No. 10-1

**定理4.14.** $n \in \mathbb{N}$ とし、任意の素数 $p$ に対し、$p^2 \nmid n$ とする。
このとき、次が成立

(1) $n$ の任意の素因数 $p$ に対し、
$$q \equiv 1 \pmod{p-1} \Rightarrow \forall a \in \mathbb{Z},\ a^q \equiv a \pmod{n}$$

(2) $\forall a \in \mathbb{Z}$ に対し、
$$q \equiv 1 \pmod{\varphi(n)} \Rightarrow a^q \equiv a \pmod{n}$$

☺ (1) まず、$a^q \equiv a \pmod{p}$ を示す

仮定より $p-1 \mid q-1$ より

$q-1 = k(p-1)$ となり、$q = k(p-1)+1$ となる

$\therefore a^q = a^{k(p-1)+1} \equiv a \pmod{p}$

↑ フェルマーの小定理。($p$ と $a$ が素のとき)。
$a$ と $p$ が素でなければ、$a \equiv 0 \pmod{p}$ より出る

$\therefore a^q \equiv a \bmod p$ である。

さて、$n = p_1 p_2 \cdots p_\ell$ と分解されるとする。ここで、
$p_i \mid a^q - a$ であるので、$n \mid a^q - a$ である。
$\therefore a^q \equiv a \pmod{n}$ がわかる。

(2) $q \equiv 1 \pmod{\varphi(n)}$ より $\varphi(n) \mid q-1$ である。

一方 $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_\ell}\right)$ より、$\varphi(n)$ は $p_i - 1$ の倍数。

$\therefore p_i - 1 \mid q-1$ なので (1) の条件をみたす。$\therefore a^q \equiv a \pmod{n}$

例. (1) $13^{100} \pmod{330}$ を計算する.

$330 = 2\times3\times5\times11$ より 定理の条件の1つをみたす. また

$\varphi(330) = 330\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{10}{11} = 80$ である.

ここで $l = \mathrm{lcm}(1, 2, 4, 10) = 20$ とすると.

$q = kl + 1$ は (1) の条件をみたす.

今. $13^{100} = 13^{101-1} \equiv 13^{1-1} = 1 \pmod{330}$ である.

13と330が素なのでこの計算ができる.

なお. フェルマーの小定理はここでは使えない.

オイラーの定理だと. $13^{80} \equiv 1$ までしか言えない.

(2). $14^{100} \pmod{330}$ はより注意が必要.

$14^{101} \equiv 14 \pmod{330}$ は上と同じにいえるが.

これをわることはできない. ここで

$14^{101} \equiv 14 \pmod{165}$ を考えると.

$14^{100} \equiv 1 \pmod{165}$ である.

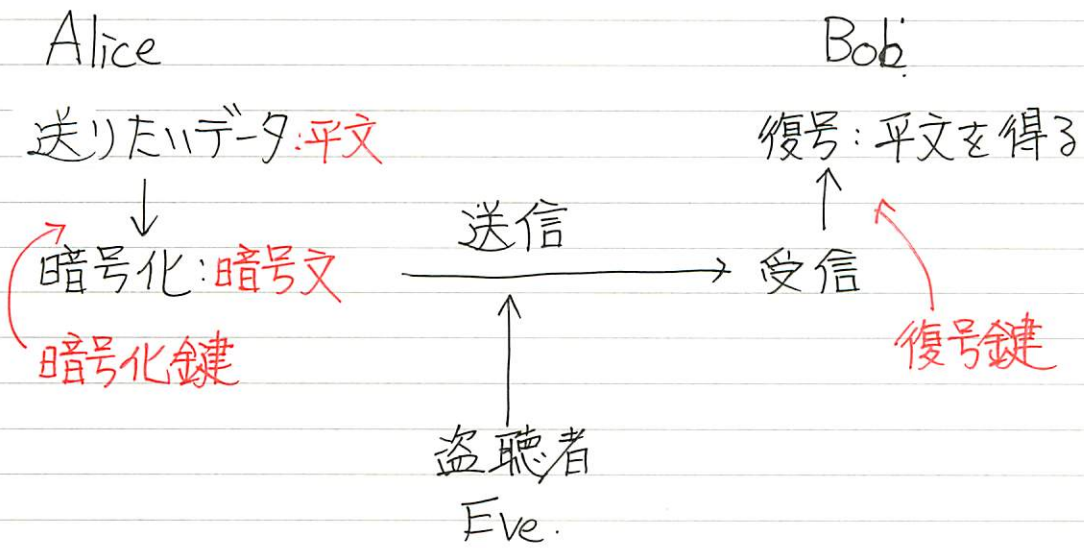
$\therefore 14^{100} \equiv 166 \text{ or } 1 \pmod{330}$ である.

$14^{100}$ も330も偶数なので.

$14^{100} \equiv 166 \pmod{330}$ となる.

# §5 暗号

暗号のイメージ.




## 公開鍵暗号.

暗号化鍵と.復号鍵が

一致している :対称暗号 ⟶ 秘密鍵暗号

一致していない:非対称暗号 ⟶ 公開鍵暗号

(暗号化鍵から復号鍵が計算できないという(を)条件)

暗号系. 暗号全体を集合で表すと次のようになる.

$CS = (P, K, C, E, D)$.

$P = \{$平文全ての集合$\}$

$C = \{$暗号文全ての集合$\}$

$K$:キーの集合. $K \ni k$ に対し.

暗号化鍵 $E_k : P \to C$ と.

復号鍵 $D_k : C \to P$ が唯一つ定まる.

ここで $D_k \cdot E_k(p) = p$. である

例. (1). アルファベットの文章に対し.

$E_k$ : abcd…xyz を2つずらすもの. とすると.

↓↓ ↓↓↓

cd …zab

$D_k$ : もとにもどすもの. とできる.

単にずらすだけだと. 解読は簡単そうだが. アルファベットの変換は

26! 通りあるので. そこまで簡単ではない.

(2) ヒル暗号. (mod 26 での)

まず. アルファベットに数字をふり. $\{0,\cdots,25\}$ と同一視しておく.

M を $d\times d$ の正則行列 とする. ただし. その成分は. $\{0,\cdots,25\}$ のどれかとする.

平文 p は. d の倍数の長さであるとし. p を d文字ずつに区切り.

$p=p_1p_2\cdots p_m$ $(|p_i|=d)$ とする.

以下この $p_i=p$ として 暗号化, 復号を考える.

$p=p_1\cdots p_d$ となっているので.

$p=\begin{bmatrix}p_1\\ \vdots\\ p_d\end{bmatrix}$ とかけるが 暗号化を $Mp \pmod{26}$ とする.

M は正則行列なので 復号化するときには $M^{-1}$ をかければよい.

例えば $d=2$ として.

$M=\begin{bmatrix}3&3\\2&5\end{bmatrix}$ とする. このとき $M^{-1}=\begin{bmatrix}15&17\\20&9\end{bmatrix}$ である.

ここで CODE という平文を送るとすると、まず、

2, 14, 3, 4 という数字に対応させ、2つずつ変換する。

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} 22 \\ 22 \end{bmatrix} = \begin{bmatrix} W \\ W \end{bmatrix}$$

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 21 \\ 0 \end{bmatrix} = \begin{bmatrix} V \\ A \end{bmatrix}$$ となる。

∴暗号文は WWVA である。これを復号すると、

$$M^{-1}\begin{bmatrix} 22 \\ 22 \end{bmatrix} = \begin{bmatrix} 2 \\ 14 \end{bmatrix}, \quad M^{-1}\begin{bmatrix} 21 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$ となり

CODE に戻る。