線形合同法における正しい数値設定

高校１年４組２８番　河口祐輝

1　はじめに

数学研究部部誌を読んでいただきありがとうございます。ここでは、線形合同法というものについて話を進めていきます。

下の定義で書いているように線形合同法は乱数と関係があります。最初はよりよい乱数列を作るということを考えてこの様なテーマにしました。

この文章ではあまり関係がなくなってしまいましたが、もしよければ最後までお付き合いください。

2　準備

記号や言葉の意味です。

(1) $a \in \mathbb{N}_0, b \in \mathbb{N}$
　それぞれ、a が非負整数、b が自然数

(2) $a \equiv b(mod\ m)$
　a と b をそれぞれ m で割った余りが等しい

(3) $a|b$
　b が a の倍数である

(4) $(a, b) = c$
　a と b の最大公約数が c である

3　線形合同について

3.1　定義

　線形合同法は、コンピューターでゲームや実験における乱数の発生のために用いられる方法のひとつである。線形合同法では、乱数列 $\{x_n\}$ を

$$\begin{cases} x_1 = a \\ x_{n+1}\text{は } x_{n+1} \equiv bx_n + c(mod\ m) \text{ を満たす最小の非負整数} \end{cases}$$

で定義する。ただし、$a, b, c \in \mathbb{N}_0, \quad m \in \mathbb{N}, \quad a, b, c < m$
$\{x_n\}$ のそれぞれぞれの項は 0 以上 m 未満の整数となる。

3.2　目的

　できた数列が乱数列として働くように a, b, c の値を定める。
すなわち、m にたいして、$\{x_n\}$ の中に 0 以上 m 未満の整数がすべて現れるような a, b, c を考える。
　これを条件 A と呼ぶことにする。

4　a, b, c を定める

定理 1　$\{x_n\}$ に 0 以上 m 未満の整数が全て現れるならば、$x_1, x_2, \ldots, x_m$ は $0, 1, \ldots, m-1$ の並び替えである。またそのとき $x_{k+ml} = x_k$ である。

証明 1　背理法により示す
$\{x_n\}$ に 0 以上 d 未満の整数が全て現れ、かつ j が $1 \leq i < j \leq m, x_j = x_i$ を満たす i が存在するもののうち最小のものとする。
定義より $x_{j+p} = x_{i+p}$ は明らか。

$$x_{j+q(j-i)+r} = x_{j+(q-1)(j-i)} = \cdots = x_{j+r} = x_{i+r} \quad (0 \leq r < j-i)$$

よって $k \geq i$ に対して x_k は $x_i, x_{i+1}, \ldots, x_{j-1}$ のうちのいずれかと一致する。
$\{x_n\}$ に現れる数は $x_1, x_2, \ldots, x_{j-1}$ の $j-1$ 個となり、矛盾する。
よって $x_1, x_2, \ldots, x_m$ は互いに異なっており、$0, 1, \ldots, m-1$ の並び替えである。

またそのとき、明らかに $x_2, x_3, \ldots, x_{m+1}$ も $0, 1, \ldots, m-1$ の並び替えであるから、$x_{m+1} = x_1$
よって $x_{m+1+p} = x_{1+p}$ なので

$$x_{k+ml} = x_{k+m(l-1)} = \cdots = x_k$$

証明終

定理 2 ある b, c に対してある a で条件 A が成り立てば全ての a で成り立つ。

証明 2 $a' \in \mathbb{N}_0, a' < m$ とする。
a で成り立つならば、$\{x_n\}$ に a' は含まれる。
$x_{n'} = a'$ とすると、$\{y_n\}$ を

$$\begin{cases} y_1 = a' \\ y_{n+1}\text{は } y_{n+1} = by_n + c(mod\ m) \text{ を満たす最小の非負整数} \end{cases}$$

で定義すれば $y_n = x_{n+n'-1}$ より $\{y_n\}$ は明らかに条件を満たす。

証明終

以上より、$a = 0$ の時に $x_1, x_2, \ldots, x_m$ が互いに異なるような b, c を調べれば十分である。

定理 3 条件 A を満たす必要十分条件は

$$\begin{cases} (i)\ \text{条件を満たさない} \quad (b = 0) \\ (ii)\ (c, m) = 1 \quad (b = 1) \\ (iii)\ 1 \leq i < j \leq m \text{ となる全ての } i, j \text{ に対して} \\ m \not| b^{i-1} \cdot (b^{j-i-1} + b^{j-i-2} + \cdots + 1) \cdot c \quad (b > 1) \end{cases}$$

証明 3
$\{X_n\}$ を

$$\begin{cases} X_1 = 0 \\ X_{n+1} = bX_n + c \end{cases}$$

で定義すれば x_n が $x_n \equiv X_n (mod\ m)$ を満たす最小の非負整数なので、
$x_1, x_2, \ldots, x_m$ が互いに異なることは
$1 \leq i < j \leq m$ なる全ての i, j に対して $m \not| X_j - X_i$ であることと
と同値である。

(i) $b = 0$ の時、

$$X_n = \begin{cases} 0 & (n = 1) \\ c & (n > 1) \end{cases}$$

となり、$1 \geq i < j \leq m$ なる i, j に対して $m | X_j - X_i$ なので、これは条件を満たさない。

(ii) $b = 1$ の時、$X_n = c(n-1)$ より $X_j - X_i = c(j-i)$
$j - i$ が 1 から $m-1$ まで動くので、c と m は互いに素であることが必要十分条件。

(iii) $b > 1$ の時、$X_n = b^{n-1}\dfrac{c}{b-1} - \dfrac{c}{b-1}$ より

$$\begin{aligned} X_j - X_i &= (b^{j-1} - b^{i-1}) \cdot \frac{c}{b-1} \\ &= b^{i-1} \cdot (b^{j-i-1} + b^{j-i-2} + \cdots + 1) \cdot c \end{aligned}$$

よって $m \not| b^{i-1} \cdot (b^{j-i-1} + b^{j-i-2} + \cdots + 1) \cdot c$ が $1 \leq i < j \leq m$ なる全ての i, j に対して成り立てばよい。

証明終

m の値に対して $m \not| b^{i-1} \cdot (b^{j-i-1} + b^{j-i-2} + \cdots + 1) \cdot c$ となる i, j が存在しないような b, c を探す。

定理 4 m が素数の時、条件を満たす 1 より大きい b は存在しない

証明 4 $1 \geq c < m, m$ は素数 なので b^{i-1}, c は m と互いに素であるから、$m \not| b^{i-1} \cdot (b^{j-i-1} + b^{j-i-2} + \cdots + 1) \cdot c \Longleftrightarrow m \not| b^{j-i-1} + b^{j-i-2} + \cdots + 1$
[1]フェルマーの定理より、$m | b^{m-1} - 1$ である。
しかし、$m \not| b - 1$ であるから、
$m | b^{j-i-1} + b^{j-i-2} + \cdots + 1 = \dfrac{b^{j-i} - 1}{b - 1}$ は $j - i = m - 1$ の時、すなわち $j = m, i = 1$ の時成り立つ。
よって m が素数のとき条件を満たす 1 より大きい b は存在しない。

定理 5 p を奇素数とし、$m = p^{\alpha} (\alpha \geq 2)$ と書けるとする。この時、条件を満たすならば $p | b - 1$ である。

証明 5 $p^{\alpha} \not| b^{i-1}(b^{j-i-1} - 1)$ が成り立てば、$c = 1$ で条件は成立する。

(i) $p | b$ の時、$m - 2 > \alpha$ となることを示せば $i = m - 2$ で $m | b^{i-1}$ となり、条件を満たさない。$\alpha = 2$ の時 3 以上の全ての素数に対して

$$p^{\alpha} - 1 > p^{\alpha} - 2 > \alpha$$

また、$p^{\alpha} - 1 > \alpha$ ならば、$(p - 1)\alpha + p > 2$ より

$$p^{\alpha+1} - 1 > (\alpha + 1)p - 1 > \alpha + 1$$

よって 2 以上の全ての α、奇素数である p に対して $p^{\alpha} - 2 > \alpha$ が帰納的に示された。よってこのとき条件 A を満たさない。

(ii) $p \not| b - 1$ の時、[2]フェルマー-オイラーの定理より
$p^{\alpha} | b^{p^{\alpha-1}(p-1)} - 1$

---

[1] p が素数ならば

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

[2] (a,m)=1 ならば

$$a^{\phi(m)} \equiv 1 (mod\ m)$$

ただし $\phi(m)$ は 1 から m までで m と互いに素な整数の個数を表す。

よって $j-i=p^{(\alpha-1)}\cdot(p-1)$ の時 ($p^{\alpha}>p^{\alpha-1}(p-1)$ よりこのような i,j の組は存在する)

$$p^{\alpha}|\frac{(b^{j-i}-1)}{b-1}=b^{j-i-1}+b^{j-i-2}+\cdots+1$$

となるので、これは条件を満たさない。

(iii) $p|b-1$ の時
次の定理を用いる。奇素数 p に対して $ord_p x$ は $p^k|n$ なる k の最大値を表す。

$$ord_p(x-1)=k\geq 1\Longleftrightarrow ord_p(x^n-1)=k+ord_p n$$

これより、

$$\begin{aligned}&ord_p(b^{j-i-1}+b^{j-i-2}+\cdots+1)\\&=ord_p(b^{j-i}-1)-ord_p(b-1)\\&=ord_p(j-i)\end{aligned}$$

$j-i<m=p^{\alpha}$ より、$ord_p(j-i)\geq ord_p m=\alpha$ となる i,j は存在しない。よって $p^{\alpha}\not|b^{j-i-1}+b^{j-i-2}+\cdots+1$ となり、
$ord_p c<\alpha-ord_p(j-i)$ となる c をとれば条件 A を満たす。

証明終

5　乱数の話

　いままでの話で気づかれたかもしれませんが、この線形合同法という方法を単独で用いて生成された擬似乱数列は乱数として全く（と言うと言いすぎかもしれませんが）役に立ちません。
たとえば $m = 9, a = 3, b = 7, c = 2$ で数列を作ると、
$3, 5, 1, 0, 2, 7, 6, 8, 4, 3 \cdots$
となり、最初は適当に数が並んでいるように見えますが、いくつも問題があります。
まず周期という問題。最大値 $m - 1$ の乱数列では正しく数値を設定しても周期は m と定まっており、そのひとつの周期の中で絶対に同じ数が 2 回以上現れるということはありません。しかも、最大値 $m - 1$ が分かっていれば最初の m 項を覚えるだけで以降の項が全て分かります。
またそれぞれの項を $mod\ 3$ で見てみると
$0, 2, 1, 0, 2, 1, 0, 2, 1, 0 \cdots$
と、$0, 2, 1$ の繰り返しになっています。このことを知っていれば、周期を全て覚えていなくてもたとえば「4 の次に 7 が現れることはない」ということが分かってしまいます。
以上のようなことから線形合同法というのは、乱数列を作る方法としてはあまりに不完全な方法だということがいえます。

　線形合同法は乱数の生成法として最も簡単なものです。ほかにもよりよい方法が多数あります。
現在最も優秀といわれている方法は、1997 年に松本眞さんと西村拓士さんによって編み出されたメルセンヌ・ツイスタ (http://www.math.sci.hiroshima-u.ac.jp/ m-mat/MT/mt.html) という方法だそうです。

6　おわりに

最後まで読んでくださった方、お疲れ様でした。またも読みにくく、おかしな点があったかもしれません。

ここでは線形合同法という簡単なものについてのみ考えましたが、本当に「乱れた」数を作るというのはとてつもなく難しいもののような気がします。新しい、よりよい方法を作り出す人たちは本当にすごいですね。

特に書くこともないのでこのあたりでおしまいにしましょう。

最後に、この文章を読んでくださった方々、協力してくれた数研部員のみんなに感謝の意を述べたいと思います。

指摘、意見などは下記のメールアドレスまでお願いします。

kawaguchi_yuki_n@hotmail.com