③桁数は必要に応じて区切ってゆく。たとえば，17行目の乱数は3桁ずつに区切り次のようになる。

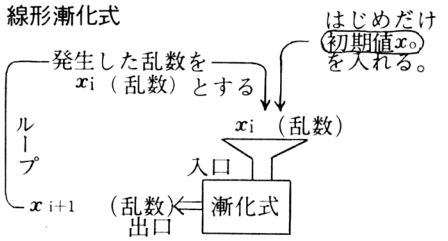
998　375　283　532　258　354　304 ‥‥

3　乱数のつくり方（算術式による）

今まで考えてきた乱数は，ある区間に出現する度数が一様に等しい乱数で，一様乱数という。この乱数は，他の特殊な乱数の基盤となり，もっとも多く用いられるので，これに重点をおきたい。そして，この節では算術乱数の発生法について調べてみよう。

(1)　乗算式合同法

Ⅰ）線形漸化式



上図は，乱数ができる機能をモデル化したものである。ある算術漸化式に初期値 x_0 が入る（代入する）と，出口から乱数 x_{i+1} が出てくる。

次に出てきた乱数を x_i として入口から入れると出口から別な乱数 x_{i+1} が出てくる。このループが繰り返されると，ループの回数だけ乱数が発生するというのが線形漸化式による発生法で，殆んどがこの方式をもちいている。

Ⅱ）合　同　式

ところで，漸化式に使われる式は何か，というと，数学の先生以外は，日頃お目に掛らない式で整数論でガウスが考案した式だといわれている。

> 与えられた正の整数をmとする。整数a，bの差がmでわりきれるとき，aとbはmを法として合同であるといい，次のようにあらわす。これを合同式という。
>
> $a \equiv b \pmod{m}$
>
> ただし，modはラテン語のmodul us（小さい尺度の意味）を略記したものである。

読み方は，「a 合同b，モードm」または「a 合同b，モジュラスm」とよむ。

いま，　$8 \equiv 14 \pmod{3}$　を例にとって考えてみよう。定義によって　$8-14=6$ が3でわれるから，なる程と思う。

しかし，「8と14は3を法として合同である」とはどんな意味か。8と14を分析すると，

$8=3\times2+2=6+2$　　3の倍数は6

$14=3\times4+2=12+2$　　3の倍数は12

となり，6，12を無視すると両数とも2と同じ，つまり，8も14も3を法とした場合，乗余が2となりお互いが同じ（合同）だということになる。そういうことになると，8と14だけでなく

$\{2,5,8,11,14,17,\cdots\} \equiv \{2,5,8,11,14,17\cdots\}$

左右の集合がすべて合同だということになる。これは，あたかも二つの合同なる図形が，位置の差を無視すれば，全く合致するのと同様である。

合同ということは，整数論だけでなく日常生活のなかで，それとなく使われている。

たとえば，1日は24時間をmodとし，1週間は7日をmodとし，1年は365日をmodとしていることに気づく。そしてもっと平たくいうと，

> $a \equiv b \pmod{m}$ は
> ○bをmで割った余りがaである　（b〉m）
> ○aをmで割った余りがbである　（a〉m）
> ○aとbを交換しても式の意味は変らない
> ○mを法とするとは，mを除数とするということ

だとわかる。次の例解をやってみよう。

(例)①　3でわって1あまる集合は

(解)$\{1,4,7,10,13\cdots\} \equiv 1 \pmod{3}$

②　3で割りきれる数 x を合同式では

(解)　$x \equiv 0 \pmod{3}$

③　$5 \equiv x+12 \pmod{12}$　の x は

(解)　$x=5$

④午前とか午後とかを使って時刻を表わすとき

7時から6時間後は　$7+6=1$時

3時から12時間後は　$3+12=3$時

2時より5時間前は何時か　$2-5=9$時

6時の8時間前は　$6-8=10$時

以上の問題を合同法で解きなさい。