第1章　整数の基本的性質

1.1　約数、倍数、最大公約数、ユークリッドの互除法

まず、整数の中で、加法、減法、乗法が自由に行えるが、除法は必ずしもできないことを注意しておく。

定理 1.1.1 a を整数、b を正の整数とするとき、

$$a = qb + r, \qquad (0 \leqq r < b)$$

を満たす整数の組 $q,\ r$ が存在し、一意的に定まる。

この定理をもとに次の定理が証明される。

定理 1.1.2 a を整数、b を 0 でない整数とするとき、

$$a = qb + r, \qquad (0 \leqq r < |b|)$$

を満たす整数の組 $q,\ r$ が存在し、一意的に定まる。

上の定理において、$r = 0$ のとき、a は b で割り切れるといい、q をその商という。このとき

$$b \mid a$$

と書き、a を b の倍数、b を a の約数という。
また、$r > 0$ のときは a は b で割り切れないといい、

$$b \nmid a$$

と書く。q はやはり商といわれ、r を、a を b で割った剰余（余り）という。この剰余を $\mathrm{Mod}(a, b)$ または $a \bmod b$ で表すと便利です。

定理 1.1.3 $c_1,\ c_2, \ldots,\ c_n$ を任意の整数とするとき、$b \mid a_1,\ b \mid a_2, \ldots,\ b \mid a_n$ ならば $b \mid c_1a_1 + c_2a_2 + \cdots + c_na_n$ である。

定理 1.1.4

$$c \mid b, \quad b \mid a \ \Rightarrow \ c \mid a$$

ここで、任意の非零整数は 0 の約数で、0 だけが 0 の倍数であることを注意しておく。いくつかの整数 $a,\ b, \ldots$ に共通の約数をそれらの公約数という。これらの公約数の最大のものをそれらの整数の最大公約数 (greatest common divisor, G.C.D.) といい、$(a, b, \ldots)$ で表す。$(a, b) = 1$ のとき、a と b は互いに素であるという。

また、いくつかの整数 $a,\ b, \ldots$ に共通の倍数をそれらの公倍数という。0 はもちろん公倍数である。$a,\ b, \ldots$ のうちどれかが 0 ならば、公倍数は 0 のみである。$a,\ b, \ldots$ のどれも 0 ではないとするとあきらかに 0 以外の正の公倍数がある。逆に 0 以外の正の公倍数があるならば、$a,\ b, \ldots$ のどれも 0 ではないことになる。これらの正の公倍数の最小のものをそれらの整数の最小公倍数 (least common multiple, L.C.M.) といい、$\{a, b, \ldots\}$ で表す。どれかが 0 である場合についても最小公倍数を定めておくと都合のよい場合があるので、この場合については 0 としておく。

定理 1.1.5 $a,\ b, \ldots$ のどれも 0 でないとして、その任意の公倍数 m はそれらの最小公倍数 ℓ の倍数である。

証明 $\ell > 0$ としてよい。

$$m = q\ell + r \qquad (0 \leqq r < \ell)$$

が成り立つ。ところが、$r = m - q\ell$ より、r が $a,\ b, \ldots$ の公倍数となる。これは ℓ の最小性から、$r = 0$ を意味する。 □

定理 1.1.6 $a,\ b, \ldots$ の任意の公約数 d はそれらの最大公約数 g の約数である。

証明 まず、次の同等性に注目

$$A \mid B \qquad \Leftrightarrow \quad \{A, B\} = B. \qquad (0 < A \leqq B)$$

これは明らかでしょう。$\{d, g\} = \ell$ とする。$d \mid a,\ g \mid a$ より、a は $d,\ g$ の公倍数となる。定理 1.1.5 によって、$\ell \mid a$ がえられる。同様にして $\ell \mid b,\ \ell \mid c, \ldots$ が得られる。すなわち、ℓ は $a,\ b, \ldots$ の公約数。g の最大性から $g \geqq \ell$ は当然である。一方、ℓ の定義によって $g \leqq \ell$ であるから、$g = \ell$. □

定理 1.1.7 整数 $a,\ b$ に対して、$a^2 + b^2 \neq 0$ ならば、$(a, b) = g,\ \{a, b\} = \ell$ とすると

$$|ab| = g\ell.$$

証明　$\ell = 0$ ならば $ab = 0$ であるから定理は成り立つ。$\ell > 0$ かつ $a,\ b > 0$ とする。g の最大性から $a = ga',\ b = gb'$ とおくと $(a', b') = 1$ となる。$ga'b' = m$ とおくとあきらかに、m は $a,\ b$ の公倍数であるから、定理 1.1.5 により、$\ell \mid m$ 。$m = n\ell$ とおくと

$$n\ell = ab' = a'b$$

しかし、$\{a, b\} = \ell$ であるから $\ell = aa'' = bb''$ とおけば上の関係から

$$a''n = b', \quad b''n = a'$$

となるが、$(a', b') = 1$ より $n = 1$ でなければならない。したがって $\ell = m$ となり、$ga'b' = \ell$ 。両辺に g を掛けて $ga'gb' = g\ell$ 、つまり、$ab = g\ell$ が証明された。　□

二つの重要な定理を証明しよう。

定理 1.1.8　正の整数 $a,\ b$ に対して $(a, b) = 1$ かつ $a \mid bc$ ならば $a \mid c$ 。

証明　定理 1.1.7 より、$(a, b)\{a, b\} = ab$ であるが、仮定によって、$(a, b) = 1$ であるから、$\{a, b\} = ab$ となる。一方、$a \mid bc,\ b \mid bc$ より、bc は $a,\ b$ の公倍数であるから、定理 1.1.5 によって、$\{a, b\} \mid bc$ であるが $\{a, b\} = ab$ であるから、$ab \mid bc$ すなわち $a \mid c$ が得られる。　□

定理 1.1.9 (ユークリッドの互除法)　$a \geqq b > 0$ なる二つの整数 $a,\ b$ に対して

$$a = qb + r \qquad (0 \leqq r < b)$$

とおくとき、$(a, b) = (b, r)$ が成り立つ。

証明　$r = a - qb$ より、$(a, b) \mid r$ であるから、(a, b) は r と b の公約数となり、$(a, b) \leqq (b, r)$ を得る。また、$a = qb + r$ より、$(b, r) \mid a$ であるから、(b, r) は a と b の公約数となり、$(b, r) \leqq (a, b)$ を得る。二つの不等式を合わせて $(a, b) = (b, r)$ が得られる。　□

この定理 1.1.9 を用いて、二つの整数の G.C.D. を求める。$a \geqq b > 0$ なる二つの整数 $a,\ b$ を考えよう。$d_0 = a,\ d_1 = b$ として $d_2 = \mathrm{Mod}(d_0, d_1)$ とする。これらを初期値として $d_{n+1} = \mathrm{Mod}(d_{n-1}, d_n)$ が定義される。このとき、$d_0 > d_1 > d_2 > d_3 > \cdots$ であるから、ある n について $d_n > 0,\ d_{n+1} = 0$ が成り立つ。これらの式を列挙して

みよう。

$$\begin{aligned} d_0 &= q_1 d_1 + d_2 \\ d_1 &= q_2 d_2 + d_3 \\ d_2 &= q_3 d_3 + d_4 \\ &\vdots \\ d_{n-1} &= q_n d_n + d_{n+1} \ = \ q_n d_n + 0 \end{aligned}$$

定理 1.1.9 より、次の一連の等式が成り立つ。

$$(a,b) = (d_0,d_1) = (d_1,d_2) = (d_2,d_3) = \cdots = (d_{n-1},d_n) = (d_n,d_{n+1}) = (d_n,0) = d_n.$$

これで、(a,b) を求める方法が理解されるであろう。

問題　$(4741,7327)$ および $\{4741,7327\}$ を求めよ。

1.2　いくつかの命題と例題

定理 1.2.1 $a,\ b$ をともには 0 でない整数とする。

$$L = ax + by \qquad (x,y \text{ はあらゆる整数})$$

の形の整数の集合のうち、最小の正の整数を $d = ax_0 + by_0$ とおくとき、$d = (a,b)$ が成り立つ。また、この集合の元はすべて d の倍数である。

証明　まず、後半を示そう。L の形の任意の整数を $ax+by$ とする。これを d で割ってみる：

$$ax + by = q(ax_0 + by_0) + r \qquad (0 \leqq r < d)$$

これから

$$r = a(x - qx_0) + b(y - qy_0)$$

を得るが、これはまた L の形の整数である。d の最小性から $r = 0$ でなければならない。これで後半が示された。

後半の部分から、$d \mid a\cdot 1 + b\cdot 0,\ d \mid a\cdot 0 + b\cdot 1$ すなわち $d \mid a,\ d \mid b$ となるので、$d \leqq (a,b)$ を得る。一方、その定義によって $(a,b) \mid a,\ (a,b) \mid b$ より、$(a,b) \mid ax_0 + by_0$ であるから、$(a,b) \mid d$ を得る。これは $d \geqq (a,b)$ を意味する。故に $d = (a,b)$ が成り立つ。　□

この定理から次のキワメテ重要な次の定理が得られるのであるよ。

定理 1.2.2 二つの整数 $a,\ b$ について $(a,b)=d$ ならば $au+bv=d$ を満たす整数の組 (u,v) が存在する。とくに $(a,b)=1$ のとき、すなわち a と b が互いに素であるとき、$au+bv=1$ を満たす組 $u,\ v$ が存在する。また，逆に $au+bv=1$ を満たす $u,\ v$ が存在するならば $(a,b)=1$ ，すなわち $a,\ b$ は互いに素である.

二つの整数 $a,\ b$ について $au+bv=(a,b)$ を満たす $u,\ v$ を見つけるにはユークリッドの互除法が有効である.

問題 二つの整数 $a=3546,\ b=53401$ について、$au+bv=(a,b)$ を満たす組 (u,v) を求めよ。

定理 1.2.3 $a,\ b$ について $(a,b)=1$ ならば

$$a \mid N \quad \text{かつ} \quad b \mid N \quad \Leftrightarrow ab \mid N.$$

証明 定理 1.2.2 と仮定により

$$ax+by=1$$

を満たす組 (x,y) が存在する。両辺に N を掛けると

$$aNx+bN=N$$

この式と仮定 $a \mid N$ かつ $b \mid N$ によって $ab \mid N$ を得る。 □

問題 連続 3 整数の積は 6 の倍数であることを示せ。

問題 n が 1 より大きい奇数のとき、n^3-n は 24 の倍数であることを示せ。

定理 1.2.4 $(a,c)=1,\ d \mid c$ ならば $(a,d)=1$.

証明 仮定と定理 1.2.2 により、$au+cv=1$ を満たす組 (u,v) が存在する。また、仮定によって $c=kd$ と書けるから、関係式 $au+dkv=1$ と書ける。これはすなわち $(a,d)=1$ を意味するのじゃ。 □

定理 1.2.5 $(a,c)=1,\ (b,c)=1$ ならば $(ab,c)=1$ である。

証明 仮定によって $au+cv=1,\ bx+cy=1$ を満たす二つの組 $(u,v),\ (x,y)$ が存在する。これらの式を掛け合わせて

$$ab(ux)+c(bvx+auy+cvy)=1$$

を得る。つまり、$(ab,c)=1$ 。 □

問題 x に関する 2 次式が x のある連続 3 整数に対して整数値をとるならば、この 2 次式はすべての整数に対して整数値をとることを示せ。

1.3 素数に関するいくつかの話題

定義 1.3.1 2 以上の自然数 n がその約数として、n と 1 のみをもつとき、n は**素数**であるという。また、2 以上の自然数 n が n と 1 以外に約数をもつとき、n は**合成数**であるという。1 は素数でも合成数でもない。

定理 1.3.1 任意の 2 以上の自然数は素数を約数にもつ。

証明 2 はそれ自身素数であるから、素数を約数にもつ。2 以上で k $(k \geqq 2)$ 以下の自然数に対して定理が成り立つと仮定する。$n = k + 1$ を考える。n が素数ならば、n に対して定理がなりたつ。n が合成数で $n = ab$ $(a, b > 1)$ とすると $a \leqq k$ または $b \leqq k$ であるから、仮定によって n に対して定理が成り立つ。 □

定理 1.3.2 素数は無限に存在する。

証明 素数が有限集合 $\{2,\ 3,\ \cdots, p_n\}$ であるとする.

$$M = 2 \cdot 3 \cdot 5 \cdots p_n + 1$$

とおくと，M はどの素数で割っても 1 余る．これは前定理に矛盾する. □

定理 1.3.3 p が素数で、二つの整数 $a,\ b$ に対して $p \mid ab$ ならば $p \mid a$ または $p \mid b$ である。

証明 $p \nmid a$ とすると $(p, a) = 1$ であるから定理 1.2.2 によって、$pu + av = 1$ を満たす整数の組 (u, v) が存在する。両辺に b を掛けると $pbu + abv = b$ となるが、この左辺は仮定によって p で割りきれる。従って、その右辺も p で割りきれる。 □

ところで、素数はどの程度であらわれるのであろうか？

定理 1.3.4 (素数定理) 自然数 n に対して n 以下の素数の個数を $\pi(n)$ で表すとき

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

が成立する。

この定理の証明は難しいので省略させて頂きます。

定理 1.3.5 2 以上の自然数は有限個の素数のべきの積として表され、その表現は順序を除いて一意である。すなわち

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t} \qquad (p_i,\ q_j \text{ は素数で小さい順})$$

ならば、$s = t$ かつすべての i について $p_i = q_i$ かつ $\alpha_i = \beta_i$ である。

定義 1.3.2 自然数 n を $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ のように素数のべきの積に表したものを n の**素因数分解**という。

例題 1.3.1 自然数 n の素因数分解を $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ とするとき、n のすべての約数の個数 $\tau(n)$ は

$$\tau(n) = (1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_s) = \prod_{i=1}^{s}(1+\alpha_i)$$

である。

例題 1.3.2 上の例題の n について、そのすべての約数の和 $\sigma(n)$ は

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}$$

である。また、$(n,m) = 1$ ならば $\sigma(nm) = \sigma(n)\sigma(m)$ である。

定義 1.3.3 $\sigma(n) = 2n$ となる n を**完全数**という。

定理 1.3.6 $a = 2^{n-1}(2^n - 1)$ は $2^n - 1$ が素数ならば完全数である。偶数の完全数はこの形の自然数にかぎる。

証明　a が上の形をとるとすると

$$\begin{aligned} \sigma(a) &= \frac{2^n-1}{2-1}\cdot\frac{(2^n-1)^2-1}{(2^n-1)-1} \\ &= (2^n-1)((2^n-1)+1) \ = \ 2^n(2^n-1) \end{aligned}$$

したがって、$\sigma(a) = 2\cdot 2^{n-1}(2^n-1) = 2a$ すなわち、a は完全数である。

次に、a を偶数の完全数とする。このとき、$a = 2^{n-1}b$ (b は奇数) と書ける。$(2,b) = 1$ より、

$$\sigma(a) = \sigma(2^{n-1})\sigma(b) = 2a.$$

故に

$$\frac{2^n-1}{2-1}\sigma(b) = 2\cdot 2^{n-1}b.$$

よって

$$\sigma(b) = \frac{2^n b}{2^n-1} = b + \frac{b}{2^n-1}$$

これは明らかに

$$\frac{b}{2^n-1} = 1$$

を意味し、さらに b はその約数として自分自身と 1 しか持たないことになる。よって、b は素数で $b = 2^n - 1$ となる。 □

さて、ここでひとつの記号を導入する。任意の実数 x に対して

$$[x] \stackrel{\text{def.}}{=} \text{the greatest integer not larger than } x$$

と定義する。

定理 1.3.7 $n!$ の素因数分解において素数 p のべき指数は

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots = \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$$

である。

証明 $2, 3, \ldots, n$ のいずれかの素因数分解に現れる素数の集合を $D = \{p_1\, p_2, \ldots, p_M\}$ とする。このとき、任意の k $(2 \leqq k \leqq n)$ に対して、$k = \prod_{i=1}^{M} p_i^{a_{ki}}$ と書ける。証明することは、各 k に対して、$n!$ に含まれる p_j の最大べき指数 $\sum_{k=1}^{n} a_{kj}$ が上の左辺において、p の代わりに p_j で置き換えた式に等しいことである。そのために、j を固定して、$\sum_{k=1}^{n} a_{kj}$ を書き換える。

$$\sum_{k=1}^{n} a_{kj} = \sum_{m=1}^{\infty}\sum_{k:a_{kj}=m} a_{kj} = \sum_{m=1}^{\infty}\sum_{k:a_{kj}=m} m.$$

ところで、各 m に対して

$$\sum_{k:a_{kj}=m} m = m\left\{\left[\frac{n}{p_j^m}\right] - \left[\frac{n}{p_j^{m+1}}\right]\right\}$$

であるから

$$\begin{aligned}\sum_{k=1}^{n} a_{kj} &= \sum_{m=1}^{\infty} m\left\{\left[\frac{n}{p_j^m}\right]-\left[\frac{n}{p_j^{m+1}}\right]\right\}\\ &= \sum_{m=1}^{\infty}\left[\frac{n}{p_j^m}\right].\end{aligned}$$

□

例題 1.3.3 n 個の連続整数の積 $m(m+1)\cdots(m+n-1)$ は $n!$ で割り切れる。

証明 任意の素数 p に対して

$$\left[\frac{m+n-1}{p^\mu}\right] \geqq \left[\frac{m-1}{p^\mu}\right]+\left[\frac{n}{p^\mu}\right] \qquad (\mu=1,2,3,\ldots)$$

であるから

$$\sum_{\mu=1}^{\infty}\left[\frac{m+n-1}{p^\mu}\right]-\sum_{\mu=1}^{\infty}\left[\frac{m-1}{p^\mu}\right] \geqq \sum_{\mu=1}^{\infty}\left[\frac{n}{p^\mu}\right].$$

これは、任意の素数 p について、$m(m+1)\cdots(m+n-1)$ に含まれる最高べき指数が $n!$ に含まれる最高べき指数より小さくないことを示しており、

$$n! \mid m(m+1)\cdots(m+n-1)$$

となる。 □

第2章　計算量、初等整数論

2.1　計算量入門

自然数 $n\ (\neq 0)$ の b 進法表現を

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \quad (0 \leqq \forall j \leqq k,\ 0 \leqq a_j < b, \quad a_k \neq 0)$$

とすると、$b^k \leqq n < b^{k+1}$ より、$k \leqq \log_b n < k+1$ となる．

定理 2.1.1 自然数 $n\ (\neq 0)$ の b 進法表現における桁数は $\lfloor \log_b n \rfloor + 1$ である．

自然数 $n\ (\neq 0)$ が b 進法表現によって

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \quad (0 \leqq \forall j \leqq k,\ 0 \leqq a_j < b, \quad a_k \neq 0)$$

と表されるとき、これを

$$(a_k a_{k-1} \cdots a_1 a_0)_b \qquad n = 0 \text{ の場合は} \quad (0)_b$$

と表す．$b = 2$ または $b = 10$ の場合は簡単に

$$a_k a_{k-1} \cdots a_1 a_0 \qquad n = 0 \text{ の場合は} \quad 0$$

で表す．これでは10進法か2進法かはっきりしないではないかと文句が出そうであるが、それは前後の文脈から判断してもらいたいものである．

以下、自然数を主に2進法で考えることにする．自然数 a の2進法表現桁数 (k) を $k - \mathrm{bit}$ という．二つの自然数 $m = a_k a_{k-1} \cdots a_1 a_0$ と $n = b_j b_{j-1} \cdots b_1 b_0$ の和を計算することを吟味しよう．$k \neq j$ のときは0 を付け加えて、同じ桁数（便宜主義と怒らないでほしい）にしておく．最初、キャリーのレジスターには0 が入っているものとする．キャリーのレジスターの値を c で表す．また、各桁の値のメモリーがある．位の低い順に $d_0,\ d_1, \ldots$ とする．和を計算するには次の手続きを小さい s から繰り返すことになる．

- $a_s,\ b_s,\ c$ のうち 1 がゼロ個の場合、$d_s = 0$ とする．

- $a_s,\ b_s,\ c$ のうち 1 が 1 個の場合、$d_s = 1$ とする.
- $a_s,\ b_s,\ c$ のうち 1 が 2 個の場合、$d_s = 0$ とし、$c = 1$ とする.
- $a_s,\ b_s,\ c$ のうち 1 が 3 個の場合、$d_s = 1$ とし、$c = 1$ とする.

各桁においてこれらの手続きのうちのいずれか一つを行うことになる．これを行うことを **1 bit-operation** といい、これを計算の単位とする.

計算機におけるあらゆる計算はこの bit-operation の積み重ねなので、ある計算において掛かる時間の長さ、あるいは計算の困難さをその計算に含まれる bit-operation の量で計るのは妥当であろう．bit-operation の量を **number of bit-operations (n.b.o.)** ということにする.

定理 2.1.2 $m,\ n$ をそれぞれ 2 進法で s 桁, r 桁 の整数とするとき

(1) $\mathrm{Time}(\text{addition of } m \text{ and } n) = \mathrm{Time}(s - \mathrm{bit} + r - \mathrm{bit}) = \max(s,\ r)$

(2) $\mathrm{Time}(\text{multiplying } m \text{ by } n) = \mathrm{Time}(s - \mathrm{bit} \times r - \mathrm{bit}) = O(sr)$

(3) $\mathrm{Time}(\text{substracting } n \text{ from } m) = \mathrm{Time}(s - \mathrm{bit} - r - \mathrm{bit}) = \max(s,\ r)$

(4) $\mathrm{Time}(\text{dividing } a \text{ by } b) = \mathrm{Time}(s - \mathrm{bit} \div r - \mathrm{bit}) = O(sr)$

となる.

例題 2.1.1 任意の $k - \mathrm{bit}$ 整数を 10 進法表現に convert する n.b.o. は？

解答　n を $k - \mathrm{bit}$ 整数とする．n を $10 = (1010)_2$ で割り、その余りを求める．1 回の除法での n.b.o. は $O(4k) = O(k)$.　次にその商をまた $10 = (1010)_2$ で割り、その余りを求める．ここでの n.b.o. も $O(k)$.　以下同様に続けるのだが、$2 < 10$ より、この procedure はせいぜい k 回で終わる．したがって

$$\mathrm{Time}(\text{converting } n \text{ to decimal}) = O(k^2) = O(\log^2 n)$$

が求める n.b.o. である.　□

例題 2.1.2 任意の $k - \mathrm{bit}$ 整数を b 進法表現に convert する n.b.o. は？

解答　b を $\ell - \mathrm{bit}$ 整数とする.

$$\mathrm{Time}(k - \mathrm{bit} \div \ell - \mathrm{bit}) = O(k\ell).$$

一方、n の b 進法表現の桁数は明らかに

$$O(k/\ell) = O(\log n/\log b)$$

であるから、例題 2.1.1 と同じような procedure は $O(k/\ell)$ 回で終わる．故に

$$\text{Time(converting } n \text{ to base} - b) = O(k/\ell)O(k\ell) = O(k^2) = O(\log^2 n)$$

となる．これは b に無関係であることに注意！ □

例題 2.1.3 階乗 $n!$ を 2 進法で計算する n.b.o. は？

解答

$$\begin{aligned}
&2 \times 3 = 6\\
&6 \times 4 = 24\\
&24 \times 5 = 120\\
&\quad\vdots\\
&(j-1)! \times j = j!\\
&\quad\vdots\\
&(n-1)! \times n = n!.
\end{aligned}$$

途中の桁数として、最後の積の桁数を考えることにする（大雑把！）．$[\log_2 n] + 1 = k$ とすると、n 個の $k-$bit integer の積の桁数は nk と $n(k+1)$ の間にある．ゆえに

$$n! \text{ は高々 } n(k+1)\text{bits} = O(nk)\text{bits.}$$

$(j-1)! \times j = j!$ を計算する n.b.o. は

$$O(nk)O(k) = O(nk^2).$$

これを $n-2$ 回繰り返すわけであるから

$$\begin{aligned}
\text{Time(Product } n!) &= O(n^2k^2)\\
&= O(n^2 \log^2 n)
\end{aligned}$$

を得る． □

定義 2.1.1 整数 $n_1, n_2, \ldots, n_r$ (n_iは $k_i - bit$) を含む計算のアルゴリズムの n.b.o. が

$$O(k_1^{d_1} k_2^{d_2} \cdots k_r^{d_r}) \quad (d_i\text{は整数})$$

であるとき、このアルゴリズムは**多項式時間 (polynomial time) アルゴリズムという**．

2.2 ユークリッドの互除法（再論）

初等整数論において次の定理は基本的である．

定理 2.2.1 いずれか一方はゼロでない 2 つの整数 $a,\ b$ に対して

$$au + bv = (a, b)$$

を満たす整数 $u,\ v$ が存在する．

この定理の証明は、$a,\ b$ をともにゼロでない自然数と仮定して行えば充分であることは明らか（であろう？）であるから、以下そのように仮定する．証明は次の事柄をもとに行われる．

補助定理 2.2.1 二つの自然数 $m,\ n\ (m > n)$ に対して

$$m = qn + r \quad (0 \leqq r < n)$$

とおくとき、$(m, n) = (n, r)$ が成り立つ．

補題の証明 $r = m - qn$ より、r が (m, n) の倍数であることがわかる．また、n は (m, n) の倍数であるから、$(m, n) \leqq (n, r)$ であることがわかる．逆に、$m = qn + r$ より、m は (n, r) の倍数であり、n は (n, r) の倍数であることから $(m, n) \geqq (n, r)$ がわかる．よって、$(m, n) = (n, r)$ が成り立つ． □

定理の証明 $a > b$ と仮定すると、次のような一連の等式が得られる．

$$\begin{aligned} a &= q_1 b + r_1 \qquad (0 \leqq r_1 < b) \\ b &= q_2 r_1 + r_2 \qquad (0 \leqq r_2 < r_1) \\ r_2 &= q_3 r_2 + r_3 \qquad (0 \leqq r_3 < r_2) \\ &\vdots \end{aligned}$$

このとき、$b > r_1 > r_2 > r_3 > \cdots \quad \geqq 0$ より、$r_{k-1} > r_k = 0$ となる k が存在する．補題によって、$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{k-1}, r_k) = (r_{k-1}, 0) = r_{k-1}$. ところが、$r_{k-1}$ を導き出す過程を逆に辿ることにより、r_{k-1} が a と b の線形結合で表されることがわかる． □

系 2.2.1 ユークリッドの互除法は有限ステップで 2 つの整数の GCD を与える．さらに、$a > b$ ならば

$$\text{Time(finding } (a, b) \text{ by the Euclidian algorithm)} = O(\log^3 a).$$

証明　前半は前定理 2.2.1 により、明らか．後半を証明しよう．

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \end{aligned}$$

このとき、$r_{j+2} < \dfrac{1}{2} r_j$ が成り立つ．なぜならば

$$r_{j+1} \leqq \frac{1}{2} r_j \ \Rightarrow r_{j+2} < r_{j+1} \leqq \frac{1}{2} r_j$$

$r_{j+1} > \dfrac{1}{2} r_j$ ならば $r_j = 1 \cdot r_{j+1} + r_{j+2}$ より

$$r_{j+2} = r_j - r_{j+1} < \frac{1}{2} r_j.$$

従って、2 ステップで余りは半分以下になる．すなわち、binary で計算すれば 2 ステップで 1 桁は必ずおちる．よって、計算の回数はせいぜい $2[\log_2 a]$．ところでどのステップでも現れる桁数は $[\log_2 a]$ 以下であるし、r_j の計算は除法と減法であるから、n.b.o. は高々$O([\log_2 a]^2)$．従って、(a, b) を計算する n.b.o. は $O(\log^3 a)$．　□

定義 2.2.1　2 つの整数 $a,\ b$ について $(a, b) = 1$ のとき、$a,\ b$ は**互いに素 (relatively prime)** であるという．

定理 2.2.2　2 つの整数 $a,\ b$ が互いに素であるとき、

$$au + bv = 1$$

を満たす整数 $u,\ v$ が存在する．この整数 $u,\ v$ をユークリッド互除法で求める n.b.o. は $O(\log^3 a)$.

定義 2.2.2　$n \geqq 1$ に対してオイラーの関数 $\varphi(n)$ を

$$\varphi(n) \stackrel{\text{def}}{=} \sharp\{a \mid 1 \leqq a \leqq n,\ (a, n) = 1\}$$

で定義する．

定理 2.2.3 自然数 n の素因数分解を $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_r^{\alpha_r}$ とする．このとき、

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

が成り立つ.

補助定理 2.2.2 有限集合の列 $A_1,\ A_2,\cdots,\ A_r$ について次の等式が成り立つ.

$$\begin{aligned}\sharp(A_1\cup A_2\cup\cdots\cup A_r) &= \sum_{i=1}^{r}\sharp(A_i)-\sum_{i<j}\sharp(A_i\cap A_j)+\sum_{i<j<k}\sharp(A_i\cap A_j\cap A_k)\\ &\quad -\cdots+(-1)^{r-1}\sharp(A_1\cap A_2\cap\cdots\cap A_r)\end{aligned}$$

補題の証明　証明は演習問題でーす. □

定理の証明　A_k によって n 以下の素数 p_k の倍数の集合とする $(1\leqq k\leqq r)$．すると n 以下の自然数で n と互いに素でないものは、$A_1\cup A_2\cup\cdots\cup A_r$ と表される．従って、補題 2.2.2 によって

$$\begin{aligned}\sharp(A_1\cup A_2\cup\cdots\cup A_r) &= \sum_{i=1}^{r}\sharp(A_i)-\sum_{i<j}\sharp(A_i\cap A_j)+\sum_{i<j<k}\sharp(A_i\cap A_j\cap A_k)\\ &\quad -\cdots+(-1)^{r-1}\sharp(A_1\cap A_2\cap\cdots\cap A_r)\\ &= \sum_{i=1}^{r}\frac{n}{p_i}-\sum_{i<j}\frac{n}{p_ip_k}+\sum_{i<j<k}\frac{n}{p_ip_kp_j}\\ &\quad -\cdots+(-1)^{r-1}\frac{n}{p_1p_2\cdots p_r}\end{aligned}$$

従って

$$\begin{aligned}\varphi(n) &= n-\sharp(A_1\cup A_2\cup\cdots\cup A_r)\\ &= n-\sum_{i=1}^{r}\frac{n}{p_i}+\sum_{i<j}\frac{n}{p_ip_k}-\sum_{i<j<k}\frac{n}{p_ip_kp_j}+\cdots-(-1)^{r-1}\frac{n}{p_1p_2\cdots p_r}\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_r}\right).\end{aligned}$$

□

系 2.2.2 p が素数ならば、$\varphi(p)=p-1$ である.

系 2.2.3 p が素数で k が正の整数ならば、$\varphi(p^k)=p^k-p^{k-1}$ である.

系 2.2.4 正の整数 $m,\ n$ が互いに素であるならば $\varphi(mn)=\varphi(m)\varphi(n)$ である.

2.3 合同式

まず，約数に関する基本的性質を思い起こす.

定理 2.3.1 以下の命題が成立する.

(1) $m \mid 0$

(2) $m \mid a$ ならば $m \mid -a$

(3) $m \mid a,\ m \mid b$ ならば $m \mid (a \pm b)$

(4) $m \mid a,\ d \mid m$ ならば $d \mid a$

(5) $m \mid a,\ n \mid a,\ (m,n) = 1$ ならば $mn \mid a$

(6) m が素数で、$m \mid ab$ ならば $m \mid a$ または $m \mid b$

証明 (5) と (6) のみを証明する．他の命題は明らかである．まず (5)．仮定 $(m,n) = 1$ と定理 2.2.2 によって $mu + nv = 1$ を満たす整数 $u,\ v$ が存在する．また、仮定によって、$a = mk = nj$ とかける．従って

$$a = 1 \cdot a = (mu + nv)a = amu + anv = nmju + mnkv$$

となるので、$mn \mid a$ が結論付けられる．つぎに (6)．$m \nmid a$ とすると $(m,a) = 1$ であるから、定理 2.2.2 によって $mu + av = 1$ を満たす整数 $u,\ v$ が存在する．よって、$mbu + abv = b$．仮定によって左辺は m で割り切れる．よって右辺 b は m で割り切れなければならない. □

定義 2.3.1 m を 2 以上の自然数とする．二つの整数 $a,\ b$ について、$m \mid (a - b)$ が成り立つとき、a と b は**法** m に関して**合同**であるといい、$a \equiv b \pmod{m}$ で表す.

この定義を別の表現をすると次のようになる：整数 a を整数 $m \geqq 2$ で割ったときの余りを $\mathrm{Mod}(a,m)$ で表すとき、関係 $a \equiv b \pmod{m}$ は $\mathrm{Mod}(a,m) = \mathrm{Mod}(b,m)$ と同等である.

定理 2.3.2 次の命題が成り立つ.

(1) $a \equiv a \pmod{m}$

(2) $a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$

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

(4) $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$ ならば $a \pm c \equiv b \pm d \pmod{m}$

(5) $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$ ならば $ac \equiv bd \pmod{m}$

(6) $a \equiv b \pmod{m},\ d \mid m$ ならば $a \equiv b \pmod{d}$

(7) $a \equiv b \pmod{m},\ a \equiv b \pmod{n},\ (m,n) = 1$ ならば $a \equiv b \pmod{mn}$

証明　(1)〜(4) および (6) は明らか．まず (5) について証明しよう．

$$ac - bd = ac - ad + ad - bd = a(c-d) + (a-b)d$$

の最後の項は明らかに m で割り切れる．よって $ac \equiv bd \pmod{m}$.
残るは (7) であるが、これは定理 2.3.1(5) から明らか．　□

定理 2.3.3 $(a,m) = 1$ ならば、$ax \equiv 1 \pmod{m}$ を満たす整数 x が存在する．この x は $1 \leqq x < m$ の範囲に存在する．

証明　定理 2.2.2 によって、$ax + my = 1$ を満たす整数 $x,\ y$ が存在する．この式は $ax \equiv 1 \pmod{m}$ と同じである．$ax + my = 1$ の一つの解の組を $x_0,\ y_0$ とする．$x = \mathrm{Mod}(x_0, m)\ (1 \leqq x < m)$ とすると、$x_0 - x = mk$ と書ける．$a(x_0 - mk) + m(y_0 + ak) = 1$ より、$ax + m(y_0 + ak) = 1$ すなわち $ax \equiv 1 \pmod{m}$ ．　□

定理 2.3.4 (中国式剰余定理) 正整数 $m_1,\ m_2,\ \ldots,\ m_r$ は互いに素であるとする．また、整数 $a_1,\ a_2,\ \ldots,\ a_r$ は各 $1 \leqq k \leqq r$ について $(a_k, m_k) = 1$ を満たすものとする．このとき、任意の整数 $b_1,\ b_2,\ \ldots,\ b_r$ に対する合同連立方程式

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_r x &\equiv b_r \pmod{m_r} \end{aligned}$$

の解は存在して、法 $M = m_1 m_2 \cdots m_r$ に関して一意である．

証明　定理 2.3.3 によって、この連立方程式は

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_r \pmod{m_r} \end{aligned}$$

という連立方程式に還元される．$M_i = M/m_i$ $(1 \leqq i \leqq r)$ とおく．各 i について、定理 2.3.3 によって $N_i M_i \equiv 1 \pmod{m_i}$ を満たす整数 N_i が存在する．

$$x = \sum_{i=1}^{r} b_i N_i M_i$$

とおくと、これが上の連立方程式を満たすことをみるのは容易い．これで存在は示された．次に法 M に関する一意性を示そう．二つの解を $x,\ x'$ とすると、各 i について $x - x' \equiv 0 \pmod{m_i}$ となる．したがって、定理 2.3.2(7) によって、$x - x' \equiv 0 \pmod{M}$. □

定理 2.3.5 (フェルマーの定理) p を素数とするとき、p と互いに素である任意の整数 a に対して

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ.

証明　各 $1 \leqq i < p$ に対して、$r_i = \mathrm{Mod}(ai, p)$ とおく．$i \neq j$ $(1 \leqq i, j < p)$ ならば $r_i \neq r_j$ であることは仮定から明らか．従って

$$\begin{aligned} \prod_{i=1}^{p-1} ai &\equiv \prod_{i=1}^{p-1} r_i \pmod{p} \\ &\equiv \prod_{i=1}^{p-1} i \pmod{p} \end{aligned}$$

よって

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

ところが $p \nmid (p-1)!$ であるから、$a^{p-1} \equiv 1 \pmod{p}$. □

系 2.3.1 $p \nmid a,\ n \equiv m \pmod{(p-1)}$ ならば $a^n \equiv a^m \pmod{p}$.

定理 2.3.6 (オイラーの定理) n を 2 以上の整数とする．整数 a が n と互いに素であるとき、

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

が成り立つ.

証明 n の素因数分解を $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ とする．まず $r = 1$ の場合を示す．$\alpha_1 = 1$ の場合はフェルマーの定理（定理 2.3.5）に帰せられる．$\alpha_1 = k$ の場合に定理が成り立つとしよう．つまり、

$$a^{p_1^k - p_1^{k-1}} \equiv 1 \pmod{p_1^k}$$

とする．このとき、

$$a^{p_1^k - p_1^{k-1}} = 1 + K p_1^k$$

と書けるので、両辺を p 乗すると

$$a^{p_1^{k+1} - p_1^k} = 1 + p_1^{k+1} K'$$

となり、これは定理が $\alpha_1 = k+1$ の場合に成り立つことを示している．すなわち、$r = 1$ の場合は任意の α_1 について定理が正しいことが言えた.

一般の場合に戻る．各 i $(1 \leqq i \leqq r)$ について同様に

$$a^{p_i^{\alpha_i} - p_i^{\alpha_i - 1}} \equiv 1 \pmod{p_i^{\alpha_i}}$$

が得られ

$$a^{\varphi(n)} \equiv 1 \pmod{p_i^{\alpha_i}}$$

となる．これと、定理 2.3.2(7) により、

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

が示された. □

系 2.3.2 $(a, m) = 1,\ n \equiv n' \pmod{\varphi(m)}$ ならば $a^m \equiv a^{n'} \pmod{m}$.

定理 2.3.6 の証明をみると肝腎なのは

$$a^K \equiv 1 \pmod{p_i^{\alpha_i}} \quad (1 \leqq \forall i \leqq r)$$

ということであり、

$$K = \mathrm{LCM}(\varphi(p_1^{\alpha_1}), \ldots,\ \varphi(p_r^{\alpha_r}))$$

とすれば上の事柄が成り立つ．よって

系 2.3.3 $K = \mathrm{LCM}(\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_r^{\alpha_r}))$ とする．$(a, m) = 1$ ならば

$$a^K \equiv 1 \pmod{m}$$

が成り立つ．

当然、系 2.3.2 でも上の K を法に使える．

定理 2.3.6 の別証明　ほぼ，フェルマーの定理と同じ方針である．n 以下で n と互いに素である正の整数の集合を $M = \{b_1,\ b_2, \cdots,\ b_{\varphi(n)}\}$ とする．$1 \leqq i \leqq \varphi(n)$ に対して $r_i = \mathrm{Mod}(ab_i, n)$ とおくと，任意の $1 \leqq i < j \leqq \varphi(n)$ について，$r_i \neq r_j$ が成り立つ．しかも各 $1 \leqq i \leqq \varphi(n)$ に対して $(r_i, n) = 1$ であるから $\{r_1,\ r_2, \cdots, r_{\varphi(n)}\} = M$ である．したがって

$$\begin{aligned} \prod_{i=1}^{\varphi(n)} ab_i &\equiv \prod_{i=1}^{\varphi(n)} r_i \pmod{n} \\ &= \prod_{i=1}^{\varphi(n)} b_i. \end{aligned}$$

ゆえに，

$$a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} b_i \equiv \prod_{i=1}^{\varphi(n)} b_i \qquad (\mathrm{mod}\ n)$$

となる．ところが $n \nmid \prod_{i=1}^{\varphi(n)} b_i$ であるから，

$$n \mid a^{\varphi(n)} - 1,$$

すなわち

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

を得る．　□

次の定理はそれ自体でも面白いが、後にその重要さが認められる．

定理 2.3.7

$$\sum_{d \mid n} \varphi(d) = n.$$

証明　左辺を $f(n)$ とおく．$(m,n)=1$ としよう．$d \mid mn$ ならば $d=d_1d_2$ $(d_1 \mid m,\ d_2 \mid n,\ (d_1,d_2)=1)$ と書けて、系 2.2.4 によって、$\varphi(d)=\varphi(d_1)\varphi(d_2)$ となるので、

$$\begin{aligned} f(mn) &= \sum_{d_1\mid m}\sum_{d_2\mid n}\varphi(d_1)\varphi(d_2) \\ &= \left(\sum_{d_1\mid m}\varphi(d_1)\right)\left(\sum_{d_2\mid n}\varphi(d_2)\right) \\ &= f(m)f(n). \end{aligned}$$

従って、$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ とすると、

$$f(n)=\prod_{i=1}^{r} f(p_i^{\alpha_i}).$$

従って、証明を完成するには $f(p^\alpha)=p^\alpha$ を示せばよい．ところが p^α の約数は p^j $(0 \leqq j \leqq \alpha)$ であるから、系 2.2.3 によって，

$$f(p^\alpha)=\sum_{i=0}^{\alpha}\varphi(p^j)=1+\sum_{j=1}^{\alpha}(p^j-p^{j-1})=p^\alpha.$$

□

2.4　反復２乗法

$m,\ n$ が非常に大きい場合、

$$b^n \pmod m$$

を単純に b^n を計算してから $\mathrm{Mod}(b^n,m)$ を計算するのは大仕事である．計算量的には $O(n^2\log^2 b)$．$b<m$ とすると、1 回毎に $\mathrm{Mod}(\cdot,m)$ をとれば、扱う整数は m^2 以上にはならない．この節のテーマの内容を具体的に説明しよう．n の２進法表現を

$110101 = 2^5 + 2^4 + 2^2 + 1$ とする．

$$\begin{aligned} b^1 &\equiv b_0 \\ b^2 &\equiv b_1 \\ b^{2^2} &\equiv b_1^2 \equiv b_2 \\ b^{2^3} &\equiv b_2^2 \equiv b_3 \\ b^{2^4} &\equiv b_3^2 \equiv b_4 \\ b^{2^5} &\equiv b_4^2 \equiv b_5 \end{aligned}$$

これから、

$$b^n \equiv b_0 b_2 b_4 b_5 \pmod{m}$$

を計算すればよい．もちろん、最後の乗算は一回行う毎に剰余をとる．

定理 2.4.1

$$\mathrm{Time}(b^n \pmod{m}) = O(\log n \log^2 m).$$

証明 b^{2^ℓ} を $\pmod{m}$ で計算する n.b.o. は $O(\log^2 m)$. これを高々 $k = [\log_2 n] + 1$ 回実行する．従って、b^{2^ℓ} をすべて $\pmod{m}$ で計算するには $O(k \log^2 m)$ の n.b.o. が必要である．また、最後の b^n を計算するには一ステップごとの計算で $b^n \equiv b_0 b_1 \cdots b_k$ を計算するが、これは $O(k \log^2 m)$ の n.b.o. が必要．よって、定理が証明された．□