再読「初等整数論講義」

ここは，解析概論よりも高校生に近いもの。入試問題に出る整数問題が多く取り上げてある。

1　ユークリッドの互除法とディオファンタスの方程式

　２元１次方程式の整数解について

2　素因数分解一意性と完全数

　完全数について

3　部分分数分解と素数

　部分分数分解について

4　合同と中国剰余定理およびピタゴラス数

　合同式について，ピタゴラス数について

5　循環小数

　オイラー関数について，循環小数について

6　連分数

　連分数について，２元１次方程式の整数解について再登場

「新式算術講義」による追記

1　整除に関する整数の性質

　最小公倍数について

2　分数に関する整数論的の研究

　フェルマーの小定理について，循環小数について，

「数学雑談」による追記

1　格子幾何学によるディオファンタス方程式の解法

　格子幾何学について，ピックの定理について

初等整数論講義　再読１　Euclid の互除法と Diophantos の方程式

別解というのは，生徒にとってはやなもんですよね。私は大好きでどんどん別解を紹介しますが，ある生徒が「それも覚えるんですか？」ときた。まあね,「解法を覚えてセンターの穴埋めで数学は決まる」なんて言われてはね。しかし，大体，意外性というのは感動の必要条件じゃないかなあ。感動すれば脳の働きもよくなって覚えもいいのに。（最近の脳科学もこれは保証している）
しかし確かに別解が多すぎるとか，あまりに乱雑だとか，初等幾何の補助線のようにそんなの思いつかないとかだと困りますよね。
私の口癖は「数学の問題は代数と解析と幾何の３通りの解き方があるんだ」です。これで，困ったときも別解も探せるし，いい発想も気がつく … こともある。

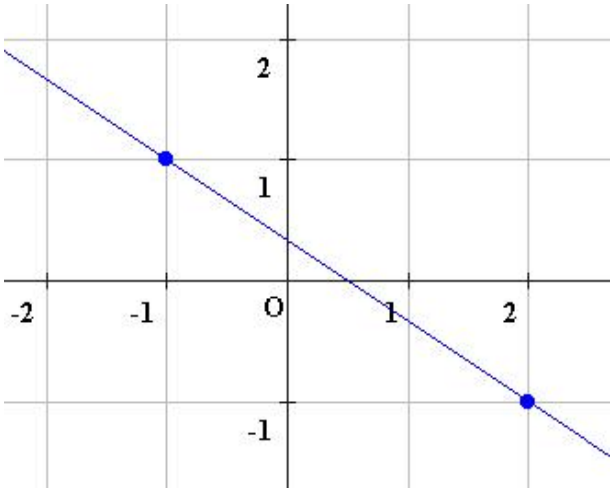
解析が一通り終わったので，代数をというわけです。で，高木貞治「**代数学講義**」といきたいのですが，内容的に高校生あるいは趣味の人にはこっちのほう（「**初等整数論講義**」）が先のほうがいいだろう，と判断しました。入試につき物の整数論ですし。このあとに,「代数学講義」。３部作ですね。

「整数論の方法は繊細である，小心である，その理想は玲瓏にして些（いささか）の陰翳をも留めざる所にある。代数学でも，函数論でも，又は幾何学でも，整数論的の試練を経て始めて精妙の境地に入るのである。」いいですよねえ。

さて，まずは　「割り算可能」から始まって「素因数分解一意」まで進みます。少し最近の言葉で言うと，ユークリッド環（割り算の可能性）ならば，単項イデアル環（最大公約数の存在），素因数分解一意環で整域とくる。

実際の問題は，**多元１次方程式の整数解（Diophantos の方程式）**です。本はいきなり３元なので２元で楽しみます。$ax+by=d$ の整数解は d が $gcd(a,b)$（最大公約数）で割り切れるときに限って無数の解を持つ。（本には証明もありますが，これが単項イデアル）

例えば $2x+3y=1$ の整数解は，高校生が解くと，$2x=1-3y$
両辺から 4 を引いて $2(x-2)=3(-1-y)$
2 と 3 は互いに素なので，k を整数として
$x-2=3k$ とおける。
このとき，$x=2+3k, y=-1-2k$
なんで 4 を引くのかという質問が当然あります。「整数解の問題だから約数・倍数の関係を使うので，両辺が 2 の倍数，3 の倍数となるようにひくのだ。」というのですが，答が無数にあるのですから，そんな数は一つに決まらない（これが生徒が整数問題を不得意とする一つの原因か？）のは当然です。
解が無数にあるのは図でも分かります。条件を満たす格子点が一つあれば周期的に繰り返す。



私の採用している解法は，$2\cdot 2+3\cdot(-1)=1$（特殊解）を与式から引くと，$2(x-2)+3(y+1)=0$ 以下同様。

こう解けるのは，$gcd(2,3)=1$ だからです。例えば $2x+4y=1$ は整数解を持ちません。左辺偶数，右辺奇数であるから不可能です。

（これは整数論が新教育課程に入ってない頃書いたもので, 今は教科書にあります。それは, 特殊解を見つけて一般解を求めるのが普通。すぐに特殊解が見つからないときは互除法でやろう, という流れです。）

具体的な解法としてユークリッドの互除法のようなものが書かれています。合同式を利用する別解も後で出てきます。

例えば $1777x+1783y=1$

オイラーが死んだのが 1783 年で，ガウスは 1777 年生誕。どちらも素数，天才は違う。

こんなものは上のやり方はすぐにはできない。大きいほうを小さいほうで割って $1777x+(1777+6)y=1$

つまり $1777(x+y)+6y=1$ ここで $x+y=x'$ とおくと，$1777x'+6y=1$

大きいほうを小さいほうで割ることを繰り返して，$(6\cdot 296+1)x'+6y=1$ つまり $x'+6(296x'+y)=1$

ここで $296x'+y=y'$ とおけば，$x'+6y'=1$ よって $x'=1-6y'$

y' を整数として，$y=-296+1777y', x=297-1783y'$ と解ける。

これは実質**ユークリッド（Euclid）の互除法**です。

1	1783	1777	296
	1777	1776	
	6	1	

右のような計算をして，1 が出れば互いに素（gcd が 1）

$g=gcd(a,b)$（最大公約数）のとき，$ax+by=g$ を満たす整数 x,y が必ずある。互いに素なときは，$g=1$。

実際，右の計算により　$1=1777-1776=1777-(6\cdot 296)=1777-((1783-1777)\cdot 296)$　なので，

$1777\cdot 297-1783\cdot 296=1$

ディオファントスの方程式の解の定理もユークリッドの互除法の計算も同じで納得。

これに関する入試問題，オリンピック予選の問題はとても多いのだ。以下示そう。年度-番号がオリンピック予選の問題。解答は次のページ。

例１ ’03 同志社女子大学　方程式 $4x+3y=55$ を満たす整数 x,y について

(1)　x,y が，ともに 1 桁の自然数であるものは，$x=$ ア ,$y=$ イ である．

(2)　x,y がともに 20 以下の自然数であるものは ウ 個あり，このうち，x と y の積が最小となるものは，$x=$ エ ,$y=$ オ である．

(3)　x^2+y^2 は最小値 カ をとる．

(4)　$|x|+|y|$ は最小値 キ をとる．

例２　’98 東女　9 で割り切れる整数全体の集合を A，15 で割り切れる整数全体の集合を B とする。

C=$\{x+y|x\in A, y\in B\}$ とするとき，C は 3 で割り切れる整数全体の集合と一致することを示せ。

ユークリッドの互除法に関する問題というか，そのもの。

例３　’00 大阪市立大

(1)　自然数 a,b,c,d に $\dfrac{b}{a}=\dfrac{c}{a}+d$ の関係があるとき，a と c が互いに素ならば，a と b も互いに素であることを証明せよ。

(2)　任意の自然数 n に対し，$28n+5$ と $21n+4$ は互いに素であることを証明せよ。

例４　’05-1　3 で割ると 2 余り 5 で割ると 3 余る 2 桁の整数はいくつあるか。

例５　’05-2　直線 $l:4x+3y=1$ 上にない格子点と l 上の点との距離としてありうる値のうち，最小のものを求めよ。ただし, 格子点とは x 座標と y 座標がともに整数であるような点である。

例１　解答

(ア)　7　　(イ)　9　　(ウ)　5　　(エ)　13　　(オ)　1　　(カ)　125　　(キ)　14

(1) 最初から整数解を出してもいいが，$1 \leqq x \leqq 9, 1 \leqq y = \dfrac{55-4x}{3} \leqq 9$ より，$7 \leqq x \leqq 9$

この中で条件を満たすのは　$x = 7, y = 9$

$4x + 3y = 55, 4 \cdot 7 + 3 \cdot 9 = 55$ より，k を整数として $x = 7 - 3k, y = 9 + 4k$

以下，これを使って解いていってもいいし，$(13, 1), (10, 5), (7, 9), (4, 13), (1, 17)$ と具体的に求めてもたいしたことない。

例２　解答

9 と 15 の最大公約数は 3 なので，$9x + 15y = 3$ なる x, y が存在し，これを何倍かすれば 3 の倍数の集合と一致する。

入試では $9m + 15n = 3(3m + 5n)$ で必要条件，$3l = \{9 \cdot 2 + 15 \cdot (-3)\}l$ で十分条件をいう。

例３　解答

$\dfrac{28n+5}{21n+4} = 1 + \dfrac{7n+1}{21n+4}, \dfrac{21n+4}{7n+1} = 3 + \dfrac{1}{7n+1}$

例４　解答 6 個

m, n を整数として $3m+2 = 5n+3$ つまり $3m-5n = 1$ 特殊解は $m = 2, n = 1$ なので $m = 2+5k, n = 1-3k$ ただし k は整数。

$3m + 2 = 3(2 + 5k) + 2 = 8 + 15k$ $10 \leqq 8 + 15k \leqq 99$ つまり $\dfrac{2}{15} \leqq k \leqq \dfrac{91}{15}$

これを満たす自然数は 6 個

例５　解答 $\dfrac{1}{5}$

点 (a, b) と直線 $4x + 3y = 1$ との距離 $d = \dfrac{|4a + 3b - 1|}{\sqrt{3^2 + 4^2}} = \dfrac{|4a + 3b - 1|}{5}$

$4a + 3b = 2$ なる解はあるので答のようになる。

初等整数論講義　再読２　素因数分解一意性と Perfect number

約数（1 と自分自身を除く約数を真の約数という）・倍数の関係で整数を分類すると
0（約数が無限），1（約数がただ一つ），
素数 prime（真の約数をもたない），合成数 composite（真の約数をもつ）
1 を素数に含めないのは，素因数分解の一意性がいえなくなるからと私は説明している。
例えば $6 = 1\cdot 2\cdot 3\cdot = 1^2\cdot 2\cdot 3\cdot = \cdots$
「素因数への分解を用いるならば，整除に関する問題が簡明に解決される。」
（私の使っている FEP は古くて，だいたいコンピュータは ME だし，この文章を打っていたら，久しぶりの見事な誤変換をした。聖女に関する問題が感銘に解決される，だって）

その例として，高校の教科書にも現れる約数の個数・総和・総積の公式
$a = p^\alpha q^\beta \cdots$ の
約数の個数　$T(a) = (1+\alpha)(1+\beta)\cdots$
約数の総和　$S(a) = \dfrac{p^{\alpha+1}-1}{p-1}\cdot\dfrac{q^{\beta+1}-1}{q-1}\cdots$
約数の総積　$a^{\frac{T(a)}{2}}$
個数の公式は指数が 0 もあること（で，$1+\alpha$），総和の公式は $(1+p+p^2+\cdots+p^\alpha)(1+q+\cdots)\cdots$ の展開が求めるもので等比数列の和の公式を使うこと，約数の総積の公式は $1\cdot p\cdots a = \sqrt{1a\cdot p\dfrac{a}{p}\cdots a1}$
ルートの中は a が約数の個数だけあること，を考えるとわかる。
入試問題から「約数の個数が奇数ならば，平方数であることを示せ。」
解例）上のような a とすると，約数の個数が奇数なので $1+\alpha, 1+\beta, \cdots$ はすべて奇数。すると $\alpha, \beta, \cdots$ はすべて偶数となり，a は平方数。

約数の総和に関係して，整数を分類することができて，
完全数（perfect number）　$S(a) = 2a$, 豊数 $S(a) > 2a$, 輸数 $S(a) < 2a$
「輸」という字は最近こういうふうには使わないので調べてみると，右側は「大きな把手（とつて）のある手術刀（余）で膿漿（のうしよう）を刺して盤（舟）に移し、治癒する意」（字通）。移ってしまって足りなくなった数という感じかな。ついでに，教諭の諭は「病を癒すように、人をことばで戒めること」，なるほど体罰をする人は教諭にあらずか。

また，入試問題から選んでみました。一つの（自分を除いた）約数の和がもう一つの数となりそのもう一つの約数の和が元の数になるという，**友愛数 amicable number**（昔は**親和数**と呼んでいたと思ったが，誰かの小説のおかげでこっちのほうが有名になった。）
例　'01 九州　正の整数 a に対し，a の正の約数全体の和を $f(a)$ で表す．
ただし，1 および a 自身も約数とする．たとえば $f(1) = 1$ であり，$a = 15$ ならば 15 の正の約数は 1，3，5，15 なので，$f(15) = 24$ となる．次の問いに答えよ．
(1)　a が正の奇数 b と正の整数 m を用いて $a = 2^m b$ と表されるとする．　このとき　$f(a) = (2^{m+1}-1)f(b)$
が成り立つことを示せ．必要ならば，$1 + r + \cdots + r^m = \dfrac{r^{m+1}-1}{r-1}$ $(r \neq 1)$ を用いてよい．
(2)　a が 2 以上の整数 p と正の整数 q を用いて $a = pq$ と表されるとする．
このとき　$f(a) \geqq (p+1)q$　が成り立つことを示せ．
また，等号が成り立つのは，$q = 1$ かつ p が素数であるときに限ることを示せ．
(3)　$a = 2^2 r$，$b = 2^4 s$ (r，s は正の奇数) の形をした偶数 a，b を考える．
$$\begin{cases} f(a) = 2b \\ f(b) = 2a \end{cases}$$ を満たす a，b を求めよ．

例1　解答　(3)　$a=124,\ b=112$

約数の個数を調べることによって，完全数の偶数のタイプを証明したのも Euler。
$a=2^{n-1}(2^n-1)\quad (n>1)$ において，2^n-1 が素数ならば，a は完全数である。ちなみに奇数の完全数は一つも 知られていない。
偶数の完全数は前のタイプしかないという見事な証明は本で読んでもらうことにして，具体的に Maxima で遊んでみるか。
Maxima　には　primep(a)　という関数があって，a　が素数なら true　を返してくれる。

```
for i:1 thru 10000 do
    if primep(2^i-1)=true then  display(i,primep(2^i-1))
```

で走らせてみると，2,3,5,7,13,17（これは本にある）,19,31,61,89,127（ここまで知られているとある）, その後にも 521,607 を出力するがどうなんだろう？昭和 6 年初版, 私がもっている本が昭和 53 年 2 版。「$2^{127}-1$ が現今知られている最大の素数であろう」とあるが。もっとやってみたら,1279,2203,2281,4253（この間に映画が一本見れたが, 機械がかわいそうになってやめた,Maxima をやめてもハードディスクがつきっぱなしで熱くなっているぞ。皆さん, やってみます？）
ネットで調べると, これが Mersenne Prime ,2006 年時点では　30402457,43 番目なんだって。
（2011 年 47 個だそうだ）
似たものに 2^n+1 というのがある。
問　n が 2 の累乗でなければ,2^n+1 は合成数であることを示せ。
この対偶，2^n が素数ならば，n が 2 の累乗である。（逆がいえるとは限らない）
この形の素数をフェルマー素数という。 $n=1,2,3,4$ $(5,17,257,65537)$ までは素数で， $n=5$ (10 桁）は素数でないことをオイラーが証明したそうだ。どうもこれ以上は素数でないらしい。
ガウスが正 n 角形の作図可能性を証明したのがこれ。
問の解　$n=2^m*d$ (d : 奇数) なら $2^n+1=((2^m)^d+1)((2^m)^{n-1}-\cdots+1)$

初等整数論講義　再読３　素数

数学オリンピック予選に出たのが最初だったか（1997 年）, 入試問題にも今では何回か出ているのが次の問題。**問**　2007!には 1 の桁から何桁 0 が並ぶか？

10 は 2 かける 5 であるが 2 の倍数は 5 の倍数より沢山あるので 5 の倍数の個数を考えればよい。5 の倍数が一つあれば 0 が一つ,25 の倍数があれば 0 が二つ,$\cdots$ なので, $\left[\frac{2007}{5}\right]+\left[\frac{2007}{5^2}\right]+\left[\frac{2007}{5^3}\right]+\left[\frac{2007}{5^4}\right]=500$

Maxima では, 次のようにします。Gauss 記号は floor 関数, 床関数で感じは出てますが。

```
floor(2007/5)+floor(2007/5^2)+floor(2007/5^3)+floor(2007/5^4)
```

なんとこれも公式として出ています。$n!$ に含まれる素因数 p の最高巾の指数は $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$

本にはこれのさらに巧妙な計算方法もありますが, 興味深いのはこの公式を使って, **二項係数 ${}_m\mathrm{C}_n$ が整数**になる証明をしていることです, これについては帰納法を使ったりして証明をしたりしますが, これがキレイ。

${}_m\mathrm{C}_n=\frac{m!}{n!n'!}(m=n+n')$ より 任意の p k について,$\left[\frac{m}{p^k}\right]\geqq\left[\frac{n}{p^k}\right]+\left[\frac{n'}{p^k}\right]$ だから明白というのです。

高校では「連続 2 整数の積は偶数」とか「連続 3 整数の積は 6（3!）の倍数」くらいで出てきます。

もっと大切な応用は数列の和を求めたり, 積分に使ったりする**部分分数**分解の一意性があります。高校では天下り的に事実を認めるだけです。「天下りはやめたい」というのは私の悲願。簡単に説明すると（簡単に説明するくらいなら天下りのほうがいいという人もいるんですよね）これもまた, ディオファンタスの方程式です。p,q 互いに素のときには,$px+qy=1$ をみたす x,y がある。両辺を p,q で割れば

$\frac{x}{q}+\frac{y}{p}=\frac{1}{pq}$ もし分子が分母より大きければ割ればいい。

さらに, 分母が p^n の形のときは, p 進法に直すことを考えれば, つまり $a=a_np^n+a_{n-1}p^{n-1}+\cdots+a_1p+a_0$ ならば, 両辺を p^n で割って,$\frac{a}{p^n}=a_n+\frac{a_{n-1}}{p}+\cdots+\frac{a_1}{p^{n-1}}+\frac{a_0}{p^n}\quad 0\leqq a_0,a_1,\cdots,a_n<p$

整数で成り立つことは整式でも成り立つ。

だいたい p **進法**をやれば, **多項式の（テーラー）展開**も同じだといって進められる。

$x^4=\square(x-1)^4+\square(x-1)^3+\square(x-1)^2+\square(x-1)+\square$

1	1	0	0	0	0
		1	1	1	1
1	1	1	1	1	1
		1	2	3	
1	1	2	3	4	
		1	3		
1	1	3	6		
		1			
	1	4			

上の空欄は左側から $1,4,6,4,1$

というのは書き方も計算も進数法と同じです。

7 を 2 進法で表すと

2	7	
2	3	$\cdots 1$
	1	$\cdots 1$

$7=111$(二)

Maxima では Number Theory に関数があります。ベルヌーイとかオイラーとかゼーターとかはこれからとして, 今のところ初等的なものが

`lcm (expr_1, ..., expr_n)` 最小公倍数　`divsum(n)` 約数の和

`partfrac (expr, var)` 変数 `var` の分数式の部分分数

`next_prime (n)` 次の素数　`prev_prime (n)` 前の素数

`totient (n)` n 以下の n と素な数の個数

初等整数論講義　再読４　合同式

素数については附記とあるので, 話題のみかな, 有名なものがいくつか紹介されている。解析では Euler が俄然登場していたが、こちらでは Gauss が多いですね。x を超えない素数の個数$\pi(x)$ の漸近値が $\dfrac{x}{\log x}$ という**素数定理**。Gauss が予想したこの定理は驚くべきことと言っているが, うーん, x 割る $\log x$ か, まさに不思議, でこれは証明済み。

素数の双生児（引き続いた奇数がともに素数）は, はたして無限に存在するかはまだ解答が無い。

Goldbach の推測（2 以上の偶数は二つの素数の和として表しうる）というのもまだ証明されていない。

さて, **合同式**です。**≡（congruent）（** $\mathrm{mod}\ .m$**）** m **を法として合同**, これも Gauss の記法とある。「数論を一つの科学まで高めたのは合同記号である」と，どこかで読みました

むかし, コンピュータのプログラミングをやっていたときに, 符号付整数の表し方が一番大きい数に 1 を加えると一番小さい数になるというふうになっていて, なるほどと思ったことがある。無限に大きな数は所詮人間には必要ないから, 有限な範囲で計算できればいいということか。

人間が無限を扱うためには二通りあって, キリスト教的な直線的に無限遠から無限遠へと続くイメージと, 仏教的な有限な円の繰り返し回るイメージと。和辻の「風土」を思い出すなあ。ところで, 高校では剰余類の簡単な場合はやる。

整数を偶数と奇数に分ける,2 で割った余りで整数をグループ分けする。

$\cdots -2 \equiv 0 \equiv 2 \equiv 4 \equiv \cdots (\ \mathrm{mod}\ .2)$ k を整数として $2k$ と表される

$\cdots -1 \equiv 1 \equiv 3 \equiv 5 \equiv \cdots (\ \mathrm{mod}\ .2)$ k を整数として $2k+1$ と表される

2 で割った余りとか, 偶数奇数の問題にはこれを使う。

整数を 3 で割った余りで整数をグループ分けする。

$\cdots -3 \equiv 0 \equiv 6 \equiv 9 \equiv \cdots (\ \mathrm{mod}\ .3)$ k を整数として $3k$ と表される

$\cdots -2 \equiv 1 \equiv 4 \equiv 7 \equiv \cdots (\ \mathrm{mod}\ .3)$ k を整数として $3k+1$ と表される

$\cdots -1 \equiv 2 \equiv 5 \equiv 8 \equiv \cdots (\ \mathrm{mod}\ .3)$ k を整数として $3k+2$（または $3k-1$）と表される

3 で割った余りとかにはこれを使う。

$ab=0$ ならば　$a=0$　or　$b=0$　つまり零因子（かけて 0 になるもの）が 0 のみのとき，その数の集合を整域（integral domain）という。

m が素数のとき，$ab \equiv 0 (\ \mathrm{mod}\ .m)$ ならば $a \equiv 0 (\ \mathrm{mod}\ .m)$　or　$b \equiv 0 (\ \mathrm{mod}\ .m)$ が成り立つ，つまり素数を法とする剰余類は整域ということで，整数（integral number,integer）とよく似た性質が成り立つ。

定理　$a \equiv a', b \equiv b' (\ \mathrm{mod}\ .m)$ のとき，もちろん　$a \pm b \equiv a' \pm b', ab \equiv a'b' (\ \mathrm{mod}\ .m)$

$ac \equiv bc (\ \mathrm{mod}\ .m)$ ならば $a \equiv b (\ \mathrm{mod}\ .m)$（ただし, $(c,m)=1$ つまり c と m が互いに素のとき）

まず**記号として便利**なので，授業ではやりませんが，数学同好会では説明しています。

例えば**倍数の見分け方**（「数字の遊戯からでも，整数論に興味が生ずるならば，幸いである」と本にはある）

2　末位の数字が偶数 $10 \equiv 0 (\ \mathrm{mod}\ .2)$ より

3　各桁の数字の和が 3 の倍数　$10^n \equiv 1 (\ \mathrm{mod}\ .3)$ より

4　下 2 桁が 4 の倍数　$100 \equiv 0 (\ \mathrm{mod}\ .4)$ より

5　末位の数字が 0 か 5　$10 \equiv 0 (\ \mathrm{mod}\ .5)$ より

6　2 の倍数でもあり，3 の倍数でもある

8　下 3 桁が 8 の倍数　$1000 \equiv 0 (\ \mathrm{mod}\ .8)$ より

9　各位の数字の和が 9 の倍数　$10^n \equiv (\ \mathrm{mod}\ .9)$ より

$$
\begin{array}{r}
111 \\
9\overline{)1000} \\
900 \\
\hline
100 \\
90 \\
\hline
10 \\
9 \\
\hline
1
\end{array}
$$

二桁の数 11 と 13 は，$1001 = 7 \cdot 11 \cdot 13$ より

$1000a+100b+10c+d = (1001-1)a+(99+1)b+(11-1)c+d = (91*11-1)a+(9*11+1)b+(11-1)c+d$

$\equiv -a+b-c+d(\mod .11)$

$1000 \equiv -1(\mod .7,11,13)$ より，とても大きな数は 3 桁ずつに区切って

例えば $123456789 \equiv 123-456+789 = 456$ と 3 桁が分かればいいというわけだ。

さて，次は　7,11,13。

簡単のために見分ける数を 4 桁の数としよう。

$1000a+100b+10c+d = (7 \cdot 142+6)a+(7 \cdot 14+2)b+(7 \cdot 1+3)c+d$

$\equiv 6a+2b+3c+d(\mod .7)$

つまり，どんな場合も次のようにすればいいことが分かる。

1 をある数で割ったときにでる余りを次の桁に掛けて足す。

その数が問題の数で割り切れれば OK！

例えば $1232 \equiv 6 \cdot 1+2 \cdot 2+3 \cdot 3+2 = 21 \equiv 0(\mod .7)$ で割り切れる。

3,9 の倍数を見つけるのは，たまたま余りに 1 が出続けるということ。

```
      142857
  7 ) 1000000
      700000
      ------
      300000
      280000
      ------
       20000
       14000
       -----
        6000
        5600
        ----
         400
         350
         ---
          50
          49
          --
           1
```

分数の答で約分ミスが多いのは圧倒的に 3 の倍数ですね。2 と 5 の倍数はすぐわかるし，それ以外はあまり割れない。で，足して 3 の倍数ぐらいのチェックは中学校でも教えてるのかな？これからは九去法にならって**三去法**と言おうかな。

九去法　以下（ mod .9）で。

12345×9876 なんて計算がたまには高校でもあります。しかたなく計算しますが合っていそうにないです。答は 121919220 と計算したとすると，$12345 \equiv 1+2+3+4+5 \equiv 6, 9876 \equiv 9+8+7+6 \equiv -6$ だから，$6 \times (-6) = 36 \equiv 3+6 \equiv 0$，一方 $121919220 \equiv = 1+2+1+1+2+2 \equiv 9 \equiv 0$ で，まあ答は合っているらしいぞと思うのが九去法。なんかコンピュータで情報が正しく送れたかチェックするパリティなんてのを思い出します。便利ですよね。

次に記号としてだけでなく，**方法として便利**だぞという面に入ります。

前にやった，ディオファンタスの方程式　$2x+3y = 1$ は　$2x \equiv 1(\mod .3) \cdots ①$ と同じです。

$2 \equiv -1(\mod .3)$　なので，$-x \equiv 1(\mod .3) \cdots ②$

① + ② より　$x \equiv 2(\mod .3)$ これで，解けている。$x = 2+3k$ というわけです。

もうひとつ $1777x+1783y = 1$ 合同式に直して $1777x \equiv 1(\mod .1783)$

$1777x \equiv 1 \cdots ①$　これから　$-6x \equiv 1 \cdots ②$ $1777 = 296 \times 6+1$ なので，① + 296 × ② より $x \equiv 297$

もちろん実質は同じですけど。

最後に和算の**百五減法**を　mod　で説明しましょう。

問　3 で割ると 2 余り,5 で割ると 1 余り,7 で割ると 5 余るような整数を求めよ。

求める数を　x とおくと

$x \equiv 2(\mod .3) \cdots ①$

$x \equiv 1(\mod .5) \cdots ②$

$x \equiv 5(\mod .7) \cdots ③$

$21 \times ②$　より　$21x \equiv 21(\mod .105) \cdots ④$

$15 \times ③$　より　$15x \equiv 75(\mod .105) \cdots ⑤$

$35 \times ①$　より　$35x \equiv 70(\mod .105) \cdots ⑥$

④ + ⑤ − ⑥より　$x \equiv 26(\mod .105)$　すなわち 105 で割ると 26 余る数。

Chinese remainder theorem,『孫子算経 』に由来すると Wiki には載ってます。証明をこの問題にそってたどると

3 と 5 と 7 は互いに素だから,

$M = 105 = m_1M_1 = 3 \cdot 35 = m_2M_2 = 5 \cdot 21 = m_3M_3 = 7 \cdot 15$ とおいて

$M_1t_1 \equiv 1 (\mod .m_1) = 35 \cdot (-1) \equiv 1 (\mod .3)$

$M_2t_2 \equiv 1 (\mod .m_2) = 21 \cdot 1 \equiv 1 (\mod .5)$

$M_3t_3 \equiv 1 (\mod .m_3) = 15 \cdot 1 \equiv 1 (\mod .7)$ と t_1, t_2, t_3 を決めれば

$x \equiv 2M_1t_1 + 1M_2t_2 + 5M_3t_3 (\mod .M) \equiv 2 \cdot 35 \cdot (-1) + 1 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 \equiv 26 (\mod .105)$ は

確かに 3 で割ると 2 余り,5 で割ると 1 余り,7 で割ると 5 余る。

この解の存在と一意性が**中国剰余定理**。

これは，部分分数分解への応用もできる。

$$\frac{26}{105} = \frac{2M_1t_1 + 1M_2t_2 + 5M_3t_3}{M} = \frac{2 \cdot 35 \cdot (-1) + 1 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1}{105} = -\frac{2}{3} + \frac{1}{5} + \frac{5}{7}$$

ここで代数になりますけど，合同式は方程式の整数解（ディオファンタスのようなもの以外でも）を探すときにも威力があります。

例えば，数学オリンピック

例１　'91-7　$135^5 + 110^5 + 84^5 + 27^5 = n^5$ なる整数 n を求めよ。

例２　'99 京大 0 以上の整数 x に対して，$C(x)$ で x の下 2 桁を表すことにする．

例えば，$C(12578) = 78$，$C(6) = 6$ である．n を 2 でも 5 でも割り切れない正の整数とする。

(1)　x，y が 0 以上の整数のとき，$C(nx) = C(ny)$ ならば，$C(x) = C(y)$ であることを示せ。

(2)　$C(nx) = 1$ となる 0 以上の整数 x が存在することを示せ。

他には，なんといっても三平方の定理。 $a^2 + b^2 = c^2$ を満たす整数解を調べるために合同式を使います。その前に，Maxima で**ピタゴラス数**を探させてみます。互いに素なものだけ出力します。

```
for a:1 thru 50 do for b:a+1 thru 50 do for c:1 thru 50 do
 if a^2+b^2=c^2 then if gcd(a,gcd(b,c))=1 then display(a,b,c)
```

3,4,5　5,12,13　7,24,25　8,15,17　9,40,41　12,35,37　20,21,29

問１　$a^2 + b^2 = c^2$ をみたす a, b, c は, すべて偶数は除くとして， a, b 奇数・ a 偶数の組合せはないことを示せ。つまり， a, b のどちらか一方が奇数,c は奇数となる。

問２　同様に,a, b のどちらかが 3 の倍数, どちらかが 3 で割ると 1 余る数, c は 3 で割ると 1 余る数となることを示せ。

問３　ピタゴラス数のどれか一つは 5 の倍数であることを示せ。

ここまでで，ピタゴラス数のどれか一つは 2 の倍数，3 の倍数，5 の倍数である。（こんなこと知らなかった）

ここからは少し脱線気味ですが，さらに，代数と幾何（図形と方程式）までいけば，すべてのピタゴラス数を作る式ができる。

問４　円 $x^2 + y^2 = 1$ と，直線 $y = \frac{m}{n}(x + 1)$ の交点の座標を求めることによって，その式を作れ。

ここらへんを問題に作るかなと思っていたら, 入試にはもうちゃんと出てます。

例３　'1 千葉大

(1)　n を自然数とする．このとき，n^2 を 4 で割った余りは 0 または 1 であることを証明せよ．

(2)　3 つの自然数 a，b，c が $a^2 + b^2 = c^2$ を満たしている．このとき，a，b の少なくとも一方は偶数であることを証明せよ．

例１, ２の解答は次のページ。問の解答は次の次のページ。

例４　'99 京大　「自然数 a,b,c について，等式 $a^2+b^2=c^2$ が成り立ち，かつ a,b は互いに素とする。このとき，次のことを証明せよ。

(1)　a が奇数ならば，b は偶数であり，したがって，c は奇数である。

(2)　a が奇数のとき，$a+c=2d^2$ となる自然数 d が存在する。」

これは, 上の問４を円の方程式などを使わず直接やる方法です。同好会の諸君でもどうして急に $x^2+y^2=1$ が出てくるのだ？という質問があった。上のように $c-a=2e^2$ もいえて, ２つを連立して解くことにより $c=d^2+e^2, a=d^2-e^2$ このとき $b=2de$ となるわけです。

例１　解答　答 144

まずは範囲をせばめよう。　$27^5<4\cdot27^5<n^5<4\cdot133^5<32\cdot133^5=2^5\cdot133^5=(2\cdot133)^5$

で,$27<n<266$

与式の左辺を m とおくと,$m\equiv1+0+0+1\equiv0(mod\quad2)$

$m\equiv1+(-1)+0+0\equiv0(mod\quad3)$

$m\equiv(-1)^5+0+(-1)^5+2^5\equiv-1(mod\quad5)$

$m\equiv0+(-2)^5+0+(-1)^5\equiv2(mod\quad7)$

つまり, n は 27 から 266 の整数でその５乗が６の倍数で５で割って４余り, ７で割ると２余る数である。

$n^5\equiv0(mod\quad6), n^5\equiv-1(mod\quad5), n^5\equiv2(mod\quad7)$

$0^5\equiv0(mod\quad6), (-1)^5\equiv-1(mod\quad5), (-3)^5\equiv2(mod\quad7)$ なので

$n\equiv0(mod\quad6)\cdots①, n\equiv-1\equiv4(mod\quad5)\cdots②, n\equiv-3\equiv4(mod\quad7)\cdots③$

よって,$6\times②-5\times①\cdots n\equiv24(mod\quad30)\cdots④$

$30\times③\cdots30n\equiv120(mod\quad210)\cdots⑤, 7\times④\cdots7n\equiv168(mod\quad210)\cdots⑥$

$13\times⑥-3\times⑤\cdots n\equiv144(mod\quad210)$

ちなみに Maxima で解くと

```
solve(133^5+110^5+84^5+27^5=x^5,x);
 [x=144*%e^((2*%i*%pi)/5),x=144*%e^((4*%i*%pi)/5),
x=144*%e^(-(4*%i*%pi)/5),x=144*%e^(-(2*%i*%pi)/5),x=144]
```

そりゃそうだ $133^5+110^5+84^5+27^5=61917364224$ の５乗根だものな。

例２　解答

(1) n と 100 は互いに素なので，$nx\equiv ny$ $(mod.100)$ ならば $x\equiv y$ $(mod.100)$

(2) n と 100 は互いに素なので，$nx+100y=1$ なる整数 x,y が存在する，つまり $nx\equiv1$ $(mod.100)$

これを直接証明させるわけだ。これは, 本にもあるとおり有名な問題ではある。こういう問題は入試にはどうなんだろう？(1) は (2) にとって絶妙な問なので, いい問題とは思いますが。

$C(n)$ が 0 から 99 まで考えると $C(nx)$ は 0 から 99 まで可能性があり，(1) から $C(nx)\fallingdotseq C(ny)$ ならば $C(x)\fallingdotseq C(y)$ なので, やはり 0 から 99 まですべてある。もちろん,$C(nx)=1$ もある。

問の解答

問１　$(2k+1)^2 = 4k^2+4k+1 \equiv 1$（ mod .4）つまり奇数の平方数は $\equiv 1$（ mod .4)。これを足しても偶数の平方数の $\equiv 0$（ mod .4）にならない。

問２　$(3k \pm 1)^2 \equiv +1$（ mod .3）a, b, c の数の組合せは（ mod 3）でいうと $0, 1, 1$ $(1, 0, 1)$ のみ。

問３　$(5k \pm 1)^2 \equiv 1, (5k \pm 2)^2 \equiv -1$（ mod .5）$a, b, c$ の数の組合せは（ mod 5）でいうと
$0, 1, 1(1, 0, 1)$ と $0, -1, -1(-1, 0, -1)$ と $1, -1, 0(-1, 1, 0)$ のみ。

問４　円 $x^2+y^2=1$ と，直線 $y = \dfrac{m}{n}(x+1)$ の交点の座標を求めることによって，その式を作れ。

```
solve([x^2+y^2=1,y=n*(x+1)/m],[x,y])
 [[x=-(n^2-m^2)/(n^2+m^2),y=(2*m*n)/(n^2+m^2)],[x=-1,y=0]]
```

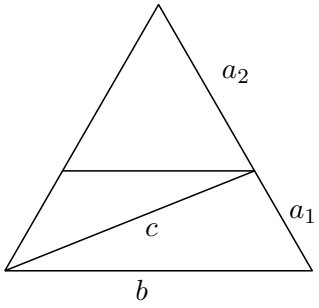
というわけで，ピタゴラス数を作るのは，$m^2-n^2, 2mn, m^2+n^2$ なる有名な式となる。

拡張ピタゴラス数

数学同好会で，一つの角が $60°$ となる整数の辺の三角形（正三角形を除いて）を同様にして調べた。（拡大ピタゴラス数とでもいおうかな）

```
for a:1 thru 30 do for b:a+1 thru 30 do for c:1 thru 30 do
 if a^2+b^2-a*b=c^2 then if gcd(a,gcd(b,c))=1 then display(a,b,c)
a=3,b=8,c=7,a=5,b=8,c=7,a=5,b=21,c=19,a=7,b=15,c=13,a=8,b=15,c=13,a=16,b=21,c=19
```

こいつをよく見ると，２つずつセットになってます。
$a=3, b=8, c=7, a=5, b=8, c=7(3+5=8)$
$a=5, b=21, c=19, a=16, b=21, c=19(5+16=21)$
$a=7, b=15, c=13, a=8, b=15, c=13(7+8=15)$
セットの理由と $120°$ の整数辺も含めて３つの三角形の図です。



a_1, b, c と a_2, b, c が双子の $60°$ 三角形，
a_1, a_2, c が $120°$ の三角形。
下を満たす数を拡張ピタゴラス数として，
Maxima で捜索。

```
solve([x^2+y^2+x*y=1,y=n*(x+1)/m],[x,y])
 [[x=-(n^2-m^2)/(n^2+m*n+m^2),y=(n^2+2*m*n)/(n^2+m*n+m^2)],[x=-1,y=0]]
```

というわけで，拡張ピタゴラス数を作るのは，$m^2-n^2, 2mn+n^2, m^2+mn+n^2$ という式となるのだった。
有名な $3, 4, 5$ には $3, 5, 7$ で ,$5, 12, 13$ には $5, 16, 19$, $\cdots$

初等整数論講義　再読５　Euler 関数　循環小数

オイラーの関数とかフェルマーの定理とか大きな定理が続くが，高校数学の範囲をまず急ごう。

と思ったら, **オイラーの関数（Euler function）** $\psi(x)$ が入試に出てるじゃないか。

'03 名古屋　n を自然数とするとき，$m \leqq n$ で m と n の最大公約数が 1 となる自然数 m の個数を $f(n)$ とする。

(1)　$f(15)$ を求めよ。

(2)　p，q を互いに異なる素数とする。このとき，$f(pq)$ を求めよ。

別にこのくらいその場で考えればいいんだけどね。

本では,$(a,b)=1$ ならば,$\psi(ab)=\psi(a)\psi(b)$ が中国剰余定理で証明してあり,

p が素数なら,$\psi(p)=p-1, \psi(p^e)=p^e-p^{e-1}$ なのでということで, 次の定理に行きついている。

$n=p^\alpha q^\beta \cdots$ と素因数分解されれば,$\psi(n)=n\left(1-\dfrac{1}{p}\right)\left(1-\dfrac{1}{q}\right)\cdots$

私は, この定理は, 全体から p の倍数の確率を引く … と理解して覚えている。

上の問題の答だけは $f(3)f(5)=(3-1)(5-1)=8$ と $f(p)f(q)=(p-1)(q-1)$ です。

循環小数 recurring [repeating] decimal は教科書にも出ます。Maxima で実験すると,

実験１ 1 から 10 まで逆数を書き出せという命令。

```
for i:1 thru 10 do display(float(1/i))
```

分母の約数が 2 と 5 しかないときは有限小数，それ以外は循環小数となることがみえる。

問１　分母の約数が 2 と 5 しかないときは有限小数になることを示せ。

実験２　10 との最大公約数（great common divisor）が 1，つまり 10 と互いに素のときだけ書け。

```
for i:1 thru 20 do if gcd(10,i)=1 then display(float(1/i))
```

興味あることは，循環節の長さ。そしてこの本にも「多くの読者はこのような数字の遊戯に興味を感ずるであろうと信ずる」とある。

問２　循環節の長さは長くとも割る数より 1 小さいことを示せ。

問３　循環節の長さに何か気づくことはないか？循環節の数字のならびに何か気づくことはないか？

もう少し例が欲しくなるし，桁数も足りないかな

実験３　浮動小数点表示を 32 桁にして，10 と互いに素で素数のときだけ書け。

```
fpprec:32;
 for i:1 thru 40 do if gcd(10,i)=1 and primep(i) then display(bfloat(1/i))
```

問４　好きな循環節になるような分数を作る方法を考えよ。

例えば $0.\dot{1}23456789\dot{}$ を分数に直せ。なんてのは，教科書レベル。

問の解答

問１は分母に 2 か 5 をいくつか掛けると 10 になるもんね。

問２は出てくる余りは割る数より小さいもんね

問３は少し時間をかけてみてほしいので次回。

```
bfloat(1/3)=3.33333333333333333333333333333333b-1
bfloat(1/7)=1.42857142857142857142857142857142b-1
bfloat(1/11)=9.09090909090909090909090909090091b-2
bfloat(1/13)=7.69230769230769230769230769230769b-2
bfloat(1/17)=5.88235294117647058823529411764705b-2
bfloat(1/19)=5.26315789473684210526315789473684b-2
bfloat(1/23)=4.34782608695652173913043478260870b-2
bfloat(1/29)=3.44827586206896551724137931034482b-2
bfloat(1/31)=3.22580645161290322580645161290322b-2
bfloat(1/37)=2.70270270270270270270270270270270b-2
```

問４　$\dfrac{1}{10^e}\left\{1+\dfrac{1}{10^e}+\cdots\right\}=\dfrac{\dfrac{1}{10^e}}{1-\dfrac{1}{10^e}}$ だから

循環節の長さを e とすれば，$\dfrac{\text{循環節がつくる数字}}{10^e-1}, 0.\dot{1}23456789\dot{0}=\dfrac{123456789}{999999999}=\dfrac{13717421}{111111111}$

ところで, 循環小数の**表記と読み方**について提言しようかな。

表記　$0.\dot{3}, 0.\dot{1}234\dot{5}$ は教科書にありますが，読み方はありません。読み方ぐらいどうでもいいかもしれませんが，決めたっていいと思いますね。数学の記号の読み方は決まっていないものが結構多くて, $\sqrt[3]{a}$ すらないんですから。

英語の翻訳をして,「零（ゼロでなくレイ）点３の循環」「零点１万２千３百４十５の循環」なら誤解ないです。

３乗根とは読まずに，３乗ルートと読んでます。これぐらい決めてくれよって気がしますがどうでしょう？

ここまでで「講義」を読んでみたくなるような興味深いところを書いてみるか。

①　問題１　$a, b, c\cdots$ は二つずつ互いに素であるとして，実数 x を超えない自然数の中で a でも， b でも， c でも， $\cdots$ 割り切れないものの個数は，[　] は Gauss 記号として

$$[x]-\left[\frac{x}{a}\right]-\left[\frac{x}{b}\right]-\left[\frac{x}{c}\right]-\cdots+\left[\frac{x}{ab}\right]+\left[\frac{x}{bc}\right]+\left[\frac{x}{ca}\right]+\cdots-\left[\frac{x}{abc}\right]-\cdots$$

教科書にもあるよね，こんな問題。

②　知ってて損はないよなあ　Fermat の定理

p が素数で， a は p で割り切れないならば，$a^{p-1}\equiv 1$（ mod $.p$）

③　付記　すべての整数は四つ以下の平方数の和に分解することができる。

次回は連分数表示で，整数論第一回はここまでかな。

初等整数論講義　再読６　連分数

循環小数について，続き。ここでも合同式が威力発揮。

10^n の mod p　での表。こんなものも Maxima で計算。

```
for a:1 thru 16 do display(mod(10^a,17))
```

n	1	2	3	4	5	6	7	8	9
7	3	2	-1						
11	-1								
13	-3	9	-1						
17	-7	-2	-3	4	6	9	5	-1	
19	-9	5	-7	6	-3	-8	-4	-2	-1

例えば，$10 \equiv 3$（ mod .7）

$10^2 \equiv 3^2 \equiv 2$（ mod .7）

$10^3 \equiv -1$（ mod .7）

ということは $10^6 \equiv (-1)^2 \equiv 1$（ mod .7）

で，循環節の長さは 6

循環節の長さは,(割る数)-1 の約数で，偶数。

偶数なら 2 つに分けられる。

前半部分と後半部分を見ると，

142,857 そう 足すと 999

何故なら　$\frac{1}{7}(0.142) + \frac{6}{7}(6 \equiv -1) = 0.\dot{9}9\dot{9} = 1$

確かにこの数字の遊戯は興味を感ずる。

$$
\begin{array}{r}
142857 \\
7\overline{)1000000} \\
700000 \\
\hline
300000 \\
280000 \\
\hline
20000 \\
14000 \\
\hline
6000 \\
5600 \\
\hline
400 \\
350 \\
\hline
50 \\
49 \\
\hline
1
\end{array}
$$

正 17 角形の作図可能性の話もあるが，さて，**連分数 continued fraction** です。

これは繁分数のときに授業でもやったので，まず例から

$\frac{8}{3} = 2 + \frac{2}{3} = 2 + \frac{1}{\frac{3}{2}} = 2 + \frac{1}{1 + \frac{1}{2}}$ これを $2 + \frac{1}{1} + \frac{1}{2}$ と書こうというわけだ。

生徒の中には $\frac{1}{1} + \frac{1}{2}$ の意味でも上のように書くのがいて,「これは意味が違うんだよ。記号は真ん中に書け！」と言っているんだが。

余りで割る数を割っていくので，互除法と同じです。前の例でやると $\frac{1783}{1777} = 1 + \frac{1}{296} + \frac{1}{6}$

無理数になるともっと面白い。

$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + \sqrt{2} - 1} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}} = \cdots$ と繰り返すので

$\sqrt{2} = 1 + \frac{1}{2} + \frac{1}{2} + \cdots$ 無理数も無限表記を許せば分数で書ける。途中で切ればいい近似となる。

入試問題でも $a_{n+1} = \frac{1}{a_n} + 2$ なる漸化式を見かけるが，これですね。

正の極限値があるとすれば（無限連分数展開の極限の証明は本にある），$\alpha = \frac{1}{\alpha} + 2$ より，$\alpha = 1 + \sqrt{2}$

$a_{n+1} = \frac{1}{a_n} + 1$ なら $\alpha = \frac{1+\sqrt{5}}{2}$(Golden Number) で $\sqrt{5} = 2 + \frac{1}{4} + \frac{1}{4} \cdots$

for i:1 thru 10 do a:2+1/a　として，a を見ると，なるほどなあと思う。

a:1 として　for i:1 thru 10 do (a:2+1/a,display(float(a))) のように書くようです。

Maxima にも命令がいくつかあります。
cf() で，連分数（continued fraction）表示（リスト表示）する。
cfdisrep() で，リスト表示（representation）連分数を普通の連分数に表示する（display)。
ratsimp() は，有理数表示簡単化。

```
cf(8/3);
```
[2,1,2]

```
cfdisrep(%);
```
$$2+\cfrac{1}{1+\cfrac{1}{2}}$$

```
ratsimp(%);
```
$$\frac{8}{3}$$

有理数なら項は有限だが, 無理数なら無限項になるので,cflength:3 とかでその長さを決める。
下は cflength:10 として tex(cfdisrep(cf(sqrt(2)))) としたもの。

$$1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\frac{1}{2}}}}}}}}}$$

さあ，この「初頭整数論講義」の再読は面白そうなところだけ拾ってきているように見えて，実は意図があるのでした。まず，Diophantus の方程式。それを Euclid の互除法で解いたり，合同式で解いたり，そして最後が連分数でしたがこれがまた互除法と同じということで元へ戻るのです。具体的な問題が入試に出てます。（生徒の質問で知りました）

早稲田　(1) α, β を互いに素な正の整数とする。
(i) $\alpha x - \beta y = 0$ の整数解をすべて求めよ。
(ii) $\dfrac{\alpha}{\beta} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}}$（$a_1, a_2, a_3, a_4$は正の整数）と書けるとする。
$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}$ を通分して得られる分子 $a_1a_2a_3 + a_1 + a_3$ を p，分母 $a_2a_3 + 1$ を q とするとき，$\alpha q - \beta p$ の値を求めよ。
(2) $157x - 68y = 3$ の整数解をすべて求めよ。
さあ，やってみて，答えは次のページ。

本の内容は格子点とか無理数の有理数での近似とかの話題が続きますが，次の機会にしようかな。中からひとつ
$\dfrac{a}{b} > \dfrac{c}{d} \Longrightarrow \dfrac{a}{b} > \dfrac{a+c}{b+d} > \dfrac{c}{d}$ なんてのは便利そう。

前のページの答え

$157x-68y=3$ を解くのは,

157 と 68 で **Euclid の互除法**をすると,

右のように, この 2 数は互いに素。

よって，$157x-68y=1$ なる解は存在し

それを 3 倍すればいい。

2	157	68	3
	136	63	
4	21	5	
	20		
	1		

ついでだから，**合同式**の復習をしよう。

$157x-68y=1$ は $157x\equiv 1 \pmod{68}\cdots①$ $\Longleftrightarrow$ $21x\equiv 1 \pmod{68}\cdots②$

$2\times(①-7\times②)+②x\equiv 13 \pmod{68}$ このとき $y\equiv -30 \pmod{157}$

Maxima でやるなら inv_mod(157,68); で 13 と出力する。inverse of n modulo m. です。

つまり，$157x-68y=3$ の整数解は $x=39+68k, y=-90+157k$ (k は整数)

連分数でいくと $2+\frac{1}{3+\frac{1}{4+\frac{1}{5}}}$ 見にくいので $2+\dfrac{1}{3}+\dfrac{1}{4}+\dfrac{1}{5}$

$2+\dfrac{1}{3}+\dfrac{1}{4}=\dfrac{30}{13}$ だから $p=30, q=13$ で（なんと上の解じゃないか！），

$157\cdot 13-68\cdot 30=1$ これを 3 倍すればいいのだよという問題だ。

Euclid の互除法よりも，**合同式**よりも，**連分数**のほうが簡単じゃあないの？(でもないか，まあ，とにかくすべて同じ)

$\dfrac{\alpha}{\beta}=a_1+\dfrac{1}{a_2+\dfrac{1}{a_3+\dfrac{1}{a_{\ 4}}}}$ より，$\dfrac{\alpha}{\beta}-a_1=\dfrac{1}{a_2+\dfrac{1}{a_3+\dfrac{1}{a_{\ 4}}}}$

$\dfrac{\beta}{\alpha-a_1\beta}=a_2+\dfrac{1}{a_3+\dfrac{1}{a_{\ 4}}}$　左辺の分母分子は互いに素，以下同様にして

$\dfrac{\alpha-a_1\beta}{\beta-a_2(\alpha-a_1\beta)}=a_3+\dfrac{1}{a_{\ 4}}$　左辺の分母分子は互いに素，以下同様にして

$\dfrac{\alpha-a_1\beta}{\alpha-a_1\beta-a_3(\beta-a_2(\alpha-a_1\beta))}=a_4$　左辺の分母分子は互いに素，つまり分母 1

よって　$\alpha(1+a_2a_3)-\beta(a_1+a_3+a_1a_2a_3)=1$

つまり，$a_1+\dfrac{1}{a_2+\dfrac{1}{a_3}}$ を通分して得られる分子 $a_1a_2a_3+a_1+a_3$ を p，分母 a_2a_3+1 を q とするとき，

$\alpha q-\beta p=1$

各行の最初の式を見れば Euclid の互除法をしていると見えますね。

最後に極めつけ，**11 年東大**

実数 x の小数部分を，$0\leqq y<1$ かつ $x-y$ が整数となる実数 y のこととし，これを記号 $\langle x\rangle$ で表す。実数 a に対して，無限数列 $\{a_n\}$ の各項 a_n $(n=1, 2, 3, \cdots)$ を次のように順次定める。

(i) $a_1=\langle a\rangle$

(ii) $\begin{cases} a_n\neq 0 \text{ のとき}, a_{n+1}=\left\langle \dfrac{1}{a_n}\right\rangle \\ a_n=0 \text{ のとき}, a_{n+1}=0 \end{cases}$

(1) $a=\sqrt{2}$ のとき，数列 $\{a_n\}$ を求めよ。

(2) 任意の自然数 n に対して $a_n=a$ となるような $\dfrac{1}{3}$ 以上の実数 a をすべて求めよ。

(3) a が有理数であるとする。a を整数 p と自然数 q を用いて $a=\dfrac{p}{q}$ と表すとき，q 以上のすべての自然数 n に対して，$a_n=0$ であることを示せ。

新式算術講義より　No.1　整除に関する整数の性質

再読「初等整数論講義」の「1ユークリッドの互除法とディオファントスの方程式」の内容を違う視点で見ることができます。

ユークリッドの互除法は最大公約数（GCD）を求める方法で，それからディオファンタスの方程式も解けるという進み方でした。こちらは，最小公倍数（LCM）を求めて，それからディオファンタスの方程式を解くという進み方です。

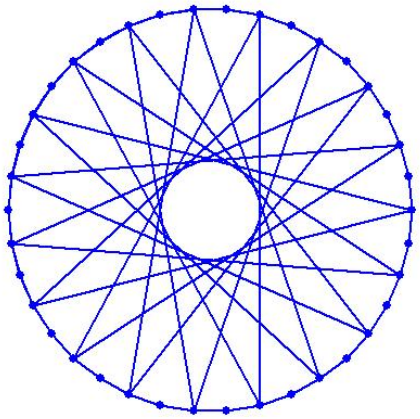
「最小公倍数を先にするの便利なること，蓋しポアンソーの創意なり」

前と同様に 38 と 16 の最小公倍数を求める。

まず，円を 38 等分する点をかき，その点を 16 ずつ進む線をかく。すると，線は最初の点に戻るまでに円を 8 回転する。つまり，38（の円を）× 8（回転する）＝ 16（の線が）× 19（本）＝ 304 が LCM。GCD は 38 等分点を 2 つずつおきに線が引かれているので 2。

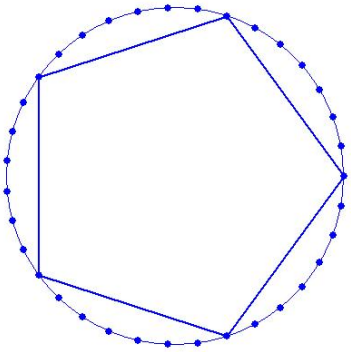
$38x + 16y = 2$ なるディオファンタスの方程式の答も図からすぐわかる。最初の点に近い 2 ずつ離れた点がそれ。つまり，38 × (-5)（回転）+16 × 12(本目) ＝ 2 と 38 × 3（回転）+16 × (-7)(本目) ＝ 2

38 と 16　回転：**8**　**LCM : 304**　本数：**19**　**GCD : 2**

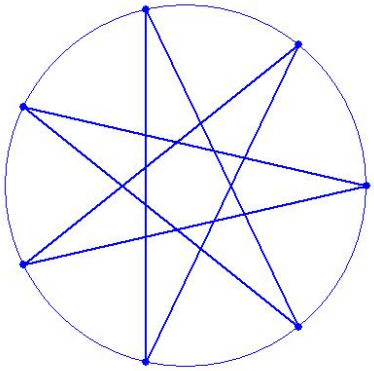


右の図画ファンクション・ビューでかいたもの。定数に 2 つの数字を入れることで，かってに図をかきます。以下数字を変えて楽しむと，

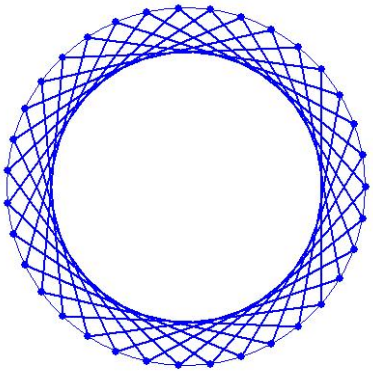
35 と 7　回転：**1**　**LCM : 35**　本数：**5**　**GCD : 7**



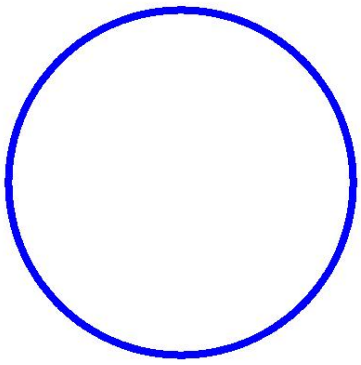
7 と 3　回転：**3**　**LCM : 21**　本数：**7**　**GCD : 1**



35 と 8　回転：**8**　**LCM : 280**　本数：**35**　**GCD : 1**



1783 と 1777　回転：**1777**　**LCM : 3168391**　本数：**1783**　**GCD : 1**



新式算術講義より　No.2　分数に関する整数論的の研究

「ガウスが其「整数論」の一節を特に循環小数の理論に割ける。以て鑑とすべし。」

ということで，再読「初等整数論講義」と重複するところもありますが（「Euler 関数と循環小数」を参照），循環小数を調べることで，オイラー関数の性質，フェルマーの小定理などを証明しているところがとても興味深いです。

まず，$\varphi(d)$ d 以下の d と互いに素な整数の個数のとき，分母が n の分数を考えることにより，

オイラー関数の性質 $\displaystyle\sum_{d\text{ は }n\text{ の約数}} \varphi(d) = n$

何故なら，分母が n の分数の個数は n 個あって，$\varphi(n)$ は約分されない分数の個数，$\varphi(d)$ は約分されて分母が d の分数の個数だから。

次に，10 と互いに素な分母を b 分子を a 分数の値を x ，循環説の長さを e とする。

$x = \dfrac{\text{循環節}}{10^e - 1}$ この分母が b の倍数だから $10^e - 1 \equiv 0\ (mod.b)$ つまり， e **は** $10^e - 1$ **を** b **の倍数たらしめるべき最小の正の整数**である。

循環節がつくられるときの割り算の余りの数字は b より小さく b と互いに素だから，その長さは， $e \leqq \varphi(b)$

よって $10^{\varphi(b)} \equiv 1\ (mod.b)$

ここで，10 を t ， b を素数 p とすれば，$t^{\varphi(p)} \equiv 1\ (mod.p)$ つまり $t^{p-1} \equiv 1\ (mod.p)$ でこれが**フェルマーの小定理**。

循環節の長さとそのダイヤル数（Wiki によると数を掛けてもその順は変わらない数のことをダイヤル数と言うらしい）を Maxima で調べると（どうもプログラミングの才能はないな），

```
repe(b):=block(
(
s:"",
for i:1 thru b-1 do
if mod(10^i-1,b)=0 then return(e:i)
),
for j:0 thru floor(log(b)/log(10))-1 do s:concat("0",s),
print(i,":","length=",e,",",(concat(s,floor((10^e/b)))))
)$
for i:2 thru 40 do if gcd(10,i)=1 and primep(i) then repe(i);
```

```
3:length=1,3
7:length=6,142857
11:length=2,09
13:length=6,076923
17:length=16,0588235294117647
19:length=18,052631578947368421
23:length=22,0434782608695652173913
29:length=28,0344827586206896551724137931
31:length=15,032258064516129
37:length=3,027
```

さらに，循環小数に出てくる数字について調べると，
タイプ１　循環節の長さが分母－１（$e=b-1$）のとき，例えば $b=7$
タイプ２　タイプ１でないもの，例えば $b=3,11,13$
があって，
タイプ１のとき，出てくる数字は 142857（余りは 7 より小さいすべての数 326451）でこれが循環する。
$\frac{1}{7}=0.\dot{1}42857\dot{}, \frac{2}{7}=0.\dot{2}85714\dot{}, \frac{3}{7}=0.\dot{4}28571\dot{}, \frac{4}{7}=0.\dot{5}71428\dot{}, \frac{5}{7}=0.\dot{7}14285\dot{}, \frac{6}{7}=0.\dot{8}57142\dot{}$
$\left(\frac{1}{7}+\frac{6}{7}=1, \text{左}+\text{右}=1 \text{だよな}\right)$

タイプ２のとき，出てくる数字はグループに別れ，そのグループごと循環する。
$\frac{1}{3}=0.\dot{3}, \frac{2}{3}=0.\dot{6}, \cdots \left(\frac{1}{3}+\frac{2}{3}=1 \text{だよな}\right)$

$\frac{1}{11}=0.\dot{0}\dot{9}, \frac{2}{11}=0.\dot{1}\dot{8}, \frac{3}{11}=0.\dot{2}\dot{7}, \frac{4}{11}=0.\dot{3}\dot{6}, \frac{5}{11}=0.\dot{4}\dot{5},$
$\frac{10}{11}=0.\dot{9}\dot{0}, \frac{9}{11}=0.\dot{8}\dot{1}, \frac{8}{11}=0.\dot{7}\dot{2}, \frac{7}{11}=0.\dot{6}\dot{3}, \frac{6}{11}=0.\dot{5}\dot{4}$ (上＋下＝1 だよな)

$\frac{1}{13}=0.\dot{0}76923\dot{}, \frac{3}{13}=0.\dot{2}30769\dot{}, \frac{4}{13}=0.\dot{3}07692\dot{}, \frac{9}{13}=0.\dot{6}92307\dot{}, \frac{10}{13}=0.\dot{7}69230\dot{}, \frac{12}{13}=0.\dot{9}23076\dot{}$
$\frac{2}{13}=0.\dot{1}53846\dot{}, \frac{5}{13}=0.\dot{3}84615\dot{}, \frac{6}{13}=0.\dot{4}61538\dot{}, \frac{7}{13}=0.\dot{5}38461\dot{}, \frac{8}{13}=0.\dot{6}15384\dot{}, \frac{11}{13}=0.\dot{8}46153\dot{}$
（上と下と別々に，左+右=1 だよな）

ひとつの循環小数の数字にもある規則があって，それは再読「初等整数論講義」の「Euler 関数と循環小数」に記した。
すると，例えば $\frac{1}{17}$ なんかは循環節の長さは 16，そのうち最初の 8 個を実際に計算して求めると 0.05882352，続きは 94117647 で循環（足して 9 になる数字）。
$\frac{2}{17}$ は 0.05882352 を 2 倍して初めを予想し $0.\dot{1}176470588235294\dot{}$ と分かるわけだ。
$\frac{16}{17}$ は $,\dot{9}411764705882352\dot{}$。
又，$\frac{1}{37}$ は循環節の長さは 3，実際に計算して求めると $0.\dot{0}27\dot{}$。$\frac{2}{37}$ は $0.\dot{0}54\dot{}$ と分かるわけだ。
$\frac{36}{37}$ は $,\dot{9}72\dot{}$。

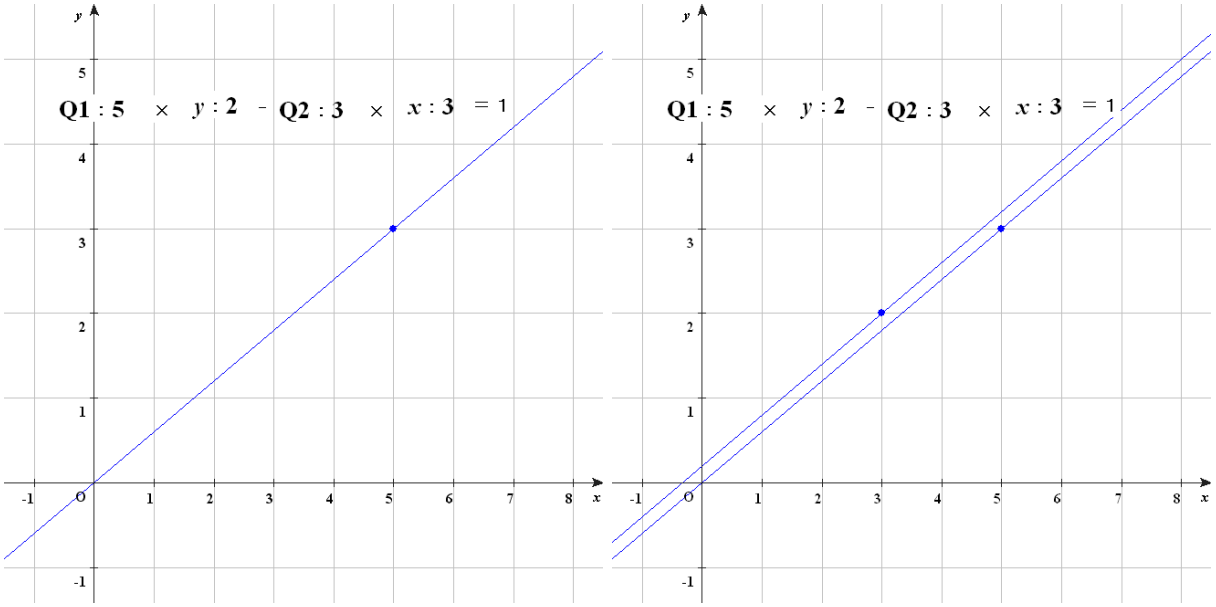
「新式算術講義」は，数の性質・演算を公理主義的に量を基本に構築している本なので，無理数論とか極限論にそのいいところがある。なので内容は「解析概論」につながるものではあるが，前半の整数のところが，面白かったので，内容が重なる「初等整数論講義」につけてみた。

発行年度を見れば 100 年前以上の本だから，読みにくいところもあるが，ヒルベルト流の公理的な実数論は若かった（29 歳）彼がオリジナルにやってみたかったことなのだろう。その意気は感ずることができる。写真は Wiki から。

数学雑談 再読１ 格子幾何学によるディオファンタス方程式の解法

ディオファンタスの方程式は, ユークリッド互除法を使う，合同式を使う，連分数を使うなど色々の方法があって，まことにきらびやかな所ですが，ここでまた，別方法，格子幾何学による解法が出てきます。

原点に一番近い格子点が $A(a,b)$ だとすると a,b は互いに素。$ay-bx=1$ は 直線 $y=\dfrac{b}{a}x+\dfrac{1}{a}$ を表し，この直線上の点 $P(x,y)$ と (a,b) と原点が作る面積が 1 ということである。
ともに整数の x,y が存在するのは，OA に平行な直線が $y=\dfrac{b}{a}x+\dfrac{1}{a}$ から $y=\dfrac{b}{a}x+\dfrac{a-1}{a}$ まで $a-1$ 本できて， $0<x<a$ に格子点が $a-1$ 個つまり直線に 1 個ずつあることからわかる。
とすれば，直線 $y=\dfrac{b}{a}x+\dfrac{1}{a}$ の x に 1 から $a-1$ まで代入してチェックすればいいことになる。
下の図は $a=5,b=3$ のとき。



格子平行四辺形に属する格子点の数を n とすればその面積は丁度 n に等しい。辺上の点は 2 辺を，頂点は一つのみ平行四辺形に属するとする。
これを拡張して，いわゆるピックの定理が成立することになる。
ピックの定理は Wiki によると「頂点がすべて格子である多角形の内部にある格子点の個数を i ，辺上にある格子点の個数を b とするとこの種の多角形の面積 $S=i+\dfrac{b}{2}-1$」Wiki のこの解説が面白い。 「日本ではこの公式は学習しないことが多いが、海外では小中学校などで教えられることもある。」