数学演習（剰余類•合同式•互除法•１次不定方程式）Ｈ２９．２．１３　　　　(　　)組(　　)番　名前(　　　　　　　　　　　)

$\boxed{1}$ a，b は整数とする。a を 7 で割ると 3 余り，b を 7 で割ると 4 余る。このとき，次の数を 7 で割った余りを求めよ。

(1) $a+2b$　　(2) ab　　(3) a^4　　(4) a^{2013}

$\boxed{2}$ n は整数とする。次のことを証明せよ。

(1) n^4+2n^2 は 3 の倍数である。　　(2) n^2+n+1 は 5 で割り切れない。

$\boxed{3}$ a，b，c は整数とし，$a^2+b^2=c^2$ とする。a，b のうち，少なくとも 1 つは 3 の倍数であることを証明せよ。

$\boxed{4}$ 次のものを求めよ。

(1) (ア) 13^{100} を 9 で割った余り　　(イ) 2000^{2000} を 12 で割った余り

(2) 47^{2011} の一の位の数

$\boxed{5}$ 次の 2 つの整数の最大公約数を，互除法を用いて求めよ。

(1)　323，884　　(2)　943，1058　　(3)　1829，2077

$\boxed{6}$ 次の方程式の整数解をすべて求めよ。

(1)　$9x+5y=1$　　(2)　$19x-24y=1$

$\boxed{7}$ 次の方程式の整数解をすべて求めよ。

(1)　$7x+6y=40$　　(2)　$37x-90y=4$

$\boxed{8}$ 3 で割ると 2 余り，5 で割ると 3 余り，7 で割ると 4 余るような自然数 n で最小のものを求めよ。

1 a, b は整数とする。a を 7 で割ると 3 余り，b を 7 で割ると 4 余る。このとき，次の数を 7 で割った余りを求めよ。

(1)　$a+2b$　　(2)　ab　　(3)　a^4　　(4)　a^{2013}

解答　(1)　4　　(2)　5　　(3)　4　　(4)　6

解説

$a=7q+3$，$b=7q'+4$ (q，q' は整数) と表される。

(1)　$a+2b=7q+3+2(7q'+4)=7(q+2q')+3+8=7(q+2q'+1)+4$

したがって，求める余りは　4

(2)　$ab=(7q+3)(7q'+4)=49qq'+7(4q+3q')+12=7(7qq'+4q+3q'+1)+5$

したがって，求める余りは　5

(3)　$a^2=(7q+3)^2=49q^2+42q+9=7(7q^2+6q+1)+2$

よって，$a^2=7m+2$ (m は整数) と表されるから

$a^4=(a^2)^2=(7m+2)^2=49m^2+28m+4=7(7m^2+4m)+4$

したがって，求める余りは　4

(4)　a^3 を 7 で割った余りは，3^3 を 7 で割った余り 6 に等しい。

よって，$(a^3)^2=a^6$ を 7 で割った余りは，$6^2=36$ を 7 で割った余り 1 に等しい。

$a^{2013}=a^{2010}a^3=(a^6)^{335}\cdot a^3$ であるから，求める余りは，$1^{335}\cdot 6=6$ を 7 で割った余りに等しい。したがって，求める余りは　6

別解　[(1)～(3) 割り算の余りの性質を利用した解法]

(1)　2 を 7 で割った余りは 2 ($2=7\cdot 0+2$) であるから，$2b$ を 7 で割った余りは $2\cdot 4=8$ を 7 で割った余り 1 に等しい。

ゆえに，$a+2b$ を 7 で割った余りは $3+1=4$ を 7 で割った余りに等しい。

よって，求める余りは　4

(2)　ab を 7 で割った余りは $3\cdot 4=12$ を 7 で割った余りに等しい。

よって，求める余りは　5

(3)　a^4 を 7 で割った余りは $3^4=81$ を 7 で割った余りに等しい。

よって，求める余りは　4

別解　[合同式を利用した解法]

mod 7 において，$a\equiv 3$，$b\equiv 4$ と表される。

(1)　$a+2b\equiv 3+2\cdot 4=11\equiv 4$　よって，求める余りは　4

(2)　$ab\equiv 3\cdot 4=12\equiv 5$　よって，求める余りは　5

(3)　$a^4\equiv 3^4=81\equiv 4$　よって，求める余りは　4

(4)　$a\equiv 3$　より　$a^2\equiv 3^2=9\equiv 2$　$a^6=(a^2)^3\equiv 2^3=8\equiv 1$　より

$a^{2013}=a^{2010}a^3=(a^6)^{335}\cdot a^3\equiv 1^{335}\cdot 3^3=27\equiv 6$

したがって，求める余りは　6

2 n は整数とする。次のことを証明せよ。

(1)　n^4+2n^2 は 3 の倍数である。　　(2)　n^2+n+1 は 5 で割り切れない。

解説

(1)　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される。

$n^4+2n^2=n^2(n^2+2)$ であるから

[1]　$n=3k$ のとき

$n^4+2n^2=9k^2(9k^2+2)=3\cdot 3k^2(9k^2+2)$

[2]　$n=3k+1$ のとき

$n^4+2n^2=(3k+1)^2(9k^2+6k+1+2)=3(3k+1)^2(3k^2+2k+1)$

[3]　$n=3k+2$ のとき

$n^4+2n^2=(3k+2)^2(9k^2+12k+4+2)=3(3k+2)^2(3k^2+4k+2)$

よって，n^4+2n^2 は 3 の倍数である。

別解　[割り算の余りの性質を利用した解法]

整数 n を3で割った余りは $0,1,2$ のどれかである。

[1]　余り 0 のとき

n^4+2n^2 を3で割った余りは $0^4+2\cdot 0^2$ を3で割った余りに等しいので，余り0

[2]　余り 1 のとき

n^4+2n^2 を3で割った余りは $1^4+2\cdot 1^2=3$ を3で割った余りに等しいので，余り0

[3]　余り 2 のとき

n^4+2n^2 を3で割った余りは $2^4+2\cdot 2^2=24$ を3で割った余りに等しいので，余り0

よって，n^4+2n^2 は 3 の倍数である。

別解　[合同式を利用した解法]

mod 3 において，整数 n は $n\equiv 0$，$n\equiv 1$，$n\equiv 2$ のどれかで表される。

[1]　$n\equiv 0$ のとき

$n^4+2n^2\equiv 0^4+2\cdot 0^2=0$

[2]　$n\equiv 1$ のとき

$n^4+2n^2\equiv 1^4+2\cdot 1^2=3\equiv 0$

[3]　$n\equiv 2$ のとき

$n^4+2n^2\equiv 2^4+2\cdot 2^2=24\equiv 0$

よって，n^4+2n^2 は 3 の倍数である。

別解　[連続する整数の積の性質を利用した解法]

$n^4+2n^2=n^2(n^2+2)=n^2\{(n^2-1)+3\}$

$=n^2(n^2-1)+3n^2$

$=n^2(n+1)(n-1)+3$ の倍数

$=n\times(n-1)n(n+1)+3$ の倍数 $=n\times 6$ の倍数 $+3$ の倍数

(2)　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される。

[1]　$n=5k$ のとき　　$n^2+n+1=5(5k^2+k)+1$

[2]　$n=5k+1$ のとき　　$n^2+n+1=5(5k^2+3k)+3$

[3]　$n=5k+2$ のとき　　$n^2+n+1=5(5k^2+5k+1)+2$

[4]　$n=5k+3$ のとき　　$n^2+n+1=5(5k^2+7k+2)+3$

[5]　$n=5k+4$ のとき　　$n^2+n+1=5(5k^2+9k+4)+1$

それぞれの場合について，n^2+n+1 を 5 で割った余りは，1，3，2，3，1 であり，n^2+n+1 は 5 で割り切れない。

別解　[割り算の余りの性質を利用した解法]

整数 n を5で割った余りは $0,1,2,3,4$ のどれかである。

[1]　余り 0 のとき

n^2+n+1 を5で割った余りは 0^2+0+1 を5で割った余りに等しいので，余り1

[2]　余り 1 のとき

n^2+n+1 を5で割った余りは 1^2+1+1 を5で割った余りに等しいので，余り3

[3]　余り 2 のとき

n^2+n+1 を5で割った余りは 2^2+2+1 を5で割った余りに等しいので，余り2

[4]　余り 3 のとき

n^2+n+1 を5で割った余りは 3^2+3+1 を5で割った余りに等しいので，余り3

[5]　余り 4 のとき

n^2+n+1 を5で割った余りは 4^2+4+1 を5で割った余りに等しいので，余り1

以上より，　n^2+n+1 は 5 で割り切れない。

別解　[合同式を利用した解法]

mod 5 において，整数 n は $n\equiv 0$，$n\equiv 1$，$n\equiv 2$，$n\equiv 3$，$n\equiv 4$ のどれかで表される。

[1]　$n\equiv 0$ のとき

$n^2+n+1\equiv 0^2+0+1=1$

[2]　$n\equiv 1$ のとき

$n^2+n+1\equiv 1^2+1+1=3$

[3]　$n\equiv 2$ のとき

$n^2+n+1\equiv 2^2+2+1=7\equiv 2$

[4]　$n\equiv 3$ のとき

$n^2+n+1\equiv 3^2+3+1=13\equiv 3$

[5]　$n\equiv 4$ のとき

$n^2+n+1\equiv 4^2+4+1=21\equiv 1$

以上より，　n^2+n+1 は 5 で割り切れない。

3 a，b，c は整数とし，$a^2+b^2=c^2$ とする。a，b のうち，少なくとも 1 つは 3 の倍数であることを証明せよ。

解説

背理法で証明する。a，b はともに 3 の倍数でないと仮定する。

このとき，a^2，b^2 は　$(3k+1)^2=3(3k^2+2k)+1$，　$(3k+2)^2=3(3k^2+4k+1)+1$

のどちらかの式の k に適当な整数を代入すると，それぞれ表される。

$3k^2+2k$，$3k^2+4k+1$ は整数であるから，3 の倍数でない数 a，b の 2 乗を 3 で割った余りはともに 1 である。

したがって，a^2+b^2 を 3 で割った余りは 2 である。　…… ①

一方，c が 3 の倍数のとき，c^2 は 3 で割り切れ，

c が 3 の倍数でないとき，c^2 を 3 で割った余りは 1 である。

すなわち，c^2 を 3 で割った余りは 0 か 1 である。　…… ②

①，② は両辺を同じ数で割ったときに余りが一致することはないことを意味し，

$a^2+b^2=c^2$ であることに矛盾する。

ゆえに，$a^2+b^2=c^2$ ならば，a，b のうち，少なくとも 1 つは 3 の倍数である。

別解　[合同式を利用した解法]

背理法で証明する。a，b はともに 3 の倍数でないと仮定する。

mod 3において　$a\equiv 1$ ならば $a^2\equiv 1$，$a\equiv 2$ ならば $a^2\equiv 2^2=4\equiv 1$ であるので

a が3の倍数でなければ $a^2\equiv 1$ である。b についても同様で b が3の倍数でなければ $b^2\equiv 1$ であるから，$a^2+b^2\equiv 1+1=2$

したがって，a^2+b^2 を 3 で割った余りは 2 である。　…… ①

一方，c が 3 の倍数のとき，$c^2\equiv 0$，c が 3 の倍数でないとき，$c^2\equiv 1$ である。

すなわち，c^2 を 3 で割った余りは 0 か 1 である。　…… ②

①，② は両辺を同じ数で割ったときに余りが一致することはないことを意味し，

$a^2+b^2=c^2$ であることに矛盾する。

ゆえに，$a^2+b^2=c^2$ ならば，a，b のうち，少なくとも 1 つは 3 の倍数である。

4 次のものを求めよ。

(1)　(ア)　13^{100} を 9 で割った余り　　(イ)　2000^{2000} を 12 で割った余り

(2)　47^{2011} の一の位の数　　解答　(1)　(ア)　4　　(イ)　4　　(2)　3

解説

(1)　(ア)　13を9で割った余りは4 であり

4^3 を9で割った余りは1 である

ゆえに　$4^{100}=4\cdot(4^3)^{33}$ より

(13^{100} を9で割った余り)=(4^{100} を9で割った余り)

=($4\cdot(4^3)^{33}$ を9で割った余り)

=($4\cdot 1^{33}$ を9で割った余り)=4

したがって，求める余りは　4

（イ） 2000を12で割った余りは8 であり

8^2 を12で割った余りは4

（$8^3=8^2\cdot 8$ を12で割った余り)=(4・8を12で割った余り)=8

（$8^4=8^3\cdot 8$ を12で割った余り)=(8・8を12で割った余り)=4

ゆえに，余りは4と8を繰り返すのでk を自然数とすると

8^{2k} (つまり，8の偶数乗)を12で割った余りは4

よって （2000^{2000} を12で割った余り)=(8^{2000}を12で割った余り)=4

したがって，求める余りは　4

(2) 47を10で割った余りは7 であり，7^2 を10で割った余りは9

(7^4 を10で割った余り)=(9^2 を10で割った余り)=1

ゆえに　$7^{2011}=(7^4)^{502}\cdot 7^3$ と変形できるので

よって　(47^{2011} を10で割った余り)=(7^{2011} を10で割った余り)

=($(7^4)^{502}\cdot 7^3$ を10で割った余り)

=($(1)^{502}\cdot 9\cdot 7$ を10で割った余り)=3

したがって，47^{2011} の一の位の数は　3

別解　［合同式を利用した解法］

(1) (ア) $13\equiv 4 \pmod 9$ であり　$4^2\equiv 16\equiv 7 \pmod 9$，$4^3\equiv 64\equiv 1 \pmod 9$

ゆえに　$4^{100}\equiv 4\cdot(4^3)^{33}\equiv 4 \pmod 9$

よって　$13^{100}\equiv 4^{100}\equiv 4 \pmod 9$

したがって，求める余りは　4

(イ) $2000\equiv 8 \pmod{12}$ であり

$8^2\equiv 64\equiv 4 \pmod{12}$，$8^3\equiv 8\cdot 4\equiv 8 \pmod{12}$，$8^4\equiv (8^2)^2\equiv 4^2\equiv 4 \pmod{12}$

ゆえに，余りは4と8を繰り返すのでkを自然数とすると　$8^{2k}\equiv 4 \pmod{12}$

よって　$2000^{2000}\equiv 8^{2000}\equiv 4 \pmod{12}$

したがって，求める余りは　4

(2) $47\equiv 7 \pmod{10}$ であり

$7^2\equiv 49\equiv 9 \pmod{10}$，$7^3\equiv 9\cdot 7\equiv 3 \pmod{10}$，$7^4\equiv 9^2\equiv 1 \pmod{10}$

ゆえに　$7^{2011}\equiv (7^4)^{502}\cdot 7^3\equiv 1^{502}\cdot 3\equiv 1\cdot 3\equiv 3 \pmod{10}$

よって　$47^{2011}\equiv 7^{2011}\equiv 3 \pmod{10}$

したがって，47^{2011} の一の位の数は　3

5 次の２つの整数の最大公約数を，互除法を用いて求めよ。

(1) 323，884　(2) 943，1058　(3) 1829，2077

解答　(1) 17　(2) 23　(3) 31

解説

(1) $884=323\cdot 2+238$

$323=238\cdot 1+85$

$238=85\cdot 2+68$

$85=68\cdot 1+17$

$68=17\cdot 4$

4	1	2	1	2
17) 68	) 85	) 238	) 323	) 884
68	68	170	238	646
0	17	68	85	238

よって，最大公約数 は　17

(2) $1058=943\cdot 1+115$

$943=115\cdot 8+23$

$115=23\cdot 5$

5	8	1
23) 115	) 943	) 1058
115	920	943
0	23	115

よって，最大公約数 は　23

(3) $2077=1829\cdot 1+248$

$1829=248\cdot 7+93$

$248=93\cdot 2+62$

$93=62\cdot 1+31$

$62=31\cdot 2$

2	1	2	7	1
31) 62	) 93	) 248	) 1829	) 2077
62	62	186	1736	1829
0	31	62	93	248

よって，最大公約数 は　31

6 次の方程式の整数解をすべて求めよ。

(1) $9x+5y=1$　(2) $19x-24y=1$

解答　(1) $x=5k-1$，$y=-9k+2$ (k は整数)

(2) $x=24k-5$，$y=19k-4$ (k は整数)

解説

(1) $9x+5y=1$ …… ①

$x=-1$，$y=2$ は ① の整数解の 1 つである。

よって　$9\cdot(-1)+5\cdot 2=1$ …… ②

①−② から　$9(x+1)+5(y-2)=0$

すなわち　$9(x+1)=-5(y-2)$ …… ③

9 と 5 は互いに素であるから，$x+1$ は 5 の倍数である。

ゆえに，k を整数として，$x+1=5k$ と表される。

③ に代入して　$9\cdot 5k=-5(y-2)$　すなわち　$y-2=-9k$

よって，解は　$x=5k-1$，$y=-9k+2$ (k は整数)

(2) $x=-5$，$y=-4$ は方程式の整数解の 1 つである。

よって　$19(x+5)-24(y+4)=0$

すなわち　$19(x+5)=24(y+4)$ …… ①

19 と 24 は互いに素であるから，$x+5$ は 24 の倍数である。

ゆえに，k を整数として，$x+5=24k$ と表される。

① に代入して　$19\cdot 24k=24(y+4)$　すなわち　$y+4=19k$

よって，解は　$x=24k-5$，$y=19k-4$ (k は整数)

注意　19 と 24 で互除法を用いて，1 組の解 $x=-5$，$y=-4$ を見つける方法

$24=19\cdot 1+5$　移項して　$24-19\cdot 1=5$

$19=5\cdot 3+4$　移項して　$19-5\cdot 3=4$

$5=4\cdot 1+1$　移項して　$5-4\cdot 1=1$

よって　$1=5-4\cdot 1=5-(19-5\cdot 3)\cdot 1=19\cdot(-1)+5\cdot 4=19\cdot(-1)+(24-19\cdot 1)\cdot 4$

$19\cdot(-1)+(24-19\cdot 1)\cdot 4$ を整理して　$1=19\cdot(-5)-24\cdot(-4)$

参考　合同式を利用した解法

(1) mod 5 において $9x+5y\equiv 4x+0y=4x$ より $4x\equiv 1 \pmod 5$ を考える。

両辺4倍すると　$16x\equiv 4$ であり，$16\equiv 1$であるから　$x\equiv 4 \pmod 5$

つまり，xを5で割ると余りが4であるので，k を整数として $x=5k+4$ と書ける。

$9x+5y=1$ に代入して　$9(5k+4)+5y=1$

yについて解いて　$y=-9k-7$

よって解は　$x=5k+4$，$y=-9k-7$　(k は整数)

(2) mod 19 において $19x-24y\equiv 0x-5y=-5y$ より $-5y\equiv 1 \pmod{19}$ を考える。

両辺(-4)倍すると　$20y\equiv -4$ であり，$20\equiv 1$，$-4\equiv 15$であるから　$y\equiv 15 \pmod{19}$

つまり，yを19で割ると余りが15であるので，k を整数として $y=19k+15$ と書ける。

$19x-24y=1$ に代入して　$19x-24(19k+15)=1$

xについて解いて　$x=24k+19$

よって解は　$x=24k+19$，$y=19k+15$　(k は整数)

7 次の方程式の整数解をすべて求めよ。

(1) $7x+6y=40$　(2) $37x-90y=4$

解答　(1) $x=6k+4$，$y=-7k+2$ (k は整数)

(2) $x=90k-68$，$y=37k-28$ (k は整数)

解説

(1) $x=4$，$y=2$ は $7x+6y=40$ の整数解の 1 つである。

ゆえに，方程式は　$7(x-4)+6(y-2)=0$

すなわち　$7(x-4)=-6(y-2)$

7 と 6 は互いに素であるから，k を整数として $x-4=6k$，$-(y-2)=7k$ と表される。

よって，解は　$x=6k+4$，$y=-7k+2$ (k は整数)

(2) ［解法 1］ $37x-90y=4$ …… ①

$m=37$，$n=90$ とする。

$90=37\cdot 2+16$ から　$16=90-37\cdot 2=n-2m$

$37=16\cdot 2+5$ から　$5=37-16\cdot 2=m-(n-2m)\cdot 2=5m-2n$

$16=5\cdot 3+1$ から　$1=16-5\cdot 3=(n-2m)-(5m-2n)\cdot 3=-17m+7n$

ゆえに　$37\cdot(-17)-90\cdot(-7)=1$

両辺に 4 を掛けて　$37\cdot(-68)-90\cdot(-28)=4$ …… ②

①−② から　$37(x+68)-90(y+28)=0$　すなわち　$37(x+68)=90(y+28)$

37 と 90 は互いに素であるから，k を整数として $x+68=90k$，$y+28=37k$ と表される。よって，解は　$x=90k-68$，$y=37k-28$ (k は整数)

参考　［解法 2］ 合同式を利用した解法

(1) 6 を法として，$7x+6y=40$ …… ① から　$7x+6y\equiv 40 \pmod 6$

$6y\equiv 0 \pmod 6$ であるから　$7x\equiv 40 \pmod 6$ …… ②

ここで，$7\equiv 1 \pmod 6$，$40\equiv 4 \pmod 6$ であるから，② は　$x\equiv 4 \pmod 6$

したがって，k を整数とすると　$x=6k+4$

① から　$6y=40-7x=40-7(6k+4)=-42k+12$　よって　$y=-7k+2$

$x=6k+4$，$y=-7k+2$ (k は整数) は ① を満たすから，解である。

(2) 37 を法として，$37x-90y=4$ …… ① から　$37x-90y\equiv 4 \pmod{37}$

$37x\equiv 0 \pmod{37}$ であるから　$-90y\equiv 4 \pmod{37}$ …… ②

ここで，$90\equiv 16 \pmod{37}$　より $-16y\equiv 4$　両辺2倍して　$-32y\equiv 8$

$-32\equiv 5 \pmod{37}$　より　$5y\equiv 8$　両辺7倍して　$35y\equiv 56\equiv 19$

$35\equiv -2 \pmod{37}$　より　$-2y\equiv 19$　両辺18倍して　$-36y\equiv 342\equiv 9$

$-36\equiv 1 \pmod{37}$　より　$y\equiv 9 \pmod{37}$

したがって，k を整数とすると　$y=37k+9$

① から　$37x=90y+4=90(37k+9)+4=37\cdot 90k+814$　よって　$x=90k+22$

$x=90k+22$，$y=37k+9$ (k は整数) は ① を満たすから，解である。

注意 1　ここで導かれた (2) の解 $x=90k+22$，$y=37k+9$ は，先に示した解

$x=90k-68$，$y=37k-28$ の k を $k+1$ におき換えると得られる。

注意 2　(1) は 7，(2) は 90 を法としてもよいが，一般に，法とする数は小さい方が処理しやすい。

8 3 で割ると 2 余り，5 で割ると 3 余り，7 で割ると 4 余るような自然数 n で最小のものを求めよ。　解答　53

解説

n は x，y，z を整数として，次のように表される。

$n=3x+2$，$n=5y+3$，$n=7z+4$

$3x+2=5y+3$ から　$3x-5y=1$ …… ①

$x=2$，$y=1$ は，①の整数解の 1 つであるから

$3(x-2)-5(y-1)=0$　すなわち　$3(x-2)=5(y-1)$

3 と 5 は互いに素であるから，k を整数として，$x-2=5k$ と表される。

よって　$x=5k+2$ (k は整数) …… ②

② を $3x+2=7z+4$ に代入して　$3(5k+2)+2=7z+4$

ゆえに　$7z-15k=4$ …… ③

$z=-8$，$k=-4$ は，③ の整数解の 1 つであるから

$7(z+8)-15(k+4)=0$　すなわち　$7(z+8)=15(k+4)$

7 と 15 は互いに素であるから，l を整数として，$z+8=15l$ と表される。

よって　$z=15l-8$ (l は整数)

これを $n=7z+4$ に代入すると　$n=7(15l-8)+4=105l-52$

最小となる自然数 n は，$l=1$ を代入して　53