平方剰余について

平方剰余とは

$x^2 = a \pmod{m}$ は解を持つとは限らない。

$x^2 = a \pmod{m}$ が解をもつ　→　aはmを法として**平方剰余（QR)**

が解をもたない　→　aはmを法として**平方非剰余（NQR)**

（例）　$x^2 = a \pmod{11}$

a	0	1	2	3	4	5	6	7	8	9	10
QR	○	○	×	○	○	○	×	×	×	○	×

ルジャンドル記号

pを奇素数とする

$$\left(\frac{a}{p}\right)=\begin{cases} 1 & x^2=a(\mathrm{mod}\,p) \text{ が解をもつ(QR)} \\ -1 & x^2=a(\mathrm{mod}\,p) \text{ が解をもたない(NQR)} \\ 0 & p\mid a \text{ のとき} \end{cases}$$

ルジャンドル記号の値はどのように計算できるのだろうか？

オイラーの基準

定理８：

pを奇素数とする。このとき、

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$$

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

が成り立つことに注意

オイラーの基準（証明）

$p \mid a$ の時は両辺とも0になるので明らか。以下、pはaを割りきらないとする。

$$\left(a^{\frac{p-1}{2}} \right)^2 = a^{p-1} = 1 \pmod p$$

であるので、 $a^{\frac{p-1}{2}} = \pm 1 \pmod p$ である。次に、gを $Z_p^* = \{1, 2, \cdots, p-1\}$

の原始元とすると、gの位数はp-1なので $g^{\frac{p-1}{2}} = -1 \pmod p$ である。

aが平方剰余であるとき、 $a = g^{2s}$ と書けるから、

$$a^{\frac{p-1}{2}} = g^{2s \times \frac{p-1}{2}} = g^{s(p-1)} = 1 \pmod p$$

一方、aが平方非剰余であるときは、 $a = g^{2s+1}$ と書けるから、

$$a^{\frac{p-1}{2}} = g^{(2s+1) \times \frac{p-1}{2}} = g^{s(p-1) + \frac{p-1}{2}} = -1 \pmod p$$

ヤコビの記号

奇数 $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_K^{\alpha_K}$ と素因数分解されるとき、(a,q)=1であるaに対して

$$\left(\frac{a}{q}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_K}\right)^{\alpha_K}$$

をヤコビの記号という（右辺の記号はルジャンドル記号）。

（注意） $\left(\frac{a}{q}\right) = 1$ であってもaはqを法とする平方剰余とは限らない。

ただし、aがqを法とする平方剰余ならば $\left(\frac{a}{q}\right) = 1$

ヤコビの記号（具体例）

q＝１５の場合

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
QR	○	×	×	○	×	○	×	×	○	○	×	×	×	×
(a/q)	+1	+1	0	+1	0	0	-1	+1	0	0	-1	0	-1	-1

ヤコビの記号＝+1だが、平方剰余ではない

a	1	2
(a/3)	+1	-1

a	1	2	3	4
(a/5)	+1	-1	-1	+1

$$\left(\frac{4}{15}\right)=\left(\frac{4}{3}\right)\left(\frac{4}{5}\right)=(+1)\cdot(+1)=+1$$

$$\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=(-1)\cdot(-1)=+1$$

（注） qの素因数分解が分からない場合
でも、ヤコビの記号の値を効率よく
計算するアルゴリズムが存在する。

法pにおける平方根

- pを$p = 3 \pmod 4$である素数とする。このとき、pを法とする平方剰余aについて、

$$x^2 = a \pmod p$$

の解は、$x = \pm a^{\frac{p+1}{4}} \pmod p$で与えられる

- $p = 1 \pmod 4$の場合でも平方根を計算できるが、やや複雑になるので省略

法pにおける平方根（証明）

- $r = a^{\frac{p+1}{4}} \pmod p$とおく（以下、$(mod\ p)$の記述を省略する）。$p = 4k + 3$とおけるので$\frac{p+1}{4} = k + 1$となり整数であることに注意。
- $r^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \times a$
- ここで、$\left(\frac{a}{p}\right) = 1$であるから、オイラーの基準より$a^{\frac{p-1}{2}} = 1$である。
- 従って、$r^2 = a$