離散数学及び演習
講義 7　2016. 6. 2（木）

素数
（教科書　pp.106-113）

素数，合成数

- $n \in \mathbf{N}$ ($n>1$) は素数(prime number)である
  - n の正の約数は 1 と n だけである

例：2, 3, 5, 7, 11, 13, …

- $n \in \mathbf{N}$ ($n>1$) は合成数(composite number)である
  - n は素数でない
- 1 は素数でも合成数でもない
- 正の約数の個数
  - 1　… 1 個
  - 素数　… 2 個
  - 合成数　… 3 個以上

定理

$n \in \mathbf{N}$ が合成数ならば，素数 p が存在して，
$p \leq \sqrt{n}$　かつ $p \mid n$.

- すべての素数 p に対して，$p \leq \sqrt{n}$ であるとき，
  $p \mid n$ でないならば，n は素数である．
  - $\sqrt{n}$ 以下のどの素数でも割り切れない n は素数である．

例：$n=1999$
- $\sqrt{n}=44.7\ldots$
- 44 以下のどの素数も1999を割り切らない
- ゆえに，1999は素数である．

証明

$n \in \mathbf{N}$ が合成数ならば，素数 p が存在して，
$p \leq \sqrt{n}$　かつ $p \mid n$.

---

n を割り切る素数のうち最小のものを p とする．
$p \mid n$ だから，$q \in \mathbf{N}$ が存在して，$n=q \cdot p$.
n は合成数だから，$q>1$.
ゆえに，素数 p' が存在して，$p' \mid q$.
$p'>0$, $q>0$ だから，定理から，$p' \leq q$.
一方，$p' \mid q$, $q \mid n$ だから，$p' \mid n$.
ゆえに，p の定義から，$p \leq p'$.
したがって，$p^2 \leq pp' \leq pq = n$. すなわち，$p \leq \sqrt{n}$.

Eratosthenes の篩（ふるい）(sieve)

- 入力：$n \in \mathbf{N}$
- 出力：n 以下のすべての素数
- 手順：
  (1) 2 から n までの自然数を並べる．
  (2) 2 に○印を付け，2 以外の 2 のすべての倍数に
  ×印を付ける．
  (3) 印が付いていない最小の数を p とする．
  (4) $p \leq \sqrt{n}$ ならば，次の操作 a)，b)を繰り返す．
  a) p に○印を付け，p 以外の p のすべての倍数で，
  ×印の付いていない数に×印を付ける．
  b) 印が付いていない最小の数を p とする．
  (5) ×印が付いていない数が求める素数である．

Eratosthenes の篩（続き）

例：$n=50$
(1) 2 から n までの自然数を並べる．

	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50				

Eratosthenes の篩（続き2）

例： $n=50$

（2） 2 に○印を付け，2 以外の 2 のすべての倍数に×印を付ける．

	②	3	✕	5	✕
7	✕	9	✕	11	✕
13	✕	15	✕	17	✕
19	✕	21	✕	23	✕
25	✕	27	✕	29	✕
31	✕	33	✕	35	✕
37	✕	39	✕	41	✕
43	✕	45	✕	47	✕
49	✕				

7

Eratosthenes の篩（続き3）

例： $n=50$

（3） 印が付いていない最小の数を p とする．

	②	$p=$ 3	✕	5	✕
7	✕	9	✕	11	✕
13	✕	15	✕	17	✕
19	✕	21	✕	23	✕
25	✕	27	✕	29	✕
31	✕	33	✕	35	✕
37	✕	39	✕	41	✕
43	✕	45	✕	47	✕
49	✕				

8

Eratosthenes の篩（続き4）

例： $n=50$ $\sqrt{n}=7.2\ldots$

（4） $p\leq\sqrt{n}$ ならば，次の操作 a)，b)を繰り返す．

a) p に○印を付け，p 以外の p のすべての倍数で，×印の付いていない数に×印を付ける．

	②	$p=$ ③	✕	5	✕
7	✕	✕	✕	11	✕
13	✕	✕	✕	17	✕
19	✕	✕	✕	23	✕
25	✕	✕	✕	29	✕
31	✕	✕	✕	35	✕
37	✕	✕	✕	41	✕
43	✕	✕	✕	47	✕
49	✕				

9

Eratosthenes の篩（続き5）

例： $n=50$ $\sqrt{n}=7.2\ldots$

（4） $p\leq\sqrt{n}$ ならば，次の操作 a)，b)を繰り返す．

b) 印が付いていない最小の数を p とする．

	②	$p=$ ③	✕	$p=$ 5	✕
7	✕	✕	✕	11	✕
13	✕	✕	✕	17	✕
19	✕	✕	✕	23	✕
25	✕	✕	✕	29	✕
31	✕	✕	✕	35	✕
37	✕	✕	✕	41	✕
43	✕	✕	✕	47	✕
49	✕				

10

Eratosthenes の篩（続き6）

例： $n=50$ $\sqrt{n}=7.2\ldots$

（4） $p\leq\sqrt{n}$ ならば，次の操作 a)，b)を繰り返す．

a) p に○印を付け，p 以外の p のすべての倍数で，×印の付いていない数に×印を付ける．

	②	③	✕	$p=$ ⑤	✕
7	✕	✕	✕	11	✕
13	✕	✕	✕	17	✕
19	✕	✕	✕	23	✕
25	✕	✕	✕	29	✕
31	✕	✕	✕	35	✕
37	✕	✕	✕	41	✕
43	✕	✕	✕	47	✕
49	✕				

11

Eratosthenes の篩（続き7）

例： $n=50$ $\sqrt{n}=7.2\ldots$

（4） $p\leq\sqrt{n}$ ならば，次の操作 a)，b)を繰り返す．

b) 印が付いていない最小の数を p とする．

	②	③	✕	$p=$ ⑤	✕
$p=$ 7	✕	✕	✕	11	✕
13	✕	✕	✕	17	✕
19	✕	✕	✕	23	✕
25	✕	✕	✕	29	✕
31	✕	✕	✕	35	✕
37	✕	✕	✕	41	✕
43	✕	✕	✕	47	✕
49	✕				

12

Eratosthenes の篩（続き8）

例：$n=50$　$\sqrt{n}=7.2\ldots$

（4）$p\leq\sqrt{n}$ ならば，次の操作 a)，b)を繰り返す．

a) p に○印を付け，p 以外の p のすべての倍数で，×印の付いていない数に×印を付ける．

$p=$ ②	③	~~④~~	⑤	~~⑥~~	
13	~~14~~	15	~~16~~	17	~~18~~
19	~~20~~	21	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~				

Eratosthenes の篩（続き9）

例：$n=50$　$\sqrt{n}=7.2\ldots$

（4）$p\leq\sqrt{n}$ ならば，次の操作 a)，b)を繰り返す．

b) 印が付いていない最小の数を p とする．

$p=$ ②	③	~~④~~	⑤	~~⑥~~	
13	~~14~~	15	~~16~~	$p=$ 17	~~18~~
19	~~20~~	21	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~				

Eratosthenes の篩（続き9）

例：$n=50$　$\sqrt{n}=7.2\ldots$

（4）$p\leq\sqrt{n}$ ならば，次の操作 a)，b)を繰り返す．

②	③	~~④~~	⑤	~~⑥~~	
~~②~~	~~③~~	~~④~~	$p=$ 11	~~⑥~~	
13	~~14~~	15	~~16~~	17	~~18~~
19	~~20~~	21	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~				

Eratosthenes の篩（続き10）

例：$n=50$　$\sqrt{n}=7.2\ldots$

（5）×印が付いていない数が求める素数である．

	②	③	~~④~~	⑤	~~⑥~~
②	~~③~~	~~④~~	~~⑤~~	~~⑥~~	
13	~~14~~	15	~~16~~	17	~~18~~
19	~~20~~	21	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~				

定理

素数は無限に存在する．

証明

素数は無限に存在する．

- 素数は有限個であると仮定して，矛盾を導く．

任意の $n\in\mathbf{N}$ に対して，n より大きい素数は存在しないと仮定する．
このとき，$m=n!+1$ とおくと，$m>n$ だから，m は合成数である．
ゆえに，素数 $p(\leq n)$ が存在して，$p \mid m$．
ところが，m は 2 以上 n 以下のどの自然数で割っても 1 だけ余る．
これは矛盾．
ゆえに，n より大きい素数は存在する．
n は任意だから，素数は無限に存在する．

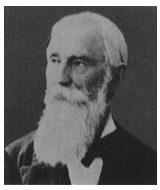
定理（素数の分布）

- Chebysev（1850年）

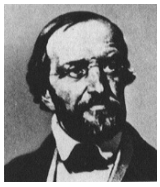
任意の実数 x（>1）に対して，$x<p<2x$ となる素数 p が存在する．

- Dirichlet の算術級数定理（1837年）

a，$n\in\mathbf{N}$ に対して，$\gcd(a, n)=1$ ならば，$p=a+kn$（$k\in\mathbf{N}$）という形の素数 p が無限に存在する．



P. L. Chebysev
（露，1821-1864）



P. G. L. Dirichlet
（露，1805-1859）

素数定理（1896年）

自然数 n より大きくない素数の個数を$\pi(n)$とすると，
十分大きな n に対して，

$$\pi(n) \fallingdotseq \frac{n}{\log_e n}$$

または，

$$\lim_{n\to\infty} \frac{\pi(n)\log_e n}{n} = 1$$

- 自然数の中に素数が含まれている割合

- $n=1000$ のとき
  - $\pi(n)=168$
  - $n/\log_e n = 144.76\ldots$
  - $\pi(n)/(n/\log_e n) \fallingdotseq 1.16$

J. Hadamard
（仏，1865-1963）

C. J. de la Vallée-Poussin
（ベルギー，1866-1963）

n	$\pi(n)/(n/\log_e n)$
1000	1.16
5000	1.14
10000	1.13
10^8	1.06

Mersenne 数（Mersenne number）

- Mersenne 数
  - $M_n=2^n-1$ （$n\in\mathbf{N}$）という形の数

例：
$M_1 = 2^1-1 = 1$
$M_2 = 2^2-1 = 3$ … 素数
$M_3 = 2^3-1 = 7$ … 素数
$M_4 = 2^4-1 = 15$
$M_5 = 2^5-1 = 31$ … 素数
$M_6 = 2^6-1 = 63$
$M_7 = 2^7-1 = 127$ … 素数
：
$M_{42,643,801}$ （12,837,064桁）（2009. 4.12，Strindmo，ノルウェー）
$M_{43,112,609}$ （12,978,189桁）（2008. 8.23，Smith，USA）
$M_{57,885,161}$ （17,425,170桁）（2013. 1.25，Cooper，USA）
$M_{74,207,281}$ （22,338,618桁）（2016. 1. 7，Cooper，USA）

M. Mersenne
（仏，1588-1648）

- 既知の Mersenne 素数は49個．
  - GIMPS（Great Internet Mersenne Prime Search）（http://www.mersenne.org/）
    - 大量のPC（CPU約120万個）で分散計算，15万人以上のボランティア
    - 1996年11月以来，Mersenne 素数15個を発見

朝日新聞 DIGITAL

過去最大の素数発見、2233万8618桁　米大学教授

ワシントン＝小林哲　2016年1月14日07時15分

新たに発見された素数

米セントラルミズーリ大は21日、1とその数自身以外では割り切れない素数を研究している同大のカーチス・クーパー教授（計算機科学）が、過去最大となる約2233万桁の素数を発見したと発表した。これまでより約500万桁大きい。

素数は無限に存在することが証明されているが、どのように出現するかは現在もわかっていない。素数は電子商取引などで使われる暗号に応用されている。大きな素数の発見は、より解読が困難な暗号の作製につながり、コンピューターによる計算技術の向上にも役立つと期待される。

クーパー教授は、世界中のコンピューターをつなげて素数を探すプロジェクト「GIMPS」のメンバー。「2●（●はn乗）－1（2をn乗して1を引いた数）」で表される「メルセンヌ数」から素数を見つける方法で素数探しを続けている。

これまでの最大は、2013年にクーパー教授が見つけたn＝57885161（1742万5170桁）。今回はn＝74207281が素数であることを約800台のコンピューターを駆使した計算で突き止めたという。3で始まり1で終わる2233万8618桁の数字だ。稼働させていた計算プログラムは、昨年9月17日に新たな素数を見つけていたが、関係者が発見に気付いたのは今年1月7日だったという。

この大きさの文字で、今回見つかった約2233万桁の素数を印刷するとしたら、A4判の紙が1万枚必要になる

朝日新聞
2016. 1.24

定理

$n\in\mathbf{N}$ に対して，$M_n=2^n-1$ が素数ならば，
n は素数である．

例：
$M_2 = 2^2-1 = 3$ … 素数
$M_3 = 2^3-1 = 7$ … 素数
$M_5 = 2^5-1 = 31$ … 素数
$M_7 = 2^7-1 = 127$ … 素数

- n が素数であっても，M_n が素数であるとは限らない．
  - $M_{11} = 2^{11}-1 = 2047 = 23\cdot 89$

証明

$n\in\mathbf{N}$ に対して，$M_n=2^n-1$ が素数ならば，
n は素数である．
- n は合成数であると仮定して，矛盾を導く．

---

n は合成数であると仮定する．
このとき，$n=k\cdot s$（$1<k<n$，k，$s\in\mathbf{N}$）とおける．
ゆえに，$2^n-1 = (2^k)^s-1$
$= (2^k-1)(2^{k(s-1)}+2^{k(s-2)}+\ldots+2^k+1)$
$2^{k(s-1)}+2^{k(s-2)}+\ldots+2^k+1 > 1$，$2^k-1>1$ だから，
2^n-1 は合成数となる．
これは矛盾．
ゆえに，n は素数である．

Fermat 数（Fermat number）

P. de Fermat
（仏，1601-1665）

- Fermat 数
  - $F_n = 2^{2^n}+1$ （$n \in \mathbf{N}_0$）という形の数

例：$F_0 = 2^{2^0}+1 =$ 3 … 素数
$F_1 = 2^{2^1}+1 =$ 5 … 素数
$F_2 = 2^{2^2}+1 =$ 17 … 素数
$F_3 = 2^{2^3}+1 =$ 257 … 素数
$F_4 = 2^{2^4}+1 =$ 65,537 … 素数
$F_5 = 2^{2^5}+1 =$ 4,294,967,297＝641・6,700,417（Euler，1732年）

- F_0，…，F_4 以外の Fermat 素数は知られていない．
- F_5，…，F_{11} の素因数分解は知られている．
  - F_6（1880年），F_7（1970年），F_8（1980年）F_9（1990年），F_{10}（1995年），F_{11}（1988年）
- 素因数が一つも知られていない最小の Fermat 合成数は F_{14}
  - http://www.fermatsearch.org/

25

定理

$n \in \mathbf{N}$ に対して，2^n+1 が素数ならば，
$m \in \mathbf{N}_0$ が存在して，$n = 2^m$．

26

証明

$n \in \mathbf{N}$ に対して，2^n+1 が素数ならば，
$m \in \mathbf{N}_0$ が存在して，$n = 2^m$．

2^n+1 は素数であるとする．
ここで，$n = k \cdot s$（$k = 2^m$，$m \geq 0$，s は奇数）とおける．
- $1=2^0\cdot1$，$2=2^1\cdot1$，$3=2^0\cdot3$，$4=2^2\cdot1$，$5=2^0\cdot5$，$6=2^1\cdot3$，…

ゆえに，$2^n+1 = (2^k)^s+1$
$= (2^k+1)(2^{k(s-1)} - 2^{k(s-2)} + \ldots - 2^k + 1)$
$2^k+1 > 1$，かつ，2^n+1 は素数だから，$2^n+1 = 2^k+1$．
ゆえに，$n = k = 2^m$．

27

定理

任意の m，$n \in \mathbf{N}$ と任意の素数 p に対して，
$p \mid mn$ ならば，$p \mid m$ または $p \mid n$．

28

証明

任意の m，$n \in \mathbf{N}$ と任意の素数 p に対して，
$p \mid mn$ ならば，$p \mid m$ または $p \mid n$．

$p \mid mn$ と仮定する．
さらに，$p \mid m$，$p \mid n$ のいずれでもないと仮定する．
このとき，$\gcd(p, m) = 1$．
ゆえに，定理から，$p \mid n$．
- 任意の p，m，$n \in \mathbf{Z}$ に対して，$\gcd(p, m) = 1$ かつ $p \mid mn$ ならば，$p \mid n$．

これは矛盾．
ゆえに，$p \mid m$ または $p \mid n$．

29

素因数分解の一意性定理

（初等整数論の基本定理）
任意の $n \in \mathbf{N}$ は素数 p_1，p_2，…，p_r（$p_1 \leq p_2 \leq \ldots \leq p_r$）に対して，$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ の形（素数の積の形）で一意に表せる．

- 自然数は素数の積の形で表すことができ，その表現は素数の順を除けば一意（ただ1通りだけ）である．

30

素因数分解

- $n \in \mathbf{N}$ の素因数分解（prime decomposition）
  - 素数 $p_1, p_2, \ldots, p_r$ に対して，$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$
  - 異なる素数 $p_1, p_2, \ldots, p_s$ と $e_1, e_2, \ldots, e_s \in \mathbf{N}_0$ に対して，$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$

例：　$p_1=2,\ p_2=3,\ p_3=5,\ p_4=7$
- $60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0$

- $n \in \mathbf{N}$ の素因数（prime divisior）
  - n の約数である素数

証明

任意の $n \in \mathbf{N}$ は素数 $p_1, p_2, \ldots, p_r$（$p_1 \leq p_2 \leq \ldots \leq p_r$）に対して，$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ の形（素数の積の形）で一意に表せる．
- a）「n は素数の積の形で表せる」を示す．
- b）「n は素数の積の形で一意に表せる」を示す．

---

a-1）　n が素数のとき．
　　$r=1$，$n=p_1$となるから，明らか．

a-2）　n が合成数のとき．
　　n に関する帰納法により示す．

証明（続き）

任意の $n \in \mathbf{N}$ は素数 $p_1, p_2, \ldots, p_r$（$p_1 \leq p_2 \leq \ldots \leq p_r$）に対して，$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ の形（素数の積の形）で一意に表せる．
- a）「$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ の形（素数の積の形）で表せる」を示す．

---

a-2）　n が合成数のとき．n に関する帰納法により示す．
　そこで，$n' < n$ となる任意の $n' \in \mathbf{N}$ に対して，n'は素数の積の形で表せると仮定する（帰納法の仮定）．
　n は合成数だから，定理から，素数 $p \leq \sqrt{n} < n$ が存在して，$p \mid n$．
　ゆえに，$k \in \mathbf{N}$ が存在して，$n = k \cdot p$．
　$k < n$ だから，帰納法の仮定より，$k = p'_1 \cdot p'_2 \cdot \ldots \cdot p'_s$とおける．
　ゆえに，$n = k \cdot p = p'_1 \cdot p'_2 \cdot \ldots \cdot p'_s \cdot p$．
　$p'_1,\ p'_2,\ \ldots,\ p'_s,\ p$ を小さい順に並べた列を $p_1, p_2, \ldots, p_r$とおけば，
　$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$（$p_1 \leq p_2 \leq \ldots \leq p_r$）．

証明（続き2）

任意の $n \in \mathbf{N}$ は素数 $p_1, p_2, \ldots, p_r$（$p_1 \leq p_2 \leq \ldots \leq p_r$）に対して，$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ の形（素数の積の形）で一意に表せる．
- b）「n は素数の積の形で一意に表せる」を示す．

---

b）　$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$（$p_1 \leq p_2 \leq \ldots \leq p_r$），かつ，
　$n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$（$q_1 \leq q_2 \leq \ldots \leq q_s$）と仮定する．
　n に関する帰納法により示す．
　そこで，$n' < n$ となる任意の $n' \in \mathbf{N}$ に対して，n' は素数の積の形で一意に表せると仮定する（帰納法の仮定）．

b-1）　$p_1 = q_1$ のとき．
　b-1-1）$r=s=1$ のとき．$n = p_1 = q_1$ だから，n は素数の積の形で一意に表せる．
　b-1-2）$r>1$ または $s>1$ のとき．　$n' = p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s \in \mathbf{N}$とおく．
　　このとき，$n' < n$ であるが，n' は素数の積の形で一意に表せない．
　　これは帰納法の仮定に矛盾．
　　ゆえに，n は素数の積の形で一意に表せる．

証明（続き3）

b）　$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$（$p_1 \leq p_2 \leq \ldots \leq p_r$），かつ，
　$n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$（$q_1 \leq q_2 \leq \ldots \leq q_s$）と仮定する．
　$n' < n$ となる任意の $n' \in \mathbf{N}$ に対して，n' は素数の積の形で一意に表せると仮定する．

---

b-2）　$p_1 < q_1$ のとき．
　除法定理から，$u,\ v \in \mathbf{N}$ が存在して，$q_1 = u \cdot p_1 + v$　$(0 \leq v < p_1)$．
　q_1 は素数だから，$v > 0$．
　このとき，$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = (u \cdot p_1 + v) \cdot q_2 \cdot \ldots \cdot q_s$ だから，
　$p_1(p_2 \cdot \ldots \cdot p_r - u \cdot q_2 \cdot \ldots \cdot q_s) = v \cdot q_2 \cdot \ldots \cdot q_s$．
　両辺を m（$\in \mathbf{N}$）とおくと，$m > 0$．
　このとき，p_1 は左辺の素因数分解における m の素因数である．
　一方，$v < p_1 < q_1 \leq q_2 \leq \ldots \leq q_s$だから，$p_1$ は右辺の素因数分解における m の素因数でない．
　したがって，m は素数の積の形で一意に表せない．
　ところが，$0 < v < q_1$ だから，$m = v \cdot q_2 \cdot \ldots \cdot q_s < q_1 \cdot q_2 \cdot \ldots \cdot q_s = n$．
　これは帰納法の仮定に矛盾．ゆえに，n は素数の積の形で一意に表せる．

b-3）　$p_1 > q_1$ のとき．同様に証明できる．

定理

$m,\ n \in \mathbf{N}$ の素因数分解をそれぞれ
$$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$
$$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_r^{h_r}$$
とすると，$m \mid n$ であるとき，かつそのときに限り，
任意の i（$1 \leq i \leq r$）に対して，$e_i \leq h_i$．

例：　$10 = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0$
　　$42 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1$
　　$60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0$
- $10 \mid 60$
  - $1 \leq 2,\ 0 \leq 1,\ 1 \leq 1,\ 0 \leq 0$
- $42 \mid 60$ でない
  - $1 \leq 2,\ 0 \leq 1,\ 0 \leq 1,\ 1 \not\leq 0$

証明

$m, n \in \mathbf{N}$ の素因数分解をそれぞれ $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$,
$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_r^{h_r}$ とすると，$m \mid n$ であるとき，かつそのときに限り，
任意の i $(1 \leq i \leq r)$ に対して，$e_i \leq h_i$.

- a) 「$m \mid n$ ならば，任意の i に対して $e_i \leq h_i$ 」を示す.
- b) 「任意の i に対して $e_i \leq h_i$ ならば，$m \mid n$ 」を示す.
- a) 「$m \mid n$ 」を仮定して，「任意の i に対して $e_i \leq h_i$ 」を示す.
  - 「ある i に対して $e_i > h_i$ 」を仮定して，矛盾を導く.

$d = p_1^{h_1 - e_1} \cdot p_2^{h_2 - e_2} \cdot \ldots \cdot p_r^{h_r - e_r}$ とおく.

a) $m \mid n$ とする. このとき，$n / m = d \in \mathbf{Z}$.
ある i $(1 \leq i \leq r)$ に対して，$e_i > h_i$ と仮定する.
このとき，$d \cdot p_i^{e_i - h_i} = p_1^{h_1 - e_1} \cdot \ldots \cdot p_{i-1}^{h_{i-1} - e_{i-1}} \cdot p_{i+1}^{h_{i+1} - e_{i+1}} \cdot \ldots \cdot p_r^{h_r - e_r}$.
ここで，両辺とも整数である.
$e_i - h_i > 0$ だから，p_i は左辺の素因数であるが，右辺の素因数ではない.
すなわち，同じ整数が素数の積の形に一意に表せなく，矛盾.
ゆえに，任意の i に対して，$e_i \leq h_i$.

証明（続き）

$m, n \in \mathbf{N}$ の素因数分解をそれぞれ $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$,
$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_r^{h_r}$ とすると，$m \mid n$ であるとき，かつそのときに限り，
任意の i $(1 \leq i \leq r)$ に対して，$e_i \leq h_i$.

- b) 「任意の i に対して，$e_i \leq h_i$ ならば，$m \mid n$ 」を示す.

$d = p_1^{h_1 - e_1} \cdot p_2^{h_2 - e_2} \cdot \ldots \cdot p_r^{h_r - e_r}$ とおく.

b) 任意の i $(1 \leq i \leq r)$ に対して，$e_i \leq h_i$ とする.
$h_i - e_i \in \mathbf{N}_0$ だから，$d \in \mathbf{Z}$.
ゆえに，$n = d \cdot m$.
したがって，$m \mid n$.

定理

$m, n \in \mathbf{N}$ の素因数分解をそれぞれ

$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$

$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_r^{h_r}$

とすると，

$\mathrm{lcm}(m, n) = p_1^{\max\{e_1, h_1\}} \cdot p_2^{\max\{e_2, h_2\}} \cdot \ldots \cdot p_r^{\max\{e_r, h_r\}}$

$\gcd(m, n) = p_1^{\min\{e_1, h_1\}} \cdot p_2^{\min\{e_2, h_2\}} \cdot \ldots \cdot p_r^{\min\{e_r, h_r\}}$

例：$60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0$
$42 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1$

- $\mathrm{lcm}(60, 42) = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 420$
- $\gcd(60, 42) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 6$

証明

$m, n \in \mathbf{N}$ の素因数分解をそれぞれ $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$,
$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_r^{h_r}$ とすると，
$\mathrm{lcm}(m, n) = p_1^{\max\{e_1, h_1\}} \cdot p_2^{\max\{e_2, h_2\}} \cdot \ldots \cdot p_r^{\max\{e_r, h_r\}}$

$p_1^{\max\{e_1, h_1\}} \cdot p_2^{\max\{e_2, h_2\}} \cdot \ldots \cdot p_r^{\max\{e_r, h_r\}} = c$ とおく.

- 「$c = \mathrm{lcm}(m, n)$」を示す.
  - a) 「c は m, n の公倍数である」を示す.
  - b) 「m, n の任意の公倍数 c' に対して，$c \mid c'$」を示す.

---

a) 任意の i $(1 \leq i \leq r)$ に対して，$e_i, h_i \leq \max\{e_i, h_i\}$.
ゆえに，定理から，$m \mid c$, かつ，$n \mid c$.
したがって，c は m, n の公倍数である.

証明（続き）

$m, n \in \mathbf{N}$ の素因数分解をそれぞれ $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$,
$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_r^{h_r}$ とすると，
$\mathrm{lcm}(m, n) = p_1^{\max\{e_1, h_1\}} \cdot p_2^{\max\{e_2, h_2\}} \cdot \ldots \cdot p_r^{\max\{e_r, h_r\}}$

$p_1^{\max\{e_1, h_1\}} \cdot p_2^{\max\{e_2, h_2\}} \cdot \ldots \cdot p_r^{\max\{e_r, h_r\}} = c$ とおく.

- 「$c = \mathrm{lcm}(m, n)$」を示す.
  - b) 「m, n の任意の公倍数 c' に対して，$c \mid c'$」を示す.

---

b) m, n の任意の公倍数を $c' = p_1^{f_1} \cdot p_2^{f_2} \cdot \ldots \cdot p_r^{f_r}$ とする.
$m \mid c'$, $n \mid c'$ だから，任意の i $(1 \leq i \leq r)$ に対して，$e_i \leq f_i$, $h_i \leq f_i$.
ゆえに，$\max\{e_i, h_i\} \leq f_i$.
したがって，定理から，$c \mid c'$.
すなわち，$c = \mathrm{lcm}(m, n)$.
同様に，$\gcd(m, n) = p_1^{\min\{e_1, h_1\}} \cdot p_2^{\min\{e_2, h_2\}} \cdot \ldots \cdot p_r^{\min\{e_r, h_r\}}$ を示せる.

まとめ

- 今回の講義
  - 素数
- 中間試験（6／9（木）　1限）
  - 試験範囲：　講義1～5（集合論）
  - 持込み不可
  - 教室：　演習時と同じ
    - 1人ずつ空けて着席すること
    - 学生証を机上に置くこと
  - 演習問題解答例（pdf 版）
    - http://www.kl.i.is.nagoya-u.ac.jp/~toyama/lecture/risan16/
- 次回の講義（6／9（木）　2限）
  - 1 次不定方程式（教科書　pp.117-127）
  - 合同式（教科書　pp.127-131）
- 今回の演習
  - 関数