§4 整数論

$a, b \in \mathbb{N} \cup \{0\}$ に対し、最大公約数を $\gcd(a, b)$ で表す。

補題4.1. $\gcd(a, b)$ は次をみたす ($a, b \in \mathbb{N}$)

(1) $\gcd(a-b, b) = \gcd(a, b)$ ($a \geq b$ とする)

(2) $\gcd(a, b) = \gcd(b, a)$

(3) $\gcd(0, b) = b$.

∵ (1) $\gcd(a, b) = m$, $\gcd(a-b, b) = n$ とすると、

$a = mk$, $b = ml$ とできるので、

$a-b = m(k-l)$, $b = ml$. ∴ m は $a-b$ と b の公約数

∴ m は n の約数.

同様に、$a-b = np$, $b = nq$ とすると

$a = n(p+q)$ より n は a と b の公約数

∴ n は m の約数 ∴ $n = m$

(2) は明らか. (3) は 0 の約数が全ての自然数よりわかる.

定理4.2 $a, b \in \mathbb{N}$ に対し，$\gcd(a,b)$ は次のアルゴリズムで求めることができる．

① $x_0 = \max\{a,b\}$, $x_1 = \min\{a,b\}$ とする．

② $n \geq 2$ に対し，$x_n = x_{n-2} \pmod{x_{n-1}}$ とし，

$x_n = 0$ となるまでこれをくり返す．

③ このとき，$\gcd(a,b) = x_{n-1}$ である．

例 $\gcd(456, 234)$ を求める

① $x_0 = 456$, $x_1 = 234$ である

② $x_2 = 456 \pmod{234}$　　　$456 = 234 \times 1 + 222$

$= 222$

$x_3 = 234 \pmod{222}$　　　$234 = 222 \times 1 + 12$

$= 12$

$x_4 = 222 \pmod{12} = 6$　　　$222 = 12 \times 18 + 6$

$x_5 = 12 \pmod 6 = 0$

$\therefore \gcd(456, 234) = 6$ である.

<u>定理の証明</u> $a > b$, $a = kb + r$ とすると.

$\gcd(a, b) = \gcd(a-b, b) = \cdots = \gcd(a-kb, b) = \gcd(b, r)$

をみたす. ∴ ② において.

$x_{n-2} = k x_{n-1} + x_n$ だったので.

$\gcd(x_{n-2}, x_{n-1}) = \gcd(x_{n-1}, x_n)$ である.

また. x_n は単調減少なので. どこかで 0 になる.

今. $x_m = 0$, $x_{m-1} \neq 0$ とすると.

$\gcd(a, b) = \gcd(x_0, x_1) = \gcd(x_{m-1}, \overset{0}{\overset{\shortparallel}{x_m}}) = x_{m-1}$ となる.

<u>定義 6.3</u> $a_{n+1} = a_n + a_{n-1}$, $a_0 = 0$, $a_1 = 1$

をみたす数列をフィボナッチ数列という.

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ⋯ とつづく.

定理6.4 フィボナッチ数列の一般項は

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \quad \text{である.}$$

$a_0 = 0$, $a_1 = 1$ はOK.

$$a_n + a_{n-1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right)$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\underbrace{\left(\frac{1+\sqrt{5}}{2}+1\right)}_{=\left(\frac{1+\sqrt{5}}{2}\right)^2} - \left(\frac{1-\sqrt{5}}{2}\right)\underbrace{\left(\frac{1-\sqrt{5}}{2}+1\right)}_{=\left(\frac{1-\sqrt{5}}{2}\right)^2}\right)$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right) = a_{n+1} \quad \text{となる} \ //$$

補題6.5 $\{x_n\}_{n=0}^{m}$ をユークリッドの互除法ででる数列とすると. $x_n \geq a_{m-n}$ である

$x_m = 0 = a_0$, $x_{m-1} \geq 1 = a_1$ であり.

$$x_n = k_{n+1}\cdot x_{n+1} + x_{n+2} \geq a_{m-n-1} + a_{m-n-2} = a_{m-n}$$

である //

<u>定理6.6</u> S を max{a, b} の桁数とすると、ユークリッドの互除法で、②が行われる回数は、6S以下である

∵ くり返しの回数は m−1回である。また、補題6.5より

$S = x_0$ のケタ数 $\geq a_m$ のケタ数 $=: t$ なので

$6t \geq m-1$ を示せばよい。ここで

$$a_m = \frac{1}{\sqrt{5}}\left(\left(\underset{\substack{\| \\ \frac{3.236}{2}}}{\frac{1+\sqrt{5}}{2}}\right)^m - \left(\underset{\substack{\| \\ \frac{-1.236}{2}}}{\frac{1-\sqrt{5}}{2}}\right)^m\right) > \frac{1}{\sqrt{5}}\left(\frac{3}{2}\right)^m - 0.3 \text{ より}$$

$$t = [\log_{10}(a_m + 0.3)] + 1 > \left[\log_{10}\left(\frac{1}{\sqrt{5}}\left(\frac{3}{2}\right)^m\right)\right] + 1$$

$$= \left[m \cdot \log_{10}\frac{3}{2} - \log_{10}\sqrt{5}\right] + 1$$

$$= \Big[m(\underset{\substack{\fallingdotseq \\ 0.477}}{\log_{10} 3} - \underset{\substack{\fallingdotseq \\ 0.301}}{\log_{10} 2}) - \frac{1}{2}\underset{\substack{\fallingdotseq \\ 0.7}}{\log_{10} 5}\Big] + 1$$

$$> [0.175(m-2)] + 1$$

$$\therefore\ t - 1 > 0.175(m-2)$$

$\therefore\ 6t-6 > m-2.$

$\therefore\ m-1 < 6t-5 < 6t$ となる$/\!/$

<u>合同式</u>. $m \in \mathbb{N},\ a, b \in \mathbb{Z}$ とする.

$a \equiv b \pmod{m} \overset{\text{def}}{\Longleftrightarrow} a-b \in m\mathbb{Z}$ とする.

このとき, a, bは mを法として合同という.

合同は同値関係である

<u>定理 6.7.</u> $m, r \in \mathbb{N},\ a, b, c, a', b' \in \mathbb{Z}$ (以下 mod mは略)

$a \equiv a',\ b \equiv b'$ のとき, 次が成立.

(1) $a+b \equiv a'+b'$ (2) $a-b \equiv a'-b'$

(3) $ab \equiv a' \cdot b'$ (4) $a^r = (a')^r$

(5) mとcが互いに素なら. ($\gcd(m, c) = 1$)

$ac \equiv bc \Rightarrow a \equiv b.$

$a \equiv b \Leftrightarrow$ a.bをmでわったときの余りが等しいに注意.

(1)(2)は省略

(3) $a = km + r$, $a' = k'm + r$
$b = lm + s$, $b' = l'm + s$ $(0 \leq r, s < m)$ とすると.

$ab = m(klm + ks + rl) + rs \equiv rs \equiv a'b'$ となる.

(4) (3)をくり返せばよい.

(5) $ac \equiv rc$, $bc \equiv sc$ より

$0 = ac - bc \equiv c(r-s)$ ∴ $c(r-s)$ は m でわれる

一方, $\gcd(m, c) = 1$ より $r-s$ は m でわりきれる

∴ $r = s$ ∴ $a \equiv b$ である. //

例(1) $5x - 4 \equiv 11 \pmod 9$ をとくと.

$5x \equiv 15$

$x \equiv 5$ となる

(2) $3x-4 \equiv 4 \pmod 9$ をとくと.

$3x \equiv 8$ より 解なし.

(3) $5x-4 \equiv 12 \pmod 9$ をとくと.

$5x \equiv 16 \equiv 25$ より $x \equiv 5$

(4) $14 \equiv 8 \pmod 6$ だが.

$7 \equiv 4 \pmod 6$ は成立しない. わり算は注意.

(5) $10^{3000} \pmod{11}$ は

$10^{3000} = (-1)^{3000} = 1$

(6) $10^{100} \pmod 7$ は,

$10 \equiv 3$. $3^6 = 9^3 \equiv 2^3 = 8 \equiv 1$ より

$10^{100} \equiv 3^{100} = (3^6)^{16} \cdot 3^4 \equiv 3^4 = 81 \equiv 4$. である

定理 6.8. $a, m \in \mathbb{N}$, $b \in \mathbb{Z}$, $(a \not\equiv 0 \bmod m)$ とする.
以下 mod m を略.

次が同値.

(1) $ax \equiv b$ が解をもつ.

(2) $ax + my = b$ が整数解をもつ.

(3) $\gcd(a, m)$ が b の約数.

さらに $\gcd(a, m) = 1$ なら解はただ1つ. (mod m で)

∵ (1) ⇒ (2). x を解とすると.

$ax - b \in m\mathbb{Z}$ ∴ $ax - b = my$ とできる.

(2) ⇒ (1)

$ax - b = -my \in b$ より $ax \equiv b$ をみたす.

(2) ⇒ (3) $c = \gcd(a, m)$ とすると.

$b = ax + my \in c\mathbb{Z}$ ∴ c は b の約数

(3)⇒(2) ユークリッドの互除法を考えると.

$x_0 = \max\{a, m\}$, $x_1 = \min\{a, m\}$,

$x_{n-1} = k_n x_n + x_{n+1}$, $\gcd(a, m) = x_\ell$ $(x_{\ell+1} = 0)$ とできた.

ここで. $x_{n+1} = x_{n-1} - k_n x_n$ より.

$$c = \gcd(a, m) = x_\ell = x_{\ell-2} - k_{\ell-1} x_{\ell-1}$$

$$= x_{\ell-2} - k_{\ell-1}(x_{\ell-3} - k_{\ell-2} x_{\ell-2}) = \cdots$$

$$= p x_0 + q x_1$$ となる

今 $b = rc$ とすれば

$b = rp x_0 + rq x_1$ となる.

x_1, x_2 を解とすると.

$a x_1 \equiv b \equiv a x_2$. もし $\gcd(a, m) = 1$ なら $x_1 \equiv x_2$ となる//.

例(1) $200x \equiv 45 \pmod{41}$ を考えると.

$200 = 41 \times 4 + 36$,

$41 = 36 \times 1 + 5$

$36 = 5 \times 7 + 1$ $\qquad\qquad \therefore \gcd(200, 41) = 1$

$5 = 1 \times 5 + 0$.

ここで $45 \equiv 4$ より $200x \equiv 4$ をとくと.

$4 = 1 \times 4 = 4(36 - 5 \times 7) = 4 \cdot 36 - 28 \cdot 5$

$= 4 \cdot 36 - 28(41 - 36)$

$= 32 \cdot 36 - 28 \cdot 41$

$= 32(200 - 41 \times 4) - 28 \times 41$

$= 32 \times 200 - 156 \times 41$. $\qquad \therefore x = 32$

(2) $10x \equiv 11 \pmod{12}$ は.

$\gcd(10, 12) = 2$ が 11 の約数でないので解なし.

オイラー関数

定義4.9 $n \in \mathbb{N}$ に対し

$$\varphi(n) := |\{m \mid 1 \leq m \leq n,\ \gcd(m,n) = 1\}|$$

をオイラー関数という

例 (1) $\varphi(6)$ を考えると 6と素なのは

1 と 5 だけ　　$\therefore \varphi(6) = 2$

(2) $\varphi(15)$ を考えると 15と素なのは

1, 2, 4, 7, 8, 11, 13, 14　　$\therefore \varphi(15) = 8$

(3) $\varphi(1) = 1$

(4) p が素数なら $\varphi(p) = p-1$

(5) $\varphi(90)$ を考える。$90 = 2 \times 3^2 \times 5$ より

1から90までのなかで.

2の倍：$90\times\frac{1}{2}=45$　　2と3の倍：$90\times\frac{1}{6}=15$

3の倍：$90\times\frac{1}{3}=30$　　2と5の倍：$90\times\frac{1}{10}=9$

5の倍：$90\times\frac{1}{5}=18$　　3と5の倍：$90\times\frac{1}{15}=6$.

2.3.5の倍：$90\times\frac{1}{30}=3$.

$\therefore \varphi(90)=90-(45+30+18)+(15+9+6)-3$

$=90\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=24$.

定理4.10. $n=p_1^{k_1}\cdots p_m^{k_m}$ のとき.

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_m}\right)=n\cdot\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right)$$

$\because$ n以下の数が p_1 と素になる確率は $\left(1-\frac{1}{p_1}\right)$

ここで p_1 と素になることと. p_2 と素になることが独立を示す.

$\because$ A：p_1 と素：$n\left(1-\frac{1}{p_1}\right)$　　B：p_2 と素：$n\left(1-\frac{1}{p_2}\right)$

$A\cap B$：p_1, p_2 と素：$n-\frac{n}{p_1}-\frac{n}{p_2}+\frac{n}{p_1p_2}=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$

$\therefore P(A\mid B)=\frac{P(A\cap B)}{P(B)}=1-\frac{1}{p_1}=P(A)$

$\therefore \varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_m}\right)$ //

補題 4.11　p を素数．$a, b \in \mathbb{Z}$ とすると．

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

$\because$ $(a+b)^p = \sum_{n=0}^{p} {}_pC_n \cdot a^n \cdot b^{p-n}$.

ここで ${}_pC_n = \frac{p!}{n!(p-n)!}$ より．$n \neq 0, p$ なら p でわり切れる．

$\therefore (a+b)^p \equiv a^p + b^p$ //.

定理 4.12 (フェルマーの小定理).

p を素数．$a \in \mathbb{Z}$ とすると．

$a^p \equiv a \pmod{p}$ である．とくに $\gcd(a, p) = 1$ なら．

$a^{p-1} \equiv 1 \pmod{p}$ である

$\because$ $a = 0$ のときは明らか．$a^p \equiv a$ を仮定すると．

$(a+1)^p \equiv a^p + 1^p \equiv a+1$ より $a \geq 0$ については ok

$a<0$ のときを考えるが、pが奇数なら

$$a^p \equiv -(-a)^p \equiv -(-a) \equiv a.$$

$p=2$ なら、

$$a^2 \equiv (-a)^2 \equiv -a \equiv -a+2a \equiv a$$ //.

例. $3^{100} \pmod{13}$ を求めると、

$3^{12} \equiv 1$ より、$3^{100} = (3^{12})^8 \cdot 3^4 \equiv 81 \equiv 3$ となる.

定理4.13. $n \in \mathbb{N}$, $a \in \mathbb{Z}$ に対し.

$\gcd(a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$ が成立

(∵) n以下で、nと互いに素な整数の集合を

$A=\{b_1, b_2, \cdots, b_{\varphi(n)}\}$ とする ここで

$B=\{ab_1, \cdots, ab_{\varphi(n)}\}$ を考えると、mod n で $a=b$ となる.

まず、$\gcd(a,n)=\gcd(b_i,n)=1$ より $\gcd(ab_i,n)=1$.

がわかる また、

$ab_i \equiv ab_j$ なら $b_i \equiv b_j$ より. $i=j$ となる.

$\therefore A = B \pmod{n}$.

$\therefore b_1 \cdots b_{\varphi(n)} \equiv ab_1 \cdots\cdots ab_{\varphi(n)} = a^{\varphi(n)} \cdot b_1 \cdots b_{\varphi(n)}$

$\therefore a^{\varphi(n)} \equiv 1 \pmod{n}$ //.

<u>定理4.14.</u> $n \in \mathbb{N}$, p_i素数. $n = p_1 \cdot p_2 \cdots p_m$ のとき次が成立

(1) $q \equiv 1 \pmod{\underset{(\forall i)}{p_i - 1}} \Rightarrow {}^\forall a \in \mathbb{Z},\ a^q \equiv a \pmod{n}$

(2) $q \equiv 1 \pmod{\varphi(n)} \Rightarrow {}^\forall a \in \mathbb{Z},\ a^q \equiv a \pmod{n}$

∵ (1) $q - 1 = k_i(p_i - 1)$ より

$a^q = a^{k_i(p_i-1)+1} \equiv a \pmod{p_i}$ (∵ フェルマー) となる

ここで $a^q - a$ は p_i $(\forall i)$ でわり切れる

$\therefore a^q - a$ は $p_1 \cdots p_m = n$ でわり切れる

$\therefore a^q \equiv a \pmod{n}$

(2) $q - 1 = k \cdot \varphi(n)$ である

一方，$\varphi(n)=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_m})=(p_1-1)\cdots(p_m-1)$ より

$q-1=k(p_1-1)\cdots(p_m-1)$.

$\therefore\ q\equiv 1 \pmod{p_i-1}$ より (1) の条件をみたす.

$\therefore\ a^q\equiv a \pmod{n}$ である.

<u>例1</u>. $13^{102} \pmod{330}$ を計算する.

$330=2\times3\times5\times11$ より定理の条件をみたす また.

$\varphi(330)=\underset{1}{(2-1)}\underset{2}{(3-1)}\underset{4}{(5-1)}\underset{10}{(11-1)}=80$ である.

ここで $\mathrm{lcm}(1,2,4,10)=20$ より.

$q=20\cdot k+1$ は (1) の条件をみたす

$\therefore\ 13^{102}=13^{101+1}=13^1\cdot13^1=169 \pmod{330}$ となる

なお，フェルマーの定理は使えない.