

「アマリの効用」

1 ユークリッドの互除法

1.1 アマリから GCD を見つける方法

自然数 a, b に対して、その最大公約数を $\text{GCD}(a, b)$ で表すのでした。みなさん、 GCD を求めなさいと言われたらどうしますか？おそらく、 a, b をそれぞれ素因数分解して求めるでしょう。しかし、もっと良い方法があります。基本原理は次の通りです。

命題 1. m と n を自然数とし、 m を n で割ったアマリを r とする。このとき、

$$\text{GCD}(m, n) = \text{GCD}(n, r)$$

が成り立つ。

証明. m と n の公約数は n と r の公約数であり、逆に n と r の公約数は m と n の公約数であることを示せばよいことに注意しましょう。大切なのは、 m を n でわったときの商を q とすると $m = nq + r$ が成り立つことです。すると、 $r = m - nq$ により、 m と n をわりきる自然数は、 r もわりきります。だから、 m と n の公約数は n と r の公約数です。逆に、 n と r をわりきれば、 $m = nq + r$ より m もわりきります。よって n と r の公約数は m と n の公約数になります。□

注意 2. もし、 $m < n$ ならば、 m を n でわったときの商は 0 でアマリが m ですから、この命題は当たり前の事しか言っていない。だから、以下でこの命題を使うときは、 m と n を取り替えて、 $m \geq n$ としておきます。

この命題を繰り返し使えば、 $\text{GCD}(m, n)$ は (m を n でわるとして) は n とアマリ r の GCD となり、命題を今度は n とアマリ r に適用すると、 $\text{GCD}(n, r)$ は r と「 n を r でわったアマリ」の GCD となり … となって、最終的に $\text{GCD}(m, n)$ が求まってしまいます。この方法をユークリッドの互除法（あるいは単に互除法）と呼びます。

例 3. (1) $\text{GCD}(20170715, 10085357)$ は, $20170715 \div 10085357 = 2$ アマリ 1 なので, $\text{GCD}(10085357, 1) = 1$ に等しい. つまり, 20170715 と 10085357 は互いに素です. 20170715 と 10085357 を因数分解して公約数を $\dots$ と求めていたら大変なことになりますね.

(2) $\text{GCD}(12345, 67890)$ は, $67890 \div 12345 = 5$ アマリ 6165 より, $\text{GCD}(12345, 6165)$ に等しい. さらに, $12345 \div 6165 = 2$ アマリ 15 より, $\text{GCD}(6165, 15)$ に等しい. ここで $6165 \div 15 = 411$ (15 でわりきれ) より, $\text{GCD}(6165, 15) = 15$ と分かります. というわけで, $\text{GCD}(12345, 67890) = 15$ と分かりました.

注意 4 (互除法がうまくいくワケ). m と n を自然数とし, $\text{GCD}(m, n)$ を求めたいとしましょう. 注意 2 でいったように, 必要ならば, m と n をいれかえて $m \geq n$ とします. m を n で割ったアマリを r としましょう. すると, アマリの性質により, $r < n$ です. これが大切です. 互除法の最初のステップでは, m を n でわりました. 次のステップでは, n を r でわります. 大切なのは, **最初のステップのわる数 n よりも次のステップのわる数 r の方が小さい**ということです. こうして, 互除法のステップが進んでいくと, わる数は確実に減っていきますから, そのステップの総数は, n を超えません. つまり有限回で終わるのです.

1.2 互除法で不定一次方程式を解く

さすがに, $\text{GCD}(65, 25)$ を求めるときは, $65 = 5 \times 13$, $25 = 5 \times 5$ と因数分解して, $\text{GCD}(65, 25) = 5$ と求める方がよいと思うでしょう. 互除法だと, $65 \div 25 = 2$ アマリ 15 より, $\text{GCD}(65, 25) = \text{GCD}(25, 15)$, $25 \div 15 = 1$ アマリ 10 より, $\text{GCD}(25, 15) = \text{GCD}(15, 10)$, $15 \div 10 = 1$ アマリ 5 より, $\text{GCD}(15, 10) = \text{GCD}(10, 5)$, ここで, 10 は 5 でわりきれるので, 結局, $\text{GCD}(65, 25) = 5$ と分かります. マドロッコシイですね. しかし, **互除法のこの計算は無駄ではない**のです. 次の問題を考えます.

$$65x + 25y = 5 \text{ となる整数 } x, y \text{ をすべて求めよ.}^1$$

実は, これが無限個の解を持つことが分かるのですが, そのうちの一つを求めるのに互除法の計算結果が役立つのです. ちなみに, この方程式は無限個の解を持つことから, **不定一次方程式**と呼ばれています. 互除法の計算結果を次のように書いておきます.

$$(a) 15 = 65 - 25 \times 2 \quad (b) 10 = 25 - 15 \quad (c) 5 = 15 - 10$$

¹両辺が 5 で割りきれることを見えているので, まず 5 でわっておいて, $13x + 5y = 1$ を解いてもよいです. この場合は 13 と 5 で互除法を行えばよいのです.

つまり、すべてのステップを「**アマリ** = ...」という形に書くわけです。これからおこなうのは、これらの右式から、65, 25 がかかっているもの以外を次々消去していくことです。具体的には次の通りになります。まず、第 (a) 式を第 (b) 式の 15 に代入すると、 $10 = 25 - (65 - 25 \times 2)$ となります（第 (b) 式の右辺から 15 が消えました）。整理すると、

$$(b') \quad 10 = -65 + 25 \times 3$$

となります。第 (a) 式と第 (b') 式を第 (c) 式の 15 と 10 に代入すると、 $5 = (65 - 25 \times 2) - (-65 + 25 \times 3)$ となりますが、これを整理すると、 $5 = 65 \times 2 - 25 \times 5$ となります。こうして、 $65x + 25y = 5$ の解の一つとして、 $x = 2, y = -5$ が得られました！

さらに、この一つの解から、他のすべての解を求めることができます。以下では互除法は使いません。 $65x + 25y = 5$ と $65 \times 2 - 25 \times 5 = 5$ の辺々を引くと、 $65(x - 2) + 25(y + 5) = 0$ を得ます。65 と 25 の最大公約数の 5 で割っておくと、 $13(x - 2) + 5(y + 5) = 0$ となります。移項して

$$13(x - 2) = -5(y + 5) \quad (1)$$

と書くと、13 と 5 が互いに素だから、 $x - 2$ は 5 の倍数でなくてはなりません。従って $x - 2 = 5k$ (k は整数) と書けます。これを第 (1) 式に代入すると、 $13k = -(y + 5)$ となって、 $x = 5k + 2, y = -13k - 5$ (k は整数) と表せます。これがすべての解です。念のため、 $65x + 25y = 5$ に代入してみると、 $65(5k + 2) + 25(-13k - 5) = 5$ となって、確かに解です。

問題 5. $17x + 5y = 1$ となる整数 x, y をすべて求めてみましょう。

2 整数の合同

ユークリッドの互除法で、アマリの効用を見ました。その効用をもっと実感するため、「アマリ以外は目をツムル」、「アマリが同じなら同じと思う」という考え方を導入します。先に進む前に、あとあと便利なので、負の数のアマリというのも定めておきましょう。

定義 6 (負の数のアマリ). m, a を自然数とします。負の整数 $-a$ を m でわったアマリとは次のように決まる 0 から $m - 1$ の自然数です。 a を m でわった商を q' 、アマリを r' とすると、 $a = mq' + r'$ が成り立ちます。よって、 $-a = -mq' - r'$ となります。まず、 $r' = 0$ のときは、 $-a$ を m でわった商を $-q'$ 、アマリを 0 と定めます。 $1 \leq r' \leq m - 1$ のときは、

$$-a = m(-q' - 1) + (m - r')$$

と書いておいて、 $-a$ を m でわった商を $-q' - 1$ 、アマリを $m - r'$ と定めます。 $1 \leq m - r' \leq m - 1$ に注意しましょう。

こうしておく、 m を自然数とすると、任意の整数 a に対して、 a を m でわった商とアマリが定まり、商を q 、アマリを r で表せば、 $0 \leq r \leq m - 1$ であり、

$$a = mq + r \quad (2)$$

が成り立ちます。

2.1 合同とは？

定義 7 (合同). m を 2 以上の整数とします。自然数 a と b が m を法とし合同であるとは、 a と b を m でわったアマリが同じであると定義します。このとき

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

と書きます。便利な言い換えは、

$$a \equiv b \pmod{m} \Leftrightarrow a - b \text{ が } m \text{ で割り切れる}$$

です。これは、(2) 式に注意すれば分かります。以後はもっぱら、この言い換えの方を使います。

整数 a に対して、(2) 式より、 $a \equiv r \pmod{m}$ が成り立ちますから、どんな整数も 0 から $m - 1$ までの自然数と合同です。

この講義では、

$$\text{アマリの世界} = \{0, 1, 2, 3, \dots, m - 1\}$$

ということにします。

2.2 たし算・かけ算との相性

$a_1 \equiv a_2 \pmod{m}$, $b_1 \equiv b_2 \pmod{m}$ であるとしましょう。これは、 $a_1 - a_2$ も $b_1 - b_2$ も m でわりきれんということでした。ということは、

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$$

も

$$(a_1 - b_1) - (a_2 - b_2) = (a_1 - a_2) - (b_1 - b_2)$$

も m でわりきれます。ですから、

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$$

が成り立ちます。すると、自然数をたしたりひいたりした結果を合同で見るのならば、たしたりひいたりする自然数を初めから、合同な別の（絶対値の小さい）整数で置き換えておいて計算できることになります。合同でありさえすれば、どう都合よく変えても構いませんが、アマリの世界の数で置き換えることが多いです。

かけ算についても同じことが成り立ちますが、証明には少し工夫が要ります。

$$a_1b_1 - a_2b_2 = a_1b_1 + (-a_2b_1 + a_2b_1) - a_2b_2 = (a_1 - a_2)b_1 + a_2(b_1 - b_2)$$

と変形するのです。これによって、 $a_1b_1 - a_2b_2$ が m でわりきれることが分かって、

$$a_1b_1 \equiv a_2b_2 \pmod{m}$$

が成り立ちます。

例 8. $10 \times 9 \times \cdots \times 2 \times 1$ のことを $10!$ と書きます。 $10! \pmod{11}$ を計算してみましょう。ここで、 $6, 7, 8, 9, 10$ を、 $10 \equiv -1 \pmod{11}$, $9 \equiv -2 \pmod{11}$, $\dots$, $6 \equiv -5 \pmod{11}$ と見ておきます。このように、できるだけ絶対値の小さい数の計算ですませられるのが、負の数の効用です。以下、 $\pmod{11}$ を何度も書くのは煩わしいので省略します。

$$\begin{aligned} 10! &\equiv 1 \times 2 \times \cdots \times 10 \\ &\equiv 1 \times (-1) \times 2 \times (-2) \times 3 \times (-3) \times 4 \times (-4) \times 5 \times (-5) \\ &\equiv (-1)^5 \times 1 \times 4 \times 9 \times 16 \times 25 \equiv (-1) \times 1 \times 4 \times (-2) \times 5 \times 3 \\ &\equiv (-3) \times 4 \equiv -1 \end{aligned}$$

例 9. 2784963 を 9 でわったアマリを合同を使って求めてみましょう。ポイントは $10 \equiv 1 \pmod{9}$ です（以下 $\pmod{9}$ を省略します）。よって、 $10^n \equiv 1^n \equiv 1$ です。これから、

$$2784963 \equiv 2 + 7 + 8 + 4 + 9 + 6 + 3 \equiv 9 + 12 + 9 + 9 \equiv 3$$

となって、アマリが 3 と分かります。

問題 10. 自然数 a が 9 でわりきれるのは、 a のすべての位の数をたしたら 9 でわりきれるときであることを、合同を使って示してみましょう。

問題 11. 6392837463 を 11 でわったアマリを合同を使って求めてみましょう。

問題 12. 自然数 a が 11 でわりきれるのは、 a のすべての位の数をどうしたときと言えるでしょうか？合同を使って示してみましょう。

問題 13. a を奇数とするとき、 a^2 を 8 でわったアマリがいつでも 1 になることを、合同を使って示してみましょう。

2.3 一次合同方程式を解く

$65x \equiv 5 \pmod{25}$ となる整数 x をすべて求めよ，という形の方程式を一次合同方程式と呼びます．この方程式は $65x - 5 \equiv 0 \pmod{25}$ と変形すると， $65x - 5$ が 25 でわりきれするような整数 x をすべて求めよ，ということになります．さらにいいかえれば， $65x - 5 = 25y$ となる整数 y が存在するような x をすべて求めよ，ということになりますから，1.2 節で考えていた不定一次方程式になります．よって，1.2 節で見たように，互除法で解くことができます．

問題 14. $17x \equiv 1 \pmod{5}$ となる整数 x をすべて求めてみましょう．

2.4 べき計算（1 乗，2 乗，3 乗，4 乗 …）

自然数 a に対して，そのべき乗 $a, a^2, a^3 \dots$ を計算していくと，それは爆発的に大きくなっていきます．例えば，

$$3^{113} = 821678234986022501332043817791314604358242170799200323$$

です．しかし，こんな大きな数でも，自然数 m を法とした合同の世界で見るとずっと小さな自然数と同じ（合同）になります．そのアマリは 0 から $m - 1$ までの整数なのですから．

ところで，そもそも，なぜ，べき乗を合同の世界で見る必要があるのか疑問に思うところでしょうが，それは，情報の暗号化において重要な役割を果たすからです．それについては，来週のお楽しみということで，ここでは，いかにして自然数 m を法としたべき乗のアマリを求めるのかについて学んでおきましょう．

まずはべきの肩に乗っている数 113 を 2 進法で表します．

2 進法とは，任意の 0 以上の整数を，0 か 1 に等しい自然数 $b_0, b_1, b_2, \dots, b_l$ を用いて，

$$b_l \times 2^l + b_{l-1} \times 2^{l-1} + \dots + b_1 \times 2 + b_0$$

というかたちに表す方法です．この結果を $b_l b_{l-1} \dots b_1 b_0$ と略記します．2 進法であることを強調するため， $(b_l b_{l-1} \dots b_1 b_0)_2$ と書くこともあります． $b_l, b_{l-1}, \dots, b_1, b_0$ を求める原理は 10 進法のときと同じです．2 進法表示したい自然数を 2 の何乗でわれるかを考え，それが l であつたら， 2^l でわった時の商が $b_l = 1$ です．次に元の数から $b_l \times 2^l$ を引いて，残りの数に同じことを考えて $\dots$ ということを繰り返すと， $b_l, b_{l-1}, \dots, b_1, b_0$ が求まっていくわけです．

113 で実行してみると，113 は $2^6 = 64$ でわれて $113 - 2^6 \times 1 = 49$ です．49 は $2^5 = 32$ でわれて $49 - 2^5 \times 1 = 17$ です．17 は $2^4 = 16$ でわれて $17 - 2^4 \times 1 = 1$ です．1 は 2^0

でしかられません．というわけで結果を書き下すと，

$$113 = 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^0 = (1110001)_2$$

となります．

すると，

$$3^{113} = 3^{1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^0} = 3^{2^6} \times 3^{2^5} \times 3^{2^4} \times 3$$

となります．ここで右側の等号は，指数法則 $a^{x+y} = a^x a^y$ によっています．こうして，べき乗の計算は，いろいろな k についての 3^{2^k} の計算に帰着されました．これが2進法の効用です．

さらに，指数法則 $a^{xy} = (a^x)^y$ を繰り返し使うと，例えば， 3^{2^4} は次のように計算できます：

$$3^{2^4} = (3^2)^{2^3} = ((3^2)^2)^2 = (((3^2)^2)^2)^2$$

ここで，自然数 m を法とする合同で考えていたことを思い出しましょう．ポイントは 3^{2^4} を計算するとき，2乗することにより，アマリの世界の数で置き換えてゆくと大きなべきを計算しなくてすむということです．

例えば， $m = 7$ としてみましょう． $\text{mod } 7$ を省略して書くと， $3 \equiv 3, 3^2 \equiv 2$ ，これを元にすれば $(3^2)^2 \equiv 2^2 \equiv 4$ ，これを元にすれば， $((3^2)^2)^2 \equiv 4^2 \equiv 2$ ，これを元にすれば， $((((3^2)^2)^2)^2 \equiv 2^2 \equiv 4$ となって求まります．つまり，常に，アマリの世界の数 $1, \dots, 6$ の2乗を計算することの繰り返しで計算できるのです．

$3^{113} \pmod{7}$ の計算を完成させるには，さらに $3^{2^6}, 3^{2^5}$ のアマリも計算しなくてはなりません．しかし，このとき， 3^{2^4} の計算が利用できることに注意します．実際，

$$3^{2^5} = (3^{2^4})^2 \equiv 4^2 \equiv 2, \quad 3^{2^6} = (3^{2^5})^2 \equiv 2^2 \equiv 4$$

となって簡単に求まります！こうして $3^{113} \equiv 4 \times 2 \times 4 \times 3 \equiv 5$ とアマリの世界の数で表すことができました．

問題 15. $m = 35$ のとき 3^{113} をアマリの世界の数で表してみよう．

参考文献

[シルヴァーマン] ジョセフ・シルヴァーマン著（鈴木治郎訳）『はじめての数論』（丸善出版）