N$ が無限にいくときの極限は $\mathbf{0}$ になることが証明できます。このようにして「偶数」の密度と「$\mathbf{2}$ のべき」の密度を比較することにします。

# 素数の密度を考える

素数の密度を考える前に、実際に素数はどれくらいあるのか、観察してみましょう。

# 素数の密度を考える

素数の密度を考える前に、実際に素数はどれくらいあるのか、観察してみましょう。まず $10$ の付近、$10^2 = 100$ の付近、$10^3 = 1000$ の付近の素数を考えるのに $10$ の次にくる素数、$10^2 = 100$ の次にくる素数、$10^3 = 1000$ の次にくる素数と見ていき、どれくらい素数があるかというのを見てみると、下の表のようになります。

# 素数の密度を考える

素数の密度を考える前に、実際に素数はどれくらいあるのか、観察してみましょう。まず $10$ の付近、$10^2 = 100$ の付近、$10^3 = 1000$ の付近の素数を考えるのに $10$ の次にくる素数、$10^2 = 100$ の次にくる素数、$10^3 = 1000$ の次にくる素数と見ていき、どれくらい素数があるかというのを見てみると、下の表のようになります。

| $10^n$ | その次の素数 | $10^n$ | その次の素数 |
|---:|---:|---:|---:|
| **1** | **2** | **10000** | **10007** |
| **10** | **11** | **100000** | **100003** |
| **100** | **101** | **1000000** | **1000003** |
| **1000** | **1009** | $10^{20}$ | |

# 素数の密度を考える

素数の密度を考える前に、実際に素数はどれくらいあるのか、観察してみましょう。まず $10$ の付近、$10^2 = 100$ の付近、$10^3 = 1000$ の付近の素数を考えるのに $10$ の次にくる素数、$10^2 = 100$ の次にくる素数、$10^3 = 1000$ の次にくる素数と見ていき、どれくらい素数があるかというのを見てみると、下の表のようになります。

| $10^n$ | その次の素数 | $10^n$ | その次の素数 |
|---:|---:|---:|---:|
| **1** | **2** | **10000** | **10007** |
| **10** | **11** | **100000** | **100003** |
| **100** | **101** | **1000000** | **1000003** |
| **1000** | **1009** | $10^{20}$ | **10000000000000000039** |

# 確率論的に考える

それでは $N$ が十分大きいとして、$1$ から $N$ までの数で素数がどれくらいあるかを大雑把に考えてみましょう。

# 確率論的に考える

それでは $N$ が十分大きいとして、$1$ から $N$ までの数で素数がどれくらいあるかを大雑把に考えてみましょう。$N$ までの素数を $2, 3, \ldots, p$ とします。

# 確率論的に考える

それでは $N$ が十分大きいとして、$1$ から $N$ までの数で素数がどれくらいあるかを大雑把に考えてみましょう。$N$ までの素数を $2, 3, \ldots, p$ とします。$N$ 以下の数 $a$ を考えたときに $a$ が素数であるためには、$2, 3, \ldots, p$ のどれでも割り切れないことが条件となります。

# 確率論的に考える

それでは $N$ が十分大きいとして、$1$ から $N$ までの数で素数がどれくらいあるかを大雑把に考えてみましょう。$N$ までの素数を $2, 3, \ldots, p$ とします。$N$ 以下の数 $a$ を考えたときに $a$ が素数であるためには、$2, 3, \ldots, p$ のどれでも割り切れないことが条件となります。

いま素数 $p$ を固定して、$1$ から $N$ の数 $a$ を考えたときに $a$ が $p$ で割り切れなる確率は $\dfrac{1}{p}$ と考えられます。

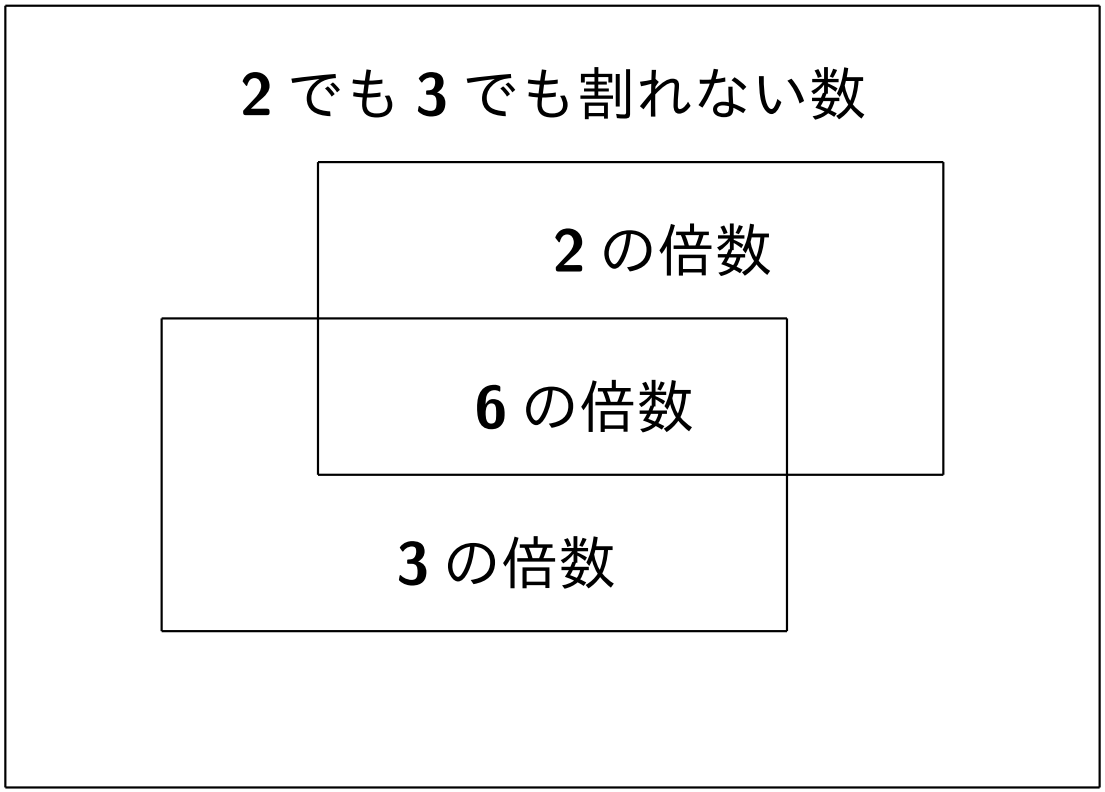
# 確率論的に考える

それでは $N$ が十分大きいとして、$1$ から $N$ までの数で素数がどれくらいあるかを大雑把に考えてみましょう。$N$ までの素数を $2, 3, \ldots, p$ とします。$N$ 以下の数 $a$ を考えたときに $a$ が素数であるためには、$2, 3, \ldots, p$ のどれでも割り切れないことが条件となります。

いま素数 $p$ を固定して、$1$ から $N$ の数 $a$ を考えたときに $a$ が $p$ で割り切れなる確率は $\dfrac{1}{p}$ と考えられます。従って $p$ で割り切れない確率は $1 - \dfrac{1}{p}$ となります。たとえば $2$ で割り切れない確率は $1 - \dfrac{1}{2}$ です。

# 確率論的に考える

次に **2** でも **3** でも割り切れない確率を考えましょう。**2** と **3** の両方で割り切れるということと **6** で割り切れるということは同値ですから、次のような図で考えてみることにします。



# 確率論的に考える

したがって $2$ でも $3$ でも割り切れない確率は

$$1-\frac{1}{2}-\frac{1}{3}+\frac{1}{2\cdot 3}=(1-\frac{1}{2})(1-\frac{1}{3})$$

となります。今 $N$ より小さい素数を $2,3,\cdots,p$ としてこれらのすべての素数で割り切れない確率は同様にして

$$C_p=(1-\frac{1}{2})(1-\frac{1}{3})\cdots(1-\frac{1}{p})$$

と考えられます。（この確率が意味があるのは、本当は $N$ が $p$ よりかなり大きい時ですが、その点は少しごまかしています。）

# 確率論的に考える

この

$$C_p = (1 - \frac{1}{2})(1 - \frac{1}{3}) \cdots (1 - \frac{1}{p})$$

は十分大きな数 $a$ が $2, 3, \ldots, p$ で割れない確率ですから 1 以下になりますが、$p$ が大きくなったとき、どのようなふるまいをするのでしょうか？

# 確率論的に考える

この

$$C_p = (1 - \frac{1}{2})(1 - \frac{1}{3}) \cdots (1 - \frac{1}{p})$$

は十分大きな数 $a$ が $2, 3, \ldots, p$ で割れない確率ですから $1$ 以下になりますが、$p$ が大きくなったとき、どのようなふるまいをするのでしょうか？$p$ が大きくなったとき、$1$ よりも小さいものをたくさん掛けていくので、どんどん小さくなっていくと思われますが、どういった速さで小さくなっていくでしょうか、次に考えてみることにします。

# $1/C_p$ の大きさ

ここでは $C_p$ がどれくらい小さくなるかを考えるために、その逆数 $\dfrac{1}{C_p}$ がどれくらい大きくなるかを見てみましょう。まず

$$\begin{aligned}&(1-r)(1+r+\cdots+r^{n-1})\\=&(1+r+\cdots+r^{n-1})-(r+\cdots+r^{n-1}+r^n)\\=&1-r^n\end{aligned}$$

という等式から次の公式が得られます。

# $1/C_p$ の大きさ

ここでは $C_p$ がどれくらい小さくなるかを考えるために、その逆数 $\dfrac{1}{C_p}$ がどれくらい大きくなるかを見てみましょう。まず

$$\begin{aligned}&(1-r)(1+r+\cdots+r^{n-1})\\=&(1+r+\cdots+r^{n-1})-(r+\cdots+r^{n-1}+r^n)\\=&1-r^n\end{aligned}$$

という等式から次の公式が得られます。

**公式 (等比級数の和の公式)**

$r \neq 1, n = 2, \ldots$ とする。このとき次が成り立つ。

$$1+r+\cdots+r^{n-1} = \frac{1-r^n}{1-r}$$

この公式に $r = \frac{1}{2}$ を代入して $n$ が無限のときの極限を考えるとつぎの式がえられれます。

$$1 + (\frac{1}{2}) + (\frac{1}{2})^2 + (\frac{1}{2})^3 + \cdots = \frac{1}{1 - \frac{1}{2}}$$

ここで左は無限の和を表し、それがある値に収束して右辺に等しくなるということです。

この公式に $r = \frac{1}{2}$ を代入して $n$ が無限のときの極限を考えるとつぎの式がえられれます。

$$1 + (\frac{1}{2}) + (\frac{1}{2})^2 + (\frac{1}{2})^3 + \cdots = \frac{1}{1 - \frac{1}{2}}$$

ここで左は無限の和を表し、それがある値に収束して右辺に等しくなるということです。この等式を

$$\frac{1}{C_p} = \frac{1}{1 - \frac{1}{2}} \cdot \frac{1}{1 - \frac{1}{3}} \cdots \frac{1}{1 - \frac{1}{p}}$$

にあてはめてみましょう。

$$\frac{1}{C_p} = \left(1 + (\frac{1}{2}) + (\frac{1}{2})^2 + (\frac{1}{2})^3 + \cdots\right)$$
$$\left(1 + (\frac{1}{3}) + (\frac{1}{3})^2 + (\frac{1}{3})^3 + \cdots\right)$$
$$\cdots$$
$$\left(1 + (\frac{1}{p}) + (\frac{1}{p})^2 + (\frac{1}{p})^3 + \cdots\right)$$

を展開する形になります。

$$\begin{aligned}\frac{1}{C_p} =& \left(1 + (\frac{1}{2}) + (\frac{1}{2})^2 + (\frac{1}{2})^3 + \cdots\right) \\ & \left(1 + (\frac{1}{3}) + (\frac{1}{3})^2 + (\frac{1}{3})^3 + \cdots\right) \\ & \cdots \\ & \left(1 + (\frac{1}{p}) + (\frac{1}{p})^2 + (\frac{1}{p})^3 + \cdots\right)\end{aligned}$$

を展開する形になります。これは各因子の中から一つの項を取り出してそれをかけ、すべての取り出し方に関する和を取るわけですから、$2, 3, \ldots, p$ を素因数にもつ $n$ に関して重複なく $\frac{1}{n}$ の値の和をとることになります。

これは式で書けば、

$$\frac{1}{C_p} = \sum_{n \text{ の素因数は } 2,3,\ldots,p \text{ に含まれる}} \frac{1}{n}$$

の形になります。$\sum$（シグマ記号）は高校でも習いますが、和の記号です。その下は和をとるべき $n$ の条件を書きました。実際右辺は無限の和になります。

これは式で書けば、

$$\frac{1}{C_p} = \sum_{n \text{ の素因数は } 2,3,\ldots,p \text{ に含まれる}} \frac{1}{n}$$

の形になります。$\sum$（シグマ記号）は高校でも習いますが、和の記号です。その下は和をとるべき $n$ の条件を書きました。実際右辺は無限の和になります。$p$ が $N$ を超えない最大の素数とすれば、$1$ から $N$ までの数の素因数はすべて $2,3,\ldots,p$ に含まれますから、

これは式で書けば、

$$\frac{1}{C_p} = \sum_{n \text{ の素因数は } 2,3,\ldots,p \text{ に含まれる}} \frac{1}{n}$$

の形になります。$\sum$（シグマ記号）は高校でも習いますが、和の記号です。その下は和をとるべき $n$ の条件を書きました。実際右辺は無限の和になります。$p$ が $N$ を超えない最大の素数とすれば、$1$ から $N$ までの数の素因数はすべて $2,3,\ldots,p$ に含まれますから、

$$\sum_{i=1}^{N} \frac{1}{i} \leq \frac{1}{C_p}$$

という等式が得られます。左辺のシグマ記号は $\frac{1}{i}$ を $i$ が $1$ から $N$ まで動かした和のことです。

# $\sum_{i=1}^{N} \frac{1}{i}$ の大きさ

それでは和

$$\sum_{i=1}^{N} \frac{1}{i} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{N}$$

の大きさを考えましょう。この和は等比級数の和などのように $N$ までの和の簡単な公式はありません。

# $\sum_{i=1}^{N} \frac{1}{i}$ の大きさ

それでは和

$$\sum_{i=1}^{N} \frac{1}{i} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{N}$$

の大きさを考えましょう。この和は等比級数の和などのように $N$ までの和の簡単な公式はありません。しかし、この和は積分を用いると大体の大きさを知ることができます。ここでは $N = 2^n$ のときに限って初等的に大雑把に大きさを計ってみましょう。

# $\sum_{i=1}^{N} \frac{1}{i}$ の大きさ

それでは和

$$\sum_{i=1}^{N} \frac{1}{i} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{N}$$

の大きさを考えましょう。この和は等比級数の和などのように $N$ までの和の簡単な公式はありません。しかし、この和は積分を用いると大体の大きさを知ることができます。ここでは $N = 2^n$ のときに限って初等的に大雑把に大きさを計ってみましょう。次のページを見てください。

# $\sum_{i=1}^{N} \frac{1}{i}$ の大きさ

$$1+\frac{1}{2}+\underbrace{\frac{1}{3}+\frac{1}{4}}+\underbrace{\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}}+\cdots+\underbrace{\frac{1}{2^{n-1}+1}+\cdots+\frac{1}{2^n}}$$

$$\geq 1+\frac{1}{2}+\underbrace{\frac{1}{4}+\frac{1}{4}}+\underbrace{\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}}+\cdots+\underbrace{\frac{1}{2^n}+\cdots+\frac{1}{2^n}}$$

$$\geq 1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\cdots+\frac{1}{2}=1+\frac{n}{2}$$

# $\sum_{i=1}^{N} \frac{1}{i}$ の大きさ

$$
\begin{aligned}
&1+\frac{1}{2}+\underbrace{\frac{1}{3}+\frac{1}{4}}+\underbrace{\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}}+\cdots+\underbrace{\frac{1}{2^{n-1}+1}+\cdots+\frac{1}{2^n}}\\
\geq&1+\frac{1}{2}+\underbrace{\frac{1}{4}+\frac{1}{4}}+\underbrace{\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}}+\cdots+\underbrace{\frac{1}{2^n}+\cdots+\frac{1}{2^n}}\\
\geq&1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\cdots+\frac{1}{2}=1+\frac{n}{2}
\end{aligned}
$$

したがって

$$\frac{1}{C_p} \geq \sum_{i=1}^{N} \frac{1}{i} \geq 1+\frac{n}{2}$$

となります。

従って $C_p \leq \dfrac{2}{n+2} = \dfrac{2}{\log_2 N + 2}$ が成り立ちます。ここで記号 $\log$ は対数と呼ばれる記号です。（$N = 2^n$ という式を思い出しておいてください。）$n$ は $N$ に対して非常にゆっくり大きくなる関数です。

従って $C_p \leq \dfrac{2}{n+2} = \dfrac{2}{\log_2 N + 2}$ が成り立ちます。ここで記号 $\log$ は対数と呼ばれる記号です。（$N = 2^n$ という式を思い出しておいてください。）$n$ は $N$ に対して非常にゆっくり大きくなる関数です。この式からわかることは、素数の密度は非常にゆっくり $0$ に近づくものでは、抑えられることがわかるということです。

従って $C_p \leq \dfrac{2}{n+2} = \dfrac{2}{\log_2 N + 2}$ が成り立ちます。ここで記号 $\log$ は対数と呼ばれる記号です。（$N = 2^n$ という式を思い出しておいてください。）$n$ は $N$ に対して非常にゆっくり大きくなる関数です。この式からわかることは、素数の密度は非常にゆっくり $0$ に近づくものでは、抑えられることがわかるということです。そして実際はこの評価はほとんど最良の評価なのです。つまり次に示す素数定理により、これ以上著しくよい評価は得られないのです。

# 素数定理

次の定理が知られています。

## 定理 (素数定理（アダマール、ド・ラ・バレ・プサン）)

# 素数定理

次の定理が知られています。

**定理 (素数定理（アダマール、ド・ラ・バレ・プサン）)**

$P(n)$ を 1 から $n$ までの間の素数の数とすると、

$$\lim_{n\to\infty} \frac{P(n)\log(n)}{n} = 1$$

となる。つまり、1 から $n$ までにある素数の密度は $\dfrac{1}{\log(x)}$ である。

この定理における対数 log の底はネーピアの定数とよばれるもので、およそ

$$e = 2.718281828459045\cdots$$

となります。

# 素数定理

この式は数学の巨星ガウスの予見したことでもあります。$\log(x)$ の値はだいたい次のようになります。

# 素数定理

この式は数学の巨星ガウスの予見したことでもあります。$\log(x)$ の値はだいたい次のようになります。

| $x$ | $\log(x)$ | $x$ | $\log(x)$ |
|---|---|---|---|
| **10** | **2.30258509** | **10000** | **9.21034037** |
| **100** | **4.60517018** | **100000** | **11.51292546** |
| **1000** | **6.90775527** | **1000000** | **13.81551055** |

つまり **10** 万位までの数で考えれば **11** 個か **12** 個に一つは素数がある勘定になります。

# 素数定理

この式は数学の巨星ガウスの予見したことでもあります。$\log(x)$ の値はだいたい次のようになります。

| $x$ | $\log(x)$ | $x$ | $\log(x)$ |
|---|---|---|---|
| **10** | **2.30258509** | **10000** | **9.21034037** |
| **100** | **4.60517018** | **100000** | **11.51292546** |
| **1000** | **6.90775527** | **1000000** | **13.81551055** |

つまり **10** 万位までの数で考えれば **11** 個か **12** 個に一つは素数がある勘定になります。

素数って、たくさんある！素敵 ♡ とは思いませんか？

# 素数定理

この式は数学の巨星ガウスの予見したことでもあります。$\log(x)$ の値はだいたい次のようになります。

| $x$ | $\log(x)$ | $x$ | $\log(x)$ |
|---|---|---|---|
| **10** | **2.30258509** | **10000** | **9.21034037** |
| **100** | **4.60517018** | **100000** | **11.51292546** |
| **1000** | **6.90775527** | **1000000** | **13.81551055** |

つまり **10** 万位までの数で考えれば **11** 個か **12** 個に一つは素数がある勘定になります。

素数って、たくさんある！素敵 ♡ とは思いませんか？

→ 実は素数がたくさんあることは暗号の鍵を作りやすくするのに役立っている。

# 素数定理

６桁の数を考えたときに確率的には $10$ 個から $14$ 個に一つは素数があることになります。

# 素数定理

6 桁の数を考えたときに確率的には $10$ 個から $14$ 個に一つは素数があることになります。6 桁の数は全部で $900{,}000$ 個あるわけですが、そのうち仮に素数が $14$ 個に一個であったとしても約 $\dfrac{900,000}{14} = 64286$ 個あることになります。

# 素数定理

6 桁の数を考えたときに確率的には 10 個から 14 個に一つは素数があることになります。6 桁の数は全部で 900,000 個あるわけですが、そのうち仮に素数が 14 個に一個であったとしても約 $\frac{900,000}{14} = 64286$ 個あることになります。(実際は計算機の計算で 6 桁の素数は 68906 個あります。)

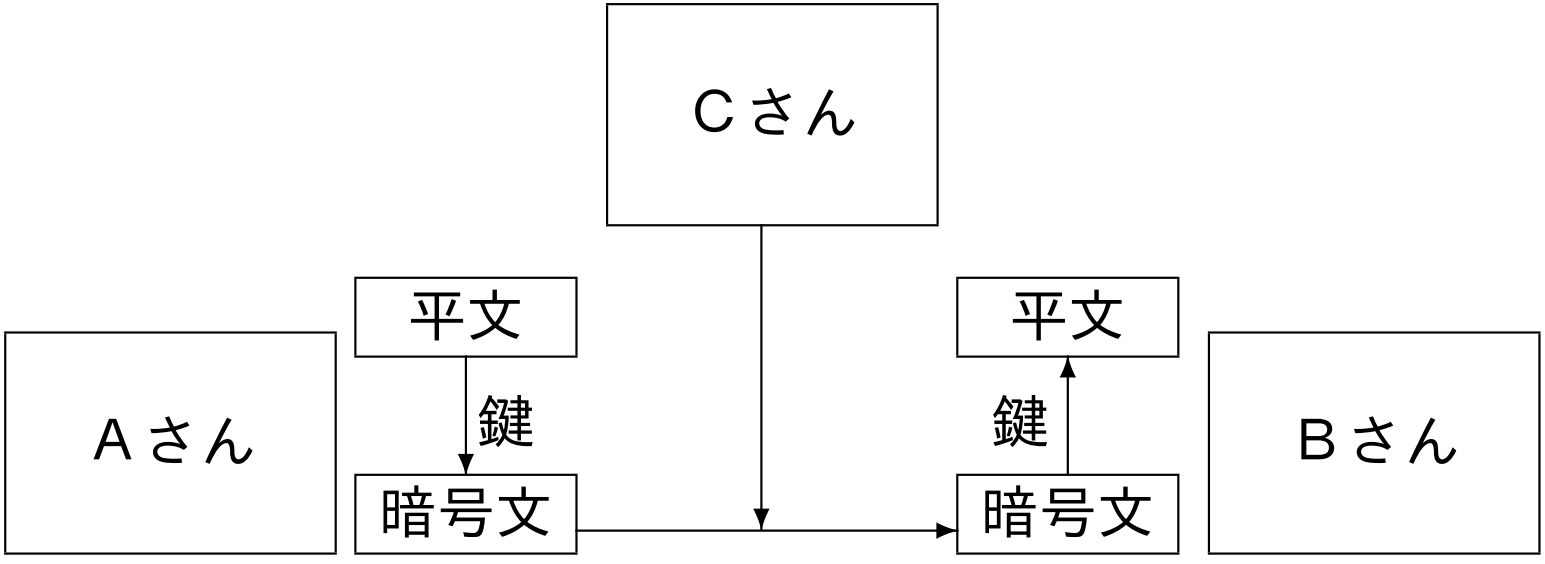
暗号に素数が使われるのですが、実際の暗号には二つの素数を掛けて 1024 ビット=300 桁になるくらいの数が使われます。

# 公開鍵暗号

# 公開鍵暗号

ここでは公開鍵暗号について述べることにします。ここで暗号というのはインターネットなどで、クレジットカードの番号の様に目的とする相手にだけは解って、その他のまわりで傍受しているひとには解らないように情報を伝える手段です。次のページの図はＡさんがＢさんに情報を伝えようとしている図です。

# 暗号化の模式図




送りたい情報を平文といいます。これは第三者のCさんにしられてはいけないのでAさんは鍵を用いて暗号化します。これをBさんが受け取って平文になおします。これを復号といいます。

# シーザー暗号

たとえば何文字か５０音順に決まった文字数だけ文字をずらすという暗号を考えます。これはシーザー暗号と呼ばれる暗号です。このとき、ずらす文字数が「鍵」になります。

# シーザー暗号

たとえば何文字か５０音順に決まった文字数だけ文字をずらすという暗号を考えます。これはシーザー暗号と呼ばれる暗号です。このとき、ずらす文字数が「鍵」になります。

- たとえばＡさんは「あしたのあさこい」といった文章を送りたいとします。ずらす文字数は「後に３文字」とします。

# シーザー暗号

たとえば何文字か５０音順に決まった文字数だけ文字をずらすという暗号を考えます。これはシーザー暗号と呼ばれる暗号です。このとき、ずらす文字数が「鍵」になります。

- たとえばＡさんは「あしたのあさこい」といった文章を送りたいとします。ずらす文字数は「後に３文字」とします。
- この規則で文章を変換した「えそてふえせすお」という文を送ります。

# シーザー暗号

たとえば何文字か５０音順に決まった文字数だけ文字をずらすという暗号を考えます。これはシーザー暗号と呼ばれる暗号です。このとき、ずらす文字数が「鍵」になります。

- たとえばＡさんは「あしたのあさこい」といった文章を送りたいとします。ずらす文字数は「後に３文字」とします。
- この規則で文章を変換した「えそてふえせすお」という文を送ります。
- Ｂさんは送られた文章を復号のための鍵「３文字前にずらす」を使ってもとの文章にもどします。もとにもどすには、３文字という解読のための鍵が必要になります。

# シーザー暗号

シーザー暗号を成り立たせるためには、ＡさんとＢさんにだけ鍵がわかっていてＣさんには解らないようにすることが必要です。このような暗号システムを共通鍵暗号といいいます。

# シーザー暗号

シーザー暗号を成り立たせるためには、ＡさんとＢさんにだけ鍵がわかっていてＣさんには解らないようにすることが必要です。
このような暗号システムを共通鍵暗号といいいます。
この暗号システムだと、通信したい相手だけと、どうやって共通の鍵をもつか？という点が問題になります。

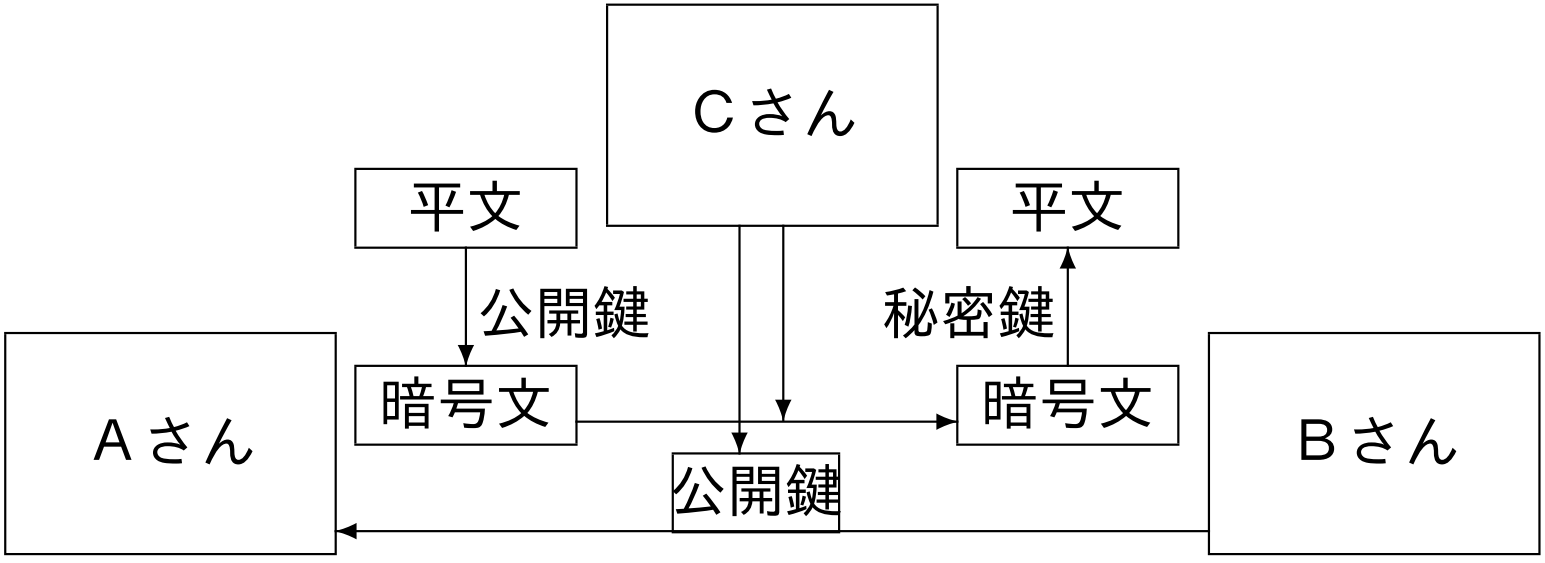
# シーザー暗号

シーザー暗号を成り立たせるためには、Ａさんとｂさんにだけ鍵がわかっていてＣさんには解らないようにすることが必要です。
このような暗号システムを共通鍵暗号といいいます。
この暗号システムだと、通信したい相手だけと、どうやって共通の鍵をもつか？という点が問題になります。
その問題を解決するのが次の公開鍵暗号です。

# シーザー暗号

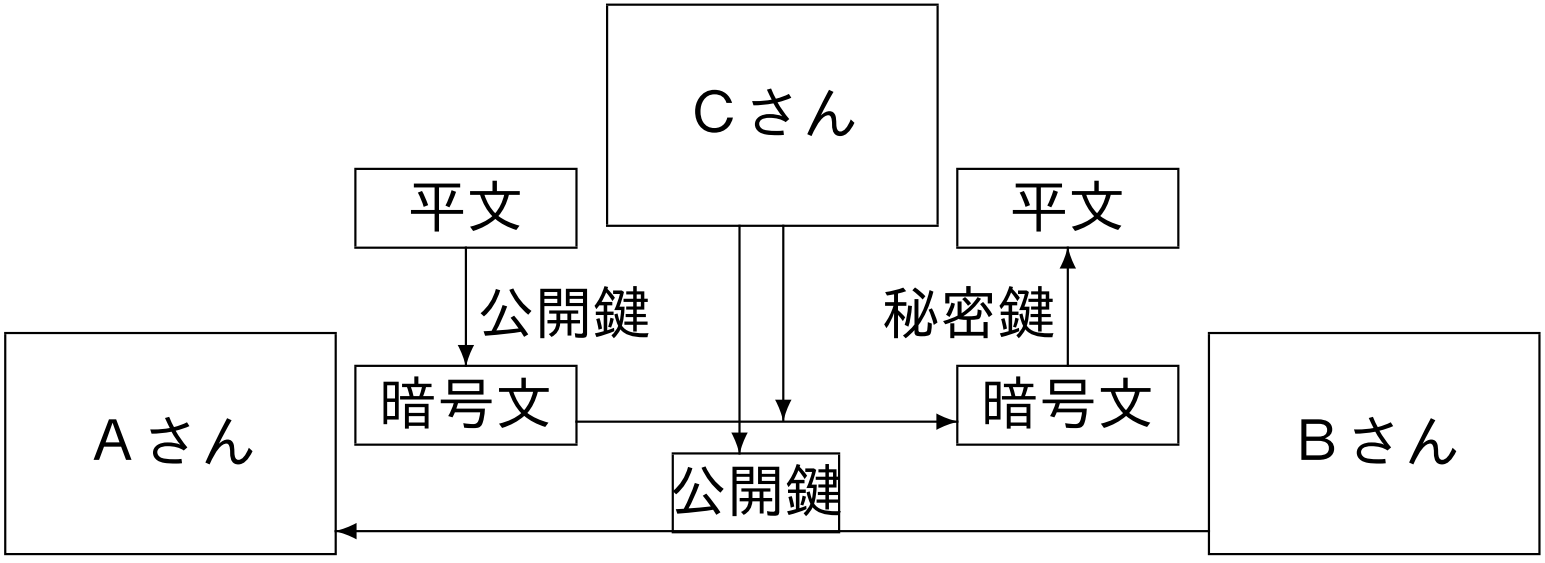
シーザー暗号を成り立たせるためには、ＡさんとＢさんにだけ鍵がわかっていてＣさんには解らないようにすることが必要です。
このような暗号システムを共通鍵暗号といいいます。
この暗号システムだと、通信したい相手だけと、どうやって共通の鍵をもつか？という点が問題になります。
その問題を解決するのが次の公開鍵暗号です。
次のページの図を見てください。

# 公開鍵暗号




公開鍵と秘密鍵の二つの鍵があることに注意してください。

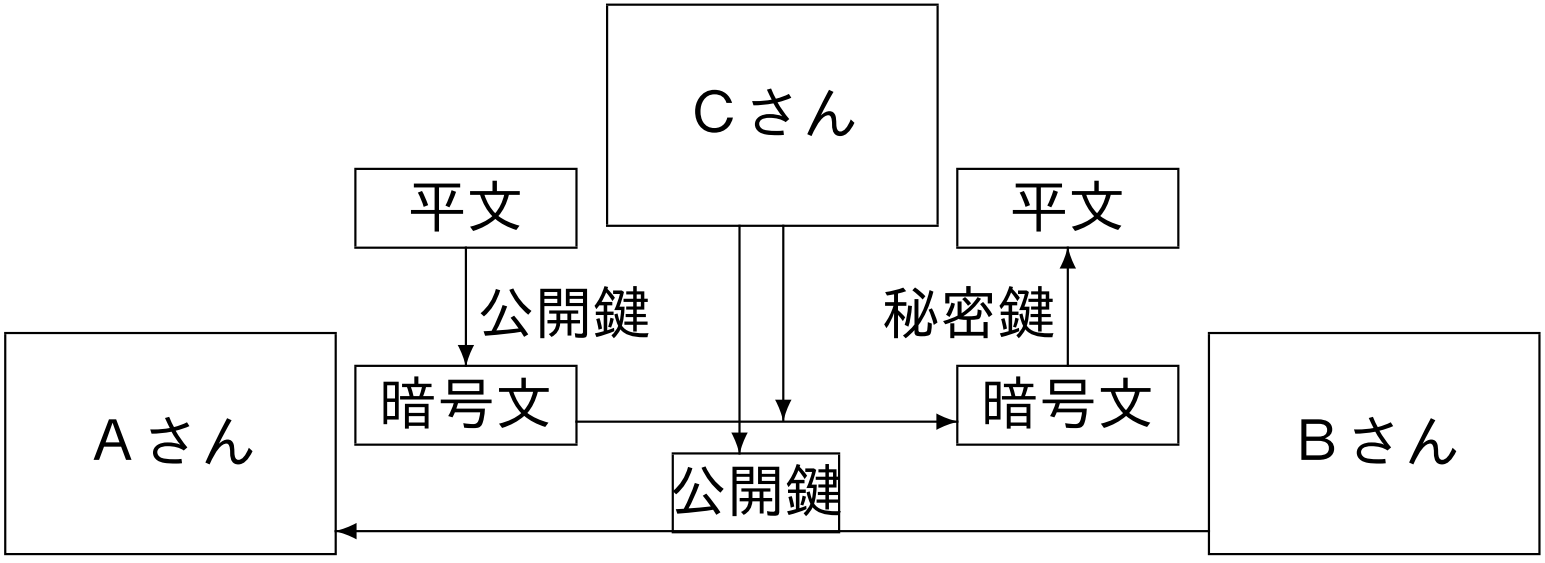
# 公開鍵暗号




公開鍵と秘密鍵の二つの鍵があることに注意してください。

- 公開鍵は暗号化用で秘密鍵は復号化用です。

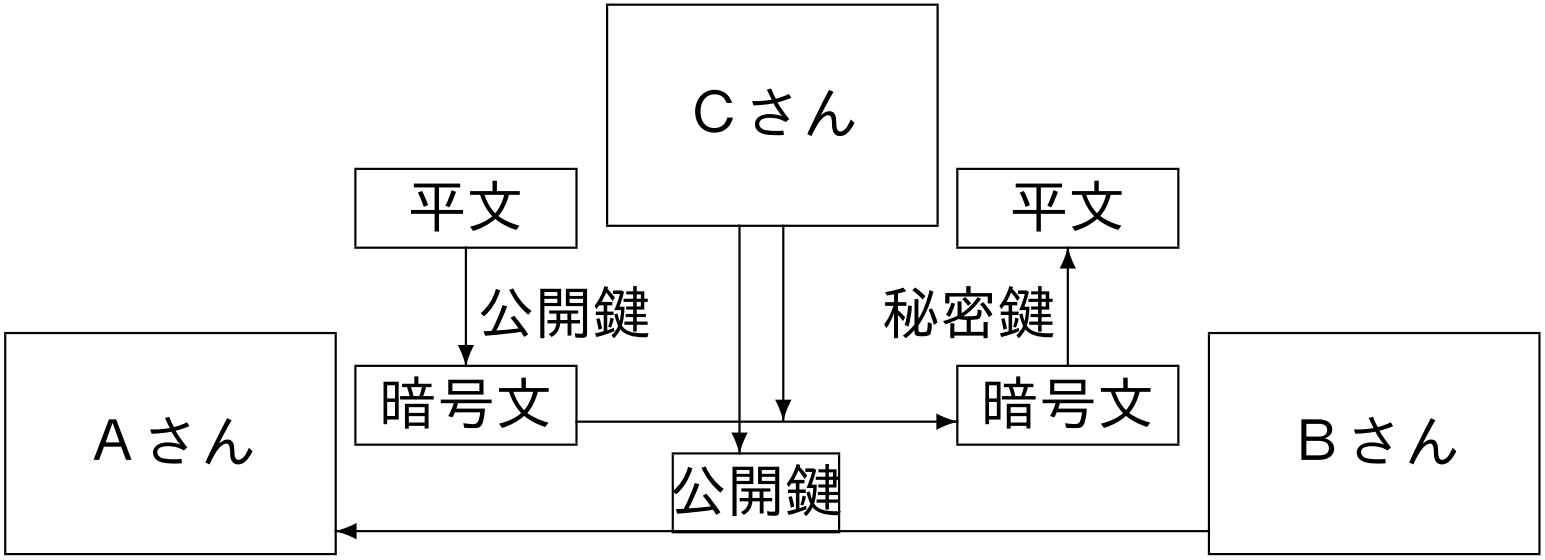
# 公開鍵暗号




公開鍵と秘密鍵の二つの鍵があることに注意してください。

- 公開鍵は暗号化用で秘密鍵は復号化用です。
- 公開鍵も秘密鍵もBさんが作り、公開鍵をAさんに送ります。

# 公開鍵暗号




公開鍵と秘密鍵の二つの鍵があることに注意してください。

- 公開鍵は暗号化用で秘密鍵は復号化用です。
- 公開鍵も秘密鍵もBさんが作り、公開鍵をAさんに送ります。
- ひとたび公開鍵で暗号化してしまうと、秘密鍵がないと復号化しにくい仕組みにしておきます。

暗号化のための公開鍵と復号化のための秘密鍵はペアでつくります。

公開鍵暗号で要請される鍵の性質

- 公開鍵、秘密鍵は容易に作り出すことができる。
- 公開鍵をもちいて、平文は容易に暗号化できる。
- 暗号文は秘密鍵を用いて容易に復号できる。
- 暗号文は公開鍵をしっていても、秘密鍵を知らなくては、復号化は著しく困難である。

公開鍵から秘密鍵が計算で求めることができても、そのために時間が著しくかかるのであれば、秘匿性が高く十分実用的である。

# RSA 暗号

前頁のような性質をもつ暗号として考えられたのが **RSA** 暗号（**Rivest-Sahmir-Adelman**）です。これは素数の次のような性質を用います。

- 大きな数に対してそれが素数かどうかな容易に判定できる。
- 二つの大きな素数をかけて得られた合成数を因数分解するのは大変時間がかかる。

# RSA 暗号

前頁のような性質をもつ暗号として考えられたのが **RSA** 暗号（**Rivest-Sahmir-Adelman**）です。これは素数の次のような性質を用います。

- 大きな数に対してそれが素数かどうかな容易に判定できる。
- 二つの大きな素数をかけて得られた合成数を因数分解するのは大変時間がかかる。

それでは **RSA** 暗号の仕組みについて説明しましょう。

# 鍵の作り方

まずは鍵の作り方を述べます。これはＢさんが行うことです。

# 鍵の作り方

まずは鍵の作り方を述べます。これはＢさんが行うことです。

- 大きな二つの異なる素数 $p < q$ を見つけます。

# 鍵の作り方

まずは鍵の作り方を述べます。これはＢさんが行うことです。

- 大きな二つの異なる素数 $p < q$ を見つけます。
- $(p-1)(q-1)$ と共通因数のない数 $e$ を選びます。

# 鍵の作り方

まずは鍵の作り方を述べます。これはＢさんが行うことです。

- 大きな二つの異なる素数 $p < q$ を見つけます。
- $(p-1)(q-1)$ と共通因数のない数 $e$ を選びます。
- ユークリッドの互除法を用いて $ed = c(p-1)(q-1)+1$ となるような $c, e, d$ をとります。

# 鍵の作り方

まずは鍵の作り方を述べます。これはＢさんが行うことです。

- 大きな二つの異なる素数 $p < q$ を見つけます。
- $(p-1)(q-1)$ と共通因数のない数 $e$ を選びます。
- ユークリッドの互除法を用いて $ed = c(p-1)(q-1)+1$ となるような $c, e, d$ をとります。
- $p, q$ の積 $n = pq$ を計算して $(n, e)$ を公開鍵、$(n, d)$ を秘密鍵とします。

# 鍵の作り方

まずは鍵の作り方を述べます。これはＢさんが行うことです。

- 大きな二つの異なる素数 $p < q$ を見つけます。
- $(p-1)(q-1)$ と共通因数のない数 $e$ を選びます。
- ユークリッドの互除法を用いて $ed = c(p-1)(q-1)+1$ となるような $c, e, d$ をとります。
- $p, q$ の積 $n = pq$ を計算して $(n, e)$ を公開鍵、$(n, d)$ を秘密鍵とします。

原理的には $n$ を因数分解してＢさんが鍵を作ったのと同様にして $e$ から $d$ を求めれば、公開鍵から秘密鍵が計算されるのですが、因数分解にはとても時間がかかるのです。

# フェルマーの小定理

暗号化や復号化のやり方をのべる前に整数論における次のフェルマーの小定理が復号化の際のキーポイントになります。$n$ を $2$ 以上の自然数としたとき、自然数 $a$ を $n$ で割ったあまり $r$ $(0 \leq r \leq n-1)$ を $a \pmod n$ と書きます。

# フェルマーの小定理

暗号化や復号化のやり方をのべる前に整数論における次のフェルマーの小定理が復号化の際のキーポイントになります。$n$ を $2$ 以上の自然数としたとき、自然数 $a$ を $n$ で割ったあまり $r$ $(0 \leq r \leq n-1)$ を $a \pmod n$ と書きます。

**定理 (一般化されたフェルマーの小定理)**

$p, q, c, d, e$ を今までのとおりとして、$pq = n$ とおく。$a$ $(0 \leq a \leq n-1)$ を $n$ と互いに素である自然数とする。このとき

$$a^{c(p-1)(q-1)+1} \pmod n = a$$

となる。

# 暗号化と復号化の方法

- Bさんはさっきの仕方で公開鍵 $(n, e)$ と秘密鍵 $(n, d)$ をつくります。公開鍵 $(n, e)$ をAさんにおくります。これは傍受者Cさんにも聞かれてしまうかもしれません。

# 暗号化と復号化の方法

- Ｂさんはさっきの仕方で公開鍵 $(n, e)$ と秘密鍵 $(n, d)$ をつくります。公開鍵 $(n, e)$ をＡさんにおくります。これは傍受者Ｃさんにも聞かれてしまうかもしれません。
- Ａさんは送りたい情報 $a$ $(< p)$ をもとに $b = a^e \pmod n$ を計算してＢさんにおくります。この計算は非常に速くできる。

# 暗号化と復号化の方法

- Ｂさんはさっきの仕方で公開鍵 $(n, e)$ と秘密鍵 $(n, d)$ をつくります。公開鍵 $(n, e)$ をＡさんにおくります。これは傍受者Ｃさんにも聞かれてしまうかもしれません。
- Ａさんは送りたい情報 $a$ $(< p)$ をもとに $b = a^e \pmod n$ を計算してＢさんにおくります。この計算は非常に速くできる。
- ＢさんはＡさんからもらった情報 $b$ を使って $b^d \pmod n$ を計算します。一般化されたフェルマーの小定理を用い、

$$\begin{aligned} b^d \pmod n &= (a^e)^d \pmod n \\ &= a^{c(p-1)(q-1)+1} \pmod n = a \end{aligned}$$

として $a$ が復元できました。

# 鍵の生成（例）

小さい数で鍵を作って見てみましょう。

# 鍵の生成（例）

小さい数で鍵を作って見てみましょう。

- 二つの異なる素数 $5$ と $11$ で実験してみます。$n = 55$ です。

# 鍵の生成（例）

小さい数で鍵を作って見てみましょう。

- 二つの異なる素数 $5$ と $11$ で実験してみます。$n = 55$ です。
- $(5-1)(11-1) = 40$ と共通因数のない数 $e = 7$ を選びます。

# 鍵の生成（例）

小さい数で鍵を作って見てみましょう。

- 二つの異なる素数 $5$ と $11$ で実験してみます。$n = 55$ です。
- $(5-1)(11-1) = 40$ と共通因数のない数 $e = 7$ を選びます。
- $ed = c(p-1)(q-1)+1$ となる数 $d, c$ を求めます。
  $7 \cdot 23 = 4(5-1)(7-1)+1$ となるので $d = 23, c = 4$ がとれます。

# 鍵の生成（例）

小さい数で鍵を作って見てみましょう。

- 二つの異なる素数 $5$ と $11$ で実験してみます。$n = 55$ です。
- $(5-1)(11-1) = 40$ と共通因数のない数 $e = 7$ を選びます。
- $ed = c(p-1)(q-1)+1$ となる数 $d, c$ を求めます。
  $7 \cdot 23 = 4(5-1)(7-1)+1$ となるので $d = 23, c = 4$ がとれます。
- 公開鍵を $(n, e) = (55, 7)$、秘密鍵を $(n, d) = (55, 23)$ とします。

# 暗号化と復号化

今度は暗号化と復号化をしてみます。

# 暗号化と復号化

今度は暗号化と復号化をしてみます。

- B さんは A さんに公開鍵 $(\mathbf{55}, \mathbf{7})$ を送ります。A さんは $p = 5$ より小さい情報が送ることができます。$a = 3$ としましょう。$3^e \pmod{n} = 3^7 \pmod{55} = 42$ と暗号化して A さんに送ります。

# 暗号化と復号化

今度は暗号化と復号化をしてみます。

- B さんは A さんに公開鍵 $(\mathbf{55}, \mathbf{7})$ を送ります。A さんは $p = 5$ より小さい情報が送ることができます。$a = 3$ としましょう。$3^e \pmod{n} = 3^7 \pmod{55} = 42$ と暗号化して A さんに送ります。
- A さんは $42$ という数字を受け取ったら、$42^d \pmod{n} = 42^{23} \pmod{55} = 3$ と計算して、欲しかった情報の $3$ が復元できました。

# 暗号化と復号化

今度は暗号化と復号化をしてみます。

- B さんは A さんに公開鍵 $(\mathbf{55}, \mathbf{7})$ を送ります。A さんは $p = 5$ より小さい情報が送ることができます。$a = 3$ としましょう。$3^e \pmod{n} = 3^7 \pmod{55} = 42$ と暗号化して A さんに送ります。
- A さんは $42$ という数字を受け取ったら、$42^d \pmod{n} = 42^{23} \pmod{55} = 3$ と計算して、欲しかった情報の $3$ が復元できました。
- C さんは $(\mathbf{55}, \mathbf{23})$ という鍵をしらないので復号できません。

# まとめ

インターネットで送る事ができる情報はすべてデジタル的な情報となりますが、目的の人にだけ解読できて、傍受者には解読できない仕組みをつくるのに離散的な数学である整数論が利用される。

# まとめ

インターネットで送る事ができる情報はすべてデジタル的な情報となりますが、目的の人にだけ解読できて、傍受者には解読できない仕組みをつくるのに離散的な数学である整数論が利用される。**RSA** 暗号において素数を用いて鍵を生成するが、鍵の生成が効率的に行われている根拠は素数がたくさんあるということである。

# まとめ

インターネットで送る事ができる情報はすべてデジタル的な情報となりますが、目的の人にだけ解読できて、傍受者には解読できない仕組みをつくるのに離散的な数学である整数論が利用される。**RSA** 暗号において素数を用いて鍵を生成するが、鍵の生成が効率的に行われている根拠は素数がたくさんあるということである。機密情報の安全は **RSA** 暗号においては因数分解の難しさという整数論の問題がかかわってきている。

# まとめ

インターネットで送る事ができる情報はすべてデジタル的な情報となりますが、目的の人にだけ解読できて、傍受者には解読できない仕組みをつくるのに離散的な数学である整数論が利用される。**RSA** 暗号において素数を用いて鍵を生成するが、鍵の生成が効率的に行われている根拠は素数がたくさんあるということである。機密情報の安全は **RSA** 暗号においては因数分解の難しさという整数論の問題がかかわってきている。実は **RSA** 暗号のほかにも整数論を基礎にした暗号理論、たとえば楕円曲線暗号などがあり、実際の場面で実用化れている。

# フェルマーの小定理

# フェルマーの小定理

$a, b$ を自然数とするとき $a, b$ に共通の素因数がないとき $a$ と $b$ は互いに素であるという。以下の話では自然数に $0$ も含める。

# フェルマーの小定理

$a, b$ を自然数とするとき $a, b$ に共通の素因数がないとき $a$ と $b$ は互いに素であるという。以下の話では自然数に $0$ も含める。

## 定理 (一般化されたフェルマーの小定理 (1))

# フェルマーの小定理

$a, b$ を自然数とするとき $a, b$ に共通の素因数がないとき $a$ と $b$ は互いに素であるという。以下の話では自然数に $0$ も含める。

## 定理 (一般化されたフェルマーの小定理 (1))

$p, q$ を素数として $a$ を $0 \leq a \leq pq - 1$ なる自然数で $p, q$ と互いに素とすると、

$$a^{(p-1)(q-1)} (\mathrm{mod}\, pq) = a$$

が成り立つ。

# フェルマーの小定理

$a, b$ を自然数とするとき $a, b$ に共通の素因数がないとき $a$ と $b$ は互いに素であるという。以下の話では自然数に $0$ も含める。

**定理 (一般化されたフェルマーの小定理 (1))**

$p, q$ を素数として $a$ を $0 \leq a \leq pq - 1$ なる自然数で $p, q$ と互いに素とすると、

$$a^{(p-1)(q-1)} (\mathrm{mod}\, pq) = a$$

が成り立つ。

この話で自然数 $n \geq 2$ に対して

$$(a(\mathrm{mod}\, n) b(\mathrm{mod}\, n))(\mathrm{mod}\, n) = ab(\mathrm{mod}\, n)$$

が成り立つ事を用いる。（この証明は省略する。）

# 証明のための補助定理

# 証明のための補助定理

$n = pq$ とおいて、集合 $A$ を次の様に定義する。

# 証明のための補助定理

$n = pq$ とおいて、集合 $A$ を次の様に定義する。

$$A = \{a \mid 0 \leq a \leq n-1, a \text{ と } pq \text{ は互いに素 }\}$$

# 証明のための補助定理

$n = pq$ とおいて、集合 $A$ を次の様に定義する。

$$A = \{a \mid 0 \leq a \leq n-1, a \text{ と } pq \text{ は互いに素 }\}$$

このとき $A$ の元の個数は $(p-1)(q-1)$ となることに注意しよう。

# 証明のための補助定理

$n = pq$ とおいて、集合 $A$ を次の様に定義する。

$$A = \{a \mid 0 \leq a \leq n-1, a \text{ と } pq \text{ は互いに素 }\}$$

このとき $A$ の元の個数は $(p-1)(q-1)$ となることに注意しよう。

**定理**

(1) $a, b$ が $A$ の元であれば、$ab \pmod n$ も $A$ の元である。
(2) $a_1, a_2, b$ を $A$ の元として、$a_1 b \pmod n = a_2 b \pmod n$ なら $a_1 = a_2$ となる。

# 補助定理の証明

## 証明

# 補助定理の証明

## 証明

(1) $a, b$ ともに $p$ で割れなければ、$ab$ も $p$ で割れない。

# 補助定理の証明

## 証明

(1) $a, b$ ともに $p$ で割れなければ、$ab$ も $p$ で割れない。同様に $ab$ は $q$ でも割れないので $ab$ は $pq$ と互いに素である。

# 補助定理の証明

## 証明

(1) $a, b$ ともに $p$ で割れなければ、$ab$ も $p$ で割れない。同様に $ab$ は $q$ でも割れないので $ab$ は $pq$ と互いに素である。
(2) $a_1 \geq a_2$ と仮定してもよい。$a_1 b (\mathrm{mod}\, n) = a_1 b (\mathrm{mod}\, n)$ であれば $(a_1 - a_2)b$ は $p$ で割れる。

# 補助定理の証明

## 証明

(1) $a, b$ ともに $p$ で割れなければ、$ab$ も $p$ で割れない。同様に $ab$ は $q$ でも割れないので $ab$ は $pq$ と互いに素である。
(2) $a_1 \geq a_2$ と仮定してもよい。$a_1 b (\mathrm{mod}\, n) = a_1 b (\mathrm{mod}\, n)$ であれば $(a_1 - a_2)b$ は $p$ で割れる。$b$ は $p$ で割れないので $(a_1 - a_2)$ が $p$ で割れる。

# 補助定理の証明

## 証明

(1) $a, b$ ともに $p$ で割れなければ、$ab$ も $p$ で割れない。同様に $ab$ は $q$ でも割れないので $ab$ は $pq$ と互いに素である。
(2) $a_1 \geq a_2$ と仮定してもよい。$a_1 b (\mathrm{mod}\, n) = a_1 b (\mathrm{mod}\, n)$ であれば $(a_1 - a_2)b$ は $p$ で割れる。$b$ は $p$ で割れないので $(a_1 - a_2)$ が $p$ で割れる。同様にして $a_1 - a_2$ は $q$ でも割れるので、$(a_1 - a_2)$ は $pq$ でわれる。

# 補助定理の証明

## 証明

(1) $a, b$ ともに $p$ で割れなければ、$ab$ も $p$ で割れない。同様に $ab$ は $q$ でも割れないので $ab$ は $pq$ と互いに素である。
(2) $a_1 \geq a_2$ と仮定してもよい。$a_1 b (\mathrm{mod}\, n) = a_1 b (\mathrm{mod}\, n)$ であれば $(a_1 - a_2)b$ は $p$ で割れる。$b$ は $p$ で割れないので $(a_1 - a_2)$ が $p$ で割れる。同様にして $a_1 - a_2$ は $q$ でも割れるので、$(a_1 - a_2)$ は $pq$ でわれる。従って $(a_1 - a_2)(\mathrm{mod}\, n) = 0$ である。従って $a_1 = a_2$ である。

# 一般化されたフェルマーの小定理 (1) の証明

# 一般化されたフェルマーの小定理 (1) の証明

$m = (p-1)(q-1)$ を $A$ の元の個数とする。

# 一般化されたフェルマーの小定理 (1) の証明

$m = (p-1)(q-1)$ を $A$ の元の個数とする。

## 証明

# 一般化されたフェルマーの小定理 (1) の証明

$m = (p-1)(q-1)$ を $A$ の元の個数とする。

## 証明

$A = \{b_1, \ldots, b_m\}$ とおき、$a \in A$ とする。

# 一般化されたフェルマーの小定理 (1) の証明

$m = (p-1)(q-1)$ を $A$ の元の個数とする。

## 証明

$A = \{b_1, \ldots, b_m\}$ とおき、$a \in A$ とする。$c_1, \ldots, c_m$ を $c_1 = ab_1 \pmod n, \ldots, c_m = ab_m \pmod n$ で定める。

# 一般化されたフェルマーの小定理 (1) の証明

$m = (p-1)(q-1)$ を $A$ の元の個数とする。

## 証明

$A = \{b_1, \ldots, b_m\}$ とおき、$a \in A$ とする。$c_1, \ldots, c_m$ を $c_1 = ab_1 \pmod n, \ldots, c_m = ab_m \pmod n$ で定める。補助定理 (1) より $c_1, \ldots, c_m \in A$ である。

# 一般化されたフェルマーの小定理 (1) の証明

$m = (p-1)(q-1)$ を $A$ の元の個数とする。

## 証明

$A = \{b_1, \ldots, b_m\}$ とおき、$a \in A$ とする。$c_1, \ldots, c_m$ を $c_1 = ab_1 (\mathrm{mod}\, n), \ldots, c_m = ab_m (\mathrm{mod}\, n)$ で定める。補助定理 (1) より $c_1, \ldots, c_m \in A$ である。また $i \neq j$ であれば、$b_i \neq b_j$ なので補助定理 (2) により $c_i \neq c_j$ がいえる。

# 一般化されたフェルマーの小定理 (1) の証明

$m = (p-1)(q-1)$ を $A$ の元の個数とする。

## 証明

$A = \{b_1, \ldots, b_m\}$ とおき、$a \in A$ とする。$c_1, \ldots, c_m$ を $c_1 = ab_1 (\mathrm{mod}\, n), \ldots, c_m = ab_m (\mathrm{mod}\, n)$ で定める。補助定理 (1) より $c_1, \ldots, c_m \in A$ である。また $i \neq j$ であれば、$b_i \neq b_j$ なので補助定理 (2) により $c_i \neq c_j$ がいえる。$A$ の元の個数を考えると $A = \{c_1, \ldots, c_m\}$ がいえる。

# 一般化されたフェルマーの小定理 (1) の証明

$m = (p-1)(q-1)$ を $A$ の元の個数とする。

## 証明

$A = \{b_1, \ldots, b_m\}$ とおき、$a \in A$ とする。$c_1, \ldots, c_m$ を $c_1 = ab_1 (\mathrm{mod}\, n), \ldots, c_m = ab_m (\mathrm{mod}\, n)$ で定める。補助定理 (1) より $c_1, \ldots, c_m \in A$ である。また $i \neq j$ であれば、$b_i \neq b_j$ なので補助定理 (2) により $c_i \neq c_j$ がいえる。$A$ の元の個数を考えると $A = \{c_1, \ldots, c_m\}$ がいえる。従って

$$
\begin{aligned}
& b_1 \cdots b_m (\mathrm{mod}\, n) \\
=& c_1 \cdots c_m (\mathrm{mod}\, n) \\
=& ((ab_1) \cdots (ab_m)) (\mathrm{mod}\, n) \\
=& (a^m (\mathrm{mod}\, n))(b_1 \cdots b_m (\mathrm{mod}\, n)) (\mathrm{mod}\, n)
\end{aligned}
$$

# 一般化されたフェルマーの小定理 (1) の証明（続き）

## 証明

# 一般化されたフェルマーの小定理 (1) の証明（続き）

## 証明

ここで等式

$$\begin{aligned} & b_1 \cdots b_m (\mathrm{mod}\, n) \\ =& (a^m (\mathrm{mod}\, n))(b_1 \cdots b_m (\mathrm{mod}\, n))(\mathrm{mod}\, n) \end{aligned}$$

に対して補助定理の (2) を用いて $a^m (\mathrm{mod}\, n) = 1$ がいえる。

# 一般化されたフェルマーの小定理 (1) の証明（続き）

## 証明

ここで等式

$$\begin{aligned} & b_1 \cdots b_m (\mathrm{mod}\, n) \\ =& (a^m (\mathrm{mod}\, n))(b_1 \cdots b_m (\mathrm{mod}\, n))(\mathrm{mod}\, n) \end{aligned}$$

に対して補助定理の (2) を用いて $a^m (\mathrm{mod}\, n) = 1$ がいえる。

一般化されたフェルマーの小定理は次のように示される。

$$\begin{aligned} a^{cm+1} (\mathrm{mod}\, n) =& ((a^m (\mathrm{mod}\, n))^c (a (\mathrm{mod}\, n)))(\mathrm{mod}\, n) \\ =& (1^c (a (\mathrm{mod}\, n)))(\mathrm{mod}\, n) \\ =& a \end{aligned}$$