$1+1=0$の世界での代数・幾何・応用

松本　眞（広島大学理学研究科数学専攻）

2014/6/2,9, 広島大学・数学概論

email: m-mat “at mark と呼ばれるもの” math.sci.hiroshima-u.ac.jp

分数と循環小数

$1 \div 7$ の 10 進小数展開の余りの列 $x_1, x_2, \ldots$ は、$x_1 = 1$ として以下の法則で求まる。

$$
\begin{aligned}
1 \times 10 &= 10,\ \div 7 = 1 \text{ 余り } 3 =: x_2 \\
3 \times 10 &= 30,\ \div 7 = 4 \text{ 余り } 2 =: x_3 \\
2 \times 10 &= 20,\ \div 7 = 2 \text{ 余り } 6 =: x_4 \\
6 \times 10 &= 60,\ \div 7 = 8 \text{ 余り } 4 =: x_5 \\
4 \times 10 &= 40,\ \div 7 = 5 \text{ 余り } 5 =: x_6 \\
5 \times 10 &= 50,\ \div 7 = 7 \text{ 余り } 1 =: x_7
\end{aligned}
$$

$$
\begin{array}{r}
0.\dot{1}4285\dot{7}\dot{1} \\
7\overline{)\,10} \\
\underline{7} \\
30 \\
\underline{28} \\
20 \\
\underline{14} \\
60 \\
\underline{56} \\
40 \\
\underline{35} \\
50 \\
\underline{49} \\
10 \\
\underline{7} \\
30
\end{array}
$$

定義　整数a, Nに対し、

$$a \mod N$$

で、

　aをNで割ったあまり（$0, 1, \ldots, N-1$のいずれか）

を表す。先の余りの列は

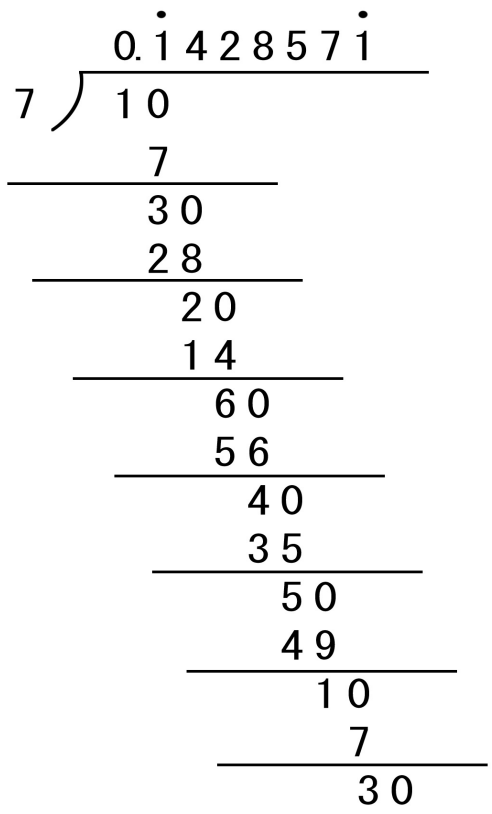
$$\begin{aligned}
x_1 &= 1 \\
x_2 &= x_1 \times 10 \mod 7 = 10^1 \mod 7 \\
x_3 &= x_2 \times 10 \mod 7 = 10^2 \mod 7 \\
&\cdots \\
x_{n+1} &= x_n \times 10 \mod 7 = 10^n \mod 7
\end{aligned}$$

定理

Nを10と互いに素な自然数とする。
$1/N$の小数展開の周期は$N-1$以下で、
$1 \equiv 10^P \mod N$となる最小の自然数
$P \geq 1$となる。

証明：余りの種類はN種。そのうち0は出てこないから、周期は$N-1$以下。
（余りに0が小数点n桁目に出てきたら、10^nをNが割り切ることが筆算の形から分かる)。

後半については、循環するのは
$10^n \mod N$が1となったとき。
筆算を見よ。



$1+1=0$の世界での多項式

二元体$\mathbb{F}_2$

$\mathbb{F}_2 := \{0,1\}$とおく。

0,1の掛け算は普通に定義して、$\mathbb{F}_2$からはみ出ない。
足し算は$1+1=2$だけが$\mathbb{F}_2$からはみ出してしまうので、

$$1+1=0$$

と定義する（2で割ったあまりを見ている）。

1+1=0から1を移項して

$$1=-1.$$

$\mathbb{F}_2$多項式$\mathbb{F}_2[t]$

$$\mathbb{F}_2[t] := \left\{ \sum_{i=0}^{n} a_i t^i \mid a_i \in \mathbb{F}_2,\ n \in \mathbb{N} \right\}$$

を考える。係数が0または1の多項式のことである。
掛け算・足し算は通常の多項式同様

$$\begin{aligned}(t+1) \times (t+1) &= t(t+1) + 1(t+1) \\ &= t^2 + t + t + 1 \ = \ t^2 + 1\end{aligned}$$

といった具合に計算できる。
（$1+1=0$より$t+t=(1+1)t=0$。）

係数のみを表記することにして、「t進くらい取り」で

$$t^3+t^2+1=1t^3+1t^2+0t+1=1101$$

と表わすことにする。

$\mathbb{F}_2$多項式での和差積商は、

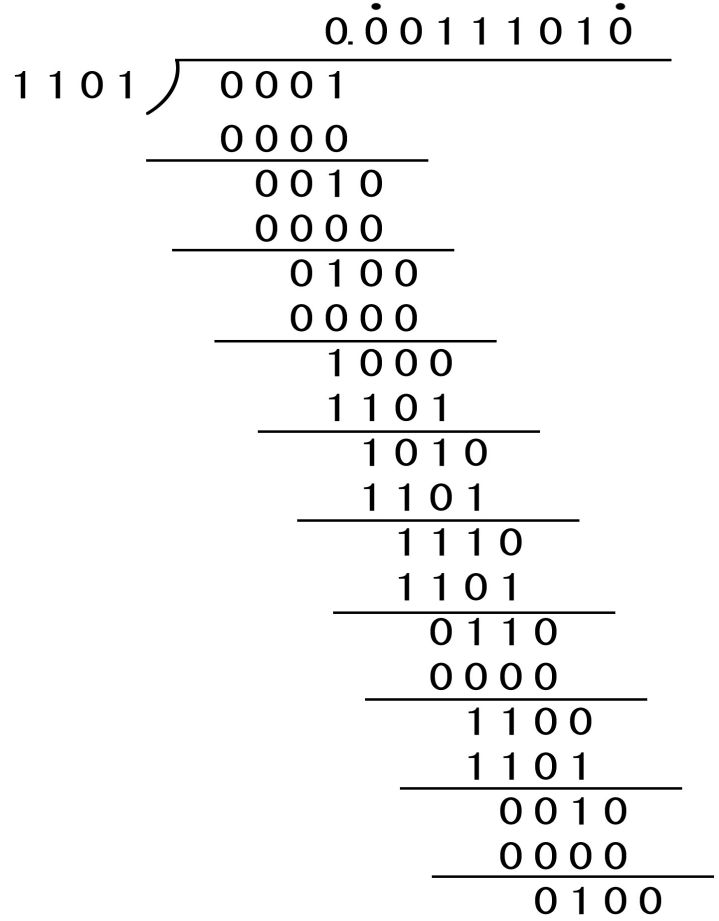
「繰り上がり・繰り下がりのない世界での計算」

になる。

$$\begin{array}{r} 1\ 1 \\ \times\ 1\ 1 \\ \hline 1\ 1 \\ 1\ 1\ \ \\ \hline 1\ 0\ 1 \end{array} \qquad \begin{array}{r} t\ \ +1 \\ \times\ \ t\ \ +1 \\ \hline t\ \ +1 \\ t^2\ +t\ \ \\ \hline t^2\ +0t\ +1 \end{array}$$

形式べき級数 ($1+1=0$ での無限小数)

$\mathbb{F}_2[t]$ の世界で $1 \div (t^3+t^2+1) = 1 \div 1101$ を小数展開すると



検算：

$$
\begin{array}{r}
0.00111010011101\cdots \\
\times\ 1101 \\
\hline
0.00111010011101\cdots \\
00.00000000000000\cdots \\
000.11101001110100\cdots \\
0001.11010011101001\cdots \\
\hline
0001.00000000000000\cdots
\end{array}
$$

$1 \div 1101 = 0.001110100111101\cdots$ は次の省略形である。

$$1 \div (t^3 + t^2 + 1) =$$
$$0 + 0t^{-1} + 0t^{-2} + 1t^{-3} + 1t^{-4} + 1t^{-5} + 0t^{-6} + 1t^{-7}\cdots$$

この無限小数のような式を$\mathbb{F}_2$**形式べき級数**と言い、
右辺を左辺の形式**べき級数展開**という。

定理：定数項が1で次数nの$\mathbb{F}_2$多項式$f(t) = t^n + \cdots + 1$に
対し、$1/f(t)$のべき級数展開の係数は循環し、
周期は$2^n - 1$以下。
周期は$1 = t^P \mod f(t)$となる最小の自然数$P \geq 1$。

証明：余りの種類が2^nで、そのうち0はあらわれないから。
後半は、筆算を見よ。

$1 \div 1101 = 0.x_1x_2x_3x_4\cdots$ とおくと $\mathbb{F}_2$ での漸化式

$$x_{n+3} + x_{n+2} + x_n = 0 \quad (n \geq 1) \quad \text{を満たす}$$

理由：

$$\begin{array}{rrrrcccccc}
 & & & 0 & . & x_1 & x_2 & x_3 & x_4 & x_5 & \cdots \\
\times & 1 & 1 & 0 & 1 & & & & & & \\
\hline
 & & & 0 & . & x_1 & x_2 & x_3 & x_4 & x_5 & \cdots \\
 & & 0 & 0 & . & 0 & 0 & 0 & 0 & 0 & \cdots \\
 & 0 & x_1 & x_2 & . & x_3 & x_4 & x_5 & x_6 & x_7 & \cdots \\
0 & x_1 & x_2 & x_3 & . & x_4 & x_5 & x_6 & x_7 & x_8 & \cdots \\
\hline
0 & 0 & 0 & 1 & . & 0 & 0 & 0 & 0 & 0 & \cdots
\end{array}$$

したがって、漸化式

$$x_{n+3} = x_{n+2} + x_n \ (n \geq 1), \quad x_1 = 0, x_2 = 0, x_3 = 1$$

を解くことで上の循環「小数」が得られる。

$$x_{n+3} = x_{n+2} + x_n \ (n \geq 1), \quad x_1 = 0, x_2 = 0, x_3 = 1$$

で$x_1x_2x_3x_4\cdots$を計算すると

0011

00111

001110

0011101

00111010

001110100

0011101001

00111010011

001110100111

周期の最大性と均等分布性

上の循環「小数」を三つずつ組にしてみると、000以外の2^3-1通りのパターンを一回ずつ一周期にとる。

$$00111010011101$$

$$001, 011, 111, 110, 101, 010, 100, 001$$

証明：漸化式が３階だから、連続する３個の数のパターンにより以後の数列は決まってしまう。000はあらわれないから、周期が2^3-1ならば他の全パターンが一個ずつ現れる。

定理

1. 任意の自然数nに対し、次数nの$\mathbb{F}_2$多項式$f(t)$であって$1/f(t)$のべき級数展開の係数の周期が2^n-1となるものがたくさん存在する。
2. このとき、連続するn個の0-1の並びは、

   $000\cdots0$を除いてすべて一回ずつ一周期に現れる。

性質1を満たす$f(t)$を$\mathbb{F}_2$**原始多項式**という。
このとき$f(t)$で割り切れない任意の$\mathbb{F}_2$多項式$g(t)$に対して、$g(t)/f(t)$の「小数部分」は周期2^n-1となる。

性質2は均等分布性と呼ばれ、数列のバランスの良さを示している。疑似乱数に用いるのに適している。

原始多項式の例：
$t^3 + t^2 + 1$(上でみた、周期$2^3 - 1 = 7$)
$t^{31} + t^3 + 1$(周期$2^{31} - 1 = 2147483647$)
$t^{607} + t^{273} + 1$(周期$2^{607} - 1 = 5.3 \times 10^{182}$)
など多数が知られている。

したがって、たとえば

$$x_{n+607} = x_{n+273} + x_n$$

を使って周期が$2^{607} - 1$で、連続する607項が均等分布する数列を、きわめて高速に作り出すことができる。
実験では確かめられないが、証明できる。数学の強み。

整数の割り算に比べてはるかに速い（桁数に無関係に高速）

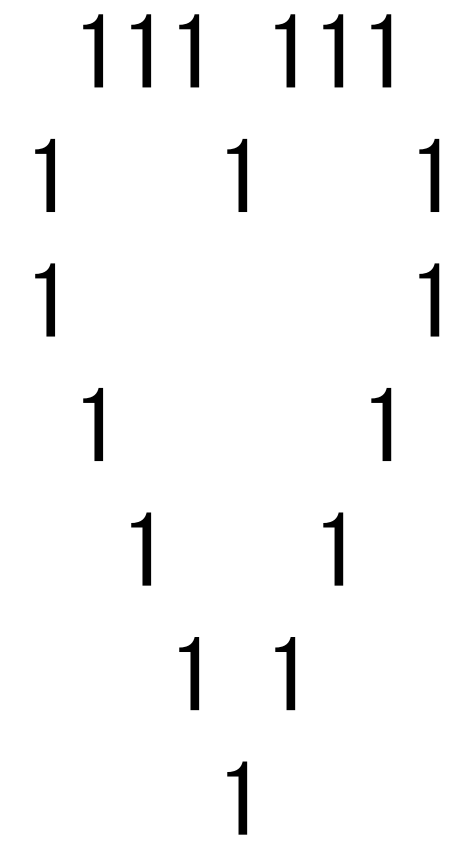
応用：ストリーム暗号

暗号化：絵に「パスワード」をかけて、パスワードを知る人だけが読めるようにしたい。

・絵のデータは膨大。一方、パスワードは短くしたい。

原始多項式$f(t)$と、任意の多項式$g(t) \neq 0$ を用意して「パスワード」とする。
（例:$f(t) = t^{31} + t^3 + 1$, $g(t)$:30次以下の任意の多項式。）

1. 送りたい絵を用意する。
2. $g(t)/f(t)$のべき級数展開の係数を、絵に合わせて長方形にならべる。
3. $1 + 1 = 0$の約束で、場所ごとに足す。暗号化文。
4. 暗号化文に、先の同じ係数を足す。復号。



絵

00000000000
00111011100
01000100010
01000000010　　0-1 化
00100000100
00010001000
00001010000
00000100000

11110111011
10000100000
10011100101　　g(t)/f(t)の展開
11011110010　　=パスワードの展開
10011100000
11100000100
10101110000
11101010111

11110111011
10111111100
11011000111　　絵＋展開
10011110000　　=暗号化文
10111100100　　赤字は展開の
11110001100　　反転したもの
10100100000
11101110111

11110111011
10111111100
11011000111　　絵＋展開
10011110000　　=暗号化文
10111100100
11110001100
10100100000
11101110111

11110111011
10000100000
10011100101　　g(t)/f(t)の展開
11011110010　　=パスワードの展開
10011100000　　を再度加える
11100000100
10101110000
11101010111

00000000000
00111011100
01000100010
01000000010　　復元（復号）
00100000100
00010001000
00001010000
00000100000

普通の幾何：互除法

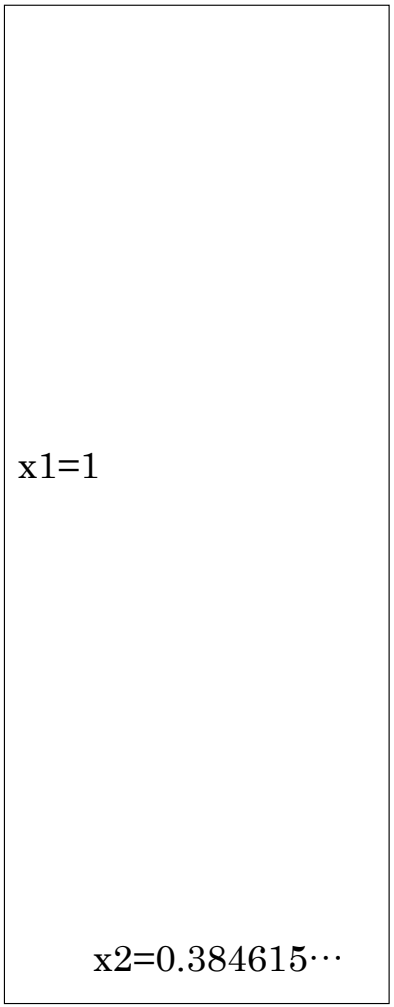
問い:比$1 : 0.384615384615\cdots$を既約整数比であらわせ。

たて $x_1 = 1$

よこ $x_2 = 0.384615384615\cdots$

$x_1 \div x_2 = 2$ 余り $0.230769230769\cdots$

$x_1 = x_2 \times 2 + 0.230769230769$



たて $x_1 = 1$

よこ $x_2 = 0.384615384615\cdots$

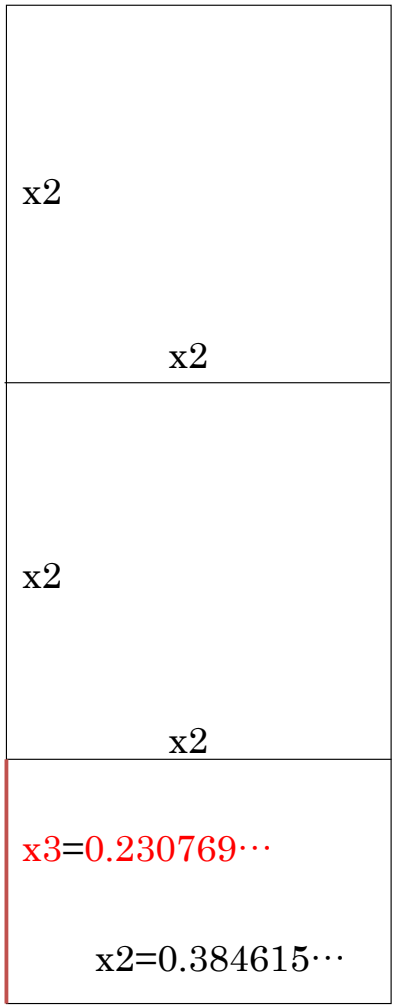
$x_1 \div x_2 = 2$ 余り $0.230769230769\cdots$

$x_1 = x_2 \times 2 + 0.230769230769$

$x_3 = 0.230769230769$ とおいて、

$$x_2 \div x_3$$

を計算

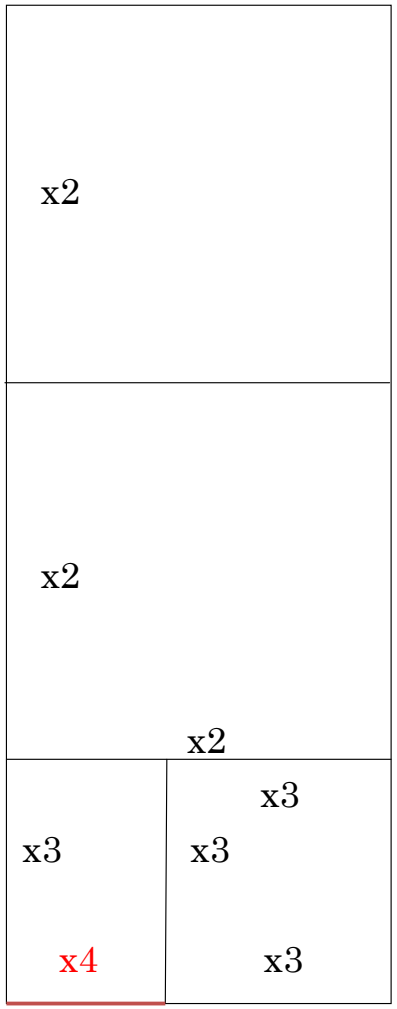


$$x_1 = x_2 \times 2 + x_3$$
$$x_2 = x_3 \times 1 + 0.153846153846\cdots$$

$x_4 = 0.153846153846\cdots$ とおいて、

$$x_3 \div x_4$$

を計算

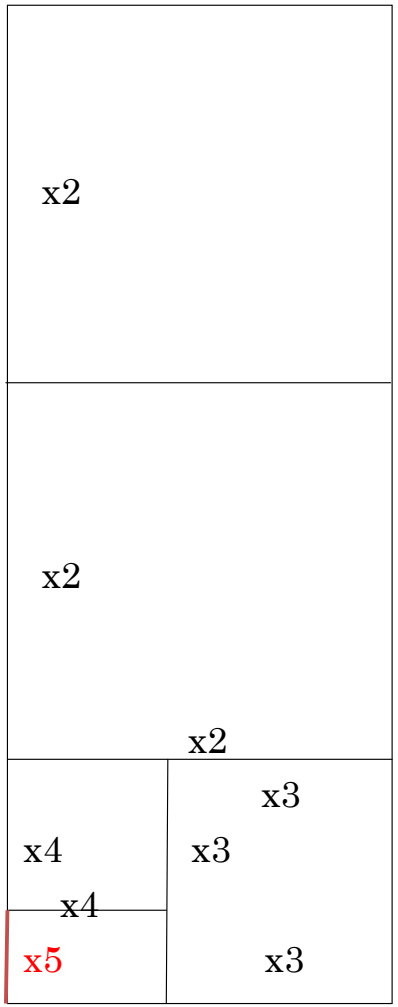


$$x_1 = x_2 \times 2 + x_3$$
$$x_2 = x_3 \times 1 + x_4$$
$$x_3 = x_4 \times 1 + 0.076923076923\cdots\cdots$$

$x_5 = 0.076923076923\cdots$ とおいて、

$$x_4 \div x_5$$

を計算



$$x_1 = x_2 \times 2 + x_3$$
$$x_2 = x_3 \times 1 + x_4$$
$$x_3 = x_4 \times 1 + x_5$$
$$x_4 = x_5 \times 2.$$

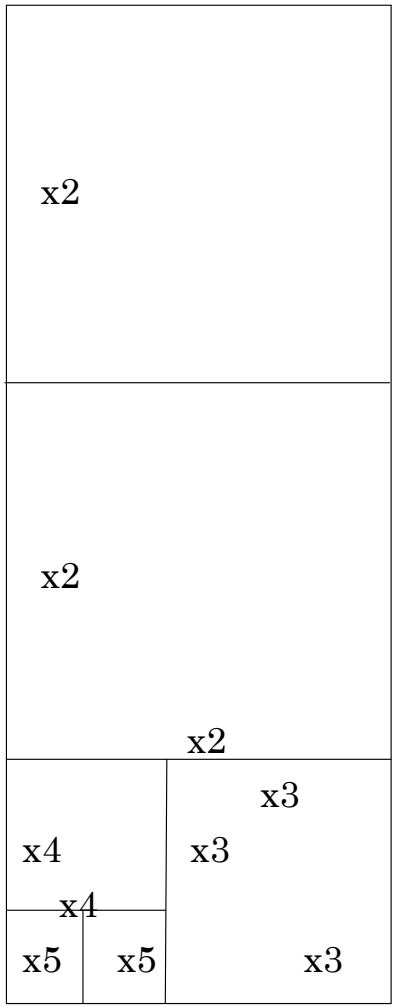
$\therefore$

$$x_4 = x_5 \times 2 = 2x_5$$
$$x_3 = x_4 \times 1 + x_5 = 3x_5$$
$$x_2 = x_3 \times 1 + x_4 = 5x_5$$
$$x_1 = x_2 \times 2 + x_3 = 13x_5.$$

最初は$x_1 = 1,$

$x_2 = 0.384615384615\cdots$だから

$$x_2 = x_2/x_1 = (5x_5/13x_5) = 5/13\,(\text{答}).$$



$1+1=0$での互除法

問い: （先に見たような）$\mathbb{F}_2$べき級数

$$0.00101110010111\cdots$$

を$\mathbb{F}_2$多項式/$\mathbb{F}_2$多項式$= g(t)/f(t)$ の形で表わせ。

解答：互除法。

整数が$\mathbb{F}_2$多項式に、大きさが「次数」に置き換わる。

$x_1 = 1, x_2 = 0.100101110010111\cdots$ とおく。

$10 \times x_2 = 1.00101110010111\cdots$

$$\begin{aligned} x_1 &= 1.00000000000000 \\ 10 \times x_2 &= 1.00101110010111\cdots \\ \text{差} \quad &\quad 0.00101110010111\cdots \end{aligned}$$

$x_1 = 10 \times x_2 + 0.00101110010111\cdots = 10 \times x_2 + x_3,$

$x_3 = 0.00101110010111\cdots$ とおく。

$$\begin{aligned} x_2 &= 0.100101110010111\cdots \\ 100 \times x_3 &= 0.101110010111\cdots \\ \text{差} \quad &\quad 0.00101110010111\cdots \end{aligned}$$

$x_2 - 100 \times x_3 = 0.00101110010111\cdots = x_3$

$x_2 = 100 \times x_3 + x_3 = 101 \times x_3$

$\therefore x_1 = 10 \times x_2 + x_3 = 1010 \times x_3 + x_3 = 1011x_3$

$x_2 = x_2/x_1 = 101/1011 = (t^2 + 1)/(t^3 + t + 1)$

定理 (Berlekamp-Massey, 1969)
べき級数xがある未知の$\mathbb{F}_2[t]$多項式の商$g(t)/f(t)$で表わされるとする。$f(t)$の次数がN以下だと分かっているとする。xが小数点以下$2N-1$桁まで与えられれば、上の互除法により$g(t), f(t)$は正確に求まる。(余りが小数点以下$2N$桁まで0になったら、それを0として逆算すれば良い。)

応用:暗号解読
先に見た暗号で、$f(t)$の次数がN以下とする。送信されたメッセージの最初の$2N-1$個が0であるとわかっているとすると、暗号化されたメッセージの最初の$2N-1$個からパスワード$g(t), f(t)$が互除法で求まる。

変形版：メッセージの最初の$2N-1$個の0-1が分かれば、残りのメッセージは解読できる。

$\because$ 暗号化文 $-$ メッセージ $= g(t)/f(t)$ だから、
その最初の$2N-1$個が特定できればよい。

$1+1=0$の応用例：メルセンヌツイスター疑似乱数

メルセンヌツイスター疑似乱数(松本-西村1998)

$\mathbb{F}_2$成分の32次元ベクトルの列を次の漸化式で生成し、

$$\vec{x}_{n+624} = \vec{x}_{n+q} + B\vec{x}_{n+1} + C\vec{x}_n$$

$T\vec{x}_n$を出力列とする。ここにB, C, Tはうまく選ばれた
３２次正方行列。

1. 周期は$2^{19937} - 1 > 10^{6000}$
2. 出力列は、623次元空間内で均等分布している
3. 高位ビットはさらに高次元
   （例えば上位3ビットは6240次元まで均等分布）
4. それまでの生成法よりも数倍高速に生成

高次元の互除法（格子簡約）など、$1+1=0$の世界
での代数・幾何を利用して周期や均等分布の次元を求めた。

まとめ：数学の予期せぬ効用

- $1+1=0$ の数学の研究は、ガロア $(1830$ ごろ$)$ に遡る
- 当時は応用の見えなかった純粋数学が、
  現在実用されている。
- $\mathbb{F}_2[t]$ と整数は良く似ており、代数・幾何が展開できる。
  前者が扱いやすい（現代整数論の指導原理の一つ）

終わり

周期保証：Mersenne素数の利用

定理 $f(t)$を定数項が1のn次$\mathbb{F}_2$多項式とする$(n \geq 2)$。
$2^n - 1$が素数とする。
$1/f(t)$のべき級数展開の周期が最大値$2^n - 1$を満たす必要十分条件は、

$$t = t^{2^n} \mod f(t)$$

となること。

n回$(\mod f(t))$で二乗すればよい。
nが１００万くらいまでなら計算機でチェックできる。

必要性：周期が$2^n - 1$ならば$1 = t^{2^n - 1} \mod f(t)$.

十分性：$t = t^{2^n} \mod f(t)$と$f(t)$がtと互いに素なことから

$$1 = t^{2^n-1} \mod f(t).$$

周期をPとすると

$$1 = t^{P} \mod f(t).$$

$2^n - 1$をPで割ったあまりを$r < P$とすると

$$1 = t^{2^n-1} \mod f(t) = t^{Pq+r} \mod f(t) = t^{r} \mod f(t).$$

周期Pの最小性から$r = 0$。
すなわちPは$2^n - 1$の約数である.

$2^n - 1$が素数であることを使うと$P = 1$または$P = 2^n - 1$。
$n \geq 2$ より$P = 1$は不可能。
よって$P = 2^n - 1$。

注　$2^n - 1$が素数となるとき、メルセンヌ素数という。
2010年11月現在で47個知られており、既知の最大は

$$2^{43,112,609} - 1。$$

メルセンヌツイスターに使った$2^{19937} - 1$は
２４番目のメルセンヌ素数。