プログラミングの背景：数論

整数の合同と一次合同式

tbasic.org [*1]

[2014 年 9 月版]

・・・

これから，２つの数の合同を表すのに記号 ≡ を使う[a]。また必要なら括弧付で法も付加する。

（ガウス Disquisitiones Arithmeticae（数論研究））

[a] 合同と通常の等号との類似性からこの記号を採用した。

整数の合同の理論は，数論での基本的概念，道具であり，数論を学ぶ者にとって，最も基本的な常識の一つです。「合同知らずして，数論学ぶべからず。」とも言えるほど基本的なものです。

また，暗号の理論などにも良く使われ，情報科学について詳しく知ろうとする人にとっても，合同の理論は常識の 1 つです。勿論，詳しい正確な説明はかなりの量の説明が必要です 。詳細な内容は整数論の教科書に譲ることにして，ここでは，合同の基本的概念とその性質，そして 1 次合同式について説明します。

目次

[*1] http://www.tbasic.org

整数, 或いは自然数の研究（数論）は古くは，古代ギリシア，ピタゴラスまで遡ります。そしてそれらの成果はユークリッド「原論」の中に見ることができます。そこでは，ユークリッドの互除法を始めとして，素数の無限性や, 完全数などが扱われています。

近代的な数論は, フェルマー (1601-1665) に始まると言われています。フェルマーは整数について多くの結果・事実を指摘しています。フェルマーに続いて多くの数学者が数論の研究に携わりました。その中でもオイラー (1707-1783) やラグランジェ (1736-1813) は有名です。そこでの基本的問題のひとつとして，ある数をある数で割ったときの余りの性質を調べることがありました。例えば，オイラーらは 4 で割って余りが 1 となる素数は，2 つの平方数の和として表されること示しています。

例えば

$$5 = 1^2 + 2^2$$

$$13 = 2^2 + 3^2$$

です。この定理はフェルマーによって直角 3 角形の基本定理と呼ばれたものです。フェルマーはこの事実を指摘していましたが，証明されたのはそれから 100 年も経ってのことでした。

整数の合同は，ある数で割ったときの余りに注目してその性質を調べるもので，上述のようにその研究は古くから行われてきました。しかし，ガウス (1777-1855) は「数論研究」(Disquitiones Arithmeticae)1801 [*2]で整数の合同についての新しい記号法を提案し，その記号を用いて従来の結果を体系的に論じ，数論の理論展開の方法を確立しました。またそれだけでなく，D.A. では，ガウスによる研究の成果も多く含まれています。ここに，合同の理論を含む数論研究の新たな進展が始まりました。

D.A. の内容は，ほぼそのままでも現在の初等整数論の高レベルの教科書として通用する内容，形式を持っていて，数論研究の歴史の中で画期的な著作でした。

以下に説明する合同の性質は，D.A. 全 7 章の内，冒頭部分第 1，2 章に既に含まれています。

1 整数の合同

1.1 合同の定義

ガウスは合同を以下の通り定義しました。

合同

a, b を整数，m を自然数とする $a-b$ が m で割り切れるとき，即ち，$m \mid a-b$ のとき，

$$a \equiv b \pmod{m}$$

と表し，a と b は m を法として合同であると言う[*3] 。

定義の通り

$$m \mid a-b \qquad \Longleftrightarrow \qquad a \equiv b \pmod{m}$$

[*2] D.A. と略記することもあります。

[*3] D.A. では混乱の恐れがない場合，しばしば法 m は省略されますが，ここでは常に法 m を括弧付で記します。

ですから，これは単なる言い換えとも見られます。しかし，ガウスが D.A. の脚注で述べているように，合同と数の相等との類似性からこの記号法が採用されました。この類似性への着目は理論の深い洞察の成果で，この記法によって，合同の理論のより深化が可能になったと言えます[*4]。

$\equiv$ と $=$ は良く似た性質を持ちますが，まず，次が成立します。

命題 1.1. 整数 a, b, c に対して，次が成立する。

(1) $a \equiv a \pmod{m}$
(2) $a \equiv b \pmod{m}$ ならば，$b \equiv a \pmod{m}$
(3) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m}$ ならば，$a \equiv c \pmod{m}$

これらは殆ど明らかな性質ですが，定義から厳密に証明できることの確認は大切です。ここでは，証明の練習として，確認してみましょう。

証明. (1) $m \mid 0 = a - a$ より，$a \equiv a \pmod{m}$ が得られる。
(2) $a \equiv b \pmod{m}$ は，$m \mid a - b$，即ち，整数 k に対して，$a - b = km$ と表されることを意味する。このとき，$b - a = -km$ だから，$m \mid b - a$，従って，$b \equiv a \pmod{m}$ となる。
(3) $a \equiv b \pmod{m}$ より，$m \mid a - b$，即ち，ある整数 k に対して，

$$a - b = km \tag{$*$}$$

と表される。同様に，$b \equiv c \pmod{m}$ より，ある整数 ℓ に対して，$b - c = \ell m$，即ち，$b = c + \ell m$ と表される。この式を $(*)$ に代入すれば，

$$a - (c + \ell m) = km$$

が得られる。これを整理すれば，$a - c = (k - \ell)m$ が得られ，従って，

$$a \equiv c \pmod{m}$$

となる。 □

このような性質 (1), (2), (3) を満たすものを**同値関係**と言います。この命題は合同が同値関係であることを示しています。同値関係は「この性質により，ものを分類することができ，その分類されたひとまとまりを，一つのもののように扱える対象である」ことを意味します。

この事実は，$\equiv$ の関係が $=$ と同様に，代入などが可能であること示しています。
例えば，$13 \equiv 5 \pmod{8}$ かつ $13 \equiv 21 \pmod{8}$ から，

$$21 \equiv 13 \equiv 5 \pmod{8}, \text{ 即ち, } 21 \equiv 5 \pmod{8}$$

を結論できます。

[*4] 数学における記号法は進化は対応する概念の進化を伴います。ですから優れた記号法の発明は，1 つの理論の発見にも匹敵します。勿論，ガウスの数学に対する膨大な貢献の中では，これはほんのささやかなものです。

合同についての色々な性質を示す準備として，合同の特徴付けを考えましょう。**整数での除法の定理**を整数 a と自然数 m に適用すると，

$$a = qm + r,\ \ 0 \leqq r < m$$

となる整数 q, r が唯 1 組存在します。この r のことを，a **を** m **で割ったときの最少非負剰余**と言います。このとき，$a - r = qm$ ですから，

$$a \equiv r \pmod{m}$$

となります。

このことを使うと合同について次の特徴付けができます。

命題 1.2. 次の (1), (2) はそれぞれ，$a \equiv b \pmod{m}$ となるための必要十分条件である。

(1) a と b の m で割ったときの最小非負剰余がそれぞれ等しい。

(2) $k \in \mathbb{Z}$ に対して，$a = b + km$ の形に書ける。

証明. a を m で割ったときの最少非負剰余を r_a, b を m で割ったときの最少非負剰余を r_b とする。このとき，

$$\begin{aligned} a &\equiv r_a \pmod{m},\ 0 \leq r_a < m \\ b &\equiv r_b \pmod{m},\ 0 \leq r_b < m \end{aligned}$$

である。

(1) $a \equiv b \pmod{m}$ とする。このとき，

$$r_a \equiv a \equiv b \equiv r_b \pmod{m}$$

より，$r_a \equiv r_b \pmod{m}$ ，即ち，$m \mid (r_a - r_b)$ である。従って，$m \mid |r_a - r_b|$ でもある。ここで，$0 \leq r_a < r_b$ とすると，$0 < |r_a - r_b| = (r_b - r_a) < m$ より矛盾である。他方，$0 \leq r_b < r_a$ とすると，$0 < |r_a - r_b| = (r_a - r_b) < m$ よりやはり矛盾である。従って，残る場合，$r_a = r_b$ が成立する。

逆に，$r_a = r_b$ なら，明らかに

$$a \equiv r_a = r_b \equiv b \pmod{m}$$

が成立する。

(2) $a \equiv b \pmod{m}$ とする。このとき定義より。$m \mid (a - b)$ であり，整数 k に対して，$a - b = km$ と表される。故に，$a = b + km$ の形に書ける。

逆に $a = b + km$ なら，$m \mid (a - b)$ であり，$a \equiv b \pmod{m}$ となる。 □

1.2 合同での演算（加法・減法・乗法）

≡ と = は良く似た性質を持ちますが，加・減・乗の演算については，特に良い性質を持っています。即ち，次が成立します。

命題 1.3. $a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m}$ とすると，次が成立する。

(1) $a + b \equiv a' + b' \pmod{m}$

(2) $a - b \equiv a' - b' \pmod{m}$

(3) $a \times b \equiv a' \times b' \pmod{m}$

証明. 上の命題 1.2 を使う。まず，仮定より， $a = a' + km$, $b = b' + jm$ の形に書ける。

(1) $a + b = a' + km + b' + jm = a' + b' + (k + j)m$ だから，
$a + b \equiv a' + b' \pmod{m}$ となる。
(2) 同様に，$a - b = a' + km - b' - jm = a' - b' + (k - j)m$ だから，
$a - b \equiv a' - b' \pmod{m}$ となる。
(3) $a \times b = (a' + km)(b' + jm) = a'b' + (kb' + a'j + kjm)m$ だから，
$a \times b \equiv a' \times b' \pmod{m}$ となる。

□

命題で，$b' = b$ とすると次の系が得られます。

系 1.1. $a \equiv a' \pmod{m}$ とすると，次が成立する。

(1) $a + b \equiv a' + b \pmod{m}$
(2) $a - b \equiv a' - b \pmod{m}$
(3) $ab \equiv a'b \pmod{m}$

また，命題で，$b = a$, $b' = a'$ とすると次の系が得られます。

系 1.2. $a \equiv a' \pmod{m}$ とすると，任意の自然数 n に対して，

$$a^n \equiv a'^n \pmod{m}$$

となる。

この命題およびその系の主張は自然で，またその証明も難しいものではありません。そしてそのことから，この命題およびその系の効力は大したことがないと思うかもしれません。しかし，そうではありません。

例えば次の問題を考えてみましょう。

例 1.1. 7^{123} を 6 で割った時の余りを求めよ。

この問題は，合同についてある程度慣れた人であれば，一瞬で答えを出すことのできる大変簡単な問題です。しかし，合同について初めて学ぶ人にとってはそうでないかも知れません。

7^{123} は 104 桁の数です。現在の計算機の能力からすれば，この数を実際に計算することは簡単です。実際

$$\begin{aligned} 7^{123} = {} & 88523570369346801684435811372718127585670061114702144933569 2 \\ & 45260093253728999880981421881473709365496343 \end{aligned}$$

ですから，この数を実際に 6 で割って余りを求めることは可能です。しかし，この計算を手で行おうとする人は少ないでしょう。実はこの余りは上の性質から瞬時に求められます。実際，$7 \equiv 1 \pmod{6}$ に注意すると，

$$7^{123} \equiv 1^{123} \equiv 1 \pmod{6}$$

となり，余りは 1 です！

このような事実は，≡ 記号が，剰余の性質を正確に表現し，この記号無しでは気の付かない事柄を，明白に示してくれることを意味しています。つまり，この記号により，整除性についてより本質的な見方を獲得したことになります。

合同の応用としてよくあげられる，曜日の問題を考えましょう。

例 1.2. 2114 年 9 月 1 日は何曜日か？

解. 曜日は 7 を法とした合同関係と考えることができます。
2014 年 9 月 1 日を第 1 日として，2114 年 9 月 1 日までのひにちを数えましょう。

何日目 (mod7)	1	2	3	4	5	6	0
曜日	月	火	水	木	金	土	日
年月日	2014/09/01	2014/09/02	2014/09/03	2014/09/04	2014/09/05	2014/09/06	···

1 年は平年は 365 日，うるう年は 366 日です[*5]。2015 年から 2114 年の間のうるう年を列挙すると，

$$2016,\ 2020,\ \ldots,\ 2096,\ 2104,\ \ldots,\ 2112$$

であり，全部で 24 回あります。従って，2014 年 9 月 1 日から 2114 年 8 月 31 日の間は

$$365 \times 76 + 366 \times 24 = 36524$$

日あり，2114 年 9 月 1 日は，36525 日目になります。ここで，

$$36525 \equiv 6 \pmod 7$$

ですから，2114 年 9 月 1 日は土曜日になります。 □

1.3 異なる法での性質

前項での法 m は同じ m についてでした。法を変えると合同関係は別なものになりますが，いくつかの相互関係もあります。ここではそれらの内，いくつか基本的な事項をまとめてみましょう。

法は大きくなればなる程，分類が精密になります。ですから，逆に，ある合同関係が成立する場合，法を小さくすれば，分類が荒くなり，その合同関係はその法でも成立します。即ち，次が成立します。

命題 1.4. $m' \mid m$ とする。このとき，

$$a \equiv b \pmod m \implies a \equiv b \pmod{m'}$$

が成立する。

証明. $a \equiv b \pmod m$ ならば，$a = b + km$ と書けるが，$m' \mid m$ より $m = \ell m'$ と書ける。従って，$a = b + km = a + k\ell m'$ と書け，$a \equiv b \pmod{m'}$ となる。 □

[*5] うるう年は 4 で割り切れて，100 で割り切れない年，だたし 400 で割り切れる年はうるう年である。

２つの法で成立する合同関係は，法の最小公倍数を法としても成立します。即ち，次が成立します。

命題 1.5. $a \equiv b \pmod{m}$，$a \equiv b \pmod{m'}$ とする。このとき，

$$a \equiv b \quad \left(\mathrm{mod}\ \frac{mm'}{\gcd(m, m')}\right)$$

が成立する[*6][*7]。特に，$\gcd(m, m') = 1$ のとき，

$$a \equiv b \pmod{mm'}$$

が成立する

命題の証明のために，補助定理を 2 つあげます。まず，次の補助定理は，最大公約数の基本的性質の一つです。証明は簡単です。

補助定理 1.1. $a,\ b \in \mathbb{Z}$ に対して，$\gcd(a, b) = c > 0$ と置く。このとき，

$$\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = 1$$

となる。

補助定理 1.1 の証明. 実際，$\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = d > 1$ なら，$d \,\Big|\, \frac{a}{c}$ かつ $d \,\Big|\, \frac{b}{c}$ であり，$cd \mid a$ かつ $cd \mid b$ となる。従って，$c < cd \mid \gcd(a, b)$ となり矛盾である。 □

次の補助定理は整除性と最大公約数との基本的関係の一つです。

補助定理 1.2. $\gcd(a, b) = 1$ とする。このとき

$$a \mid c \ \text{ かつ } \ b \mid c \quad \text{ならば，} \quad ab \mid c$$

となる。

この補助定理は，拡張ユークリッドの互除法を用いる証明が標準的ですが，ここでは，素因数分解の一意性を使った証明を与えましょう[*8]。

補助定理 1.2 の証明. a，b を素因数分解して

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r} \qquad (e_i \in \mathbb{N},\ e_i > 0)$$

$$b = q_1^{f_1} \cdot q_2^{f_2} \cdots q_r^{f_s} \qquad (f_j \in \mathbb{N},\ f_j > 0)$$

[*6] $\gcd(m, m')$ は m と m' の最大公約数を表します。

[*7] m と m' の最小公倍数を $\mathrm{lcm}(m, m')$ としたとき，$mm' = \gcd(m, m')\mathrm{lcm(m, m')}$ に注意すれば，上の式は，

$$a \equiv b \pmod{\mathrm{lcm}(m, m')}$$

とも表されます。

[*8] 拡張ユークリッドの互除法を用いる証明は「拡張ユークリッドの互除法」の稿で紹介します。

と表したとする。$a \mid c$ より，各 i に対して，$p_i^{e_i} \mid c$ である。即ち，c の素因数分解には，$p_i^{e_i}$ が含まれる。同様に，c の素因数分解には，$q_j^{f_j}$ も含まれる。ここで，$\gcd(a,b) = 1$ より，p_i と q_j はすべて異なる。従って，c の素因数分解には，

$$ab = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r} \cdot q_1^{f_1} \cdot q_2^{f_2} \cdots q_r^{f_s}$$

が含まれる。従って，$ab \mid c$ である。 □

命題の証明. $a \equiv b \pmod{m}$，$a \equiv b \pmod{m'}$ より，$a - b = km = \ell m'$ となる。$d = \gcd(m, m')$ と置くと，

$$\frac{a-b}{d} = k\frac{m}{d} = \ell\frac{m'}{d}$$

となる。即ち，

$$\frac{m}{d} \;\Big|\; \frac{a-b}{d} \quad \text{かつ} \quad \frac{m'}{d} \;\Big|\; \frac{a-b}{d}$$

である。ここで，補助定理 1.1 より，

$$\gcd\left(\frac{m}{d}, \frac{m'}{d}\right) = 1$$

だから，補助定理 1.2 より，

$$\frac{m}{d}\frac{m'}{d} \;\Big|\; \frac{a-b}{d}, \quad \text{即ち}, \frac{a-b}{d} = s\frac{m}{d}\frac{m'}{d}$$

と表される。従って，

$$\frac{mm'}{d} \,\Big|\, (a-b)$$

を得る。 □

次の命題は系 1.1(3) と似た内容ですが，それより少し強い結果になっています。

命題 1.6. $a \equiv b \pmod{m}$ とする。このとき，$c \in \mathbb{Z}$ に対して，

$$ac \equiv bc \pmod{|cm|}$$

となる。

証明. $a = b + km$ より，$ac = bc + kcm$ である。これから，$ac \equiv bc \pmod{|cm|}$ を得る。 □

1.4 剰余代表系

整数は無限にありますが，m で割ったときの余りは $0, 1, \ldots, m-1$ と有限個です。ですから，m を法とする合同計算は，本質的には有限個の数の間の演算になります。このことに注目すると，m を法とする合同を考えるとき，同じ最少非負剰余を持つ整数の集まりを考え，その中からひとつずつ代表を選び，それらについて演算を行うことが考えられます。このようなことを考えることで，好都合な場合もあります。

ことのようにして選ばれた代表の集まりを**代表系**と言います。代表系についての一般的定義もありますが，ここでは，よく使われる２種の代表系について説明しましょう。

除法の定理で扱った最小非負剰余を代表とするのが最もよく使われる代表系です。

最小非負剰余代表系

任意の整数 a は，$0 \leqq r \leqq m-1$ となる整数 r に対して，

$$a \equiv r \pmod{m}$$

とただ一通りに表される。この r を m **を法とする** a **の最小非負剰余**と言う。
集合 $\{0, 1, 2, \ldots, m-1\}$ を m **を法とする最小 (非負) 剰余代表系という。**

すべての整数は，これらの代表系の数と合同ですから，すべての合同に関する議論は，実際には，これらの数について行えば良いことが分かります。代表系は有限集合ですから，小さな数での法の場合，そべての場合を計算することで，厳密な結果を得ることができます。

例えば，次のような問題を，すべての場合の具体的計算で解くことができます。

例 1.3.

$$x^3 = 6y^3 + 3 \tag{$*$}$$

となる 正整数 x, y は存在しない。

一見すると難しいと思われる問題ですが，上の式が (mod 7) で解を持たないことに気が付けば簡単な問題になります。

証明. $(*)$ を法 7 での式として，

$$x^3 \equiv 6y^3 + 3 \pmod{7} \tag{$*'$}$$

を考える。ここで，7 を法とする最小非負代表系は $\{0, 1, 2, 3, 4, 5, 6\}$ である。そこで，左辺 x^3 を $x \equiv 0, 1, 2, 3, 4, 5, 6$ について計算し，対応する代表系でみると，それぞれ $0, 1, 1, 6, 1, 6, 6$ となる。

同様に，右辺 $6y^3 + 3$ を $y \equiv 0, 1, 2, 3, 4, 5, 6$ について計算し，対応する代表系でみると，$3, 2, 2, 4, 2, 4, 4$ となる。左辺と右辺が一致する場合が無く， 従って，$(*')$ は解を持たない。故に，$(*)$ も解を持たない。 □

剰余代表系を使って簡単に示すことのできる例をもう一つあげましょう。これは直角三角形の基本定理の逆です。

例 1.4. p を奇素数として，平方数の和として表される，即ち，$a, b \in \mathbb{N}$ に対して

$$p = a^2 + b^2$$

と表されるとする。このとき，

$$p \equiv 1 \pmod{4}$$

である。

証明. 4 を法とする合同式

$$p \equiv a^2 + b^2 \pmod{4}$$

を考え，この右辺をすべての場合について計算する。4 を法とする最小非負剰余代表系は $\{0,1,2,3\}$ である。これについて，a^2，b^2 を計算し，対応する 4 を法とする最小非負剰余代表を取ると，それぞれ $\{0,1,0,1\}$ である。従って，a^2+b^2 の 4 を法とする最小非負剰余代表系で取り得る値は，

$$0+0=0,\ 0+1=1,\ 1+0=1,\ 1+1=2 \qquad (*)$$

の 4 通りである。ここで，p は奇数だから，a^2+b^2 は奇数になる。$(*)$ で取る値は，$0,1,2$ であり，その値が奇数になるのは，1 の場合である。即ち

$$p \equiv 1 \pmod 4$$

である。 □

よく使われる代表系として，別の代表系をもう一つあげましょう。

絶対値最小剰余代表系

(1) m が正の奇数の場合。
このとき，$a \in \mathbb{Z}$ に対して，$a \equiv r \pmod m$, $|r| \leq \dfrac{m-1}{2}$ となる $r \in \mathbb{Z}$ が丁度 1 つ存在する。
この r を m **を法とする絶対値最小剰余**と言う。
集合 $\{-\dfrac{m-1}{2}, \ldots, -1, 0, 1, 2, \ldots, \dfrac{m-1}{2}\}$ を m **を法とする絶対値最小剰余代表系という。**

(2) m を正の偶数の場合。
このとき，$a \in \mathbb{Z}$ に対して，$a \equiv r \pmod m$, $-\dfrac{m}{2} \leq r < \dfrac{m}{2}$ となる $r \in \mathbb{Z}$ が丁度 1 つ存在する。
この r を m **を法とする絶対値最小剰余**と言う。
集合 $\{-\dfrac{m}{2}, \ldots, -1, 0, 1, 2, \ldots, \dfrac{m}{2}-1\}$ を m **を法とする絶対値最小剰余代表系**という。

こちらの代表系は，最小非負剰余代表系に比べて，技術的に感じるかもしれません。しかし，実際はそうでもありません。例えば次が成立します。

例 1.5 (8 ビットの符号付整数)**.** $m = 2^8$ の場合の，絶対値最小剰余系は，

$$\{-128, -127, \ldots, -2, -1, 0, 1, 2, \ldots, 126, 127\}$$

であり，8 ビットでの 2 の補数による符号付整数全体に一致する。

このことは一般的に言えます。即ち，

> n ビットでの 2 の補数による符号付整数は，
> $m = 2^n$ を法とする絶対値最小剰余代表系に一致する。

となります。

このように，合同の理論は計算機における符号付整数の表現と密接に結びついています。[*9]

絶対値最小剰余代表系の例をあげましょう。

[*9] コンピューターにおける整数の表現法については項を改めて説明しますが，その際，絶対値最小剰余代表系は鍵となる概念です。

例 1.6.

奇数の場合：0 を中心とした対称形になる。

- $m = 3$ の場合，絶対値最小剰余代表系は，$\{-1, 0, 1\}$
- $m = 5$ の場合，絶対値最小剰余代表系は，$\{-2, -1, 0, 1, 2\}$
- $m = 7$ の場合，絶対値最小剰余代表系は，$\{-3, -2, -1, 0, 1, 2, 3\}$
- ・・・

偶数の場合：負，非負によって 2 等分したものになる。

- $m = 2$ の場合，絶対値最小剰余代表系は，$\{-1, 0\}$
- $m = 4$ の場合，絶対値最小剰余代表系は，$\{-2, -1, 0, 1\}$
- $m = 6$ の場合，絶対値最小剰余代表系は，$\{-3, -2, -1, 0, 1, 2\}$
- ・・・

代表系を使った例をもう一つあげます。

例 1.7.

$$x^2 - 2y^2 = 3 \tag{**}$$

を満たす整数 x，y は存在しない。

これも，3 を法とする問題として考えば良いことに気づけば，簡単な計算問題になります。

証明. (**) を満たす整数 x，y が存在したとする。このとき，x，y ともに 3 では割り切れない。実際，例えば，$3 \mid x$ とする。(**) の右辺 = 3 は 3 で割り切れるからこのとき，左辺も割り切れ，$3 \mid y$ となる。しかし，この場合，$3^2 \mid x^2$，$3^2 \mid y^2$ となるから，左辺は，3^2 で割り切れる。従って，右辺 = 3 も 3^2 で割り切れることになり，矛盾である。$3 \mid y$ としても同様である。

そこで，(**) を 3 を法とする合同式

$$x^2 - 2y^2 \equiv 0 \pmod 3$$

とみる。3 を法とする絶対値最小剰余代表系は，$\{-1, 0, 1\}$ である。そこで，x^2 を $x \equiv -1, 0, 1$ について計算し，対応する代表系でみると，それぞれ $1, 0, 1$ となる。$-2y^2 \equiv y^2 \pmod 3$ を $y \equiv -1, 0, 1$ について計算し，対応する代表系でみると，それぞれ $1, 0, 1$ となる。従って，$x^2 + (-2y^2) \equiv 0 \pmod 3$ となるのは，$x \equiv y \equiv 0 \pmod 3$ の場合だけである。これは，「x，y ともに 3 では割り切れない」ことに矛盾する。 □

2　一次合同式

2.1　合同での演算（除法）

合同 $\equiv$ は加減乗演算については，良い性質を持ち，扱いも簡単でした。しかし，除法（割り算）についてはそうではありません。元々合同は整数の範囲での記号法です。そして整数を整数で割った場合，整数にならないこともあります。ですから，$\equiv$ で割り算を考えるときは少し注意が必要なのです。

例えば，

$$ab \equiv ac \pmod{m}$$

でも，両辺を a で割って $b \equiv c \pmod{m}$ できるとは限りません。実際，

$$3 \cdot 5 \equiv 15 \equiv 9 \equiv 3 \cdot 3 \pmod{6}$$

ですが，

$$5 \equiv 3 \pmod{6}$$

ではありません。

この場合 $3 \cdot 5 \equiv 3 \cdot 3 \pmod{6}$ から $5 \equiv 3 \pmod{6}$ を得ようとする推論には，見かけ上はありませんが，実は商が整数にならない割り算が含まれています。実際，$3 \cdot 5 \equiv 3 \cdot 3 \pmod{6}$ は

$$6 \mid (3 \cdot 5 - 3 \cdot 3) = 3 \cdot (5 - 3) = 3 \cdot 2$$

を意味し，この式から，$6 \mid (5 - 3) = 2$ を導くことはできません。

しかし，割り算を注意深く，上手に解釈すると，割り算ができる場合もあります。例えば，上の式で

$$5 \equiv 3 \left(\mod 2 = \frac{6}{3}\right)$$

を得ることはできます。この事実は，一般化され，次が成立します。

命題 2.1.

$$ab \equiv ac \pmod{m}$$

ならば，$d = \gcd(a, m)$ に対して，

$$b \equiv c \left(\mod \frac{m}{d}\right)$$

となる

証明のために次の補助定理を示しましょう。

補助定理 2.1. $\gcd(a, b) = 1$ とする。このとき

$$a \mid bc \quad \text{ならば，} \quad a \mid c$$

となる。

この補助定理も，拡張ユークリッドの互除法を用いる証明が標準的ですが，ここでは，素因数分解の一意性を使った証明を与えます。

補助定理 2.1 の証明. a を素因数分解して

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r} \qquad (e_i \in \mathbb{N},\ e_i > 0)$$

と表したとする。$a \mid bc$ より，各 i に対して，$p_i^{e_i} \mid bc$ である。即ち，bc の素因数分解には，$p_i^{e_i}$ が含まれる。ここで，$\gcd(a,b) = 1$ より，b の素因数分解には p_i が含まれない。従って，c の素因数分解には，$p_i^{e_i}$ が含まれる。故に，c の素因数分解には，$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$ が含まれる。従って，$a \mid c$ である。 □

命題の証明. $ab \equiv ac \pmod{m}$ より，$m \mid (ab - ac) = a(b-c)$ となる。即ち，ある整数 k に対して，$a(b-c) = km$ と表される。この両辺を $d = \gcd(a,m)$ で割ると，

$$\frac{a}{d}(b-c) = k\frac{m}{d} \tag{$*$}$$

を得る。ここで，補助定理 1.1 より，$\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ である。従って，$(*)$ に補助定理 2.1 を適用して，

$$\frac{m}{d} \ \Big|\ (b-c), \quad \text{即ち，} b \equiv c \pmod{\frac{m}{d}}$$

を得る。 □

例 2.1. 合同式

$$3 \cdot 5 \equiv 3 \cdot 3 \pmod{6}$$

で，$\gcd(3,6) = 3$ より，

$$5 \equiv 3 \pmod{2 = \frac{6}{3}}$$

となる。

系 2.1 (命題の系：簡約律). $\gcd(a,m) = 1$ のとき，

$$ab \equiv ac \pmod{m} \quad \text{ならば，} \quad b \equiv c \pmod{m}$$

となる。

この系（簡約律）の応用例をひとつあげましょう。

例 2.2.

$$2x \equiv 5 \pmod{123}$$

となる x を求める。

このように未知数を含む合同式に対してその式を満たす未知数を求めることを，**合同式を解く**と言います。合同式を解くことは，合同の理論での重要な問題ですが，上のような問題は簡単に解くことができます。

解. 123 が奇数であることに注意すると，

$$2x \equiv 5 \equiv 5 + 123 = 128 = 2 \cdot 64 \pmod{123}$$

より，簡約律を用いて，$x \equiv 64 \pmod{123}$ を得る。 □

一般に，奇数 m に対しての

$$2x \equiv c \pmod{m}$$

となる x は同様にして，簡約律を使える形に変形することで，簡単に求めることができます。

2.2 m を法とする逆元

合同式で割り算を考える場合，割り算ではなく，「逆元[*10]を掛ける」と考えると状況が分かり易くなります。合同関係でも掛け算は常に可能でしたから，「割り算ができる $\Longleftrightarrow$ 逆元が存在する」と解釈することができます。

普通の数での逆数は掛けて 1 になる数として特徴付けができましたが，m を法とする逆元も掛けて 1 $\pmod{m}$ となる数として特徴付けられます。その存在については次が成立します。

命題 2.2. $\gcd(a, m) = 1$ とする。このとき，

$$ax \equiv 1 \pmod{m} \tag{$*$}$$

は m を法として 1 個の解を持つ。

証明.

（存在性） $A = \{0, 1, 2, \ldots, m-1\}$ を最小非負剰余代表系とする。各 $i = 0, 1, 2, \ldots, m-1$ に対して，ai の m を法とする最小非負剰余を，r_i とする。即ち，

$$ai \equiv r_i \pmod{m};\ \ r_i \in A$$

とする。

このとき，$i, j = 0, 1, 2, \ldots, m-1$ に対して，$i \neq j$ ならば，$r_i \neq r_j$ である。実際，$r_i = r_j$ ならば，

$$ai \equiv r_i = r_j \equiv aj \pmod{m}$$

である。$\gcd(a, m) = 1$ だから，簡約律より，

$$i \equiv j \pmod{m}$$

となる。従って，整数 k に対して，$i = j + km$ と表される。ここで，$0 \leqq i, j \leqq m-1$ だから，$k = 0$ となり，$i = j$ となる。以上から，$i, j = 0, 1, 2, \ldots, m-1$ に対して，$i \neq j$ ならば，$r_i \neq r_j$ が示された。

従って，$r_0, r_1, r_2, \ldots, r_{m-1}$ はすべて異なる。ここで，$r_i \in A$ で A の元の個数は $m-1$ だから，

$$\{r_0, r_1, r_2, \ldots, r_{m-1}\} = A = \{0, 1, 2, \ldots, m-1\}$$

[*10] 普通の数では逆数と言う用語を使いますが，合同式では逆元と言う用語を使います。

である。従って特に，$1 = r_x$ となる 整数 x $(0 \leq x \leq m-1)$ が存在する。このとき，

$$ax \equiv r_x = 1 \pmod{m}$$

である。即ち，$(*)$ は解 x を持つ[*11]。

（一意性） x_1, x_2 を $(*)$ の解とする。即ち，

$$ax_1 \equiv ax_2 \equiv 1 \pmod{m}$$

とする。このとき，$x_1 \equiv x_2 \pmod{m}$ を示す。$ax_2 \equiv 1 \pmod{m}$ の両辺に x_1 を乗ずると

$$ax_2x_1 \equiv x_1 \pmod{m}$$

となる。ここで，$ax_1 \equiv 1 \pmod{m}$ より，上式の左辺は

$$ax_2x_1 = ax_1x_2 \equiv 1 \cdot x_2 \equiv x_2 \pmod{m}$$

である。故に，

$$x_1 \equiv x_2 \pmod{m}$$

である。 □

m を法とする逆元は次のように定義されます。

m を法とする逆元

合同式

$$ax \equiv 1 \pmod{m} \qquad (*)$$

の解 x を **m を法とする a の逆元**と言う。

上の命題から，$\gcd(a, m) = 1$ のとき，m を法とする a の逆元が存在することが得られます。実は，この逆も成立します。即ち，a の逆元が存在すれば，$\gcd(a, m) = 1$ となります。実際，a の逆元が存在すれば，ある整数 k に対して，$ax = 1 + km$ と表されます。従って，

$$ax - km = 1$$

と表されます。ここで，$\gcd(a, m) = c > 0$ とすると，c は上式の左辺を割り切り，$c \mid 1$ となります。従って，$c = 1$ が得られます。以上から，

$$m \text{ を法とする } a \text{ の逆元が存在する} \iff \gcd(a, m) = 1$$

となります。

[*11] この証明では，解の存在は示されましたが，その解を「どのようにして求めることができるのか」は示されていません。このような証明を非構成的存在証明と言います。これに対して，「解を具体的に与える方法を示して，存在を示す」証明法を構成的存在証明と言います。拡張ユークリッドの互除法を用いると構成的存在証明が可能です。それについては，「拡張ユークリッドの互除法」の稿で説明します。

$\gcd(a,m)=1$ の場合，m を法とする a の逆元を求めることを考えてみましょう。a の絶対値が小さい場合，以下のような試行錯誤によって求めることができます。

例 2.3.

$$15x \equiv 1 \pmod{101}$$

を解く。

解. まず，

$$15x = 3\cdot 5x \equiv 1 \equiv 1+101 = 102 = 3\cdot 34 \mod 101$$

だから，簡約律より，

$$5x \equiv 34 \pmod{101}$$

を得る。更に，

$$5x \equiv 34 \equiv 34+101 = 135 = 5\cdot 27 \pmod{101}$$

だから，簡約律より，

$$x \equiv 27 \pmod{101}$$

を得る。 □

今の場合，$a = 15 = 3\cdot 5$ で，$a=3$ と $a=5$ の場合に帰着されました。そしてそのことから，a が小さい場合として，簡単な手計算で結果を求めることができました。しかし，次のような場合，この方法では解くことは困難です。

例 2.4.

$$1234567890337x \equiv 1 \pmod{1234567891969}$$

を解く。

この問題は，次の問題を解けば良いことが分かります。

$$1234567890337\cdot x = 1 + 1234567891969\cdot k$$

となる整数 x,k の組を求める。更に，この問題は，一般的に，整数 a,b,c に対して

$$ax+by=c$$

となる整数 x,y の組を求める問題に拡張されます。この形の方程式は**一次不定方程式**と言われ，古くからこの方程式の解の存在の条件や，その解を具体的に求めることが研究されてきました。それらの研究の中で，その解は，拡張ユークリッドの互除法と言われる方法を用いて，求めることができることが示されました。

拡張ユークリッドの互除法の詳細や上記合同式の解法は，別稿で説明することとして，ここでは，一組の解を求める具体的な解法について例で説明します。

比較的小さな数の例で説明しましょう。

例 2.5.

$$13x \equiv 1 \pmod{17}$$

を解く。

これは，次の不定方程式の一組の解を求めることから，解くことができます。

例 2.6.

$$13x + 17y = 1$$

の一組の解を求める。

この不定方程式の一組の解は，13 と 17 の最大公約数を求めるユークリッドの計算過程を逆にたどることで求めることができます。ユークリッドの互除法[*12]の過程は次のようになります。

$$\begin{aligned} 17 &= 1 \cdot 13 + 4 && (1)\\ 13 &= 3 \cdot 4 + 1 && (2)\\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

上式 (1)，(2) を剰余項を残して移項すると，

$$\begin{aligned} 17 - 1 \cdot 13 &= 4 && (1')\\ 13 - 3 \cdot 4 &= 1 && (2') \end{aligned}$$

となります。ここで，(1′) を (2′) に代入すると，

$$1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 13) = 4 \cdot 13 - 3 \cdot 17$$

より，

$$13 \cdot 4 + 17 \cdot (-3) = 1 \qquad (*)$$

を得ます。即ち，$x = 4$，$y = -3$ が例 2.6 の一組の解を与えます。(∗) の両辺を 17 を法としてみると，

$$13 \cdot 4 \equiv 1 \pmod{17}$$

が得られます。従って，$x = 4$ は例 2.5 の一つの解を与え，解が (mod 17) で一意に存在することから，

$$x \equiv 4 \pmod{17}$$

が解であることが分かりました。

これと同様に，先ほどの問題を解いてみましょう。

例 2.4 (再掲)**.**

$$1234567890337x \equiv 1 \pmod{1234567891969}$$

を解く。

[*12] ユークリッドの互除法については別稿を参照してください。

例 2.4 の解法. 1234567891969 と 1234567890337 にユークリッドの互除法を適用すると，

$$\begin{aligned} 1234567891969 &= 1 \cdot 1234567890337 + 1632 && (1)\\ 1234567890337 &= 756475423 \cdot 1632 + 1 && (2)\\ 1632 &= 1632 \cdot 1 + 0 \end{aligned}$$

が得られる。これから

$$\begin{aligned} 1234567891969 - 1 \cdot 1234567890337 &= 1632 && (1')\\ 1234567890337 - 756475423 \cdot 1632 &= 1 && (2') \end{aligned}$$

が得られる。(1′) を (2′) に代入すると，

$$\begin{aligned} 1 &= 1234567890337 - 756475423 \cdot 1632\\ &= 1234567890337 - 756475423 \cdot (1234567891969 - 1 \cdot 1234567890337)\\ &= 756475424 \cdot 1234567890337 - 756475423 \cdot 1234567891969 \end{aligned}$$

より，

$$1234567890337 \cdot 756475424 + 1234567891969 \cdot (-756475423) = 1$$

を得る。これを $\pmod{1234567891969}$ で考えて，

$$1234567890337 \cdot 756475424 \equiv 1 \pmod{1234567891969}$$

を得る。即ち，

$$x \equiv 756475424 \pmod{1234567891969}$$

である。 □

この計算は，例 2.6 に比べると多少複雑な計算になりますが，多少頑張れば，また電卓があれば簡単に計算，確認できる内容です。実はこの形の不定方程式はどのようなものでも，この方法によって解くことが可能です。また，適切にプログラムを組めば，どのような大きな数で与えられるものであっても，計算機を用いて高速に解くことができます。

2.3 一次合同式

前々項で，$2x \equiv c \pmod{m}$ の形の合同式の解法を考えました。ここではそれを少し一般化して，

$$ax \equiv b \pmod{m} \qquad (*)$$

の形の合同式（一次合同式）について考えましょう。

$(*)$ を満たす x を $(*)$ の解と言いますが，解は合同式として与えられることが分かります。即ち，次が成立します。

命題 2.3. 一次合同式 $(*)$ の解は m を法として存在する。即ち，次が成立する。

- x_0 が $(*)$ の解ならば，$x_0 \equiv x_1 \pmod{m}$ となる x_1 は $(*)$ の解になる。

証明. 実際，$ax_0 \equiv b \pmod{m}$ で，$x_0 \equiv x_1 \pmod{m}$ ならば，$ax_1 \equiv ax_0 \equiv b \pmod{m}$ となり，x_1 も解になります。 □

この命題から，合同式の解は m を法として表す，即ち，

$$x \pmod{m}$$

の形または，その代表で表すことにします。また，**解の個数とは合同でない解の個数**，または同じことですが，**異なる代表の個数**のこととします。

合同式の場合，解がある場合も無い場合も，またある場合でも，1 個とは限らず，複数の場合もあります。

例 2.7 (解が 1 個ある例)**.**

$$3x \equiv 4 \pmod{13}$$

の解は，$x \equiv 10 \pmod{13}$ である[*13]。

解.

$$3x \equiv 4 \equiv 4 + 13 = 17 \equiv 17 + 13 = 30 = 3 \cdot 10 \pmod{13}$$

だから，簡約律より，$x \equiv 10 \pmod{13}$ である[*14]。 □

例 2.8 (解が複数ある例)**.**

$$3x \equiv 6 \pmod{12}$$

の解は，$x \equiv 2, 6, 10 \pmod{12}$ である。

解. $3x \equiv 6 \equiv 3 \cdot 2 \pmod{12}$ に命題 2.1 を適用して，

$$x \equiv 2 \pmod{4}$$

を得る。従って，解の全体は，$x = 2 \pm 4i$ の形の整数である。これは，

$$x = 2 \pm 12i,\ \ x = 2 + 4 \pm 12j = 6 \pm 12j,\ x = 2 + 2 \cdot 4 \pm 12k = 10 \pm 12k$$

の形の整数であり，

$$x \equiv 2, 6, 10 \pmod{12}$$

である。 □

例 2.9 (解が無い例)**.**

$$3x \equiv 1 \pmod{12}$$

の解は存在しない。

解. 実際，

$$3x_0 = 1 + 12k$$

となる整数 x_0, k が存在したとすると，

$$3x_0 - 12k = 1$$

となる。しかし，この左辺は 3 で割り切れ，右辺は 3 で割り切れず，矛盾である。 □

[*13] 代表を使って表すときは，$x = 10$ が解であると言います。

[*14] 厳密には，「$x \equiv 10 \pmod{13}$ が実際に解になる」ことの確認をする必要がありますが，簡約律の逆操作は常に可能ですから，自明なこととして特に説明を加えないこととします。

一次合同式の解の存在については，次が成立します。

定理 2.1. 一次合同式

$$ax \equiv b \pmod{m} \tag{$*$}$$

が解 x を持つための必要十分条件は a と m の最大公約数 $\gcd(a,m)$ が，b を割り切ること，即ち

$$\gcd(a,m) \mid b$$

である。

更に解が存在するとき，解は m を法として，$\gcd(a,m)$ 個存在する。

証明.

（必要性） x を $ax \equiv b \pmod{m}$ の解とする。このとき， 整数 k に対して $ax = b + km$ と表される。km を移項すると，$ax - km = b$ と表される。ここで，$\gcd(a,m)$ は左辺を割り切り，従って，右辺 b も割り切る。

（十分性） $\gcd(a,m) \mid b$ とする。$\gcd(a,m) = c$ と置き，$a = ca_0$，$m = cm_0$ とする。また，$c \mid b$ より，$b = cb_0$ と表される。このとき，命題 2.1 より，$(*)$ は

$$a_0 x \equiv b_0 \pmod{m_0} \tag{$*'$}$$

と変形される。逆に命題 1.6 を使うと $(*')$ から $(*)$ が得られる。即ち，合同式 $(*')$ と合同式 $(*)$ の解の存在性は同値である。

ここで，$\gcd(a_0, m_0) = 1$ だから，命題 2.2 より，

$$a_0 x \equiv 1 \pmod{m_0} \tag{$*''$}$$

は， $\pmod{m_0}$ を法としてただ一つの解 x_0 を持つ。このとき，

$$a_0(b_0 x_0) \equiv (a_0 x_0) b_0 \equiv 1 \cdot b_0 = b_0 \pmod{m_0}$$

より，$x = b_0 x_0$ は $(*')$ の解，従って，$(*)$ の解になる。

（解の個数） $(*)$ の解が存在したとする。$(*')$ の解を x_0, x_1 とする。このとき，

$$a_0 x_1 \equiv b_0 \equiv a_0 x_0 \pmod{m_0}$$

より，簡約律を用いて，

$$x_1 \equiv x_0 \pmod{m_0}$$

を得る。即ち，$(*')$ の解は m_0 を法として唯一つである。そこで，$(*')$ の一つの解を x_0 とすると，

$$x_0,\ x_0 + m_0,\ x_0 + 2m_0,\ \ldots,\ x_0 + (c-1)m_0 \tag{$**$}$$

は， $\pmod{m}$ で相異なる c 個 $(*)$ の解である。逆に，x を $(*)$ の解とすると，x は $(*')$ の解でもあるから，

$$x \equiv x_0 \pmod{m_0}$$

である。従って，$x = x_0 + km_0$ と表される。ここで，k の c を法とする最小非負剰余を i とすると，

$$k = i + jc,\ 0 \leqq i \leqq c-1$$

であり，

$$x = x_0 + im_0 + ijcm_0 \equiv x_0 + im_0 \pmod{m}$$

となる。従って，x は m を法として，(∗∗) のどれかと合同である。即ち，(∗) は m を法として c 個の解を持つ。 □

前にあげた例で解の存在について確認してみましょう。

例 2.10 (再掲)**.**

(1) $3x \equiv 4 \pmod{13}$
gcd(3, 13) = 1 より，解は 13 を法として唯一つ存在する。

(2) $3x \equiv 6 \pmod{12}$
gcd(3, 12) = 3 | 6 より，解は 12 を法として 3 個存在する。

(3) $3x \equiv 1 \pmod{12}$
gcd(3, 12) = 3 ∤ 1 より，解は存在しない。

まず，$ax \equiv b \pmod{m}$ が簡約律を順次適用して解ける例をあげます。a が比較的小さな素数の積になる場合適用可能です。

例 2.11.

$$60x \equiv 1 \pmod{101}$$

を解く。

解. gcd(60, 101) = 1 より解は 101 を法として 1 個ある。

$$60x = 2 \cdot 30x \equiv 1 \equiv 1 + 101 = 102 = 2 \cdot 51 \pmod{101}$$

より，簡約律を使って，

$$30x \equiv 51 \pmod{101}$$

を得る。更に

$$30x = 2 \cdot 15x \equiv 51 \equiv 51 + 101 = 152 = 2 \cdot 76 \pmod{101}$$

より，簡約律を使って，

$$15x \equiv 76 \pmod{101}$$

を得る。更に

$$15x = 3 \cdot 5x \equiv 76 \equiv 76 + 101 = 177 = 3 \cdot 59 \pmod{101}$$

より，簡約律を使って，

$$5x \equiv 59 \pmod{101}$$

を得る。更に

$$5x \equiv 59 \equiv 59 + 101 = 160 = 5 \cdot 32 \pmod{101}$$

より，簡約律を使って，

$$x \equiv 32 \pmod{101}$$

を得る。 □

最後に拡張ユークリッドの互除法を用いる例をあげましょう。

例 2.12.

$$123x \equiv 456 \pmod{789} \tag{$*$}$$

を解く。

解. $\gcd(123, 789) = 3 \mid 456$ より解は 789 を法として 3 個ある。両辺を 3 で割ると，

$$41x \equiv 152 \pmod{263} \tag{$*'$}$$

を得る。41 と 263 に対してユークリッドの互除法を適用すると

$$\begin{aligned} 263 &= 6 \cdot 41 + 17 && (1)\\ 41 &= 2 \cdot 17 + 7 && (2)\\ 17 &= 2 \cdot 7 + 3 && (3)\\ 7 &= 2 \cdot 3 + 1 && (4) \end{aligned}$$

を得る。それぞれ右辺の剰余項を残して移項すると，

$$\begin{aligned} 263 - 6 \cdot 41 &= 17 && (1')\\ 41 - 2 \cdot 17 &= 7 && (2')\\ 17 - 2 \cdot 7 &= 3 && (3')\\ 7 - 2 \cdot 3 &= 1 && (4') \end{aligned}$$

を得る。(4′) 式に，(3′), (2′), (1′) を順次代入すると，

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 && = 7 - 2(17 - 2 \cdot 7)\\ &= 5 \cdot 7 - 2 \cdot 17 && = 5 \cdot (41 - 2 \cdot 17) - 2 \cdot 17\\ &= 5 \cdot 41 - 12 \cdot 17 && = 5 \cdot 41 - 12 \cdot (263 - 6 \cdot 41)\\ &= 77 \cdot 41 - 12 \cdot 263 \end{aligned}$$

となる。最後の式を 253 を法としてみると，

$$41 \cdot 77 \equiv 1 \pmod{263}$$

を得る。従って，両辺に 152 を掛けると

$$41 \cdot (77 \cdot 152) \equiv 41 \cdot 132 \equiv 152 \pmod{263}$$

を得，(∗′) の一つの解として，$x = 132$ を得る。故に，789 を法とした (∗) の 3 個の解は，

$$x \equiv 132,\ 132 + 263 = 395,\ 132 + 2 \cdot 263 = 658 \pmod{789}$$

である。 □

■最後に

ここで説明した，整数の合同の理論はまだまだほんの入り口です。
コンピュータと関係の深い部分を中心に更に項を改めて追加します。