第1章　合同式

整数を正の整数 n で割った余りは $0, 1, 2, \cdots, n-1$ のうちのどれかであることに注意する．

定義 1.1

n は 2 以上の整数とする．このとき，整数 a, b に対して，a を n で割った余りと b を n で割った余りが等しいとき，a, b は n を法として合同であるといい，

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

と書く．また，このような式を合同式という．

例 1　*1.* $n = 10$ とする．$1567 \equiv 237 \pmod{10}$ である．

2. $n = 9$ とする．$1567 \equiv 1826578 \pmod{9}$ である．

「n を法として合同」という関係は「同値関係」である（数学演習 II でやった）．そして，その代表系として，$\mathbf{Z}_n := \{0, 1, 2, \cdots, n-1\}$ をとるのが標準的である．

定義 1.2

整数 a と正の整数 b が与えられたとき，

$$a = bq + r \quad (0 \leq r < b)$$

をみたす整数 q, r がある（一意的に決まる）．このとき，q を a を b で割ったときの商，r を余りという．

例 2　*1.* $a = 456, b = 11$ とすると，$456 = 11 \times 41 + 5$ つまり，456 を 11 で割ったときの商は 41, 余りは 5 である．

2. $a = -38, b = 7$ とすると，$-38 = 7 \times (-6) + 4$ つまり，-38 を 7 で割ったときの商は -6, 余りは 4 である．

命題 1.3

$a \equiv b \pmod{n} \Longleftrightarrow a - b$ が n で割り切れる．

証明: まず，$\Longleftarrow$ を示す．仮定より，$a - b$ を n で割り切れる．いま，$a =$

$na'+r_1, b=nb'+r_2$ とおくと（$0 \le r_1, r_2 < n$），$a-b=n(a'-b')+(r_1-r_2)$ となるから，r_1-r_2 が n で割り切れる．それが可能なのは，$r_1=r_2$ のときのみ．実際，r_1-r_2 が n で割り切れるなら，整数 t があって $r_1-r_2=nt$ となるが，$0 \le r_1 < n, 0 \le r_2 < n$ より，$0 \le |r_1-r_2| < n$ であるので，$t=0$ でないといけない．すなわち，$r_1=r_2$. ゆえに，$a \equiv b \pmod{n}$ である．

次に，$\Longrightarrow$ を示す．a, b を n で割ったときの余りが等しいとすると，$a=na'+r, b=nb'+r$ とかける．ゆえに，$a-b=n(a'-b')$ なので n で割り切れる．□

命題 1.4

(a) $a \equiv b \pmod{n}, c \equiv d \pmod{n} \Longrightarrow a \pm c \equiv b \pm d \pmod{n}$.

(b) $a \equiv b \pmod{n}, c \equiv d \pmod{n} \Longrightarrow a \cdot c \equiv b \cdot d \pmod{n}$.

証明: (b) だけ示す．(a) は各自証明せよ．$a \equiv b \pmod{n}$ とする．命題 1.2 より，$a-b$ は n で割り切れるので，ある整数 k があって $a-b=nk$ と書ける．同様に，ある整数 ℓ があって $c-d=n\ell$ と書ける．

$ac-bd=ac-bc+bc-bd=(a-b)c+b(c-d)=nkc+bn\ell=n(kc+b\ell)$ なので，$ac-bd$ は n で割り切れる．ゆえに，$a \cdot c \equiv b \cdot d \pmod{n}$. □

例 3

- $3143 \times 68932 \pmod{10}$ の計算は，$3143 \equiv 3 \pmod{10}, 68932 \equiv 2 \pmod{10}$ なので，$3143 \times 68932 \equiv 2 \cdot 3 = 6 \pmod{10}$ である．つまり，3143×68932 を 10 で割った余りは 6 である．
- 3143×68932 を 3 で割った余りは求めよ．$3143 \equiv 2 \pmod{3}, 68932 \equiv 1 \pmod{3}$ なので，3143×68932 を 3 で割った余りは $3143 \times 68932 \equiv 2 \times 1 \pmod{3}$ より，2 である．

これより，$n \ge 2$ を自然数として，$\bmod n$ の代表系 $\{0, 1, 2, \cdots, n-1\}$ を $\mathbf{Z}_n$ で表す.

定義 1.5

任意の $a, b \in \mathbf{Z}_n$ に対し，

1. 整数 a, b に対し，$a+b$ を n で割った余りを $a +_n b$ で表す.
2. 整数 a, b に対し，$a-b$ を n で割った余りを $a -_n b$ で表す.
3. 整数 a, b に対し，$a \times b$ を n で割った余りを $a \times_n b$ で表す.

もちろん，$a \pm_n b, a \times_n b$ は全て $\mathbf{Z}_n$ の元である．

例 4　*1.* $n=10$ とする．$3 +_{10} 9 = 2$，$3 -_{10} 9 = 4$，$3 \times_{10} 9 = 7$ である．

2. $n = 11$ とする．$89 +_{11} 34 = 2$，$36 -_{11} 52 = 6$，$7 \times_{11} 8 = 1$ である．

次の諸性質が成り立つ．これらの諸性質が成り立つ集合を「環 (ring)」という.（特に，(f) が成り立つので,「可換環」という.）よって，$\mathbf{Z}_n$ は環である．

命題 1.6

足し算に関するもの：

(a) （結合法則） $(a +_n b) +_n c = a +_n (b +_n c)$

(b) （交換法則） $a +_n b = b +_n a$

(c) （零元） $a +_n 0 = 0 +_n a = a$

(d) （逆元） $a +_n (n - a) = (n - a) +_n a = 0$

掛け算に関するもの：

(e) （結合法則） $(a \times_n b) \times_n c = a \times_n (b \times_n c)$

(f) （交換法則） $a \times_n b = b \times_n a$

(g) （単位元） $a \times_n 1 = 1 \times_n a = a$

足し算と掛け算に関するもの：

(h) （分配法則） $(a +_n b) \times_n c = (a \times_n c) + (b \times_n c)$

証明: いずれもやさしい．□

注意 1 *(a)* から *(d)* までの条件を満たしている集合を演算 $+$ に関して群（*group*）の構造を持つという．したがって，$(\mathbf{Z}_n, +)$ は群である.（特に，*(b)* が成り立つので,「可換群」または「アーベル群」という.）

演習問題 1

1. 次の計算を実行せよ．$7 +_{13} 10$ (2) $7 -_{13} 10$ (3) $7 \times_{13} 10$
   (4) $17 +_{28} 26$ (5) $17 -_{28} 26$ (6) $17 \times_{28} 26$
2. $\mathbf{Z}_{12}$ の元 a のうち，$4 \times_{12} a = 0$ となるような a を全て求めよ．(とりあえず，$a = 0, 1, \cdots, 11$ まで代入してみる．)
3. $\mathbf{Z}_{16}$ の元 a のうち，$6 \times_{16} a = 0$ となるような a を全て求めよ．
4. $1 +_{11} 2 +_{11} 3 +_{11} 4 +_{11} 5 +_{11} 6 +_{11} 7 +_{11} 8 +_{11} 9 +_{11} 10$ を求めよ．
5. (1) $1 +_{10} 2 +_{10} 3 +_{10} 4 +_{10} 5 +_{10} 6 +_{10} 7 +_{10} 8 +_{10} 9$ を求めよ．
   (2) $1 +_9 2 +_9 3 +_9 4 +_9 5 +_9 6 +_9 7 +_9 8$ を求めよ．
   (3) $1 +_8 2 +_8 3 +_8 4 +_8 5 +_8 6 +_8 7$ を求めよ．
6. 問 4 と問 5 の計算結果を見て 1 つの定理を作れ．そしてそれを証明せよ．
7. (1) $1 \times_5 2 \times_5 3 \times_5 4$ を求めよ．
   (2) $1 \times_6 2 \times_6 3 \times_6 4 \times_6 5 \times_6 6$ を求めよ．
   (3) $1 \times_{11} 2 \times_{11} 3 \times_{11} 4 \times_{11} 5 \times_{11} 6 \times_{11} 7 \times_{11} 8 \times_{11} 9 \times_{11} 10$ を求めよ．
8. 問 7 の計算結果を見て 1 つの定理を作れ．(証明はしなくても良い．)

第2章　最大公約数と互除法

割り算だけで最大公約数を求める方法が互除法である．

定義 2.1

整数 a, d が与えられているとする．もし $a = qd$ となるような整数 q があるならば，d は a の**約数**である，あるいはまた，a は d の**倍数**であるという．このとき，$d|a$ という記号で表す．

定義 2.2

整数 a, d が与えられているとする．整数 d が a の約数であり，b の約数でもあるとき，d は a, b の**公約数**であるという．

定義 2.3

整数 a, b が与えられているとする．もし $a = a'd, b = b'd$ となるような整数 d は a, b の公約数であるという．a, b の**最大公約数**(greatest common divisor) を $\gcd(a, b)$ または簡単に (a, b) で表す．
整数 a, b の最大公約数が 1 のとき，整数 a, b は**互いに素**であるという．

例 5　$a = 18, b = 30$ のとき，公約数 d は $d = 1, 2, 3, 6, -1, -2, -3, -6$ と 8 つある．最大公約数は 6 である：$(18, 30) = 6$.

例 6　$a = 40, b = 27$ のとき，公約数 d は $d = 1, -1$ だけである．最大公約数は 1 である：$(40, 27) = 1$. つまり，40 と 27 は互いに素である．

命題 2.4

正の整数 a, b が与えられていて，$a > b$ であるとする．このとき，a を b で割ったときのあまりを r とすると，

$$(a, b) = (b, r)$$

が成り立つ．

証明: $(a, b) = d, (b, r) = d'$ とする．

(i) $a = bq + r$ なので，$d|r$ である：実際，$a = da', b = db'$ と書くと，$r = a - bq = d(a' - b'q)$ と表せる．ゆえに，d は b, r の公約数である．したがって，$d \leq d'$.

(ii) 次に，$b = d'b_0, r = d'r_0$ と表すと，$a = bq + r = d'(b_0q + r_0)$ なので，$d'|a$ である．ゆえに，d' は a, b の公約数であるから，$d' \leq d$.

(iii) 上の二つの不等式より，$d = d'$. □

命題 2.5(ユークリッドの互除法)

正の整数 a, b が与えられたとする $(a > b)$.　最大公約数 (a, b) は以下のように，余り r_{i-1} を余り r_i で割っていくことで得られる．：

1. a を b で割ったときの商を q_1，余りを r_1 とする：$a = bq_1 + r_1$，$(0 \leq r_1 < b)$. ここで，$r_0 = b$ とおいておく.
2. $r_1 \neq 0$ ならば，$r_0(= b)$ を r_1 で割ったときの商を q_2，余りを r_2 とする：$b = r_1q_2 + r_2$，$(0 \leq r_2 < r_1)$.
3. $r_2 \neq 0$ ならば，r_1 を r_2 で割ったときの商を q_3，余りを r_3 とする：$r_1 = r_2q_3 + r_3$，$(0 \leq r_3 < r_2)$.
4. r_{i-1} を余り r_i で割って $r_{i-1} = r_iq_{i+1} + r_{i+1}$，$(0 \leq r_{i+1} < r_i)$.
5. これを繰り返して，ついには，$r_{k-1} = r_kq_{k+1}$ となったとする（つまり，$r_{k+1} = 0$）．このとき，$(a, b) = r_k$ である.

証明: 命題 1 を繰り返し適用すると，$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_k, r_{k-1}) = (r_k, 0) = r_k$ なので. □

命題 2.6

整数 a, b に対して，$(a, b) = d$ とする．このとき，

$$ax + by = d$$

となる整数 x, y が存在する.

証明: ユークリッドの互除法の手続きを下から上に上がってけばよい. □

例 7 $(40, 27) = 1$ なので，$40x + 27y = 1$ となる x, y を見つける.

ステップ	割り算	
1	$40 = 27 \times 1 + 13$	$13 = a - b$
2	$27 = 13 \times 2 + 1$	$1 = 27 - 13 \times 2 = b - 2(a - b) = 13 = -2a + 3b$

$1 = -2a + 3b$ となるので，$x = -2, y = 3$ は $40x + 27y = 1$ の一つの整数解である.

例 8 $(123456, 789)$ をユークリッドの互除法で求めよう．$a = 123456, b = 789$

とおく．

ステップ	割り算	
1	$123456 = 789 \times 156 + 372$	$372 = a - 156b$
2	$789 = 372 \times 2 + 45$	$45 = -2a + 313b$
3	$372 = 45 \times 8 + \underline{12}$	$12 = 17a - 2660b$
4	$45 = 12 \times 3 + 9$	$9 = -53a + 8293b$
5	$12 = 9 \times 1 + 3$	$3 = 70a - 10953b$
6	$9 = 3 \times 3 + 0$	

ここで，余りが 0 になったので，これ以上続けられない．最後の下線が付いている数字が最大公約数，つまり $(123456, 789) = 3$ である．

また，$123456x + 789y = 3$ を満たす整数解として，$(x, y) = (70, -10953)$ がとれる．□

命題 2.7

整数 a, b, c に対して，$a|bc$ で $(a, b) = 1$ ならば，$a|c$ である．

証明: $(a, b) = 1$ ならば，命題 2.6 より，$ax + by = 1$ となる整数 x, y がある．ここで，両辺に c をかけると $acx + bcy = c$ となる．$a|bc$ より，$bc = at$ となる整数 t があるから，左辺は $acx + aty = a(cx + ty)$ となり，a の倍数．したがって，右辺 c も a の倍数 □

定義 2.8

2 以上の整数 p が**素数**であるとは，p が $\pm 1, \pm p$ 以外の約数を持たないことを言う．素数でない整数を**合成数**という．

問題 1 100 以下の素数を全て挙げよ．

問題 2 119 は素数，合成数のどちらか．

命題 2.9

p は素数とする．整数 a, b に対して，$p|ab$ ならば，$p|a$ または $p|b$ である．

証明: $p|a$ でないとすると，$(p, a) = 1$ なので，命題 2.7 より，$p|b$ が従う．□

演習問題 2

1. 次の最大公約数を互除法によって求めよ.

   (1) $(18, 45)$　　(2) $(182, 143)$　　(3) $(102, 84)$

2. 問 1 の計算結果を用いて，次の方程式を満たす整数 x, y を 1 組求めよ.

   (1) $18x + 45y = (18, 45)$.

   (2) $182x + 143y = (182, 143)$.

   (3) $102x + 84y = (102, 84)$.

3. 1 以上 12 以下の整数のうち，12 と最大公約数が 1 であるものを全て求めよ．同様に，最大公約数が $2, 3, 4, 6$ となるものを求めよ.

4. 13 と 21 の最大公約数を互除法で計算してみて気ずくことはなにか.

5. 4 と同様の現象が起きるような整数の組をつくるにはどうしたらよいか.（ヒント：$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \cdots$ という数列をフィボナッチ数列という．この数列はどのような規則で出来ているか考えよ.）

6. 12345 と 67890 の最大公約数 $(12345, 67890)$ を求めよ．また，$12345x + 67890y = (12345, 67890)$ の整数解を一組求めよ.

第3章　有限環$\mathbf{Z}_n$

集合 $\mathbf{Z}_n = \{0, 1, 2, \cdots, n-1\}$ には，足し算 $+_n$ と掛け算 $\times_n$ が定義された．それについて，もう少し詳しく見る．

足し算と掛け算 $\times_n$ は集合 $\mathbf{Z}_n$ 上の 2 項演算である．この足し算に関して $\mathbf{Z}_n$ は「群」になっている．この群の定義を以下に与える．

一般に，集合 M 上の **2 項演算**とは，写像 $M \times M \to M$ のことである（ここで，$M \times M = \{(a, b) \mid a, b \in M\}$ は数学演習 II で習った**直積**である.）

定義 1　*1.* 集合 G に *2* 項演算 $\circ : G \times G \to G$ があり，G がこの演算に関し**群**である，または群構造を持つとは，次のことが成り立つときにいう：

- $\exists e \in G, \forall x \in G\,(x \circ e = e \circ x = x)$．このような元 e を（群 G の）**単位元**という．
- $\forall x \in G, \exists y \in G\,(x \circ y = y \circ x = e)$．このとき，$y$ を x の**逆元**という．
- $\forall x, y, z \in G\,((x \circ y) \circ z = x \circ (y \circ z))$．これを**結合法則**というという．

注意 2 群において，単位元は一意的である．実際，e_1, e_2 を単位元とすると，$e_1 = e_1 \circ e_2 = e_2$ となるから．

例 9 $\mathbf{Z}_6$ の乗積表*:* $n = 6$ の場合の $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ の乗積表（掛け算の表のこと）を作ってみよう．以下のようになる．

$\times$	*0*	*1*	*2*	*3*	*4*	*5*
0	*0*	*0*	*0*	*0*	*0*	*0*
1	*0*	*1*	*2*	*3*	*4*	*5*
2	*0*	*2*	*4*	*0*	*2*	*4*
3	*0*	*3*	*0*	*3*	*0*	*3*
4	*0*	*4*	*2*	*0*	*4*	*2*
5	*0*	*5*	*4*	*3*	*2*	*1*

問題 3 $\mathbf{Z}_7$ の乗積表*:* $n = 7$ の場合の $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5, 6\}$ の乗積表を作ってみよ．

$\times$	*0*	*1*	*2*	*3*	*4*	*5*	*6*
0							
1							
2							
3							
4							
5							
6							

$\mathbf{Z}_n$ は足し算と掛け算の 2 つの 2 項演算を持つが，これらの演算に関して「環」の構造を持っている．以下に「環」の定義を提示する．

定義 2　*1.* 集合 R が *2* つの演算 $\circ : R \times R \to R$ と $\star : R \times R \to R$ を有しているとする．R がこれらの演算に関し**環**であるとは，次のことが成り立つときにいう：

- R は演算 $\circ$ に関し群になっている．この演算に関する単位元を以下 0 と書く．
- $\exists e \in R, \forall x \in R\,(x \star e = e \star x = x)$. この元 e を演算 $\star$ の単位元という．
- 演算 $\star$ に関して結合法則が成り立っている：
  $\forall x, y, z \in R\,((x \star y) \star z = x \star (y \star z))$.
- 演算 $\circ$ と演算 $\star$ に関してつぎのような分配法則が成り立っている：
  $\forall x, y, z \in R\,((x \circ y) \star z = (x \star z) \circ (y \star z))$.

2. R が環であり，群演算 $\circ$ の単位元を 0 とするとき，

$\forall x \in R\,(x \neq 0 \Longrightarrow \exists y \in R\,(x \star y = e))$; つまり 0 でない任意の元に $\star$ に関する逆元が存在するならば，環 R は**体**であるという．

例 10　$R = \mathbf{Z}_n$ とし，演算 $\circ$ に $+_n$, $\star$ に $\times_n$ をとれば，これらの演算に関し $\mathbf{Z}_n$ は環になっている．分配法則

$$(a +_n b) \times_n c = a \times_n c +_n b \times_n c$$

も明らかであろう．特に，$\mathbf{Z}_n$ は n 個の元からなる有限集合なので有限環ともいう．体になっていれば有限体という．

命題 3.1

整数 n を固定する．$\mathbf{Z}_n$ の元 a が n と互いに素，すなわち最大公約数 $(a, n) = 1$ ならば，$a \times_n r = 1$ となる $r \in \mathbf{Z}_n$ が存在する．

証明: $(a, n) = 1$ ならば，$ax + ny = 1$ となる $x, y \in \mathbf{Z}$ が存在する（第 2 章の

命題 2.6)．これは，$ax \equiv 1 \pmod{n}$ を意味する．x を n で割ったときの余りを r とすると，$x \equiv r \pmod{n}$ かつ $r \in \mathbf{Z}_n$ で，$a \times_n r = 1$ となる．□

定理 3.2

$n = p$ が素数ならば，$\mathbf{Z}_p$ は有限体である．

証明: 演算 $\times_p$ に関し，0 以外の元に逆元があることを言えばよい．$a = 1, 2, \cdots, p-1$ は p と互いに素だから，命題 3.1 から $a \times_p x = 1$ となる $x \in \mathbf{Z}_p$ がある．□

命題 3.3

n が合成数ならば，$\mathbf{Z}_n$ は体ではない．

証明: n が合成数ならば，$1 < a, b < n$ なる整数があって $n = ab$ となる．このとき，$\mathbf{Z}_n$ の元として $a, b \neq 0$ である．もし $\mathbf{Z}_n$ が体ならば，$b \times_n x = 1$ となる $x \in \mathbf{Z}_n$ がある．両辺左から a を掛けると，$a \times_n (b \times_n x) = (a \times_n b) \times_x = 0 \times_n x = 0$ で，また $a \times_n 1 = a$ だから，$a = 0$ となり矛盾である．ゆえに，n が合成数ならば，$\mathbf{Z}_n$ は体ではない．□

命題 3.4

$\mathbf{Z}_n$ の元 a が与えられていて n と互いに素であるとする．また，もうひとつ $\mathbf{Z}_n$ の元 b が与えられているとする（b は n と互いに素である必要はない）．このとき，$a \times_n x = b$ となるような x が $\mathbf{Z}_n$ のなかに存在する．

証明: a は n と互いに素だから，命題 3.1 より $a \times_n y = 1$ となる $y \in \mathbf{Z}_n$ が存在する．両辺に b を掛けると，$(a \times_n y) \times_n b = a \times_n (y \times_n b) = b$ であるから，$x = y \times_n b$ とすればよい．□

命題 3.5

$\mathbf{Z}_n$ の乗積表において，n と互いに素な $\mathbf{Z}_n$ の元 a の行には，0 から $n-1$ まで $\mathbf{Z}_n$ の全ての元が 1 回ずつ現れる．

証明:a は n と互いに素だから，命題 3.1 より $a \times_n y = y \times_n a = 1$ となる $y \in \mathbf{Z}_n$ が存在する．$a \times_n x_1 = a \times_n x_2$ とすると，y を掛けて，$y \times_n (a \times_n x_1) = y \times_n (a \times_n x_2)$. しかし，$y \times_n (a \times_n x_1) = (y \times_n a) \times_n x_1 = 1 \times_n x_1 = x_1$, $y \times_n (a \times_n x_2) = (y \times_n a) \times_n x_2 = 1 \times_n x_2 = x_2$ より，$x_1 = x_2$．すなわち $x = 0, 1, \cdots, n-1$ に対して，$a \times x$ は n 個の異なる元である．□

演習問題 3

1. $\mathbf{Z}_6$ の乗積表を利用して，次の等式をみたす $\mathbf{Z}_6$ の元 x を全て求めよ．

   (1) $5 \times_6 x = 2$　　(2) $3 \times_6 x = 3$　　(3) $x \times_6 4 = 2$

2. $\mathbf{Z}_6$ の乗積表を利用して，次の等式をみたす $\mathbf{Z}_6$ の元 x を（あれば）全て求めよ．

   (1) $(5 \times_6 x) +_6 3 = 1$

   (2) $(5 \times_6 x) +_6 3 = (3 \times_6 x) +_6 1$

   (3) $(2 \times_6 x) +_6 4 = (5 \times_6 x) +_6 5$

3. $\mathbf{Z}_{11}$ において，1 から 10 までの逆元を求めよ．

4. 問 3 の結果を利用して，次の等式をみたす $\mathbf{Z}_{11}$ の元 x を求めよ．

   (1) $4 \times_{11} x = 3$

   (2) $(8 \times_{11} x) +_{11} 7 = (5 \times_{11} x) +_{11} 10$

   (3) $(2 \times_{11} x) +_{11} 5 = (9 \times_{11} x) +_{11} 3$

5. $\mathbf{Z}_{13}$ において，1 から 12 までの逆元を求めよ．

6. 問 5 の結果を利用して，次の等式をみたす $\mathbf{Z}_{13}$ の元 x を求めよ．

   (1) $6 \times_{13} x = 5$

   (2) $(9 \times_{13} x) +_{13} 3 = (3 \times_{13} x) +_{13} 11$

   (3) $(2 \times_{13} x) +_{13} 5 = (7 \times_{13} x) +_{13} 3$

7. たとえば，$\mathbf{Z}_6$ の乗積表を見てみると，0 の行以外のどの行にも，0 が続けて 2 回現れることはない，ということに気ずく．これが一般に成り立つこと，つまり，$\mathbf{Z}_n$ の乗積表において，0 の行以外のどの行にも，0 が続けて 2 回現れることはないことを証明せよ．

第4章　1次不定方程式

整数係数1次不定方程式 $2x+5y=1$ にはどのような整数解 $(x,y)\in \mathbf{Z}\times\mathbf{Z}$ があるだろうか？あればいくつあるか，有限個か無限個か？　今回は整数係数の一次方程式を考える．さて，$2x+5y=1$ には $(x,y)=(-2,1)$ という整数解がすぐに見つかる．1つでも整数解があれば，必ず無限個の整数解が存在することを以下に見る．他方，$6x+9y=2$ には整数解は1つもない．なぜなら，$x,y\in\mathbf{Z}$ ならば，左辺は必ず3の倍数だが，右辺は2なので3の倍数でないからである．整数係数の1次方程式に，整数解があるかないかについては，次の判定法がある．

定理 4.1

$a,b,c\in\mathbf{Z}$ とする．不定方程式 $ax+by=c$ を満たす整数 x,y が存在する $\Longleftrightarrow$ 最大公約数 (a,b) が c を割る．

証明: (1) $\Longrightarrow$ を示す．$(a,b)=d, a=a'd, b=b'd$ とする．このとき，$ax+by=d(a'x+b'y)=c$ で $a'x+b'y\in\mathbf{Z}$ なので，$d|c$ である．

(2) $\Longleftarrow$ を示す．$c=dk$ とする．第2章の命題2.6より，$ax+by=d$ となる $x,y\in\mathbf{Z}$ が存在する．このとき，$a(xk)+b(yk)=dk=c$ となり，$xk,yk\in\mathbf{Z}$ である．□

整数係数の1次方程式 $ax+bc=c$ は a,b の最大公約数 $d=(a,b)$ が c の約数のときは整数解が存在する．

その一つの解は互除法を使って求めることができる．$c=c'd$ とおくと，$ax+cy=d$ を満たす x,y が互除法により求まる．両辺に c' をかけると，$a(c'x)+b(c'y)=c'd=c$ なので，$x_0=c'x, y_0=c'y$ が一つの整数解になる．

その他の解はどのようにして求まるか．それが次の命題である．

定理 4.2

整数 $a, b, c \in \mathbf{Z}$ が与えられ, 最大公約数 $d = (a, b)$ が c を割るとする．また $a = a'd, b = b'd$ とかく．このとき，不定方程式 $ax+by = c$ を満たす全ての整数解は次のように得られる．すなわち，一つの解を $x = x_0, y = y_0$ とすると，他の全ての解は

$$\begin{cases} x = x_0 + b't \\ y = y_0 - a't \end{cases}$$

の t に全ての整数を代入することによって得られる．

証明: 仮定から $ax_0+by_0 = c$ である．他の任意の解を x, y として $ax+by = c$ とすると，2 つの式の差から，$a(x-x_0)+b(y-y_0) = 0$ となる．これを $a(x-x_0) = b(y_0-y)$ とし，両辺を最大公約数 $(a, b) = d$ で割ると，$a'(x-x_0) = b'(y_0-y)$ となる．

$a'(x - x_0) = b'(y_0 - y)$ だから，$a = a'd, b = b'd$ とする．$(a', b') = 1$ なので，第 2 章の命題 2.7 より，$a'|y_0 - y$ であるから，$y_0 - y = a't$ となる $t \in \mathbf{Z}$ がある．これより，$y = y_0 - a't$. $a'(x - x_0) = b'a'$ t より，$x - x_0 = b't$ となり，$x = x_0 + b't$ を得る．

逆にこの形をした整数の組 $(x_0 + b't, y_0 - a't)$ は全て $ax + by = c$ を満たす．実際，$a(x_0+b't)+b(y_0-a't) = ax_0+by_0+ab't-ba't = c+da'b't-db'a't = c$ となる．□

例 11 $18x + 30y = 12$ の 1 つ整数解は $x = 4, y = -2$ である．ゆえに，全ての解は

$$\begin{cases} x = 4 + 5t \\ y = -2 - 3t \end{cases}$$

で与えられる．ただし，$t \in \mathbf{Z}$ は任意の整数である．したがって，$t = \pm 1, \pm 2, \pm 3, \cdots$ と代入していくと，

$$(x, y) = (9, -5), (-1, 1), (14, -8), (-6, 4), (19, -11), (-11, 7), \cdots$$

と全ての整数解が与えられていく．

例 12 $40x + 27 = 3$ の解を求める．ユークリッドの互除法により，　$40x + 27y = 1$ の 1 つの整数解として，$x = -2, y = 3$ を作ることが出来る（前回の講義ノートの最後の例を参照）．ゆえに 3 倍して，$(x, y) = (-6, 9)$ という一つの解が求まる．したがって，全ての解は

$$\begin{cases} x = -6 + 27t \\ y = 9 - 40t \end{cases}$$

で与えられる．ただし，$t \in \mathbf{Z}$は任意の整数である．例えば，$(x, y) = (21, -31), (-33, 49)$ など（$t = \pm 1$ のとき）．

最大公約数 $(a, b) = d$ のとき，不定方程式 $ax + by = d$ は，まずユークリッドの互除法を逆にたどって特殊解 (x_0, y_0) を求め（互除法を用いなくとも，簡単に見つかる場合もある），

1 次不定方程式の解法

1. 不定方程式に対して $ax + by = c$ が与えられる．$(a, b, c \in \mathbf{Z})$
2. $(a, b) = d$ を求める．
3. d が c の約数でないならば，整数解は存在しない．
4. d が c を割り切れば整数解は存在する．$(a, b) = d$ が c を割るならば，$a = a'd, b = b'd, c = dc'$ とおく．
5. 互除法で，$ax_o + by_o = d$ となる整数解 x_o, y_o を求める．
6. 一般解は，$\begin{cases} x = c'x_o + b't \\ y = c'y_o - a't \end{cases}$ $(t \in \mathbf{Z})$

注意 3 あらかじめ方程式 $ax + by = c$ の両辺を d で割り，

$$a'x + b'y = c'$$

を解いてもよい．$(a', b') = 1$ なので，ユークリッドの互除法を逆にたどって $a'k + b'm = 1$ をみたす整数 k, m が求められ，$x_0 = kc', y_0 = mc'$ とおくと，(x_0, y_0) は，$a'x + b'y = c'$ の解である．一般解は $\begin{cases} x = x_0 + b't \\ y = y_0 - a't \end{cases}$ $(t \in \mathbf{Z})$ で与えられる．

演習問題 4

1. 次の 1 次方程式の一般解を求めよ.

   (1) $3x + 5y = 1$　　(2) $4x + 10y = 6$　　(3) $6x - 15y = 9$

2. 次の 1 次不定方程式の解であって，x が 1 以上 10 以下の範囲にあるものを全て求めよ.

   (1) $2x - 7y = 3$.

   (2) $7x - 3y = 2$.

   (3) $6x + 4y = 8$.

3. 次の 1 次不定方程式の解であって，x, y が共に正の整数であるものを求めよ.

   (1) $3x + 2y = 20$.

   (2) $5x + 3y = 35$.

   (3) $7x + 4y = 40$.

4. (1) つるとかめがどちらも一匹以上いて，足の本数の合計が 10 本であるという．それぞれ何匹いるか.

   (2) たこといかがどちらも一匹以上いて，足の本数の合計が 72 本であるという．それぞれ何匹いるか.

5. 問 4 の (1) の答えが 1 通りになるためには，足の本数が何本でなければならないか.

6. 1 次不定方程式 $ax + by = 6$ が正の整数解を 1 組だけもつような a, b であって，$1 \leq a \leq b \leq 6$ を満たすものを全て求めよ.（ヒント：$b = 6$ だったら a はいくつになりうるか，$b = 5$ だったら，$\cdots$ というふうに，場合わけしてみよう.）

7. (2016 年実施センター試験数学 IA) 不定方程式 $92x + 197y = 1$ をみたす整数 x, y の組の中で, x の絶対値が最小のものは $x = \boxed{a}, y = \boxed{b}$ である．また，不定方程式 $92x + 197y = 10$ をみたす整数 x, y の組の中で, x の絶対値が最小のものは $x = \boxed{c}, y = \boxed{d}$ である.

第5章　1次合同式

1次合同式は $ax \equiv c \pmod{n}$ という形の方程式である．これは1次不定方程式の応用として解ける．

1次合同式

$ax \equiv c \pmod{n} \iff \exists y(ax - c = ny) \iff ax - ny = c$ の整数解を求める

1次合同式 $ax \equiv c \pmod{n}$ に解 $x = x_o$ があれば，$ax_o \equiv c \pmod{n}$ より，$ax_o - c$ は n の倍数なので,$ax_o - c = ny_o$ という整数 y_o が存在する．これを書きなすと，$ax_o - ny_o = c$ であるから，1次不定方程式 $ax - ny = c$ に整数解 (x_o, y_o) が存在することになる．一般解は $d = (a, n)$ とおくと，$\begin{cases} x = x_o - \dfrac{n}{d}t \\ y = y_o - \dfrac{a}{d}t \end{cases}$ $(t \in \mathbf{Z})$ である．したがって，$x = x_o - \dfrac{n}{d}t$ $(t \in \mathbf{Z})$ は1次合同式 $ax \equiv c \pmod{n}$ の（全ての）解である．1次合同式の解をもとめるには，1次不定方程式の整数解を求めればよい (合同式の解として使うのは x だけであるが）．

定義 5.1

正の整数 n と整数 a, c が与えられたとき，$ax \equiv c \pmod{n}$ の形の式を **1次合同式**といい，これを満たすような全ての整数 x を求めることを，この1次合同式を解く，という．

まず，合同式の解は有限個求めれば十分であるに注意する．

命題 5.2

1次合同式 $ax \equiv c \pmod{n}$ において，もし $x = x_o$ がひとつの解ならば，$x_1 \equiv x_o \pmod{n}$ となる x_1 はすべて解である．

証明: $x_1 \equiv x_o \pmod{n}$ ならば，$x_1 = x_o + nt$ の形である．

$ax_o \equiv c \pmod{n} \iff \exists y_o(ax_o - ny_o = c)$ だから，$y_1 = y_o + at$ とおけば，$ax_1 - ny_1 = a(x_o + nt) - n(y_o + at) = ax_o - ny_o + ant - ant = ax_o - ny_o = c$ なので，$ax_1 \equiv c \pmod{n}$ である．□

注意 4 したがって，*1* 次合同式 $ax \equiv c \pmod{n}$ の解は $0 \leq x < n$ の範囲で求めれば十分である．

命題 5.3

$d = (a, n)$ は a, n の最大公約数である．このとき，1 次合同式 $ax \equiv c \pmod{n}$ に解がある $\Longleftrightarrow d|c$ である．
解があるときは，$0 \leq x < b$ の範囲で d 個ある: $n' = \dfrac{n}{d}$ とし，最小の解を x_1 とすれば，$x = x_1, x_1 + n', x_1 + 2n', \cdots, x_1 + (d-1)n'$ の d 個が解である．

証明: 1 次合同式 $ax \equiv c \pmod{n}$ に解がある $\Longleftrightarrow ax - c$ が n の倍数，したがって，ある整数 y があって，$ax - c = ny$．これは $ax - ny = c$ と書けるから，1 次合同式 $ax \equiv c \pmod{n}$ に解がある $\Longleftrightarrow$ 1 次不定方程式 $ax - ny = c$ に整数解がある $\Longleftrightarrow (a, n)|c$ である（定理 4.1）．

1 次合同式 $ax \equiv c \pmod{n}$ に解があるがあるとすると，ひとつの解 (x_0, y_0) と任意の整数を表すパラメータ t を用いて，$d = (a, n)$ とおくと，一般解は $x = x_0 - \dfrac{n}{d}t = x_o - n't, y = y_0 - \dfrac{a}{d}t$ という形に表される．$0 \leq x < n$ は従って $0 \leq x_0 - n't < n$ と同じだから，この不等式を変形すると，$\dfrac{x_o}{n'} - d < t \leq \dfrac{x_o}{n'}$. この範囲に整数 x は d 個ある: 0 以上の整数で最小のものを x_1 とすると，$x = x_1, x_1 + n', x_1 + 2n', \cdots, x_1 + (d-1)n'$ は $\dfrac{x_0}{n'} - d < t \leq \dfrac{x_0}{n'}$ の範囲にある整数 t に対応する x である．ゆえに，$0 \leq x < n$ の範囲の解は d 個あることが分かる．□

命題 5.3 を有限環 $\mathbf{Z}_n$ (3 章でやる内容）の言葉で言い換えると，以下のようになる．

命題 5.4

$\mathbf{Z}_n$ の元 a, c が与えられたとして，$\mathbf{Z}_n$ での方程式 $a \times_n x = c$ を考える．もし $(a, n) = d$ が c の約数でないならば，解は無い．もし $(a, n) = d$ が c の約数ならば，解はちょうど d 個あり，解の最小のものを x_1 とすれば，$x = x_1, x_1 + n', x_1 + 2n', \cdots, x_1 + (d-1)n'$ で与えられる．

例 13 *(a)* $72x \equiv 47 \pmod{200}$ の解を求めよ．
(b) $8x \equiv 6 \pmod{14}$ の解を求めよ．

解: (a) $(72, 200) = 8$ で 8 は 47 を割らないから，解はない．(b) $(8, 14) = 2$ だから，$0 \leq x < 14$ の範囲の解は 2 個ある．$8x - 14y = 6$ を解くと，$(x, y) = (-1, -1)$ がすぐ求まる．他の解は $x = -1 - 7t$ の形だが[1]，$t = -1, -2$ のときの $x = 6, 13$ が求める解である．□

[1] とりあえず今は y は関係ない．

1 次合同式の解法

1. 1 次合同式 $ax \equiv c \pmod{n}$ が与えられる.
2. $d = (a, n)$ を求める.
3. d が c の約数でないならば，解は無い.
4. d が c の約数ならば，$n = n'd$ とおくとき，互除法を用いて，$ax - ny = c$ の解を 1 つ求めて，それを x_o とおく.
5. x_o を n' で割ったあまりを r とおく.
6. 解は $x = r, r + n', r + 2n', \cdots, r + (d-1)n' \pmod{n}$ で与えられる.

演習問題 5

1. 次の 1 次合同式を解け.
   (1) $3x \equiv 4 \pmod{5}$
   (2) $4x \equiv 7 \pmod{9}$
   (3) $10x \equiv 4 \pmod{12}$
2. 次の 1 次合同式を解け.
   (1) $4x + 2 \equiv x + 6 \pmod{7}$
   (2) $8x + 2 \equiv 2x - 7 \pmod{15}$
   (3) $3x - 4 \equiv 7x - 2 \pmod{18}$
3. 1 次合同式 $4x \equiv a \pmod{10}$ が解を持たないような，0 以上 9 以下の整数 a を全て求めよ.
4. 財布の中に 10 円玉が 10 個，5 円玉が 1 個，1 円玉が 4 個ある．1 個 13 円の卵をできるだけ沢山買って，しかも 1 円玉が 1 個も残らないようにしたい．何個買えばよいか.

第6章　素数

命題 6.1

整数 n が合成数ならば，必ず 2 以上 $\sqrt{n}$ 以下の約数がある．

証明: $n = ab$ で $1 < a, b < n$ とする．もし $a > \sqrt{n}, a > \sqrt{n}$ ならば，$n = ab > (\sqrt{n})^2 = n$ となり矛盾．ゆえに，$a \leq \sqrt{n}$ または $b \leq \sqrt{n}$ である．□

素数の求め方（与えられた数以下の素数をすべて求める方法

1. 正の整数 n が与えられる．
2. $S = \{2, 3, 4, \cdots, n\}$ とおく．
3. $p = 2$ とおく．
4. p 以外の p の倍数をすべて取り去る．
5. S の元で p より大きいもののうち最小の数を p' とおく．
6. p' が $\sqrt{n}$ より小さければ，それをあらためて p とおいて 4 に戻る．そうでなければ 7 に行く．
7. S の元が n 以下の素数のすべてである．

注意 5 いわゆる「エラストテネスの篩」とよばれる方法である．

命題 6.2

正の整数 n が与えられているとする．このとき，n は少なくとも 1 つの素数の約数（「**素因数**」という）を持つ．

定理 6.3

素数は無限にたくさんある．

証明: いま，有限個の素数 $p_1, p_2, \cdots, p_n$ が勝手に与えられたとする．このとき，このリストに入っていない素数が必ず存在することを示す．$N = p_1 \times p_2 \times \cdots \times p_n + 1$ とおく．命題 6.2 より N を割る素因数 q が存在する（$q = N$ かもしれない）．q は $p_1, p_2, \cdots, p_n$ のどれでもない．なぜなら，q は N の約数だが，N はどの p_i で割っても 1 余るから．□

注意 6 *(Euler* の別証明）$\Omega := \{$ 素数全体 $\}$ とおく．

1. $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n}=\infty$ である．

2. 素因数分解の可能性と一意性より，$\displaystyle\sum_{n=1}^{\infty}\frac{1}{n}=\prod_{\text{素数全体}}(1+2^{-1}+2^{-2}+2^{-3}+\cdots+2^{-k}+\cdots)\times(1+3^{-1}+3^{-2}+3^{-3}+\cdots+3^{-k}+\cdots)\times(1+5^{-1}+5^{-2}+5^{-3}+\cdots+5^{-k}+\cdots)\times(1+7^{-1}+7^{-2}+7^{-3}+\cdots+7^{-k}+\cdots)\times\cdots\times(1+p^{-1}+p^{-2}+p^{-3}+\cdots+p^{-k}+\cdots)\times\cdots=\displaystyle\prod_{p\in\Omega}\frac{1}{1-p^{-1}}$.

3. もし Ω が有限集合ならば，$\displaystyle\prod_{p\in\Omega}\frac{1}{1-p^{-1}}<\infty$ であるから，最初の $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n}=\infty$ に矛盾．したがって，Ω は無限集合．

定理 6.4

素数 p について次の 3 つの条件は同じである：

1. n^2-n+p に $n=1,2,3,\cdots,p-1$ を代入すると，すべて素数になる．
2. p は $2,3,4,11,17,41$ のうちのどれかである．
3. 虚 2 次体 $\mathbf{Q}(\sqrt{1-4p})$ の類数は 1 である．

証明: 「2 次体の整数論」の本を参照．□

定理 6.5

正の整数 n が与えられたとする．このとき，

$$n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$$

（ここに，$p_1,p_2,\cdots,p_r$ は素数で，$e_1,e_2,\cdots,e_r$ は正の整数）と表すことができる．またこの表し方は $p_1,p_2,\cdots,p_r$ の順序を変えることを除けば一意的である．

証明: 省略．□

注意 7 *2* 次体 $\mathbf{Q}(\sqrt{-5})$ では，$6=2\times3=(1-\sqrt{-5})(1+\sqrt{-5})$ と素因数分解の一意性が失われる．

演習問題 6

1. たとえば，$4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 3 + 7$ というように，$4, 6, 8, 10$ は二つの素数の和として表せる．同じことを 12 以上 30 以下の偶数に対しても実行せよ.（4 以上のどんな偶数も二つの素数の和に表せるというのは「ゴールドバッハの予想」と呼ばれる.）

2. 正の整数 n と素数 p に対して $p^s | n$ だが，$p^{s+1} \nmid n$ のとき，$v_p(n) = s$ と表す．以下の値を求めよ.

   (1) $v_2(100)$　(2) $v_3(162)$　(3) $v_5(1234)$　(4) $v_7(1029)$

3. 2 の記号の元で，次のことを証明せよ.

   (1) 整数 n, m と素数 p に対し，$v_p(nm) = v_p(n) + v_p(m)$ が成り立つ.

   (2) 整数 n, m と素数 p に対し，$v_p(n + m) \geq \min(v_p(n), v_p(m))$ が成り立つ．ここで，$\min(a, b)$ は a, b のうち小さい方を指す.

第7章　フェルマーの定理

フェルマーの最終定理は,「$n \geq 3$ のとき，$x^n + y^x = z^n$ という方程式の整数解で $xyz \neq 0$ となるものは，存在しない」というもので，17 世紀にフェルマー (P. Fermat) によって予想された[1]．$n = 4$ のときはフェルマーが，$n = 3$ のときはオイラー (L. Euler) が示した．クンマー (E. Kummer) の革新的な仕事の後，1994 年に全く違う方法で[2]ワイルス (A. Wiles) によって最終的に証明された．この章のフェルマーの定理にはこの「大定理」ではなくて，以下に述べる小定理である．

$\mathbf{Z}_p = \{0, 1, 2, \cdots, p-1\}$ を $\mathbf{F}_p$ とあらためて書く．

命題 1 (「初等代数学」3 章定理 3.2) *p が素数のとき，$\mathbf{F}_p$ は体 (Field) という代数的構造をもつ．とくに，0 でない元は乗法に関して逆元をもつ：$\forall x \in \mathbf{F}_p (x \neq 0 \Longrightarrow x^{-1} \in \mathbf{F}_p)$.*

証明: $a \in \mathbf{F}_p$ が 0 でないということは，a が p で割れないということなので，$(a, p) = 1$ である．ゆえに，命題 2.6 より $\exists x, y \in \mathbf{Z}(ax + py = 1)$ である．これは $ax \equiv 1 \pmod{p}$ を示す．この x を p で割った余りを b とすると，$b \in \mathbf{F}_p$ で $ab = 1$ なので，$b = a^{-1}$ である．□

フェルマーの小定理

(a) a は p で割れない整数とする．このとき，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ．つまり，p で割れない整数 a に対して，$a^{p-1} - 1$ は p の倍数である．

(b) 全ての整数 a に対して，$a^p \equiv a \pmod{p}$ という合同式が成り立つ．つまり，どんな整数 a に対しても，$a^p - a$ は p の倍数である．

(a') $\forall a \in \mathbf{F}_p (a \neq 0 \Longrightarrow a^{p-1} = 1)$.

(b') $\forall a \in \mathbf{F}_p (a^p = a)$.

注意 8 上の二つ *(a), (b)* と下の二つ *(a'), (b')* はそれぞれ同じことである．

[1] $n = 1, 2$ のときは整数解は無限個ある．例えば，$3^2 + 4^2 = 5^2$ など．

[2] 有理数体上の楕円曲線に対する谷山・志村予想を証明することで，その副産物としてフェルマーの最終定理が証明された．

注意 9 *(b), (b')* は *(a), (a')* からの帰結である．整数 a が p で割れるのならば，a^p も p で割れるので，$a \equiv 0 \pmod{p}$，$a^p \equiv 0 \pmod{p}$ だから，自明に $a^p \equiv a \pmod{p}$ が成り立つ．整数 a が p で割れないのならば，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つから，両辺に a をかけて，$a^p \equiv a \pmod{p}$ が成り立つ．

証明: 2 つの証明を与える．$p = 2$ のときは当たり前なので，p は奇素数とする（$p > 2$）．

(i) 任意の自然数 $a = 1, 2, \cdots$ に対して，$a^p \equiv a \pmod{p}$ を数学的帰納法で示す．まず，$a = 1$ に対して，$a^p \equiv 1 \pmod{p}$ は明らかである．次に，$n^p \equiv n \pmod{p}$ と仮定して（帰納法の仮定），$(n+1)^p \equiv n+1 \pmod{p}$ を示す．2 項定理より，$(n+1)^p = n^p + pn^{p-1} + \dfrac{p(p-1)}{2}n^{p-2} + \cdots + pn + 1$ である．ここで，1 以外の係数は p で割れるので，$(n+1)^p \equiv n^p + 1 \pmod{p}$ である．仮定から，$n^p \equiv n \pmod{p}$ なので，$(n+1)^p \equiv n+1 \pmod{p}$ である．ゆえに，どんな $a = 1, 2, 3, 4, \cdots$ に対して，$a^p \equiv a \pmod{p}$ が成り立つことが分かる．

もし a が負の数であれば，$a = -b$ とすると，$b > 0$ より，$b^p \equiv b \pmod{p}$ が成り立つので，p はいま奇数であることより，$a^p = (-1)^p b^p = -b^p \equiv -b = a \pmod{p}$ が成り立つ

a が p で割れない数ならば，$ax \equiv 1 \pmod{p}$ なる整数 x が存在し，$a^p \equiv a \pmod{p}$ の両辺にその x をかけて，$a^p x \equiv ax \equiv 1 \pmod{p}$ である．$a^p x = a^{p-1} ax \equiv a^{p-1} \pmod{p}$ だから，$a^{p-1} \equiv 1 \pmod{p}$ を得る．

(ii) $\mathbf{F}_p = \{x_1, x_2, \cdots, x_p\}$ とすると，$\{ax_1, ax_2, \cdots, ax_p\} = \{x_1, x_2, \cdots, x_p\}$ である．実際，もし $ax_i = ax_j$ となるなら，$a^{-1} \in \mathbf{F}_p$ より，a^{-1} を両辺左からかけて，$x_i = x_j$ となるから，$\{ax_1, ax_2, \cdots, ax_p\}$ は $\mathbf{F}_p$ の異なる p 個の元である．

ゆえに，$ax_1 \times ax_2 \times \cdots \times ax_p = a^{p-1} x_1 \times x_2 \times \cdots \times x_p = x_1 \times x_2 \times \cdots \times x_p$ という等式が得られ，したがって $a^{p-1} = 1$ である．

□

例 14 2^{10000} を 13 で割ったときのあまりを求める．まず，10000 を $13-1 = 12$ で割ったときのあまりを求める．なぜならフェルマーの小定理より，$2^{12} \equiv 1 \pmod{13}$ だから，これを利用する．$12 \times 8 = 96$ なので，9600 は 12 で割れる．$400 = (96+4) \times 4$ を 12 で割ったときの余りは，4 である．ゆえに，$10000 = 12 \times m + 4$ であり，商 m が何であるかは重要ではない．$2^{12} \equiv 1 \pmod{13}$ に注意して，$2^{10000} = 2^{12 \times m + 4} = 2^{12 \times m} 2^3 = (2^{12})^m 2^4 \equiv 2^4 = 16 \equiv 3 \pmod{13}$ となり，余りは 3 であることが分かった．

例 15 3^{10000} を 17 で割ったときのあまりを求める．まず，10000 を $17-1 = 16$ で割ったときのあまりを求める．$10000 = 16 \times 625$ だから，$3^{10000} = 3^{16 \times 625} =$

$2^{12\times m}2^3 = (3^{16})^{625} \equiv 1 \pmod{13}$ となり，余りは 1 であることが分かった．

以下，裕文夫「初等代数学」の 7 章の命題を挙げておく．

命題 7.1

有限体 $\mathbf{F}_p$ の 0 以外の元 a が与えられたとする．このとき，a を p 回足すと 0 になる．しかし，それより少ない回数足しても決して 0 にはならない，

証明: どんな数 a に対しても $a+a+\cdots+a = p\cdot a \equiv 0 \pmod{p}$ である．p で割れない整数 a に対して，$0 < m < p$ なる m で $a+a+\cdots+a = ma \equiv 0 \pmod{p}$ となったとすると，$p|ma$ である．命題 2.7 または命題 2.9 より，$p \nmid a$ なので，$p|m$ である．これは矛盾．□

定理 7.2

$\mathbf{F}_p$ において，0 以外のどんな数も，$(p-1)$ 回掛けると 1 に等しくなる．

証明: 上で示した．□

定理 7.2'

p で割れない整数 a に対してつねにこのとき，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ．

証明: 上で示した．□

系 7.3

0 以外の元 a が与えられたとき，a^{p-2} が a の逆元である．

証明: フェルマーの小定理 $a^{p-1} = 1$ より，$a^{p-1} = a\cdots a^{p-2} = 1$ だから，$a^{-1} = a^{p-2}$ である．□

演習問題 7

1. (1) 2^{123} を 7 で割った余りを求めよ.

   (2) 3^{3333} を 11 で割った余りを求めよ.

   (3) 10^{10000} を 7 で割った余りを求めよ.

2. (1) $1^2 + 2^2 + \cdots + 99^2$ は 3 で割りきれることを証明せよ.

   (2) $1^4 + 2^4 + \cdots + 100^4$ は 5 で割りきれることを証明せよ.

   (3) $1^6 + 2^6 + \cdots + 98^6$ は 7 で割りきれることを証明せよ.

3. $1^{10} - 2^{10} + 3^{10} - 4^{10} + \cdots + 99^{10}$ は 11 で割りきれることを証明せよ.

4. 問 3 をやってみて，定理を 1 つ作れ．証明はしなくて良い.

5. $1^5 + 2^5 + \cdots + 98^5$ は 7 で割りきれることを証明せよ.

6. どんな自然数 n に対しても，$1^n + 2^n + \cdots + 98^n$ は 7 で割りきれることを証明せよ.

7. 問 6 をやってみて，もっと一般化してみよ.

第8章　多項式

数学において重要な類似の一つが次のものである：

整数と整式の類似

整数のなす環と多項式（「整式」）のなす環は似た構造を持つ．

この類似は重要である．

この章での体 K としては，主に有限体 $\mathbf{F}_p$ を指しているが，実数体 $\mathbf{R}$ や複素数体 $\mathbf{C}$ や有理数体 $\mathbf{Q}$ などの体でも同じなので，K を使う．

注意: 「体 (field)」とは，足し算・掛け算があって，すべての 0 でない元は掛け算に関する逆元を持っているものを言う．

定義 8.1

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ という形の式（ただし，すべて係数 a_i は体 K の元とする）を K-係数の多項式 (polynomial) という．また，$a_n \neq 0$ のとき，$f(x)$ の次数 (degree) は n であるといい，$\deg f(x) = n$ と書く．

注意 10 *1* 次式の次数は 1 で，*2* 次式の次数は 2 で，*3* 次式の次数は 3 である．定数 $f(x) = a_0$ も多項式だが，$a_0 \neq 0$ ならその次数は 0 である．ただし，定数 0 の次数だけは $-\infty$ とする．

注意 11　多項式 $f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$ において，x は「不定元」と呼ばれるが，これが x である必要は無い．$f(t) = a_0+a_1t+a_2t^2+\cdots+a_nt^n$ と表しても K-係数の多項式である．

定義 8.2

2 つの K-係数多項式 $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, g(x) = b_0 + b_1x + \cdots + b_mx^m$ の和を，$f(x) + g(x) := \sum_{i=0}^{max\{n,m\}} (a_i + b_i)x^i$ と定義する．

注意 12 0 も多項式であり，どんな多項式 $f(x)$ に対しても $f(x) + 0 = 0 + f(x) = f(x)$ である．

例 16 $\mathbf{F}_5$-係数の多項式 $f(x)=4x^2+3x+1$ と $g(x)=2x+1$ の和を求める．
$f(x)+g(x)=4x^2+5x+2=4x^2+2$ である．$\mathbf{F}_5$ では，$5=0$ に注意する．

定義 8.3

2 つの K-係数多項式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n, g(x)=b_0+b_1x+\cdots+b_mx^m$ の差を，$f(x)-g(x):=\sum_{i=0}^{max\{n,m\}}(a_i-b_i)x^i$ と定義する．

例 17 $\mathbf{F}_5$-係数の多項式 $f(x)=4x^2+3x+1$ と $g(x)=2x+1$ の差 $f(x)-g(x)$ は，$f(x)-g(x)=4x^2+x$ である．
また，$g(x)-f(x)=-4x^2-x=x^2+4x$ である．
$\mathbf{F}_5$ では，$-4=1,-1=4$ に注意する．

定義 8.4

2 つの K-係数多項式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n, g(x)=b_0+b_1x+\cdots+b_mx^m$ の積を，$f(x)\cdot g(x)=f(x)\times g(x):=\sum_{\ell=0}^{nm}(\sum_{i+j=\ell}a_ib_j)x^\ell$ と定義する．

注意 13 1 も多項式であり，どんな多項式 $f(x)$ に対しても $f(x)\times 1=1\times f(x)=f(x)$ である．

例 18 $\mathbf{F}_5$-係数の多項式 $f(x)=4x^2+3x+1$ と $g(x)=2x+1$ の積を求める．
$f(x)\times g(x)=8x^3+4x^2+6x^2+3x+2x+1=8x^3+10x^2+5x+1=3x^3+1$ である．$\mathbf{F}_5$ では，$8=3,10=0,5=0$ に注意する．$5=0$ に注意する．

例 19 $\mathbf{F}_7$ において，$(x^2+3x+5)\times(2x+4)=2x^3+4x^2+6x^2+12x+10x+20=2x^3+10x^2+22x+20=2x^3+3x^2+x+6$ である．$\mathbf{F}_7$ では，$10=3,22=1,20=6$ に注意する．$5=0$ に注意する．

定義 8.5

K-係数多項式の全体を $K[x]$ と書く．

注意 14 先に注意したように，不定元の名前が x である必要は無い．t でもよく，代数的には $K[x]\cong K[t]$ である．

命題 8.6

$K[x]$ は，自然に定義される多項式の足し算と掛け算に関して，可換環である．つまり，次が成り立つ：

(a) （結合法則） $(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$

(b) （交換法則） $f(x)+g(x)=g(x)+h(x)$

(c) （零元） $f(x)+0=0+f(x)=f(x)$

(d) （逆元） $f(x)+(-f(x))=(-f(x))+f(x)=0$

掛け算に関するもの：

(e) （結合法則） $(f(x)\times g(x))\times h(x)=f(x)\times(g(x)\times h(x))$

(f) （交換法則） $f(x)\times g(x)=g(x)\times f(x)$

(g) （単位元） $f(x)\times 1=1\times f(x)=f(x)$

足し算と掛け算に関するもの：

(h) （分配法則） $(f(x)+g(x))\times h(x)=(f(x)\times h(x))+(g(x)\times h(x))$

証明: 明らかである．□

注意 15 命題 *1.6*（$\mathbf{Z}_n$ が可換環であること）と命題 *8.6* の相似に注意しよう．

命題 8.7

任意の $f(x),g(x)\in K[x]$ に対して，$\deg g(x)>0$ のとき，

$$f(x)=g(x)q(x)+r(x)\qquad \deg r(x)<\deg g(x)$$

を満たす多項式 $q(x),r(x)\in K[x]$ が一意的に存在する．

これは整数の割り算と同じことが多項式でもできることを示している．$q(x)$ を $f(x)$ を $g(x)$ で割った時の「商」，$r(x)$ を $f(x)$ を $g(x)$ で割った時の「余り（剰余）」という．以下で例を 1 つ示し，命題の証明は省略する．

例 20 $K=\mathbf{F}_5=\{0,1,2,3,4\}$ とし，$f(x)=2x^3+3x^2+4x+2$ を $g(x)=3x^2+x+2$ を割った時の商と余り $q(x),r(x)$ を求めてみよう．普通の（つまり実数係数の）多項式の割り算と同じようにすればよい．ただし，係数の足し算・掛け算は $\bmod 5$ で実行する．答えは，$q(x)=4x+3, r(x)=3x+1$ である．講義で解説する．

演習問題　8

1. $\mathbf{F}_7$-係数の多項式 $f(x) = 4x^3 + 5x + 6, g(x) = 2x^2 + 3x + 2$ に対し，次の演算を実行せよ．

   (1) $f(x) + g(x)$ (2) $f(x) - g(x)$ (3) $g(x) - f(x)$ (4) $f(x) \times g(x)$

2. (1) $\mathbf{F}_2$ において，$(x+1)^2$ を計算せよ．

   (2) $\mathbf{F}_3$ において，$(x+1)^3$ を計算せよ．

   (3) $\mathbf{F}_5$ において，$(x+1)^5$ を計算せよ．

3. 問 2 をやってみて，1 つの定理を作れ．証明はしなくてよい．

4. (1) $\mathbf{F}_5$ において，$3x^3 + 2x^2 + 2x + 4$ を $4x^2 + 3x + 2$ で割ったときの商と余りを求めよ．

   (2) $\mathbf{F}_7$ において，$5x^3 + 6x^2 + 2$ を $3x + 4$ で割ったときの商と余りを求めよ．

   (3) $\mathbf{F}_{11}$ において，$x^4 + 10$ を $x^3 + x^2 + x + 1$ で割ったときの商と余りを求めよ．

5. $\mathbf{F}_5$ において，次の多項式を 1 次式の積として表せ．

   (1) $x^2 + 3x + 2$ (2) $x^2 + 4$ (3) $x^2 + 2x + 2$

第9章　方程式

定義 9.1

体 K に係数を持つ多項式 $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ に対して，$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$ を K-係数の n 次方程式 (equation) という．また，$f(\alpha) = 0$ となる $\alpha \in K$ を, 方程式の解，または多項式 $f(x)$ の根（root）であるという．

命題 9.2

体 K に係数を持つ n 次方程式の根の数は n 個以下である．

証明: 次の定理 9.3 より明らか．□

定理 9.3

体 K に係数を持つ方程式 $f(x) = 0$ が α を根にもつとすると，$f(x)$ は $f(x) = (x - \alpha)g(x)$ と因数分解できる．ここで，$g(x)$ は K に係数を持つある多項式で次数は $n - 1$ である．

証明: $f(x)$ を $x - \alpha$ で割ると，余りは定数である．すなわち，$f(x) = (x - \alpha)g(x) + r$ と表せて，$r \in K$ である．ここで，$x = \alpha$ を代入すると，$f(\alpha) = r$ で $f(\alpha) = 0$ より，$r = 0$ である．ゆえに，$f(x) = (x - \alpha)g(x)$．$\deg f(x) = \deg(x - \alpha) + \deg g(x)$ より，$\deg g(x) = n - 1$ である．□

例 21 $K = \mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ とし，$f(x) = 2x^2 + 4x + 5$ とおき，$f(x) = 0$ を解く．つまり，$f(\alpha) = 0$ となる $\alpha \in \mathbf{F}_7$ をすべて求める．

それには x に $\mathbf{F}_7$ の元を代入していけばよい．すると，$f(2) = 0$ がわかる．$f(x)$ を $x - 2$ で割ると，$f(x) = (x - 2)(2x + 1)$ である．$2x + 1 = 0$ を満たす $\mathbf{F}_7$ の元は，$x = 3$ である．ゆえに，求める根は $2, 3$ である．

例 22 $K = \mathbf{F}_{23} = \{0, 1, 2, 3, 4, 5, 6, \cdots, 21, 22\}$ とし，$\mathbf{F}_{23}$-係数の *3* 次方程式 $x^3 + 2x^2 + 2x + 18 = 0$ を解く．

$f(x) = x^3 + 2x^2 + 2x + 18$ とおくと，運良く $f(1) = 0$ がすぐに分かる．よって，$f(x)$ を $x - 1(= x + 22)$ で割ると，$f(x) = (x - 1)(x^2 + 3x + 5)$ となる．

$g(x) = x^2 + 3x + 5$ とおくと，運よく $g(3) = 0$ が分かる．よって，$g(x)$ を $x - 3(= 2 + 20)$ でわると，$g(x) = (x - 3)(x + 6)$ となるので，$g(x)$ のもうひ

とつの解は $x = -6\ = 17$ である．

ゆえに，$x^3 + 2x^2 + 2x + 18 = 0$ の $\mathbf{F}_{23}$ における解は $1, 3, 17$ である．

注意 16 多項式 $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ が $f(x) = g(x)h(x)$ となるような $0 < \deg g(x) < n, 0 < \deg h(x) < n$ となる K-係数多項式 g, h が存在するとき，$f(x)$ は K は可約であるという．可約でないとき，既約多項式という．整数の合成数に対応するのが可約多項式，素数に対応するのが既約多項式である．

例 23 $K = \mathbf{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ とし，$f(x) = x^5 + 1$ とおく．この多項式は $\mathbf{F}_{11}$ で可約である．実際，$f(\alpha) = 0$ となる $\alpha \in \mathbf{F}_{11}$ があれば，$f(x) = (x - \alpha)g(x)$ と因数分解できるので可約であることがわかる．そこで，$\mathbf{F}_{11}$ の元を代入していくと，$2^5 = 10$ なので，$f(2) = 0$ となり，可約である．

他方，多項式 $h(x) = x^2 + 3$ は $\mathbf{F}_{11}$ 上で既約である．実際，もし可約ならば，$h(x) = (x - \alpha)(x - \beta)$ となり，$h(\alpha) = 0, h(\beta) = 0$ だが，どの $\mathbf{F}_{11}$ の元 α を代入しても $h(\alpha) = 0$ とはならない．

演習問題 9

1. 次の $\mathbf{F}_7$-係数の方程式の根を求めよ．

   (1) $x^2 + x + 1 = 0$ (2) $3x^2 + 3x + 1 = 0$ (3) $x^3 + 2x^2 + 2x + 1 = 0$

2. 次の $\mathbf{F}_{13}$-係数の方程式の根を求めよ．

   (1) $x^2 + 4 = 0$ (2) $8x^2 + 4x + 1 = 0$ (3) $x^4 - 1 = 0$

3. p を素数とし有限体 $\mathbf{F}_p$ において，$x^{p-1} = 1 = (x - 1)(x - 2)\cdots(x - (p - 1))$ と分解されることを証明せよ．

4. 素数 p に対し，常に $(p - 1)! \equiv -1 \pmod{p}$ が成り立つことを証明せよ．（ヒント：問 3 を利用せよ．これは「ウィルソンの定理」と呼ばれる．演習問題 1 の問 7, 8 を参）

5. $\mathbf{F}_{17}$ において，$2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8$ を根に持つ 8 次方程式を作れ．ただし，最高次係数は 1 とする．

第10章　原始根

10.1　複素数の1の原始n乗根

定義 3 複素数$\alpha \in \mathbf{C}$が1のn乗根とは，αが$x^n = 1$の根であること．複素数$\alpha \in \mathbf{C}$が1のn乗根とは，$\alpha^n = 1, \alpha^m \neq 1 (m = 1, 2, 3, \cdots, n-1)$となることである．

1の4乗根は$x^4 = 1$の根のことで，$\mu_4 = \{1, i, -1, -i\}$である．$i^2 = -1, i^3 = -i, i^4 = 1$なので，$\mu_4 = \{i, i^2, i^3, i^4\}$と表せる．1の4乗根のすべてが$i$のべき乗で表せるので，$i$は1の原始4乗根という．$-i$も1の原始4乗根である．1の原始4乗根は2個ある．± 1は2乗したら1になるので，原始4乗根ではない．(-1は原始2乗根であるが，1は原始2乗根ではない.）1の位数は1, -1の位数は2，$\pm i$の位数は4という．

例 24 1の8乗根は$x^8 = 1$の根のことで，その全体をμ_8で表す．$\zeta = e^{\frac{2\pi i}{8}} = \cos\dfrac{2\pi i}{8} + i \cdot \sin\dfrac{2\pi i}{8}$とおくと，$\mu_8 = \{\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7, \zeta^8\}$と表せる．1の8乗根のすべてが$\zeta$のべき乗で表せるので，$\zeta$は1の原始8乗根という．$\pm 1, \pm i$も1の8乗根だが，原始8乗根ではない．

8と互いに素な$3, 5, 7$に対して，$\alpha = \zeta^3, \beta = \zeta^5, \gamma = \zeta^7$も1の原始8乗根となることがわかる．これらはすべて位数8で，1の原始8乗根は4個ある．

定義 4 自然数nに対して，$\varphi(n) := {}^{\#}\{m; 1 \leq m \leq n, (n, m) = 1\}$と定義される関数をオイラー関数という．

例 25 $\varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4.$

注意 17 1の原始n乗根は$\varphi(n)$個ある．

10.2　有限体の原始根

以上は複素数の話であったが，今度は，有限体の原始根を定義する．pを素数とし，有限体$\mathbf{F}_p = \{0, 1, 2, \cdots, p-1\}$から0を除いた集合$\mathbf{F}_p^*$とかく：$\mathbf{F}_p^* = \{1, 2, 3, \cdots, p-1\}$.

フェルマの小定理より，任意の$a \in \mathbf{F}_p^*$は$a^{p-1} = 1$より$p-1$乗根である：つまり$\mathbf{F}_p$において，aは多項式$x^{p-1} = 1$の根である．

定義 10.1

$a \in \mathbf{F}_p^*$ に対して，$a^n = 1$ となる最小の $n\,(1 \leq n \leq p-1)$ を a の**位数**という．

$p = 3, 5, 7,$ の場合について，以下，各元のべき乗を少し調べてみよう．$\mathbf{F}_3^* = \{1, 2\}$ で，$1^2 = 1, 2^2 = 1$ である．

$\mathbf{F}_5^*$:

a	a^2	a^3	a^4
1	1	1	1
2	4	3	1
3	4	2	1
4	1	4	1

$\mathbf{F}_7^*$:

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

以上の表から観察できること：

- 一番右側の列はすべて 1 である．(これは「フェルマーの小定理」$a^{p-1} = 1$ である．)
- どの元 $a \in \mathbf{F}_p^*$ に対しても $a^{p-1} = 1$ となるが，$1 \leq n < p-1$ となる n で $a^n = 1$ となるものもある．($\mathbf{F}_5^*$ では，$1, 4$ がそうで，$\mathbf{F}_7^*$ では，$1, 2, 4, 6$ がそうである．) しかし，$1 \leq n < p-1$ となるどの n でも $a^n \neq 1$ で，$n = p-1$ で初めて $a^n = 1$ となるものもある．($\mathbf{F}_5^*$ では，$2, 3$ がそうで，$\mathbf{F}_7^*$ では，$3, 5$ がそうである．)
- $a^n = 1$ となる最小の $n\,(1 \leq n \leq p-1)$ は $p-1$ の約数になっている．

命題 10.2

どんな $a \in \mathbf{F}_p^*$ に対しても，a の位数は $p-1$ の約数である．

証明: $a \in \mathbf{F}_p^*, a \neq 1$ に対して a の位数を k とする．すなわち，$a^m \neq 1\,(1 \leq m \leq k-1), a^k = 1$ とする．$k \leq p-1$ だから，$p-1$ を k で割ってその余りが r とすると，$p-1 = kq + r\,(0 \leq r < k)$ と表せる（q は商）．このとき，$r = (p-1) - kq$ なので，$a^r = a^{(p-1)-kq} = a^{p-1}(a^k)^{-q} = 1$ だから，も

し $r \neq 0$ ならば，$0 < r < k$ より a の位数が k であることに反する．ゆえに，$r = 0$，すなわち k は $p-1$ の約数である．□

定義 10.3

$a \in \mathbf{F}_p^*$ に対して，a の位数が $p-1$ であるものを $\mathbf{F}_p$ の**原始根**という．

合同式を用いると次のようになる：

定義 10.3'

p と互いに素な整数 a が**法 p での原始根**であるとは，a が $p-1$ 乗して初めて 1 と合同になるものをいう．

定理 10.4

任意の素数 p に対して，$\mathbf{F}_p$ の原始根は存在する．(唯一つではない，$\varphi(n)$ 個ある．)

この定理の証明は長いので，別ノートにする．

命題 10.5

$\mathbf{F}_p$ の原始根 g に対して，$g^{\frac{p-1}{2}} = -1 (= p-1)$ である．

証明: $x = g^{\frac{p-1}{2}}$ とおくと，フェルマの小定理より，$x^2 = g^{p-1} = 1$ である．ゆえに，$x = \pm 1$．しかし，g は原始根であるから，$x \neq 1$．ゆえに，$x = g^{\frac{p-1}{2}} = -1$．

□

原始根か否かのチェック方法

任意の素数 p に対して，$a \in \mathbf{F}_p^*$ の原始根か否かのチェックするには，1 と $p-1$ 以外の $p-1$ の約数 m で，a^m が 1 にならないことをチェックすればよい．

例 26

- $3 \in \mathbf{F}_{13}$ が原始根か否かを調べる．3 の位数は，$p-1 = 13-1 = 12$ の約数なので，$2, 3, 4, 6$ 乗を調べればよい．$3^2 = 9 \neq 1, 3^4 = 3 \neq 1, 3^6 = 27 = 1$ となる．したがって，3 の位数は 6 であり，原始根ではない．

- $4 \in \mathbf{F}_{13}$ が原始根か否かを調べる．4 の位数は，$p-1 = 13-1 = 12$ の約数なので，$2, 3, 4, 6$ 乗を調べればよい．$4^2 = 3 \neq 1, 4^4 = 9 \neq 1, 4^6 = 27 = 1$ となる．したがって，4 の位数は 6 であり，原始根ではない．

  5 も原始根でないことがすぐ分かる．

- $6 \in \mathbf{F}_{13}$ が原始根か否かを調べる．6 の位数は，$p-1 = 13-1 = 12$ の約数なので，$2, 3, 4, 6$ 乗を調べればよい．$6^2 = 10 \neq 1, 6^4 = 9 \neq 1, 6^6 = 12 = -1 \neq 1$ となる．したがって，6 の位数は 12 であり，原始根である．

演習問題 10

1. (1) $\mathbf{F}_{11}$ において 2 は原始根であることを証明せよ．

   (2) $\mathbf{F}_{13}$ において 2 は原始根であることを証明せよ．

   (3) $\mathbf{F}_{17}$ において 2 は原始根でないことと，3 は原始根であることを証明せよ．

2. (1) $1+2+2^2+2^3+\cdots+2^{100}$ を 11 で割ったあまりを求めよ．

   (2) $1+2+2^2+2^3+\cdots+2^{100}$ を 13 で割ったあまりを求めよ．

   (3) $1+3+3^2+3^3+\cdots+3^{100}$ を 17 で割ったあまりを求めよ．

3. 問 2(1) より定理を 1 つ作ってみよ．またそれを証明せよ．

4. 有理数 $\frac{1}{17}$ の小数展開を筆算で計算して，小数第何位で循環し始めるか観察せよ．一方，$\mathbf{F}_{17}$ において 10 は原始根であることを証明せよ．

5. 問 4 より定理を 1 つ作ってみよ．証明はしなくて良い．

解法のヒント：例えば，1 (1) では，$\mathbf{F}_{11}$ においては，位数は $p-1=11-1=10$ の約数なので，$1,2,5$ を調べればよい．$2^2 \neq 1, 2^5 \neq 1$ ならば，自動的に 2 は $\mathbf{F}_{11}$ の原始根となる．

例 27　上の乗積表より，$\mathbf{F}_5$ の原始根は $2,3$ の *2* つで，$\mathbf{F}_5^* = \{2, 2^2, 2^3, 2^4\} = \{3, 3^2, 3^3, 3^4\}$ であり，$\mathbf{F}_7$ の原始根は $3,5$ の *2* つで，$\mathbf{F}_7^* = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{5, 5^2, 5^3, 5^4, 5^5, 5^6\}$ であることがわかる．

注意 18　$\mathbf{F}_p^*$ は自然に群の構造を持つが，上に見たように原始根のべき乗ですべての元が表される．そのような群を *1* つの元で生成された群だから「巡回群」*(cyclic group)* といい，今の場合原始根 r で生成されるから $\mathbf{F}_p^* =< r >$ と書く．$\mathbf{F}_p^* =< 2 >$ また $\mathbf{F}_5^* =< 3 >$ でもあり，$\mathbf{F}_7^* =< 3 >$ で $\mathbf{F}_7^* =< 5 >$ でもある．

第11章　指数

（前回の復習）p を素数とし，有限体 $\mathbf{F}_p = \{0, 1, 2, \cdots, p-1\}$ から 0 を除いた集合 $\mathbf{F}_p^*$ に原始根とよばれる元が存在する（唯一つではなく，複数個）．

$a \in \mathbf{F}_p^*$ に対して，最初に $a^n = 1$ となる $n > 0$ を a の位数といい，$\mathrm{ord}(a)$ で表す．

命題 11.1

$\mathbf{F}_p$ の一つの原始根を r とすると，$\mathbf{F}_p^*$ のすべての元は $r^i\,(0 \leq i \leq p-2)$ という形に書ける：$\mathbf{F}_p^* = \{r^0, r, r^2, r^3, \cdots, r^{p-2}\}$．ただし，$r^0 = 1$ と約束する．

証明: 原始根とは位数 $p-1$ の元である: $\mathrm{ord}(r) = p-1$．今，$1 \leq i, j < p-1$ で $r^i = r^j$ となったとすると $(j \leq i)$，$r^{i-j} = 1$ だから，$i-j$ は $p-1$ の倍数である．$1 \leq i, j < p-1$ より $i = j$ である．

よって，$\{r^0, r, r^2, r^3, \cdots, r^{p-2}\}$ は個数が $p-1$ の集合だから，$\mathbf{F}_p^* = \{r^0, r, r^2, r^3, \cdots, r^{p-2}\}$ となる．

□

定義 11.2

$a \in \mathbf{F}_p^*$ に対して，$a = r^k$ となる $k\,(0 \leq k \leq p-1)$ が唯一つ定まる．これを

$$\mathrm{ind}_r(a)$$

と表し $a \in \mathbf{F}_p^*$ の原始根 r に関する**指数**という．

注意: どんな原始根に関しても 1 の指数は 0 である：$\mathrm{ind}_r(1) = 0$.

$\mathbf{F}_5$ の原始根は $2, 3$ の 2 つだから，それぞれの原始根に関する $1, 2, 3, 4$ の指数を求めてみよう．

表

a	2	3
a^2	4	4
a^3	3	2
a^4	1	1

から，以下のようになる：

a	1	2	3	4
$\mathrm{ord}(a)$	1	4	4	2
$\mathrm{ind}_2(a)$	0	1	3	2
$\mathrm{ind}_3(a)$	0	3	1	2

例 28 $\mathbf{F}_7$ の原始根は $3, 5$ の *2*つだから，それぞれの原始根に関する $1, 2, 3, 4, 5, 6$ の指数を求めてみよう．

a	3	5
a^2	2	4
a^3	6	6
a^4	4	2
a^5	5	3
a^6	1	1

から，以下のようになる：

a	1	2	3	4	5	6
$\mathrm{ord}(a)$	1	3	6	3	6	2
$\mathrm{ind}_3(a)$	0	2	1	4	5	3
$\mathrm{ind}_5(a)$	0	4	5	2	1	3

補題

$\mathbf{F}_p$ の任意の原始根 r に対して，$r^n = 1$ ならば n は $p-1$ の倍数である．
合同式の言葉では，$r^n \equiv 1 (\mathrm{mod}\, p)$ ならば，n は $p-1$ の倍数である．

証明: $n = q(p-1) + k$ $(0 \leq k < p-1)$ とする．$1 = r^n = r^{q(p-1)} r^k = (r^{p-1})^q r^k = r^k$ で，$0 \leq k < p-1$ なので，$k = 0$ でなければならない．□

指数 $\mathrm{ind}_r(a)$ はその定義の仕方から対数 log に似ているが，それを以下の命題で示す：

命題 11.3

$\mathbf{F}_p$ の一つの原始根を r を一つ固定する．このとき

- $\mathrm{ind}_r(ab) \equiv \mathrm{ind}_r(a) + \mathrm{ind}_r(b) \pmod{p-1}$
- $\mathrm{ind}_r(a^n) \equiv n \times \mathrm{ind}_r(a) \pmod{p-1}$

が成り立つ．

証明: $\mathrm{ind}_r(a) = m, \mathrm{ind}_r(b) = n, \mathrm{ind}_r(ab) = k$ とおくと，$r^m = a, r^n = b, r^k = ab$ である．$r^k = ab = r^m r^n = r^{n+m}$ であるから，$r^{k-(n+m)} = 1$ である．「補題」より，$k - (n+m)$ は $p-1$ の倍数，すなわち，$k \equiv n + m \pmod{p-1}$ である．これは，$\mathrm{ind}_r(ab) \equiv \mathrm{ind}_r(a) + \mathrm{ind}_r(b) \pmod{p-1}$ に他ならない．□

注意 19 対数法則 $\log(ab) = \log(a) + \log(b)$ の証明も同じである．

定理 11.4

$\mathbf{F}_p$ における原始根 r を一つ決めておく．このとき，$\mathbf{F}_p^*$ の元の位数は

$$\frac{p-1}{(p-1, \mathrm{ind}_r(a))}$$

で与えられる．

証明: $(p-1, \mathrm{ind}_r(a)) = s$, $p-1 = sk, m = \mathrm{ind}_r(a) = s\ell$ とおく．$(k, \ell) = 1$ である．定義から，$a = r^m = r^{s\ell}$ である．$\mathrm{ord}(a) = t$ とおくと，$a^t = r^{mt} = r^{st\ell} = 1$ で t はそのような最小の正の整数である．$mt = s\ell t$ は $p-1$ の倍数であることと合わせて，$t = k$ である．ゆえに，$\mathrm{ord}(a) = t = k = \dfrac{p-1}{s} = \dfrac{p-1}{(p-1, \mathrm{ind}_r(a))}$.
□

定理 11.5

$\mathbf{F}_p$-係数の方程式 $x^n - 1 = 0$ が $\mathbf{F}_p$ のなかに 1 以外の根を持つための必要十分条件は $(n, p-1) > 1$ が成り立つことである．特に，$n | p-1$ のとき，根は n 個あり，1 つ原始根 r を決めておけば，$p-1 = ns$ としたとき，根は $1, r^s, r^{2s}, \cdots, r^{(n-1)s}$ で与えられる．

証明: $r \in \mathbf{F}_p$ を原始根とする．$x^n - 1 = 0$ が $\mathbf{F}_p$ のなかに 1 以外の根を持つならば $(n, p-1) > 1$ であることを，対偶の形で示す．そのため，$(n, p-1) = 1$ と仮定し，$\forall \alpha \in \mathbf{F}_p (\alpha^n = 1) \Longrightarrow \alpha = 1$ を示す．$(n, p-1) = 1$ ならば，$nk + (p-1)\ell = 1$ となる $, k, \ell \in \mathbf{Z}$ が存在する．よって，$\alpha = \alpha^{nk+(p-1)\ell} = (\alpha^n)^k (\alpha^{p-1})^\ell = 1$ である．

逆に，$(n, p-1) = d > 1$ ならば，$x^n - 1 = 0$ が $\mathbf{F}_p$ のなかに 1 以外の根を持つことを示す．$n = dn', p-1 = dm$ とおく．このとき，$d > 1$ より $m < p-1$ なので，$r^m \neq 1$ で，$(r^m)^n = r^{nm} = r^{n'(p-1)} = (r^{p-1})^{n'} = 1^{n'} = 1$ だから，r^m は $x^n - 1 = 0$ の解である．

特に，$n | p-1$ ならば，$p-1 = ns$ とするとき，$j = 1, 2, \cdots, n-1$ に対して，r^{js} は $\mathbf{F}_p^*$ の相異なる元で，$(x^{js})^n = x^{jns} = n^{j(p-1)} = 1$ である．方程式 $x^n - 1 = 0$ の $\mathbf{F}_p$-解は高々 n 個なので（第 7 回講義ノート命題 3），$1, r^s, r^{2s}, \cdots, r^{(n-1)s}$ が解のすべてである．□

例 29 $\mathbf{F}_7$-係数の方程式 $x^3 - 1 = 0$ の解は上の命題より存在し，$p-1 = 3 \times 2$ なので，r を $\mathbf{F}_7$ の任意の原始根とするとき，$1, r^2, r^4$ が解である，$r = 3$ ならば，$1, 3^2 = 2, 3^4 = 4$，$r = 5$ ならば，$1, 5^2 = 4, 5^4 = 2$ であるから，解は $1, 2, 4$ である．

演習問題 11

1. $\mathbf{F}_p^*$ は $\mathbf{F}_p$ から 0 を除いたものである.

   (1) $\mathbf{F}_{11}$ において 2 は原始根である（演習問題 8 の 1(1)）. 各 $x \in \mathbf{F}_{11}^*$ の 2 に関する指数 $\mathrm{ind}_2(x)$ と位数 $\mathrm{ord}(x)$ を求めよ.

   (2) $\mathbf{F}_{13}$ において 2 は原始根である（演習問題 8 の 1(2)）. 各 $x \in \mathbf{F}_{13}^*$ の 2 に関する指数 $\mathrm{ind}_2(x)$ と位数 $\mathrm{ord}(x)$ を求めよ.

2. (1) $\mathbf{F}_{11}$ において $x^5 - 1 = 0$ を解け.

   (2) $\mathbf{F}_{13}$ において $x^4 - 1 = 0$ を解け.

   (3) $\mathbf{F}_{17}$ において $x^8 - 1 = 0$ を解け.

3. 1 から 12 までの整数のうち，100 乗して 13 で割ると余りが 1 になるものをすべて求めよ.

第12章　2項方程式

（今回の目的）$\mathbf{F}_p$-係数の 2 項方程式 $x^n = a$ の解がいつ存在し，解があるときの解の記述が原始根と指数を使って解明できることを示す.

$\mathbf{F}_p$-係数の 2 項方程式 $x^n - a = 0$ を「2 項方程式」という．前回，$a = 1$ の場合の解の存在条件と解の記述について調べた．今回は，$a \in \mathbf{F}_p, a \neq 0$ として方程式を考える．$p = 2$ のときは，$a \in \mathbf{F}_2, a \neq 0 \Longrightarrow a = 1$ なので，方程式は $x^n = 1$ で解はもちろん存在し $x = 1$ である．したがって，以下では $p > 2$ を奇素数としよう.

まず，$\mathbf{F}_p^*$ の原始根の一つを r として固定する．いま，$x^n = a$ をみたす $x \in \mathbf{F}_p, x \neq 0$ が存在するとしよう．$k = \mathrm{ind}_k(x)$，$x = r^k$ とする．このとき，

$$\mathrm{ind}_r(x^n) \equiv n \cdot \mathrm{ind}_r(x) = n \cdot k \cdot \mathrm{ind}_r(r) = nk \equiv \mathrm{ind}_r(a) \pmod{p-1}.$$

したがって $x^n = a$ をみたす $x \in \mathbf{F}_p, x = r^k$ が存在すれば，1 次合同式 $nX \equiv \mathrm{ind}_r(a) \pmod{p-1}$ に解 $X = k$ が存在する.

逆に，もし 1 次合同式 $nX \equiv \mathrm{ind}_r(a) \pmod{p-1}$ に解 $X = k$ が存在すれば，$x = r^k$ とおくと，$x^n = a$ となる．実際，$nk - \mathrm{ind}_r(a) = m(p-1)$ とすると，$x^n = (r^k)^n = r^{nk} = r^{\mathrm{ind}_r(a)+m(p-1)} = r^{\mathrm{ind}_r(a)} r^{m(p-1)} = a \cdot 1 = a$ となるから.

そして，1 次合同式 $nX \equiv \mathrm{ind}_r(a) \pmod{p-1}$ に解が存在するための必要十分条件は $(n, p-1)$ が $\mathrm{ind}_r(a)$ を割り切ることである．そのとき，1 次合同式 $nX \equiv \mathrm{ind}_r(a) \pmod{p-1}$ の解は $(n, p-1) = d$ 個あり，$X = k_1, k_2, \cdots, k_d$ とすると，$r^{k_1}, r^{k_2}, \cdots, r^{k_d}$ が $x^n = a$ の $\mathbf{F}_p$-解のすべてである.

$\mathbf{F}_p$-係数の 2 項方程式 $x^n = a$ の解法

$\mathbf{F}_p^*$ の原始根 r を一つとっておく.

- $d = (n, p-1)$ を求める.
- $\mathrm{ind}_r(a)$ を求める.
- $d|\mathrm{ind}_r(a)$ ならば解はあり，そうでないなら解はない.
- $d|\mathrm{ind}_r(a)$ ならば，1 次合同式 $nX \equiv \mathrm{ind}_r(a) \pmod{p-1}$ の解を d 個求め，それらを $X = k_1, k_2, \cdots, k_d$ とすると，$r^{k_1}, r^{k_2}, \cdots, r^{k_d}$ が $x^n = a$ の $\mathbf{F}_p$-解のすべてである.

例 30 $\mathbf{F}_7$ における *2* 項方程式 $x^4 = 2$ の解を求める．まず，$\mathbf{F}_7$ の原始根 3 をとっておこう．このとき，$2 = \mathrm{ind}_3(2)$ であり，$(4, 7-1) = 2$ なので，解は存在する．次に，*1* 次合同式 $4x \equiv 2 \pmod 6$ を解く（解は *2* 個ある）．$x = 2, 5$ とすぐにわかり，$x^4 = 2$ の $\mathbf{F}_7$ における解は，$3^2 = 2, 3^5 = 5$ の *2* つである．（原始根として 5 をとってももちろん解は同じ.）

特に $n = 2$ のときは，より簡単に以下のようになる.

$\mathbf{F}_p$-係数の 2 次の 2 項方程式 $x^2 = a$ の解法

$\mathbf{F}_p^*$ の原始根 r を一つとっておく.

- $(2, p-1) = 2$ である.（$p > 2$ は奇数だから.）
- $\mathrm{ind}_r(a)$ を求める.
- $\mathrm{ind}_r(a)$ が偶数ならば解はあり，奇数なら解はない.
- $\mathrm{ind}_r(a)$ が偶数のとき，1 次合同式 $2x \equiv \mathrm{ind}_r(a) \pmod{p-1}$ の解の 1 つは，$x = \dfrac{\mathrm{ind}_r(a)}{2}$ で, したがって $\pm r^{\frac{\mathrm{ind}_r(a)}{2}}$ が $x^2 = a$ の $\mathbf{F}_p$-解である.

例 31 $\mathbf{F}_7$ における *2* 項方程式 $x^2 = 2$ の解を求める．ここでは，$\mathbf{F}_7$ の原始根 5 をとっておこう．このとき，$4 = \mathrm{ind}_5(2)$ は偶数だから解は存在する．次に，*1* 次合同式 $2x \equiv 4 \pmod 6$ を解く（解は *2* 個ある）．$x = 2, 5$ とすぐにわかり，$x^2 = 2$ の $\mathbf{F}_7$ における解は，$5^2 = 4, 5^5 = 3$ の *2* つである.（原始根として 3 をとってももちろん解は同じ.）

最後に $a = -1$ の場合を調べよう．$\mathbf{F}_p$ において $p-1$ を -1 と表す.

命題 12.1

$\mathbf{F}_p$ における任意の原始根 r に対して，$\mathrm{ind}_r(-1) = \dfrac{p-1}{2}$ である．

証明: $r^{p-1} = 1$ なので，$x = r^{\frac{p-1}{2}}$ とおくと，$x^2 = 1$ である．ゆえに，$x = \pm 1$ だが，r は原始根なので，$x = -1$；つまり，$r^{\frac{p-1}{2}} = -1$. ゆえに，$\mathrm{ind}_r(-1) = \dfrac{p-1}{2}$ である．□

命題 12.2

p は 3 以上の素数とする．このとき，$\mathbf{F}_p$-係数の 2 項方程式 $x^2 = -1$ の方程式の解は $p = 4k+1$ の形の素数のときに存在し，$\pm r^{\frac{p-1}{4}}$ が $x^2 = -1$ の $\mathbf{F}_p$-解である．

証明: 方程式 $x^2 = 1$ の解はもちろん $x = \pm 1$ である．ところで，$(r^{\frac{p-1}{2}})^2 = r^{p-1} = 1$ なので，$r^{\frac{p-1}{2}} = \pm 1$ である．しかし，r は原始根なので，$r^{\frac{p-1}{2}} = -1$ である．ゆえに，$\mathrm{ind}_r(-1) = \dfrac{p-1}{2}$ である．$p > 2$ なる素数は $p = 4k+1$ か $p = 4m+3$ という形に表される（p は奇数なので 4 で割って余りが $1, 3$ のどちらかなので）．$\mathrm{ind}_r(-1) = \dfrac{p-1}{2}$ が偶数になるのは，$p = 4k+1$ の形の素数のときである．残りは上の一般的な結果から従う．□

演習問題 12

1. (1) $\mathbf{F}_{11}$ において $x^6 = 5$ を解け.
   (2) $\mathbf{F}_{13}$ において $x^8 = 3$ を解け.
   (3) $\mathbf{F}_{17}$ において $x^{10} = 13$ を解け.
2. (1) $\mathbf{F}_{11}$ において $x^2 = 3$ を解け.
   (2) $\mathbf{F}_{11}$ において $x^2 = 7$ を解け.
   (3) $\mathbf{F}_{13}$ において $x^2 = 10$ を解け.
3. $\mathbf{F}_{13}$ における方程式 $x^2 = -1$ は根を持つか，もし持つならば，根をすべて求めよ.
4. 平方完成によって次の 2 次方程式を解け.
   (1) $\mathbf{F}_{11}$ における $x^2 + 2x + 4 = 0$.
   (2) $\mathbf{F}_{13}$ における $x^2 + 4x + 2 = 0$.
   (3) $\mathbf{F}_{17}$ における $x^2 + 9x + 7 = 0$.