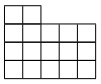
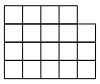
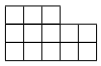
中学生のための玉原数学教室　　東京大学玉原国際セミナーハウス
講義 (2)　大島 利雄　　2010 年 10 月 16 日

「役に立つ素数」

1　余りの計算

- ある数を 5 で割った余りの数は、その数に 5 で割り切れる数を足しても変わりません。ある 2 つの数の和を 5 で割った余りは、それぞれの数を 5 で割った「余りの和」を 5 で割った数と等しくなります。


+

: 余り 3　　

+

; 余り 2

このことは、5 を別の数にしても同じです。

5 で割った余りのみに注目して、余りの和の計算の表を完成して下さい。余りは 0 から 4 までなので、表には 0 から 4 までの数が出てきます。

5 でなくて、6 の場合も和の表を作りましょう。

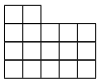
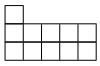
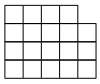
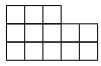
+	0	1	2	3	4
0					
1					
2					
3					
4					

5 で割った余りの和の表

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

6 で割った余りの和の表

- ある 2 つの数の積を 5 で割った余りは、それぞれの数を 5 で割った余りの積を 5 で割った余りと等しくなります。


×

: 余り 2　　

×

; 余り 2

このことは、5 を別の数にしても同じです。

5 で割った余りのみに注目して、余りの積の計算の表を完成して下さい。

5 でなくて、6 の場合も積の表を作りましょう。

×	0	1	2	3	4
0					
1					
2					
3					
4					

5 で割った余りの積の表

×	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

6 で割った余りの積の表

- ある数で割った余りに注目すると、数の余りのみに注目した和と積の演算をすることができます。これをその数を**法**とする演算といいます。法とする数を括弧で囲んで、以下のように表します。

$5 \equiv 0 \quad (5)$

$24 \equiv 4 \quad (5)$

$2+1 \equiv 3 \quad (5), \quad 3+4 \equiv 2 \quad (5), \quad 2 \times 1 \equiv 2 \quad (5), \quad 3 \times 4 \equiv 2 \quad (5)$

- 以下の $\equiv$ の右辺を ( ) の数より小さな数で表して下さい（割り算の余り）。

$10 \equiv \quad (9)$ $\qquad$ $100 \equiv \quad (9)$

$1000 \equiv \quad (9)$ $\qquad$ $1000000 \equiv \quad (9)$

$1234567 \equiv \quad (9)$ $\qquad$ $7654321 \equiv \quad (9)$

$1234567 \times 7654321 \equiv \quad (9)$ $\qquad$ $2^{100} \equiv \quad (9)$

- 1234567×7654321 は 13 桁の数で、$944977\square114007$ となります。$\square$ に当てはまる数字は何でしょうか？

- 次も同様な計算をして下さい

$10 \equiv \quad (11)$ $\qquad$ $100 \equiv \quad (11)$

$1000 \equiv \quad (11)$ $\qquad$ $1000000 \equiv \quad (11)$

$1234567 \equiv \quad (11)$ $\qquad$ $7654321 \equiv \quad (11)$

$1234567 \times 7654321 \equiv \quad (11)$ $\qquad$ $2^{100} \equiv \quad (11)$

- 3 で割った余りが 2 の数や、5 で割った余りが 2 や 3 の数は平方数でない。7 で割った余りで考えると？

2　引き算と割り算

5 および 6 を法とする足し算とかけ算の表を作りました。ある数を法とすると少ない数で表すことができます。その少ない数の中で、引き算と割り算が出来るかどうか調べて見ましょう。

- （0 でない数で）割り算が出来るのは、素数を法とする演算のときである。

  割り算を計算する方法として、ユークリッドの互除法がある。

$$5 \times \square \equiv 1 \quad (13)$$

を解いてみよう（13 を法とする、5 の逆数の計算）

$$\begin{aligned} \mathbf{13} &= 2 \times \mathbf{5} + \underline{3} \\ \mathbf{5} &= 1 \times \underline{\mathbf{3}} + \underline{\underline{2}} \\ \mathbf{3} &= 1 \times \underline{\underline{\mathbf{2}}} + 1 \end{aligned} \qquad \begin{aligned} 1 &= \mathbf{3} - 1 \times \mathbf{2} \\ &= \mathbf{3} - 1 \times (\mathbf{5} - 1 \times \mathbf{3}) \\ &= 2 \times \mathbf{3} - 1 \times \mathbf{5} \\ &= 2 \times (\mathbf{13} - 2 \times \mathbf{5}) - 1 \times \mathbf{5} \\ &= 2 \times \mathbf{13} - 5 \times \mathbf{5} \\ &= (13 - 5) \times \mathbf{5} - (5 - 2) \times \mathbf{13} \end{aligned}$$

よって

$$5 \times 8 \equiv 1 \quad (13)$$

逆数が分かったので、たとえば

$$5 \times \square \equiv 3 \quad (13)$$

の □ を求めるには、上の式を 3 倍して

$$5 \times 24 \equiv 3 \quad (13)$$

より

$$5 \times 11 \equiv 3 \quad (13)$$

とすればよい。

3　素数の性質

自然数 p が素数かどうかの判定するには？

p が素数のときに成り立つ公式がある

Wilson の定理.　　$2 \times 3 \times \cdots \times (p-2) \equiv 1 \quad (p)$

たとえば

$$\begin{aligned} 2 \times 3 &\equiv 1 \quad (5) \\ 2 \times 3 \times 4 \times 5 &\equiv 1 \quad (7) \end{aligned}$$

Fermat の小定理. $a^{p-1} \equiv 1 \quad (p) \qquad (a = 1, 2, \ldots, p-1)$

たとえば

$$1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \quad (5)$$

証明. $p = 5$ のとき、積の表の各列に現れる数を見てみよう。

$a = 1, 2, \ldots, p-1$ とする。p は素数であるから、$p-1$ 個の数 $a, 2a, \ldots, (p-1)a$ を p で割った余りは全て異なり、並び替えると $1, \ldots, p-1$ となる。

$$\begin{aligned} 1 \times 2 \times \cdots \times (p-1) \times a^{p-1} &= a \times 2a \times \cdots \times (p-1)a \\ &\equiv 1 \times 2 \times \cdots \times (p-1) \quad (p) \end{aligned}$$

$1 \times 2 \times \cdots \times (p-1)$ を p で割った余り（それは Wilson の定理から $p-1$ となることがわかる）の（p を法とした）逆数をかけると、Fermat の小定理が得られる。

$p = 5$ のときは

$$1 \times 2 \times 3 \times 4 \times a^4 \equiv 1 \times 2 \times 3 \times 4 \quad (5)$$

の両辺に 4 をかける（$4 \times 1 \times 2 \times 3 \times 4 \equiv 1 \quad (5)$）。

- Wilson の定理は、2 以上 $p-2$ 以下の数の p を法とした逆数は元の数と異なることから示される（$m^2 \equiv 1 \quad (p)$ ならば $(m-1)(m+1) \equiv 0 \quad (p)$）。

フェルマーテスト. 与えられた p に対し、いくつかの a で Fermat の小定理が成り立つかどうかテストして、p が素数かどうかを調べる。

- $a = 2, 3, 5, 7$ に対してフェルマーテストをパスしてしまう 2.5×10^{10} 以下の素数でない数は $3215031751 = 151 \cdot 751 \cdot 28351$ のみ。

4 RSA 暗号

RSA 暗号は、最初に発見された公開鍵暗号で、最もよく使われている。

- 暗号の方法は公開される。それを用いて文章を暗号化したものが漏れても、復元できるのは公開元のみ。

  大きな 2 つの素数の積が与えられても、それを 2 つの素数に分解するのが困難な（実際上不可能な）ことに基づいている（2 つの素数は公開元のみが知っている）。

  [1] 異なる（大きな）素数 p, q を選び、$n = pq$ と $r = (p-1)(q-1)$ を計算する。

  [2] r と互いに素な（大きな）自然数 e を選ぶ。

  [3] $de \equiv 1 \quad (r)$ となる d を求める（ユークリッドの互除法）。

  [4] p, q, d を秘密にして、e, n を公開する。

  [5] **暗号化**：n 未満の自然数 m を暗号化した数は m^e を n で割った余り（x とする）。

  [6] **復元**：x^d を n で割った余りが m。

原理：$m^{(p-1)(q-1)} - 1 = (m^{q-1})^{p-1} - 1$ は p で割り切れる。同様に q でも割り切れるので、$n = pq$ で割り切れる。よって $m^r \equiv 1 \quad (n)$

$de = kr + 1$ となる自然数 k があるが

$$x^d \equiv (m^e)^d = m^{de} = m^{kr+1} = (m^r)^k \cdot m \equiv m \quad (n)$$