RSA 暗号から代数をみてみよう！

Nova： Twitter @prod103kanre

2020/09/25

1　はじめに

読者は高校生や数学科でない大学生を想定しています。mod(割った余りを考えるやつ) にある程度慣れていることは仮定しますがそれ以外の知識は仮定しません。また筆者の TEX の練習も兼ねているので書き方や内容が乱れていると思いますが大目に見てください。

2　RSA 暗号について

2.1　RSA 暗号とは？

RSA 暗号とは公開鍵と呼ばれる 2 つの数を使って送りたい情報 (数字) を暗号化し、秘密鍵と呼ばれる数字を使って復号する暗号です。暗号の安全性は十分大きな数では素因数分解が難しいことに拠ります。

2.2　暗号化してみよう

暗号を作るには予め用意された公開鍵といわれる 2 つの数、r と e を使います。r は実は 2 つの素数 p,q の積ですが、この p, q は公開しません。また e は、$(p-1)(q-1)$ との最大公約数が 1 となるようにとります。これを公開してしまうと誰でも復号できてしまいます。では実際に暗号化しましょう。暗号化したい数字 x をとります。これは r 未満である必要があるので必要なだけ大きく用意しておく必要があります。この x を e 乗した x^e が暗号化された数字です。

余談ですが、n 乗は $o(\log n)$ で計算でき十分高速なので実用に耐えます。

2.3　復号してみよう

復号するひとは r がなんの素数の積かを知っているので、それを p,q とおきましょう (つまり $r = pq$)。ところで e は、$\gcd(e, (p-1)(q-1)) = 1$ となるようにとっていたので、$L := (p-1)(q-1)$ と L を定めておき、

$$^{\exists}d, k \in \mathbb{Z} \ \text{ s.t. } \ de - kL = 1 \tag{1}$$

となる d, k がとれます。また、

$$x^L \equiv 1 \pmod{r} \tag{2}$$

なので、

$$\begin{aligned} x^{ed} &\equiv x^{1+kL} \pmod{r} \\ &\equiv x \times 1^k \pmod{r} \\ &\equiv x \pmod{r} \end{aligned}$$

となり、暗号化されて受信した数 x^e を d 乗すると暗号化する前の x が復元できます。ただし上の (1) と (2) は非自明なので証明する必要があります。そこで以下の定理が欲しくなります。

定理 1. $x, y \in \mathbb{Z}$ かつ $\gcd(x, y) = 1$ なる x, y に対し、$^{\exists}a, b \in \mathbb{Z}$ s.t. $ax + by = 1$

定理 2. フェルマーの小定理
素数 p、整数 a に対して、$a^p \equiv a \pmod{p}$
特に $\gcd(p, a) = 1$ なら、$a^{p-1} \equiv 1 \pmod{p}$

定理 3. p, q は素数で、$x \in \mathbb{Z}$ が $x \equiv 1 \pmod{p}$ かつ $x \equiv 1 \pmod{q}$ なら、$x \equiv 1 \pmod{pq}$

定理 1 より (1) がわかり、定理 2 と定理 3 を用いて (2) もわかります。以降の章でこの 3 つの証明を高校数学で先ず行い、そして代数学を用いてもう一度捉え直します。

2.4 試しに暗号を作ってみよう

暗号を作りたい人が、$r = 35$ と $e = 5$ の公開鍵を用いて、$x = 2$ を暗号化するとします (勿論 r は簡単に素因数分解できないくらい大きくすべきですが計算しやすいよう小さくしています)。では先ず、

$$2 \mapsto 2^5 \equiv 32 \pmod{35}$$

となるので、32 が暗号です。では次にこれを復号します。復号する人は $r = 35 = 5 \times 7$ と知っているので、$L = (5 - 1)(7 - 1) = 24$ がわかります。また $5 \times 5 - 1 \times 24 = 1$ なので $d = 5$ もわかります。以上より、

$$32 \mapsto 32^5 \equiv 2 \pmod{35}$$

となり復号できていることが確認できます。

3 高校流で理解しよう！

先ず、定理 1 を証明するたに以下の命題を示そう。

命題 1. ユークリッドの互除法
$a = qb + r \Rightarrow \gcd(a, b) = \gcd(b, r)$ となる。

Proof. ググったらでてきます。 □

命題 1 を使えば、定理 1 を証明できます。

Proof. 定理 1
$x \geq y$ として、$a_1 = x, a_2 = y$ とおく。以降、a_n を順次ユークリッドの互除法のやり方に従って作っていくと $^{\exists}n \in \mathbb{N}$ ： $a_n = \gcd(x, y)$ となる。作った式を用いてもとに戻すと欲しかった a, b が求められる。 □

次は定理 2 と定理 3 をそれぞれ証明します。

Proof. 定理 2
帰納法で示す。

$$(n+1)^p \equiv n^p + 1 \pmod{p}$$

となる。上式は二項定理を用いて分解した式のコンビネーション部分をよく見ると実はすべて p の倍数になっていることからわかる。よって、

$$n^p \equiv n \pmod{p} \Rightarrow (n+1)^p \equiv n+1 \pmod{p}$$

$n = 1$ のときは自明なので一般の n に対して示された。また特に $\gcd(n, p) = 1$ のときは、定理 1 より $^{\exists}a \in \mathbb{Z} \ : \ an \equiv 1 \pmod{p}$ なので、

$$\begin{aligned} n^{p-1} &\equiv n^{p-1}an \\ &\equiv n^p a \\ &\equiv na \\ &\equiv 1 \pmod{p} \end{aligned}$$

より示された。 □

Proof. 定理 3
合同式を真面目に等号で書き直せばすぐわかる。 □

4 大学流で理解しよう！

先ず必要な概念を定義をしていきます。

定義 1. 商集合
X を集合とする。$a, b \in X$ の組を $a \sim b$ と書きこれを関係と呼ぶ。以下の 3 つの条件を満たす関係を特に同値関係と呼ぶ。

- $^{\forall}a \in X \ : \ a \sim a$
- $a \sim b \Rightarrow b \sim a$
- $a \sim b$ かつ $b \sim c \Rightarrow a \sim c$

次に $C(a) := \{b \in X | a \sim b\}$ と $C(a)$ を定義する。すると a と b が同値関係にないなら $C(a) \cup C(b) = \emptyset$ となり、$X = \bigcup_{a \in X} C(a)$ と分解できる。$X/\sim := \{C(a) | a \in X\}$ と $X/\sim$ を定義しこれを商集合という。

例 1. $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Q}$

定義 2. 可換群、環、整域、体
略 *(イメージは、可換群は足し算ができる、環は足し算と掛け算ができる、整域はかけて 0 ならどっちかは 0，体は四則演算ができる)*

例 2. $\mathbb{R}^2$, $\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{R}$

定義 3. 部分群

G を群とし、H が部分群とは、H が群かつ $H \subset G$ であることをいう。

定義 4. イデアル

イデアル　A を環とし、I が A のイデアルとは、I が加法に関して A の部分群かつ A からの作用が定まるものである。

素イデアル　$\mathfrak{p}$ が素イデアルとは、$\mathfrak{p}$ がイデアルかつ $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}$ を満たすことをいう。

極大イデアル　$\mathfrak{m}$ が極大イデアルとは、$\mathfrak{m}$ がイデアルかつ $\mathfrak{m} \subsetneq I \subsetneq A$ となるイデアル I が存在しないことをいう。

命題 2. イデアルの諸性質

1. $ab \in I$ のとき $a \sim b$ と関係を定義するとこれは同値関係であり、$A/\sim$ を A/I と書く。
2. $a \in A$ に対し、$\{x \in A | \exists n \in \mathbb{N} : an = x\}$ はイデアルであり、これを (a) と書く。
3. I, J が A のイデアルなら、$I + J := \{i + j \in A | i \in I,\ j \in J\}$ もイデアルである。
4. $\mathfrak{p}$ が素イデアル $\Leftrightarrow A/\mathfrak{p}$ が整域
5. $\mathfrak{m}$ が極大イデアル $\Leftrightarrow A/\mathfrak{m}$ が体

定義 5. ユークリッド環、単項イデアル整域

ユークリッド環　あまりのような概念が定義できる環

単項イデアル整域　任意のイデアルはひとつの元で生成されるような整域（整域は環の一種として定義していた）

命題 3. ユークリッド環は単項イデアル整域

命題 4. 整数環 $\mathbb{Z}$ はユークリッド環。特に単項イデアル整域。

以上を用いて定理 1 を証明することができる。定理 2、定理 3 もそれぞれ群論のラグランジュの定理、準同型定理を使えば見通しがよい。が、書く時間がなくなったので割愛します。