オイラーの関数

オイラーの関数は、重要な公開鍵暗号の一つであるRSA暗号において重要な役割を果たしている。ここでは、オイラーの関数の定義と求め方、また、オイラーの定理について説明する。

既約剰余類とは（復習）

- 法nの合同関係を考えると、全ての整数は0,1,⋯,n-1のどれか一つと必ず合同になる。集合{0,1,⋯,n-1}は法nにおける剰余類と呼ばれる。
- 剰余類{0,1,⋯,n-1}のうち、nと互いに素なものだけからなる集合を既約剰余類という。
- （例１）n=10のとき、既約剰余類は、{1,3,7,9}である
- （例２）n=7のとき、既約剰余類は、{1,2,3,4,5,6}である。一般に、n=p（素数）であるとき、既約剰余類は、{1,2,⋯,p-1}となる

既約剰余類と逆元

- 法nにおける剰余類{0,1,⋯,n-1}において乗算を考えるとき、既約剰余類に含まれる要素は逆元を持つことがわかる

×	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

- n=6の場合、既約剰余類は{1,5}である
- 元1と5は逆元を持つ（1の逆元は1、5の逆元は5）
- 元0,2,3,4は逆元を持たない
- 既約剰余類同士の乗算は群になっている
- n=p（素数）の場合、0以外の全ての元が逆元を持つことがわかる

オイラーの関数（定義）

- オイラーの関数φ(n)の定義
  法nにおける既約剰余類の要素の数をφ(n)と定義する
  （言い換えると、0,1,⋯,n-1のうち、nと互いに素な数の個数）

n	φ(n)
1	1
2	1
3	2
4	2
5	4
6	2

n	φ(n)
7	6
8	4
9	6
10	4
11	10
12	4

オイラーの関数の値

1. $n=p$(素数) の場合： 明らかに1,2,…,p-1はpと互いに素なので、$\varphi(n)=p-1$
2. Pを素数として、$n=p^e$の場合$(e>1)$：0,1,…,p^e-1のうち、p^eと互いに素でないものは、0,p,2p,3p,…,$p^{e-2}p$のp^{e-1}個である。従って、$\varphi(n)=p^e-p^{e-1}$となる
3. mとnが互いに素であるとき、$\varphi(mn)=\varphi(m)\varphi(n)$がいえる（証明次頁）

上記１～３を組み合わせることで、任意のnについて$\varphi(n)$の値を求めることができる。

（例） $\varphi(12)=\varphi(2^2\times 3)=\varphi(2^2)\times\varphi(3)=(2^2-2^1)\times(3-1)=2\times 2=4$

（注） $\varphi(n)$の値を求めるためには、nの素因数分解が必要

オイラーの関数の性質

- mとnが互いに素であるとき、$\varphi(mn) = \varphi(m)\varphi(n)$である
- （証明）$1 \sim m$のうちmと互いに素な数を$a_1, a_2, \ldots, a_{\varphi(m)}$とおき、$1 \sim n$のうち$n$と互いに素な数を$b_1, b_2, \ldots, b_{\varphi(n)}$とおく。$(m, n) = 1$なので、

$$\begin{cases} c = a_i \pmod{m} \\ c = b_j \pmod{n} \end{cases}$$

を満たすcが法mnの下で一意に定まる（中国人の剰余定理）。
このとき、$(c, mn) = 1$であることを示すことができる。
なぜなら、

オイラーの関数の性質（続き）

- もし、$(c, mn) > 1$ならば、cはmまたはn（またはその両方）と公約数を有することになるが、それは矛盾である。

（一般性を失わずに）$(c, m) = g(> 1)$と仮定する。

すると、仮定から$c = a_i (mod\ m)$、すなわち$m|(c - a_i)$なので、a_iもmの約数gを有することになり、a_iがmと互いに素なことに矛盾するからである。

- 以上より、$\varphi(m)\varphi(n)$通りだけある(a_i, b_j)の組を一つ決めると対応するcが一つきまり、それはmnと互いに素である。
- 逆に$(c, mn) = 1$のとき、$(c, m) = 1$かつ$(c, n) = 1$でありこれは前頁の連立一次合同式の解のどれかに一致する

オイラーの関数の値

- 自然数$n=p^{\alpha}q^{\beta}r^{\gamma}\cdots$と素因数分解されるとき、
$$\varphi(n)=n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots$$
である。
- （証明）$p^{\alpha},q^{\beta},r^{\gamma},\ldots$はそれぞれ互いに素であるので、性質3より
$$\varphi(n)=\varphi(p^{\alpha})\varphi\left(q^{\beta}\right)\varphi(r^{\gamma})\cdots$$
がいえる。（次ページに続く）

オイラーの関数の値（続き）

- 次に性質2より

$$
\begin{aligned}
\varphi(n) &= (p^{\alpha} - p^{\alpha-1})(q^{\beta} - q^{\beta-1})(r^{\gamma} - r^{\gamma-1})\cdots \\
&= p^{\alpha}q^{\beta}r^{\gamma}\cdots\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots \\
&= n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots
\end{aligned}
$$

オイラーの関数の値（例）

- $\varphi(11) = 10$　　（素数の場合は$p-1$）
- $\varphi(64) = \varphi(2^6) = 2^6 - 2^5 = 64 - 32 = 32$
- $\varphi(187) = \varphi(11 \times 17) = \varphi(11)\varphi(17) = 10 \times 16 = 160$
- $\varphi(1400) = \varphi(2^3 \times 5^2 \times 7) = (2^3 - 2^2)(5^2 - 5) \times 6$
  $= 4 \times 20 \times 6 = 480$

オイラーの定理

- $(a,q)=1$であるとき、$a^{\varphi(q)}=1 \pmod q$が成り立つ

（証明）法qにおける既約剰余類を$\{a_1,a_2,\cdots,a_{\varphi(q)}\}$とする。
$(a,q)=1$であるので、$a\times a_i$も既約剰余類の要素である。また、
$a_i\neq a_j$であるとき、$a\times a_i\neq a\times a_j \pmod q$である。これらより、
$\{aa_1,aa_2,\cdots,a\,a_{\varphi(q)}\}$は（順番が異なるだけで）$\{a_1,a_2,\cdots,a_{\varphi(q)}\}$と
同じである（定理3'）。従って、

$$aa_1\times aa_2\times\cdots\times a\,a_{\varphi(q)}= a_1\times a_2\times\cdots\times a_{\varphi(q)} \pmod q$$

両辺を$a_1\times a_2\times\cdots\times a_{\varphi(q)}$で割ることができて、

$$a^{\varphi(q)}=1 \pmod q$$

オイラーの定理（例）

- $a=3$, $q=10$とする。$(3,10)=1$であり、 $\varphi(10)=4$なので、オイラーの定理より、$3^4=1 \pmod{10}$のはずである。
  実際、$3^4=81=1 \pmod{10}$と確認できる。
  （オイラーの定理により、著しく大きな数であっても何乗すれば１になるのか実際に計算しなくても分かる）
- 【フェルマーの小定理】法qが素数pのとき、 $\varphi(p)=p-1$であるので、任意の$0<a<p$について、

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

  が成り立つ

指数とは

- 正整数aに対して、$(a,q)=1$であるとき、$a^e = 1\ (mod\ q)$である最小の正整数eをaの指数（または位数）と呼ぶ。
- （例１）$a=2, q=15$とする。このとき、$2^1=2(mod\ 15), 2^2=4(mod\ 15), 2^3=8(mod\ 15), 2^4=1(mod\ 15)$なので、$a=2$の指数は４である。なお、$\varphi(15)=8$であり、オイラーの定理より$2^8=1(mod\ 15)$であることに注意しよう。
- （例２）$a=2, q=11$とする。このとき$a=2$の指数は10である。(確認してみなさい)
- （例３）$a=3, q=11$とする。このとき$a=3$の指数は５である。(確認してみなさい)

指数の性質

- eを法qの下でのaの指数とする。このとき、
$$a^n = 1 \ (mod\ q)$$
ならば、$e|n$である。
- （証明）背理法による。nがeで割り切れないと仮定する。すると、$n = se + r (0 < r < e)$とおける。このとき、
$$1 = a^n = a^{se+r} = (a^e)^s a^r = a^r (mod\ q)$$
となるので、eが指数であることに矛盾する。よって$e|n$がいえた。
- オイラーの定理より、$a^{\varphi(q)} = 1 (mod\ q)$であるから、$e|\varphi(q)$であることもわかる。（前頁の例で確認してみなさい）