Dispelling of Confusion of Equations in Learning Affine Cipher and An Application of the Result

アファイン暗号を学ぶ場合における方程式の混乱の解消とその応用

川　口　雄　一
Yuuichi KAWAGUCHI

The affine cipher is a criptographic technique. Many text books explain it using some algebraic calculi, especially with remainders and congruence equations. There are two algebraic difficulties for novices. One is a confusion among the notations of usual equations and congruence equations, and the other is the method of decryption. This paper aims to show that (1) we can use usual equations and congruence equations together, and (2) the equation of decryption is obtained from the equation of encryption as an application of (1).

アファイン暗号は文字を暗号化するひとつの方法である。たくさんの教科書によって解説がなされ、その中では代数的な計算法が使われる。特に、剰余と合同式が用いられる。初学者にとって困難な代数的内容がふたつある。ひとつは、等式と合同式がまるで混用されているかのように現われることである。もうひとつは、復号するための計算式を求める困難さである。本稿は、(1) 剰余計算における等式と合同式は意味として同値であること、および、(2) その応用として、暗号化の計算式から復号の計算式を導く方法を示す。

Key words:
Affine Cipher	アファイン暗号
Coding Theory	符号理論
Applied Algebra	応用代数学
Number Theory	整数論
Congruence Equation	合同式

天使大学 看護栄養学部 教養教育科　(2012 年 7 月 2 日 受稿, 2012 年 11 月 21 日 審査終了受理)

1 Introduction

1.1 Objective

I am in charge of the subject "Coding Theory" at Tomakomai National College of Technology (TNCT). The "affine cipher" [1] is one of the topics that students learn. Many algebraic calculi [2][3], especially remainders, which use a binary operation $x \bmod y$, and congruence equations by $\equiv$ and $\pmod m$, are used for descriptions.

An affine cipher $y = 9x + 7 \bmod 26$, where x is an input (*i.e.*, plain) letter and y is the output (*i.e.*, encrypted) letter, is used in [1], as an example. In order to decrypt y into the original x, a congruence equation $y \equiv 9x + 7 \pmod{26}$ must be solved for x, as described in [1].

It is difficult for students to realize a reason why we should use a congruence equation for solving an usual equation. They get confused about the confusion between symbols $=$ and $\equiv$.

This paper aims to

(1) dispel the confusion, and
(2) show a method for decrypting as an application of (1).

1.2 Definition

There are two definitions for $\equiv$ and $\pmod{\ }$. Given x and y are integer numbers and m is a positive integer number.

Definition 1. $x \equiv y \pmod m$
$\iff x \bmod m = y \bmod m.$
where $x \bmod y \ (0 < y)$ is defined by the floor function $\lfloor\ \rfloor$ as $x \bmod y = x - \lfloor x/y \rfloor \times y$.

Definition 2. $x \equiv y \pmod m$
$\iff m \mid (x - y),$
where $m \mid a$ shows that $a = Qm$ holds for some $Q \in \mathbb{Z}$.

The two definitions are equivalent, *i.e.*, one derives the other and *vice versa*.

2 Main Subject

2.1 Affine Cipher

The affine cipher is a method for cryptography. An input letter x, which is given by a character code, *i.e.,* an integer number, is encrypted into an output letter y according to the equation

$$y = kx + s \bmod m \qquad (\dagger),$$

where k and s are integers, and they are the cipher keys. The binary operator 'mod' calculates a remainder y in dividing $kx + s$ by m.

The condition for decrypting y into the original (*i.e.*, plain) x uniquely is $k \perp m$, *i.e.*, $\gcd(k, m) = 1$. If the above-mentioned condition holds, we obtain x according to an equation

$$x = k^{-1}(y - s) \bmod m \qquad (*),$$

where the k^{-1} is known as the reciprocal number of k and $k \cdot k^{-1} \equiv 1 \pmod m$ holds.

2.2 Confusion among Notations

In obtaining the equation $(*)$ from the equation $(\dagger)$, which is denoted by '$=$' and a binary operator '$\bmod m$,' we must solve another congruence equation '$y \equiv kx + s \pmod m$,' which is denoted by '$\equiv$' and '$\pmod m$.' There seems

to be a confusion among notations, especially for students.

There are two facts.

Fact 1.　$y = kx + s \bmod m$

$$\Longrightarrow \quad y \equiv kx + s \pmod{m}.$$

$\because$ The equation at the left-hand side yields

$$\begin{aligned} y = \quad & kx + s - Qm, \\ & \text{where } Q = \left\lfloor \frac{kx+s}{m} \right\rfloor \in \mathbb{Z}; \\ \therefore \quad & y - (kx + s) = -Qm. \end{aligned}$$

Therefore, it holds that $m \mid y - (kx + s)$ and by Definition 2, this implies that $y \equiv kx + s \pmod{m}$, which is the equation at the right hand side.

□

Fact 2.　Given　$0 \leqq y < m$,

$$y \equiv kx + s \pmod{m} \quad \Longrightarrow \quad y = kx + s \bmod m.$$

$\because$ By Definition 1, it can be seen that the equation on the left-hand side yields a formula $y \bmod m = kx + s \bmod m$. When $0 \leqq y < m$, it holds that $y \bmod m = y$, and then it holds that $y = kx + s \bmod m$, which is the equation on the right-hand side.

□

Using these two facts, as far as the condition $0 \leqq y < m$ is holding, it holds that

$$y = kx + s \bmod m \quad \Longleftrightarrow \quad y \equiv kx + s \pmod{m}.$$

The two formulae are equivalent. Thus, the confusion is dispelled.

2.3 Method of Decryption

As an application of the result above, we demonstrate a method of decryption.

In decrypting an encrypted letter y, which is denoted by an integer code, into a plain letter x, the equation (†) is solved into the equation (∗).

Two facts are needed for the solution.

Fact 3.　Given　$a, b, c, m, x \in \mathbb{Z},\ m \neq 0$,

$$ab \equiv 1 \pmod{m} \ \wedge \ ax \equiv c \pmod{m} \quad \Longrightarrow \quad x \equiv bc \pmod{m}.$$

$\because$ $ab \equiv 1 \pmod{m}$ implies that $ab - 1 = mQ$ holds for $\exists Q \in \mathbb{Z}$; further, $ab = mQ + 1$ is derived. $ax \equiv c \pmod{m}$ implies that $abx \equiv bc \pmod{m}$. We then have

$$\begin{aligned} abx &\equiv bc \pmod{m}, \\ (mQ + 1)x &\equiv bc \pmod{m}, \\ x + mQx &\equiv bc \pmod{m}, \\ x &\equiv bc \pmod{m}. \end{aligned}$$

□

Note that the number b is known as the "*reciprocal number*" of a, which is usually denoted by a^{-1}, and *vice versa*.

Fact 4.　Given　$k \perp m$,

$$\begin{cases} kk^{-1} \equiv 1 \pmod{m} \ \wedge \\ y \equiv kx + s \pmod{m} \end{cases} \Longrightarrow \quad x \equiv k^{-1}(y - s) \pmod{m}.$$

$\because$ $y \equiv kx + s \pmod{m}$ implies that

$$\begin{aligned} kx + s &\equiv y \pmod{m}, \\ kx &\equiv y - s \pmod{m}, \\ x &\equiv k^{-1}(y - s) \pmod{m} \quad \cdots \text{by Fact 3.} \end{aligned}$$

□

Moreover, by Fact 2, as far as we ensure that $0 \leqq x < m$, it is derived that

$$x = k^{-1}(y - s) \bmod m \quad (\ddagger).$$

This is an equation (∗), which shows a method of decrypting.

3 Related Work

The book [1] describes the affine cipher method. It does not describe algebraic calculi in detail. We owe those descriptions to books [2] and [3].

There is a theorem shown below:

> **Theorem 1.13** ([2], Chapter 1, § 6) A first order congruence equation $ax \equiv b \pmod{m}$ has only one solution, if $a \perp m$ holds.

By applying this theorem, we obtain k^{-1} from k ($\because k \perp m$) and then obtain $x \equiv k^{-1}(y - s) \pmod{m}$ from $y \equiv kx + s \pmod{m}$. As far as Fact 3 and 4 are concerned, they are well-known mathematically.

In this paper, as an application of the result obtained in Section 2.2, we obtain an equation $x = k^{-1}(y - s) \bmod m$ (‡), which gives a concrete plain letter 'x.' On the other hand, congruence equations give an equivalence class, and then the plain letter is not specified as an unique number.

4 Conclusion

This paper shows that

(1) when $0 \leqq y < m$, we can use a usual equation with '=' and a congruence equation with '≡' together in the explanation, and

(2) the equation for decrypting is obtained from the equation of encryption as an application of the result above.

Acknowledgement

I am very thankful to Matsuda K. (1965-2011) and the staff at TNCT for giving me an opportunity to be in charge of the subject "Coding Theory." It would give me great pleasure if this paper improves the student's appreciation of the affine cipher. The work is partly supported by the collaborative research program 2011, information initiative center, Hokkaido University, Sapporo, Japan.

参考文献

[1] D W. Hardy, F. Richman, and C. L. Walker, Applied Algebra – Codes, Ciphers, and Discrete Algorithms, second edition, CRC Press, 2009.

[2] 高木 貞治, 初等整数論講義 (第 2 版), 共立出版, 1971 年.

[3] 松坂 和夫, 代数系入門, 岩波書店, 1976 年.