積

tubuann

定義

$$g^x \equiv 1 \, mod \, p$$

を満たす最小の自然数xを $Or_p(g)$ と定義する。

- フェルマーの小定理

$$g^{p-1} \equiv 1 \, mod \, p$$

より、このようなxは必ず存在する。

定義

また、

$$g^a \equiv 1 \, mod \, p$$

$$g^b \equiv 1 \, mod \, p$$

ならば、

- $$g^{a-b} \equiv g^a g^{-b} \equiv 1 \, mod \, p$$

だから、ユークリッドの互除法と同様に

$$g^{\mathrm{Gcd}(a,b)} \equiv 1 \, mod \, p$$

である。

定義

以上から次の性質が導かれる。

$$g^a \equiv 1 \, mod \, p \Leftrightarrow Or_p(g) | a \, .$$

特に、

$$g^a \equiv 1 \, mod \, p$$

- かつ、aの任意の素因数eに対して、

$$g^{\frac{a}{e}} \not\equiv 1 \, mod \, p$$

ならば、

$$Or_p(g) = a \, .$$

考察 1

$$g^a \equiv g^b \bmod p \iff g^{a-b} \equiv 1 \bmod p$$

だから、

$$g^1, g^2 \dots\dots g^{Or_p(g)}$$

は、全て互いに異なる1の$Or_p(g)$乗根である。

また、因数定理から1の$Or_p(g)$乗根はたかだか$Or_p(g)$個であることがいえる。

よって、上の数列は1の$Or_p(g)$乗根全体に等しい。

考察 1

ところで、

$$Or_p(g_1) = Or_p(g_2)$$

ならば、g_1とg_2は同一視できる。

- $$N = Or_p(g_1) = Or_p(g_2)$$

とすると、g_1もg_2も1のN乗根だから、

$$g_1^{x_1} \equiv g_2 \ mod \ p$$
$$g_2^{x_2} \equiv g_1 \ mod \ p$$

となるx_1, x_2が存在する。

考察２

$$y = g_1^{x_1} g_2^{x_2}$$

$$L = Lcm\left(Or_p(g_1), Or_p(g_2)\right)$$

とする。

- $$y^L \equiv \left(g_1^{x_1} g_2^{x_2}\right)^L \equiv (g_1^L)^{x_1} (g_2^L)^{x_2} \equiv 1 \ mod\ p$$

よりyは1のL乗根である。

$$Or_p(y) = L$$

となるx_1, x_2が存在する。

考察２

$$Gcd\left(Or_p(g_1), Or_p(g_2)\right) = 1$$

ならば、

$$Or_p\ (g^x) | Or_p(g)$$

より、

$$g_1^{x_1} g_2^{x_2} \equiv 1\ mod\ p \Leftrightarrow g_1^{x_1} \equiv g_2^{-x_2}\ mod\ p \Leftrightarrow g_1^{x_1} \equiv g_2^{x_2} \equiv 1\ mod\ p$$

だから、

$$Or_p(g_1 g_2) = Or_p(g_1) Or_p(g_2)$$

である。

考察２

$$Gcd\left(Or_p(g_1), Or_p(g_2)\right) \neq 1$$

ならば、

$$Or_p(g^x) = \frac{Or_p(g)}{Gcd\left(Or_p(g), x\right)}$$

だから、

$$Gcd\left(Or_p(g_1^{x_1}), Or_p(g_2^{x_2})\right) = 1$$

$$Or_p(g_1^{x_1})Or_p(g_2^{x_2}) = Lcm\left(Or_p(g_1), Or_p(g_2)\right)$$

となるx_1, x_2が存在する。

解法

$$\prod_i g_i^{x_i} \equiv A \bmod p$$

の解が存在する必要十分条件は、

$$Or_p(A) | Lcm_{g \in G}\left(Or_p(g)\right)$$

である。

解法

$p-1$の素因数の多重集合をEとする。

$Or_p(g)$は以下のようなアルゴリズムで求めることができる。

$$q \coloneqq p-1$$

- $$while(e \in E)\ if\ g^{\frac{q}{e}} \equiv 1\ mod\ p\ \ then\ q \coloneqq \frac{q}{e}$$

計算量$O\left(\sqrt{p}+\sum|G|\ log^2 p+Tlogp\right)$

別解

pが素数ならば、任意のnに対して、

$$r^x \equiv n \bmod p$$

の解を持つrが存在する。

$$r^a r^b \equiv r^{(a+b) \bmod p-1} \bmod p$$

だから、pを法としたときの乗法は、$p-1$を法とした加法と同じ代数的構造を持つ。

別解

$$f: \mathbb{F}_p \setminus \{0\} \longrightarrow \mathbb{Z}_{p-1}$$
$$r^x \longmapsto x$$

と定義すると、

- $$a \equiv b^x \bmod p$$
$$\Leftrightarrow$$
$$f(b)x \equiv f(a) \bmod p-1$$

の解が存在する必要十分条件は、

$$Gcd(f(b), p-1) | Gcd(f(a), p-1)$$

である。

別解

- $\prod_i g_i^{x_i} \equiv A \bmod p$の解が存在する

$\Leftrightarrow$

$\sum_i f(g_i)x_i \equiv f(A) \bmod p-1$の解が存在する

$\Leftrightarrow$

$Gcd_{g\in G}\big(Gcd(f(g),p-1)\big) | Gcd(f(A),p-1)$

別解

先ほどの解法との対応は、

$$\frac{p-1}{Gcd(f(g),p-1)} = Or_p(g)$$

- と与えられる。

よって、$Gcd(f(g),p-1)$は同様のアルゴリズムで求めることができる。

いつもの

オンサイトFA　rupc_KU_NO_FA　さん　(02:22:38)

オンラインFA　gifted_infants　さん　(00:59:47)

Success Rate 5/94 (5.3%)

ジャッジ解

tubuann	c++	92行
beet	c++	123行