1.2　剰余の問題

(1) 割り算における商と余り

　自然数を自然数で割る割り算を行い，商と余りを求めることは，小学校で学んでいます。
例えば，52 を 3 で割ると，商は 17 で余りは 1 であり，

$$52=3\cdot 17+1$$

と表すことができます。ここで，商の 17 は，余りの 1 が割る数 3 よりも小さくなるように求めています。
ここでは，割られる数を自然数から整数に拡張します (負の整数を割ることも考える)。一般に，次のことが成り立ちます。

整数の割り算

整数 a と正の整数 b に対して，

$$a=bq+r\ ,\quad 0\leqq r<b$$

を満たす q と r がただ 1 通りに定まる

q を， a を b で割ったときの**商**， r を**余り**といいます。
$r=0$ のとき， a は b で**割り切れる**といい，
$r\neq 0$ のとき，**割り切れない**といいます。
例えば， $-52=3\cdot(-18)+2$ であるから，
-52 を 3 で割ったときの商は -18，余りは 2 です。

例1
a，b は自然数とする。b を a で割ると 5 余り，$b+15$ は a で割り切れるとき，a の値をすべて求めると $a=$ ア $\boxed{}$，イ $\boxed{}$ である。

(解説)
b を a で割ると 5 余り，$b+15$ は a で割り切れるから，

$b=ak+5$ (k は整数， $k\geqq 0$) … ①

$b+15=al$ (l は整数， $l\geqq 0$) … ②

とおける
① を ② に代入して，

$$(ak+5)+15=al$$

$$a(l-k)=20$$

$l-k$ は整数であり，
b を a で割った余りが 5 であるから，$a \geqq 6$ より
a は 20 の約数で，$a \geqq 6$ を満たす自然数より
$a = {}^{ア}10$，${}^{イ}20$

(2) 割り算の余りの性質

割り算の余りについて，以下の性質が成り立ちます。

割り算の余りの性質
2 つの整数 a, b を正の整数 m で割った余りがそれぞれ r, r' であるとき，
(1) $a+b$ を m で割った余りは，$r+r'$ を m で割った余りに等しい
(2) $a-b$ を m で割った余りは，$r-r'$ を m で割った余りに等しい
(3) ab を m で割った余りは，rr' を m で割った余りに等しい
(4) a^n (n は正の整数) を m で割った余りは，r^n を m で割った余りに等しい

$a = mk + r, b = ml + r'$ (k, l は整数，$k, l \geqq 0$) とおけるから，
(1) $a+b = m(k+l) + r + r'$ より
$m(k+l)$ は m で割り切れるので，
$a+b$ を m で割った余りは，$r+r'$ を m で割った余りに等しい。
(2) 同様
(3) $ab = (mk+r)(ml+r') = m(mkl + kr' + lr) + rr'$ より
$m(mkl + kr' + lr)$ は m で割り切れるので，
ab を m で割った余りは，rr' を m で割った余りに等しい。
(4) (3)より，$a^2 = aa$ を m で割った余りは，$r^2 = rr$ を m で割った余りに等しい。また，これを利用して，$a^3 = a^2 a$ を m で割った余りは，$r^2 r = r^3$ を m で割った余りに等しい。
これをくり返せばよい。

例2

m は 7 で割れば 3 余る整数，n は 7 で割れば 4 余る整数とする．このとき，

$m+2n$ を 7 で割ると余りは $^{ア}\boxed{}$ である.

mn を 7 で割ると余りは $^{イ}\boxed{}$ である.

n^3 を 7 で割ると余りは $^{ウ}\boxed{}$ である.

n^{2001} を 7 で割ると余りは $^{エ}\boxed{}$ である.

解説

$m=7k+3$，$n=7l+4$ (k, l は整数) とおける

(ア) $m+2n=(7k+3)+2(7l+4)=7(k+2l+1)+4$

よって，$m+2n$ を 7 で割ると余りは 4 である

別解 上の性質より，

$2n$ を 7 で割った余りは，$2\cdot4$ を 7 で割った余りに等しいから，

$m+2n$ を 7 で割った余りは，$3+2\cdot4$ を 7 で割った余りに等しい

よって，求める余りは 4

(イ) $mn=(7k+3)(7l+4)=7(7kl+4k+3l+1)+5$

よって，mn を 7 で割ると余りは 5 である

(ウ) $n^3=(7l+4)^3=7\{7^2l^3+3\cdot7\cdot4l^2+3\cdot4^2\cdot l+9\}+1$

よって，n^3 を 7 で割ると余りは 1 である

(エ) $n^{2001}=(n^3)^{667}$

n^3 を 7 で割った余りは 1 より，

$(n^3)^{667}$ を 7 で割った余りは，1^{667} を 7 で割った余りに等しいから，

求める余りは 1

例3

(1) 5^{100} を 4 で割った余りを求めよ.

(2) 15^{100} を 7 で割った余りを求めよ.

(3) 7^{100} を 5 で割った余りを求めよ。

(4) 1997^{1997} を 9 で割ったときの余りを求めよ.

解説

(1) 5 を 4 で割った余りは 1 であるから，

5^{100} を 4 で割った余りは， 1^{100} を 4 で割った余りに等しい

よって，求める余りは 1

(2) 15 を 7 で割った余りは 1 であるから，

15^{100} を 7 で割った余りは， 1^{100} を 7 で割った余りに等しい

よって，求める余りは 1

(3) $7^{100}=(7^4)^{25}$

7^4 を 5 で割った余りは 1 より($7^2=49, 7^3=343, 7^4=2401$)

$(7^4)^{25}$ を 5 で割った余りは， 1^{25} を 5 で割った余りに等しい

よって，求める余りは 1

(4) 1997 を 9 で割った余りは 8 であるから，

1997^{1997} を 9 で割った余りは， 8^{1997} を 9 で割った余りに等しい

$8^{1997}=8\cdot(8^2)^{998}$， 8^2 を 9 で割った余りは 1 より

$8\cdot(8^2)^{998}$ を 9 で割った余りは， $8\cdot1^{998}$ を 9 で割った余りに等しい

よって，求める余りは 8

例4

(1) 2^{2001} の一の位の数字は $\boxed{}$ である．

(2) 47^{2003} の一の位の数を求めよ．

解説

(1) $2^1=2$，$2^2=4$，$2^3=8$，$2^4=16$，$2^5=32$，…

一の位の数字は， 2，4，8，6，2，… より

周期が 4 で一の位の数字は繰り返す

$2001=4\cdot500+1$ より，2^{2001} の一の位の数字は 2

(2) 47 を 10 で割った余りは 7 であるから，

47^{2003} を 10 で割った余りは， 7^{2003} を 10 で割った余りに等しい

7^n ($n=1, 2, 3, \cdots$) の一の位の数字は，7, 9, 3, 1, 7, … より

周期が 4 で一の位の数字は繰り返す

$2003=4\cdot500+3$ より， 7^{2003} の一の位の数字は 3

よって，求める数は 3

注 一の位の数は 10 で割ったときの余りに等しい

例5

(1) n が負の整数でない整数であるとき， $10^{2n+1}+1, 10^{2n}-1$ が 11 の倍数であることを示せ。

(2) 自然数 m の 10 進表示を $a_l a_{l-1} \cdots a_2 a_1$ (各 a_i は0 以上 9 以下の整数) とする。$a_1-a_2+a_3-a_4+\cdots+(-1)^{l+1}a_l$ が 11 の倍数であれば， m も 11 の倍数であることを示せ。

(解説)

(1) $10^{2n+1}+1=10\cdot 100^n+1$

100 を 11 で割った余りは 1 より，

100^n を11で割った余りは， 1^n を11で割った余りに等しいから 1

よって， $10^{2n+1}+1$ を 11 で割った余りは， $10\cdot 1+1$ を 11 で割った余りに等しいから 0，すなわち， $10^{2n+1}+1$ は 11 の倍数である

同様に， $10^{2n}-1=100^n-1$ であるから，

11 で割った余りは， 1^n-1 を 11 で割った余りと等しく 0

よって， $10^{2n}-1$ は 11 の倍数である

(2) $m=a_l\cdot 10^{l-1}+a_{l-1}\cdot 10^{l-2}+\cdots+a_1\cdot 1$

(ⅰ) $l=2k-1$(k は自然数) のとき

$$\begin{aligned} m&=a_{2k-1}\cdot 10^{2k-2}+a_{2k-2}\cdot 10^{2k-3}+\cdots+a_1\cdot 1 \\ &=a_{2k-1}(10^{2k-2}-1)+a_{2k-2}(10^{2k-3}+1)+\cdots+a_2(10^2+1) \\ &\qquad +a_{2k-1}-a_{2k-2}+\cdots-a_2+a_1 \end{aligned}$$

(1)より， $a_{2k-1}(10^{2k-2}-1)+a_{2k-2}(10^{2k-3}+1)+\cdots+a_2(10^2+1)$ は 11 の倍数であるから，

$a_{2k-1}-a_{2k-2}+\cdots-a_2+a_1$ が 11 の倍数であれば， m も 11 の倍数

(ⅱ) $l=2k$ (k は自然数) のとき

$$\begin{aligned} m&=a_{2k}\cdot 10^{2k-1}+a_{2k-1}\cdot 10^{2k-2}+\cdots+a_1\cdot 1 \\ &=a_{2k}(10^{2k-1}+1)+a_{2k-1}(10^{2k-2}-1)+\cdots+a_2(10^2+1) \\ &\qquad -a_{2k}+a_{2k-1}-\cdots-a_2+a_1 \end{aligned}$$

(1)より， $a_{2k}(10^{2k-1}-1)+a_{2k-1}(10^{2k-2}+1)+\cdots+a_2(10^2+1)$ は 11 の倍数であるから，

$-a_{2k}+a_{2k-1}-\cdots-a_2+a_1$ が 11 の倍数であれば， m も 11 の倍数

(ⅰ), (ⅱ) より題意は示された

(3) 余りによる整数の分類

整数を 2 で割ると余りは 0 か 1 であるから，すべての整数 n は

$2k,\ 2k+1$ (k は整数)

のいずれかの形で表すことができます。 $2k$ は偶数， $2k+1$ は奇数です。

整数を 3 で割ると余りは 0 か 1 か 2 であるから，すべての整数 n は

$3k,\ 3k+1,\ 3k+2$ (k は整数)

のいずれかの形で表すことができます。

一般に，正の整数 m に対して，すべての整数 n は

$mk,\ mk+1,\ mk+2,\ \cdots,\ mk+(m-1)$ (k は整数)

のいずれかの形で表すことができます。

注 $\{2k-1 \mid k$ は整数$\}$ と $\{2k+1 \mid k$ は整数$\}$ は同じ集合を表すので，
すべての整数 n は，

$2k,\ 2k-1$ (k は整数)

のいずれかの形で表すことができる，としてもよい。
同様に，すべての整数 n は，

$3k,\ 3k+1,\ 3k-1$ (k は整数)

のいずれかの形で表すことができる，としてもよい。

例6
どのような整数 n に対しても，n^2+n+1 は 5 で割り切れないことを示せ.

(解説)
すべての整数 n は，

$5k,\ 5k+1,\ 5k+2,\ 5k+3,\ 5k+4$ (k は整数)

のいずれかの形で表すことができる
$n=5k$ のとき， $n^2+n+1=5(5k^2+k)+1$
$n=5k+1$ のとき， $n^2+n+1=5(5k^2+3k)+3$
$n=5k+2$ のとき， $n^2+n+1=5(5k^2+5k+1)+2$
$n=5k+3$ のとき， $n^2+n+1=5(5k^2+7k+2)+3$
$n=5k+4$ のとき， $n^2+n+1=5(5k^2+9k+4)+1$
よって，n^2+n+1 は 5 で割り切れない

別解
すべての整数 n は，

$5k,\ 5k\pm1,\ 5k\pm2$ (k は整数)

のいずれかで表すことができる

$n=5k$ のとき， $n^2+n+1=5(5k^2+k)+1$

$n=5k\pm1$ のとき， $n^2+n+1=5(5k^2\pm2k+k)+1\pm1+1$ (複号同順)

$n=5k\pm2$ のとき， $n^2+n+1=5(5k^2\pm4k+k)+4\pm2+1$ (複号同順)

よって， n^2+n+1 は 5 で割り切れない

例7

n は整数とする。$n(n+2)(n+4)$ は 3 の倍数であることを証明せよ。

解説

すべての整数 n は

$3k$，$3k+1$，$3k-1$ (k は整数)

のいずれかの形で表すことができる

$n=3k$ のとき， $n(n+2)(n+4)=3k(3k+2)(3k+4)=3\cdot k(3k+2)(3k+4)$

$n=3k+1$ のとき， $n(n+2)(n+4)=3\cdot(3k+1)(k+1)(3k+5)$

$n=3k-1$ のとき， $n(n+2)(n+4)=3\cdot(3k-1)(3k+1)(k+1)$

よって，$n(n+2)(n+4)$ は 3 の倍数である

確認問題1

a，b は自然数とする．a を 8 で割った余りを r，b を 8 で割った余りを s とする．

(1)　$a+b$ を 8 で割った余りと $r+s$ を 8 で割った余りが等しいことを示せ．

(2)　a^2 を 8 で割った余りと r^2 を 8 で割った余りが等しいことを示せ．

(3)　平方数を 8 で割ったとき，余りとして得られる数をすべて求めよ．ただし，平方数とは自然数の平方となっている数のことである．

(4)　2 つの平方数の和を 8 で割ると余りは 3 にはならないことを示せ．

解説

$a=8p+r$，$b=8q+s$ (p, q, r, s は整数，$0\leqq r\leqq 7$，$0\leqq s\leqq 7$) とおく

(1) $a+b=8(p+q)+r+s$

$8(p+q)$ は 8 で割り切れるから，

$a+b$ を 8 で割った余りと $r+s$ を 8 で割った余りは等しい　終

(2) $a^2=(8p+r)^2=8(8p^2+2pr)+r^2$

$8(8p^2+2pr)$ は 8 で割り切れるから

a^2を 8 で割った余りと，r^2 を 8 で割った余りは等しい　終

(3) 平方数 n^2 に対して，すべての整数 n は

　$8k+m$ (k は整数，$m=0, 1, 2, \cdots, 7$)

のいずれかの形で表すことができる

(2)より，$n^2=(8k+m)^2$ を 8 で割った余りは，m^2 を 8 で割った余りに等しいから，n^2 の余りとして得られる数は，

　$0, 1, 4, 1, 0, 1, 4, 1$

すなわち，$0, 1, 4$　答

(4) (1)より，2 つの平方数の和を 8 で割った余りは，

2 つの平方数をそれぞれ 8 で割った余りの和に等しいから

(3)の結果より，$0, 1, 2, 4, 5$

よって，題意は示された　終

確認問題2

(1) 2020^{10} を 7 で割ったときの余りを求めよ。

(2) 2000^{2000} を 12 で割ったときの余りを求めよ.

(解説)

(1) 2020 を 7 で割った余りは 4 より

2020^{10} を 7 で割った余りは，4^{10} を 7 で割った余りに等しい

$4^3=64$ を 7 で割った余りは 1 より

$4^{10}=4\cdot(4^3)^3$ を 7 で割った余りは，$4\cdot1^3$ を 7 で割った余りに等しい

よって，求める余りは 4　答

(2) 2000 を 12 で割った余りは 8 より

2000^{2000} を 12 で割った余りは，8^{2000} を 12 で割った余りに等しい

8^n (n は自然数)を 12 で割った余りは,

　$8, 4, 8, 4, \cdots$

と周期 2 で循環する

$2000=2\cdot1000$ より，8^{2000} を 12 で割った余りは 4　答

注

$8^{n+1}=8\cdot8^n$ (n は自然数) を 12 で割った余りは，8^n を 12 で割った余りに 8 をかけたものを 12 で割った余りに等しい

12 で割った余りは，$0, 1, 2, \cdots, 11$ の 12 通りなので,

8^m において，多くとも m が 13 以上となれば，鳩ノ巣原理より，12 で割った余りが同じものが存在し，そこから 12 で割った余りの循環が起こります。

確認問題3

今日は日曜日で，10 日後は水曜日である。100 日後および 100 万日後はそれぞれ何曜日か。理由とともに答えよ。

解説

曜日は，日，月，火，水，木，金，土の 7 日周期であるから，
n 日後の曜日は，n を 7 で割った余りによって分類される
n を 7 で割った余りを r とすると，
$r=0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$ のとき，日曜日から n 日後の曜日はそれぞれ日，月，火，水，木，金，土となる
$100=14\cdot7+2$ より，日曜日から 100 日後は火曜日，
$1000000=142857\cdot7+1$ より，日曜日から 100 万日後は月曜日である　答

確認問題4

n は整数とする。

(1)　$n(n+1)$ が偶数であることを示せ。

(2)　$n(n+1)(2n+1)$ が 6 の倍数であることを示せ。

(3)　$n(n+1)(2n+1)(3n^2+3n-1)$ が 30 の倍数であることを示せ。

解説

(1) $n(n+1)$ は連続 2 整数の積であるから，

$2!=2$ の倍数，すなわち偶数である　終

(2) $n(n+1)(2n+1)=n(n+1)\{(n+2)+(n-1)\}$

$=n(n+1)(n+2)+(n-1)n(n+1)$

$n(n+1)(n+2)$，$(n-1)n(n+1)$ は連続 3 整数の積であるから，

ともに $3!=6$ の倍数である

よって，$n(n+1)(2n+1)$ は 6 の倍数である　終

(3) $P(n)=n(n+1)(2n+1)(3n^2+3n-1)$ とおく

$n(n+1)(2n+1)$ は 6 の倍数であり，

$30=6\cdot5$ で，5 と 6 は互いに素であるから，

$P(n)$ が 5 の倍数であることを示せばよい

すべての整数は，$5k, 5k\pm1, 5k\pm2$ (k は整数)のいずれかの形で表すことができる

$n=5k$ のとき，n は 5 の倍数より，$P(n)$ は 5 の倍数

$n=5k+1$ のとき，

$3n^2+3n-1=3(5k+1)^2+3(5k+1)-1=5(15k^2+9k+1)$ は 5 の倍数より，

$P(n)$ は 5 の倍数

$n=5k+2$ のとき，$2n+1=2(5k+2)+1=5(2k+1)$ は 5 の倍数より，

$P(n)$ は 5 の倍数

$n=5k-2$ のとき，

$3n^2+3n-1=3(5k-2)^2+3(5k-2)-1=5(15k^2-3k+1)$ は 5 の倍数より，

$P(n)$ は 5 の倍数

$n=5k-1$ のとき，$n+1=5k$ は 5 の倍数より，$P(n)$ は 5 の倍数

よって，題意は示された　終

発展 合同式

合同式
2つの整数 a, b に対して， $a-b$ が m の倍数(m は正の整数)，すなわち，$a-b=km$ (k は整数) と表されるとき， a と b は m を**法**として**合同**であるといい， $a\equiv b \pmod{m}$ と表す。この式を**合同式**という。

合同式に関して，一般に次のことが成り立ちます。

$a\equiv b \pmod{m} \Leftrightarrow a, b$ を m で割った余りが等しい

$a=mq_1+r_1, b=mq_2+r_2$ (q_1, q_2, r_1, r_2 は整数， $0\leqq r_1, r_2<m$) とおくと，
$\rightarrow$
$a-b=m(q_1-q_2)+r_1-r_2$
$a\equiv b \pmod{m}$ であるから， $a-b=km$ (k は整数) より
$r_1-r_2=m(k-q_1+q_2)$
よって， r_1-r_2 は m の倍数である。
$0\leqq r_1, r_2<m$ であるから， $-m<r_1-r_2<m$ より
$r_1-r_2=0 \quad \therefore r_1=r_2$
$\leftarrow$
$r_1=r_2$ であるから，
$a-b=m(q_1-q_2)$
よって， $a-b$ は m の倍数より
$a\equiv b \pmod{m}$

この定理より，合同とは余りが等しいものを類別することであり，合同を使えば，余りが等しいグループに類別できます。
注 今節で，割られる数を0や負の整数も含めて整数まで拡張しました。
例えば， $-1=3\cdot(-1)+2$ より，
$-1\equiv 2 \pmod{3}$
とすることができます。

合同式の性質
a, b, c, d を整数， m, n を正の整数とする
以下， m を法として， $a \equiv c, b \equiv d$ のとき
(1) $a+b \equiv c+d$
(2) $a-b \equiv c-d$
(3) $ab \equiv cd$
(4) $a^n \equiv c^n$

$a \equiv c, b \equiv d$ より
$a-c=k_1m, b-d=k_2m$ (k_1, k_2 は整数)
(1) $(a+b)-(c+d)=(a-c)+(b-d)=(k_1+k_2)m$
よって， $a+b \equiv c+d$
(2) $(a-b)-(c-d)=(a-c)-(b-d)=(k_1-k_2)m$
よって， $a-b \equiv c-d$
(3) $ab-cd=ab-bc+bc-cd=b(a-c)+c(b-d)=(k_1b+k_2c)m$
よって， $ab \equiv cd$
(4) (3)より， $aa \equiv cc \quad \therefore a^2 \equiv c^2$
$a \equiv c, a^2 \equiv c^2$ より， $a^2a \equiv c^2c \quad \therefore a^3 \equiv c^3$
以下，これをくり返して， $a^n \equiv c^n$

この性質を利用すると，答案を簡潔に書くことができます。
例えば,
例3 の(3)は，5 を法として考えて， $7^{100}=49^{50} \equiv (-1)^{50}=1$
よって，余りは 1
例6 は,
以下，5 を法として考える
すべての整数 n は， $n \equiv 0, \pm 1, \pm 2$ のいずれかで表すことができる
$n \equiv 0$ のとき， $n^2+n+1 \equiv 0^2+0+1=1$
$n \equiv \pm 1$ のとき， $n^2+n+1 \equiv 1 \pm 1+1 \not\equiv 0$ (複合同順)
$n \equiv \pm 2$ のとき， $n^2+n+1 \equiv 4 \pm 2+1 \not\equiv 0$ (複合同順)
よって， n^2+n+1 は 5 の倍数ではない
のように，簡潔に書くことができます。