

Algebraic Arithmetic

Hajime Mashima

Abstract

The more difficult the problem, the more limited the path.

Contents

1	introduction	1
1.1	$\delta \perp xyz$	2
1.1.1	$p \mid x$	4
1.1.2	$p \perp x$	5
1.2	同値変換 (Equivalence Transformation)	6
1.3	解の条件 (Solution Conditions)	10
1.4	合同条件 (Congruent Conditions)	13
1.4.1	$x - y \equiv -z \pmod{\delta}$	13
1.4.2	$x + z \equiv y \pmod{\delta}$	14
1.4.3	共通 (Common)	15
1.4.4	$L \equiv 0 \pmod{\delta}$	16
1.4.5	$R \equiv 0 \pmod{\delta}$	17
1.4.6	$2 \mid x$, $2 \perp yz$	22

1 introduction

最後に残った Fermat の命題が現代数学の総力を結集し ” 定理 ” と認められて以降も、微かな火が未だ燻り続けている。それは Fermat の証明が知りたいという探求心そのものである。

1.1 $\delta \perp xyz$

Proposition 1 p は奇素数で次の等式 $x^p + y^p = z^p$ を満たすとき

$$p \mid x, p \mid yz \Rightarrow p^n \mid x \ (n \geq 2), p^{p^{n-1}} \mid z - y$$

Proof 2

$x^p + y^p - z^p = 0 \Rightarrow p \mid (x + y - z)^p$
よって $p \mid (z - y)$ と置ける。一般的に

$$x^p = (z - y) \left(py^{p-1} + \frac{p!}{(p-2)!2!} y^{p-2}(z - y) + \cdots + \frac{p!}{1!(p-1)!} y(z - y)^{p-2} + (z - y)^{p-1} \right)$$

$$x^p = (L)(R)$$

$$R = py^{p-1} + \frac{p!}{(p-2)!2!} y^{p-2}(z - y) + \cdots + \frac{p!}{1!(p-1)!} y(z - y)^{p-2} + (z - y)^{p-1}$$

$p^2 \mid R \Rightarrow p \mid y^{p-1}$ となってしまうため

$$p^1 \mid R \tag{1}$$

また、 p を除く素数に関して

$$L \perp R \tag{2}$$

Definition 3 $p \perp abc$

- (1) より $z - y = p^{p-1}a^p$
- (2) より $z - x = b^p$
- (2) より $x + y = c^p$

$$\begin{aligned} (z - x) - (x + y) &= b^p - c^p \\ (z - y) - 2x &= b^p - c^p \equiv 0 \pmod{p} \end{aligned}$$

$p \mid L \Leftrightarrow p \mid R$ なので、少なくとも $p^2 \mid b^p - c^p$

$$p^{p-1}a^p - 2x = b^p - c^p \equiv 0 \pmod{p^2}$$

$$p^2 \mid x \tag{3}$$

$$\begin{aligned} (x - (z - y))^p &= x^p - \frac{p!}{(p-1)!1!} x^{p-1}(z - y) + \frac{p!}{(p-2)!2!} x^{p-2}(z - y)^2 - \frac{p!}{(p-3)!3!} x^{p-3}(z - y)^3 + \\ &\cdots + \frac{p!}{1!(p-1)!} x(z - y)^{p-1} - (z - y)^p \end{aligned}$$

$x^p = (z - y) \cdot p\alpha^p$ と置き、上式に代入する。

$$(x + y - z)^p = (z - y) \left(p\alpha^p - \frac{p!}{(p-1)!1!} x^{p-1} + \cdots + \frac{p!}{1!(p-1)!} x(z - y)^{p-2} - (z - y)^{p-1} \right)$$

$$K = p\alpha^p - \frac{p!}{(p-1)!1!}x^{p-1} + \cdots + \frac{p!}{1!(p-1)!}x(z-y)^{p-2} - (z-y)^{p-1} \quad (4)$$

(3) より $x = p^2a\alpha$ と置けるので

$$\begin{aligned} (x - (z-y))^p &= (z-y) \cdot K \\ (p^2a\alpha - p^{p-1}a^p)^p &= p^{p-1}a^p K \\ (p^2a(\alpha - p^{p-3}a^{p-1}))^p &= p^{p-1}a^p K \\ p^{2p}a^p(\alpha - p^{p-3}a^{p-1})^p &= p^{p-1}a^p K \\ p^{p+1}(\alpha - p^{p-3}a^{p-1})^p &= K \end{aligned}$$

$$p^{p+1} \mid K$$

(4) , $p \perp \alpha^p$ より

$$p^1 \mid K \text{ でなければならぬ。}$$

よって

$$p^2 \mid x \Rightarrow p^{2p-1} \mid (z-y)$$

一般的に

$$p^n \mid x \ (n \geq 2) \Rightarrow p^{pn} \mid x^p \Rightarrow p^{pn-1} \mid L$$

$$\begin{aligned} (x - (z-y))^p &= (z-y) \cdot K \\ (p^n a \alpha - p^{pn-1} a^p)^p &= p^{pn-1} a^p K \\ (p^n a (\alpha - p^{pn-1-n} a^{p-1}))^p &= p^{pn-1} a^p K \\ p^{pn} a^p (\alpha - p^{pn-1-n} a^{p-1})^p &= p^{pn-1} a^p K \\ p(\alpha - p^{n(p-1)-1} a^{p-1})^p &= K \end{aligned}$$

$$\begin{aligned} (\alpha - p^{n(p-1)-1} a^{p-1}) &\perp p \\ p^1 &\mid K \end{aligned}$$

□

また

$$\begin{aligned} x + y - z &= x - (z-y) \\ x + y - z &= p^n a \alpha - p^{pn-1} a^p \\ x + y - z &= p^n (a \alpha - p^{n(p-1)-1} a^p) \\ p^n &\mid x + y - z \end{aligned}$$

1.1.1 $p \mid x$

$$\begin{array}{ll} x = p^n a \alpha & z - y = p^{pn-1} a^p \\ y = b \beta & z - x = b^p \\ z = c \gamma & x + y = c^p \\ p \perp a \alpha y z S & 2 \perp \delta \end{array}$$

Proposition 4 $x + z - y = p^n a S$, $\delta \mid S \Rightarrow \delta \perp xyz$

Proof 5

$$\begin{aligned} x + z - y &= p^n a \alpha + p^{pn-1} a^p \\ &= p^n a (\alpha + p^{(p-1)n-1} a^{p-1}) \end{aligned}$$

$$p \alpha^p = R = p y^{p-1} + (z - y)(\dots)$$

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

$$p y^{p-1} \perp a$$

$$\alpha \perp a$$

$\delta \mid S$, $\delta \mid a$ ならば矛盾する。よって

$$\delta \perp x$$

$$2x = (x + y - z) + (x + z - y)$$

$$bc \mid x + y - z$$

$$x \perp bc$$

$\delta \mid bc$ ならば $\delta \mid 2x$ でなければならず矛盾する。よって

$$\delta \perp bc$$

$\delta \mid \beta$ ならば $\delta \mid x + z$

$$x \equiv -z \pmod{\delta}$$

$$x^p \equiv -z^p \pmod{\delta}$$

$$x^p + z^p \equiv 0 \pmod{\delta}$$

$z^p - x^p = y^p \equiv 0 \pmod{\delta}$ なので

$$x^p + z^p - (z^p - x^p) \equiv 0 \pmod{\delta}$$

$$2x^p \not\equiv 0 \pmod{\delta}$$

よって

$$\delta \perp \beta$$

$\delta \mid \gamma$, $\delta \mid x - y$ ならば同様に

$$x^p - y^p + (x^p + y^p) \equiv 0 \pmod{\delta}$$

$$2x^p \not\equiv 0 \pmod{\delta}$$

よって

$$\delta \perp \gamma$$

□

1.1.2 $p \perp x$

$$\begin{array}{ll}
 x = a'\alpha' & z - y = a'^p \\
 y = b'\beta' & z - x = b'^p \\
 z = c'\gamma' & x + y = c'^p \\
 p \perp a'\alpha'S' (\ast p \mid x - z + y) & 2 \perp \delta
 \end{array}$$

Proposition 6 $x + z - y = a'S'$, $\delta \mid S' \Rightarrow \delta \perp xyz$

Proof 7

$$\begin{aligned}
 x + z - y &= a'\alpha' + a'^p \\
 &= a'(\alpha' + a'^{p-1})
 \end{aligned}$$

$$\begin{aligned}
 \alpha'^p &= R = py^{p-1} + (z - y)(\dots) \\
 R &\equiv py^{p-1} \pmod{a'} \\
 py^{p-1} &\perp a' \\
 \alpha' &\perp a'
 \end{aligned}$$

$\delta \mid S'$, $\delta \mid a'$ ならば矛盾する。よって

$$\delta \perp x$$

$$\begin{aligned}
 2x &= (x + y - z) + (x + z - y) \\
 b'c' &\mid x + y - z \\
 x &\perp b'c'
 \end{aligned}$$

$\delta \mid b'c'$ ならば $\delta \mid 2x$ でなければならず矛盾する。よって

$$\delta \perp b'c'$$

$\delta \mid \beta'$ ならば $\delta \mid x + z$

$$\begin{aligned}
 x &\equiv -z \pmod{\delta} \\
 x^p &\equiv -z^p \pmod{\delta} \\
 x^p + z^p &\equiv 0 \pmod{\delta}
 \end{aligned}$$

$z^p - x^p = y^p \equiv 0 \pmod{\delta}$ なので

$$\begin{aligned}
 x^p + z^p - (z^p - x^p) &\equiv 0 \pmod{\delta} \\
 2x^p &\not\equiv 0 \pmod{\delta}
 \end{aligned}$$

よって

$$\delta \perp \beta'$$

$\delta \mid \gamma'$, $\delta \mid x - y$ ならば同様に

$$\begin{aligned}
 x^p - y^p + (x^p + y^p) &\equiv 0 \pmod{\delta} \\
 2x^p &\not\equiv 0 \pmod{\delta}
 \end{aligned}$$

よって

$$\delta \perp \gamma'$$

□

Theorem 8 (Fermat's Last Theorem)

自然数 n の冪について、以下の等式を満たす x, y, z の自然数解は存在しない。

$$x^n + y^n \neq z^n \quad (0 < x < y < z, n \geq 3)$$

これは以下と同値である。

$$x^p + y^p \neq z^p \quad (p \geq 3, x, y, z \text{ は一つが偶数で互いに素})$$

1.2 同値変換 (Equivalence Transformation)

Definition 9

$$\theta \perp xyz$$

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

$$\begin{aligned} x^p + y^p &\equiv z^p \pmod{\theta} \\ sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \end{aligned}$$

$$\begin{aligned} sz^{p-1} \cdot tx^{p-1} &\equiv x^p y^p \pmod{\theta} \\ stz^{p-1} &\equiv xy^p \pmod{\theta} \end{aligned} \tag{5}$$

$$\begin{aligned} tx^{p-1} \cdot uy^{p-1} &\equiv y^p z^p \pmod{\theta} \\ tux^{p-1} &\equiv yz^p \pmod{\theta} \end{aligned} \tag{6}$$

$$\begin{aligned} sz^{p-1} \cdot uy^{p-1} &\equiv x^p z^p \pmod{\theta} \\ suy^{p-1} &\equiv x^p z \pmod{\theta} \end{aligned} \tag{7}$$

$$\begin{aligned} sz^{p-1} \cdot tx^{p-1} \cdot uy^{p-1} &\equiv x^p y^p z^p \pmod{\theta} \\ stu &\equiv xyz \pmod{\theta} \end{aligned} \tag{8}$$

$$\begin{aligned}sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \\tu \cdot sz^{p-1} + t^2ux^{p-1} &\equiv tu^2y^{p-1} \pmod{\theta}\end{aligned}$$

(8) より

$$\begin{aligned}xyz^p + t^2ux^{p-1} &\equiv tu^2y^{p-1} \pmod{\theta} \\xy(x^p + y^p) + t^2ux^{p-1} &\equiv tu^2y^{p-1} \pmod{\theta} \\x^{p+1}y + xy^{p+1} + t^2ux^{p-1} &\equiv tu^2y^{p-1} \pmod{\theta} \\x^{p+1}y + t^2ux^{p-1} &\equiv tu^2y^{p-1} - xy^{p+1} \pmod{\theta} \\x^{p+1}y + t^2ux^{p-1} &\equiv y^{p-1}(tu^2 - xy^2) \pmod{\theta} \\tx^{p-1}(x^{p+1}y + t \cdot tux^{p-1}) &\equiv y^{p-1}(t^2u^2x^{p-1} - xy^2 \cdot tx^{p-1}) \pmod{\theta}\end{aligned}$$

(6) より

$$\begin{aligned}tx^{p-1}(x^{p+1}y + tyz^p) &\equiv y^{p-1}(tu \cdot yz^p - tx^py^2) \pmod{\theta} \\tx^{p-1}(x^{p+1}y + tyz^p) &\equiv y^p(tuz^p - tx^py) \pmod{\theta}\end{aligned}$$

$tx^{p-1} \equiv y^p$ ならば

$$\begin{aligned}x^{p+1}y + tyz^p &\equiv tuz^p - tx^py \pmod{\theta} \\x^{p+1}y + tx^py &\equiv tuz^p - tyz^p \pmod{\theta} \\x^p(xy + ty) &\equiv z^{p-1}(tuz - tyz) \pmod{\theta} \\x^p(sxy + sty) &\equiv sz^{p-1}(tuz - tyz) \pmod{\theta}\end{aligned}$$

$x^p \equiv sz^{p-1}$ ならば

$$sy(x + t) \equiv tz(u - y) \pmod{\theta}$$

$$\begin{aligned}sy(x^p + tx^{p-1}) &\equiv tx^{p-1}z(u - y) \pmod{\theta} \\sy(x^p + y^p) &\equiv y^pz(u - y) \pmod{\theta} \\syx^p &\equiv y^pz(u - y) \pmod{\theta} \\sz^{p-1} &\equiv y^{p-1}(u - y) \pmod{\theta} \\x^p &\equiv y^{p-1}(u - y) \pmod{\theta}\end{aligned}$$

(9)

同様に

$$\begin{aligned} sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \\ s^2uz^{p-1} + su \cdot tx^{p-1} &\equiv su^2y^{p-1} \pmod{\theta} \end{aligned}$$

(8) より

$$\begin{aligned} s^2uz^{p-1} + yzx^p &\equiv su^2y^{p-1} \pmod{\theta} \\ s^2uz^{p-1} + yz(z^p - y^p) &\equiv su^2y^{p-1} \pmod{\theta} \\ s^2uz^{p-1} + yz^{p+1} - y^{p+1}z &\equiv su^2y^{p-1} \pmod{\theta} \\ s^2uz^{p-1} + yz^{p+1} &\equiv su^2y^{p-1} + y^{p+1}z \pmod{\theta} \\ z^{p-1}(s^2u + yz^2) &\equiv su^2y^{p-1} + y^{p+1}z \pmod{\theta} \\ z^{p-1}(s^2u^2y^{p-1} + uy^pz^2) &\equiv uy^{p-1}(u \cdot suy^{p-1} + y^{p+1}z) \pmod{\theta} \end{aligned}$$

(7) より

$$\begin{aligned} z^{p-1}(sux^pz + uy^pz^2) &\equiv uy^{p-1}(ux^pz + y^{p+1}z) \pmod{\theta} \\ z^p(sux^p + uy^pz) &\equiv uy^{p-1}(ux^pz + y^{p+1}z) \pmod{\theta} \end{aligned}$$

$z^p \equiv uy^{p-1}$ ならば

$$\begin{aligned} sux^p + uy^pz &\equiv ux^pz + y^{p+1}z \pmod{\theta} \\ sux^p - ux^pz &\equiv y^{p+1}z - uy^pz \pmod{\theta} \\ x^{p-1}(sux - uxz) &\equiv y^p(yz - uz) \pmod{\theta} \\ tx^{p-1}(sux - uxz) &\equiv y^p(tyz - tuz) \pmod{\theta} \end{aligned}$$

$tx^{p-1} \equiv y^p$ ならば

$$ux(s - z) \equiv tz(y - u) \pmod{\theta}$$

$$uy^{p-1}x(s - z) \equiv tz(y^p - uy^{p-1}) \pmod{\theta}$$

$$z^px(s - z) \equiv tz(y^p - z^p) \pmod{\theta}$$

$$z^{p-1}x(s - z) \equiv -tx^p \pmod{\theta}$$

$$z^{p-1}(s - z) \equiv -tx^{p-1} \pmod{\theta}$$

$$z^{p-1}(z - s) \equiv y^p \pmod{\theta} \tag{10}$$

同様に

$$\begin{aligned} sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \\ s^2tz^{p-1} + st^2x^{p-1} &\equiv st \cdot uy^{p-1} \pmod{\theta} \end{aligned}$$

(8) より

$$\begin{aligned} s^2tz^{p-1} + st^2x^{p-1} &\equiv xzy^p \pmod{\theta} \\ s^2tz^{p-1} + st^2x^{p-1} &\equiv xz(z^p - x^p) \pmod{\theta} \\ s^2tz^{p-1} + st^2x^{p-1} &\equiv xz^{p+1} - x^{p+1}z \pmod{\theta} \\ x^{p+1}z + st^2x^{p-1} &\equiv xz^{p+1} - s^2tz^{p-1} \pmod{\theta} \\ x^{p-1}(x^2z + st^2) &\equiv xz^{p+1} - s^2tz^{p-1} \pmod{\theta} \\ x^{p-1}(sx^2z^p + s^2t^2z^{p-1}) &\equiv sz^{p-1}(xz^{p+1} - s \cdot stz^{p-1}) \pmod{\theta} \end{aligned}$$

(5) より

$$\begin{aligned} x^{p-1}(sx^2z^p + st \cdot xy^p) &\equiv sz^{p-1}(xz^{p+1} - sxy^p) \pmod{\theta} \\ x^p(sxz^p + sty^p) &\equiv sz^{p-1}(xz^{p+1} - sxy^p) \pmod{\theta} \end{aligned}$$

$x^p \equiv sz^{p-1}$ なるば

$$\begin{aligned} sxz^p + sty^p &\equiv xz^{p+1} - sxy^p \pmod{\theta} \\ sty^p + sxy^p &\equiv xz^{p+1} - sxz^p \pmod{\theta} \\ y^{p-1}(sty + sxy) &\equiv z^p(xz - sx) \pmod{\theta} \\ uy^{p-1}(sty + sxy) &\equiv z^p(uxz - sux) \pmod{\theta} \end{aligned}$$

$uy^{p-1} \equiv z^p$ なるば

$$sy(t+x) \equiv ux(z-s) \pmod{\theta}$$

$$sz^{p-1}y(t+x) \equiv ux(z^p - sz^{p-1}) \pmod{\theta}$$

$$x^py(t+x) \equiv ux(z^p - x^p) \pmod{\theta}$$

$$x^{p-1}y(t+x) \equiv uy^p \pmod{\theta}$$

$$x^{p-1}(t+x) \equiv uy^{p-1} \pmod{\theta}$$

$$x^{p-1}(t+x) \equiv z^p \pmod{\theta} \tag{11}$$

1.3 解の条件 (Solution Conditions)

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

$$x^p + Uz^{p-1} \equiv Ty^{p-1} \pmod{\theta}$$

$$\begin{aligned} z^p - y^p + Uz^{p-1} &\equiv Ty^{p-1} \pmod{\theta} \\ z^p + Uz^{p-1} &\equiv y^p + Ty^{p-1} \pmod{\theta} \\ z^{p-1}(z + U) &\equiv y^{p-1}(y + T) \pmod{\theta} \\ z^{p-1}(yz + yU) &\equiv y \cdot y^{p-1}(y + T) \pmod{\theta} \end{aligned} \tag{12}$$

$$yz \equiv UT \pmod{\theta} \Rightarrow \tag{13}$$

$$\begin{aligned} z^{p-1}(UT + yU) &\equiv y^p(y + T) \pmod{\theta} \\ Uz^{p-1}(T + y) &\equiv y^p(T + y) \pmod{\theta} \end{aligned}$$

同様に

$$\begin{aligned} z \cdot z^{p-1}(z + U) &\equiv y^{p-1}(yz + zT) \pmod{\theta} \\ z^p(z + U) &\equiv y^{p-1}(UT + zT) \pmod{\theta} \\ z^p(U + z) &\equiv Ty^{p-1}(U + z) \pmod{\theta} \end{aligned}$$

よって解の候補は以下の2通りである。

$$\begin{aligned} Uz^{p-1} &\equiv y^p \pmod{\theta} \\ Ty^{p-1} &\equiv z^p \pmod{\theta} \\ \text{or} & \\ Uz^{p-1} &\equiv -z^p \pmod{\theta} \\ Ty^{p-1} &\equiv -y^p \pmod{\theta} \end{aligned} \tag{14}$$

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

$$-U'z^{p-1} + y^p \equiv -T'x^{p-1} \pmod{\theta}$$

$$\begin{aligned} -U'z^{p-1} + z^p - x^p &\equiv -T'x^{p-1} \pmod{\theta} \\ -U'z^{p-1} + z^p &\equiv x^p - T'x^{p-1} \pmod{\theta} \\ -z^{p-1}(U' - z) &\equiv x^{p-1}(x - T') \pmod{\theta} \\ -z^{p-1}(U'x - xz) &\equiv x \cdot x^{p-1}(x - T') \pmod{\theta} \end{aligned} \quad (15)$$

$$xz \equiv U'T' \pmod{\theta} \Rightarrow \quad (16)$$

$$\begin{aligned} -z^{p-1}(U'x - U'T') &\equiv x^p(x - T') \pmod{\theta} \\ -U'z^{p-1}(x - T') &\equiv x^p(x - T') \pmod{\theta} \end{aligned}$$

同様に

$$\begin{aligned} -z \cdot z^{p-1}(U' - z) &\equiv x^{p-1}(xz - T'z) \pmod{\theta} \\ -z^p(U' - z) &\equiv x^{p-1}(U'T' - T'z) \pmod{\theta} \\ z^p(U' - z) &\equiv -T'x^{p-1}(U' - z) \pmod{\theta} \end{aligned}$$

よって解の候補は以下の2通りである。

$$\begin{aligned} -U'z^{p-1} &\equiv x^p \pmod{\theta} \\ -T'x^{p-1} &\equiv z^p \pmod{\theta} \\ &or \\ -U'z^{p-1} &\equiv -z^p \pmod{\theta} \\ -T'x^{p-1} &\equiv -x^p \pmod{\theta} \end{aligned} \quad (17)$$

$\theta \perp xyz$ ならば、その逆元が存在するので以下のように表すことができる。

$$-U''y^{p-1} - T''x^{p-1} \equiv z^p \pmod{\theta}$$

$$\begin{aligned} -U''y^{p-1} - T''x^{p-1} &\equiv x^p + y^p \pmod{\theta} \\ -x^p - T''x^{p-1} &\equiv y^p + U''y^{p-1} \pmod{\theta} \\ -x^{p-1}(x + T'') &\equiv y^{p-1}(y + U'') \pmod{\theta} \\ -x^{p-1}(xy + T''y) &\equiv y \cdot y^{p-1}(y + U'') \pmod{\theta} \end{aligned} \quad (18)$$

$$xy \equiv U''T'' \pmod{\theta} \Rightarrow \quad (19)$$

$$\begin{aligned} -x^{p-1}(U''T'' + T''y) &\equiv y^p(y + U'') \pmod{\theta} \\ -T''x^{p-1}(U'' + y) &\equiv y^p(y + U'') \pmod{\theta} \end{aligned}$$

同様に

$$\begin{aligned} -x \cdot x^{p-1}(x + T'') &\equiv y^{p-1}(xy + xU'') \pmod{\theta} \\ -x^p(x + T'') &\equiv y^{p-1}(U''T'' + xU'') \pmod{\theta} \\ x^p(x + T'') &\equiv -U''y^{p-1}(T'' + x) \pmod{\theta} \end{aligned}$$

よって解の候補は以下の2通りである。

$$\begin{aligned} -U''y^{p-1} &\equiv x^p \pmod{\theta} \\ -T''x^{p-1} &\equiv y^p \pmod{\theta} \\ &or \\ -U''y^{p-1} &\equiv y^p \pmod{\theta} \\ -T''x^{p-1} &\equiv x^p \pmod{\theta} \end{aligned} \quad (20)$$

1.4 合同条件 (Congruent Conditions)

Proposition 10 $x^p + y^p \equiv z^p \pmod{\delta}$ との合同条件は

$$\begin{aligned} xyz &\perp \theta \\ xyz &\equiv stu \pmod{\theta} \\ xyz &\equiv (u-y)(z-s)(t+x) \pmod{\theta} \end{aligned}$$

および解の条件を満たし、
(9)(11)(10) より以下に示す同値変換が成り立つものである。

$$\begin{aligned} sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\theta} \\ &\Leftrightarrow \\ (u-y)y^{p-1} + (z-s)z^{p-1} &\equiv (t+x)x^{p-1} \pmod{\theta} \end{aligned}$$

1.4.1 $x - y \equiv -z \pmod{\delta}$

- $x^p - yx^{p-1} \equiv -zx^{p-1} \pmod{\delta}$
- $xy^{p-1} - y^p \equiv -zy^{p-1} \pmod{\delta}$
- $xz^{p-1} - yz^{p-1} \equiv -z^p \pmod{\delta}$

上式を並び替える。

Definition 11

$$L_1 : \quad x^p - yx^{p-1} \equiv -zx^{p-1} \pmod{\delta} \quad (21)$$

$$L_2 : \quad -xy^{p-1} + y^p \equiv zy^{p-1} \pmod{\delta} \quad (22)$$

$$L_3 : \quad -xz^{p-1} + yz^{p-1} \equiv z^p \pmod{\delta} \quad (23)$$

$$\begin{aligned} x^p &+ tx^{p-1} &&\equiv (t+x)x^{p-1} \pmod{\delta} \\ (u-y)y^{p-1} &+ y^p &&\equiv uy^{p-1} \pmod{\delta} \\ sz^{p-1} &+ (z-s)z^{p-1} &&\equiv z^p \pmod{\delta} \end{aligned}$$

$$\begin{aligned} xyz &\perp \delta \\ xyz &\equiv stu \pmod{\delta} \\ xyz &\equiv (u-y)(z-s)(t+x) \pmod{\delta} \end{aligned}$$

を満たす適当な仮定をする。

$$\begin{aligned} s &\equiv -x \pmod{\delta} \\ t &\equiv -y \pmod{\delta} \\ u &\equiv z \pmod{\delta} \end{aligned} \quad (24)$$

$$\begin{aligned}
sz^{p-1} \cdot (t+x)x^{p-1} &\equiv x^p z^p \pmod{\delta} \\
s \cdot (t+x) &\equiv xz \pmod{\delta} \\
-x \cdot (-z) &\equiv xz \pmod{\delta} \\
(u-y)y^{p-1} \cdot tx^{p-1} &\equiv x^p y^p \pmod{\delta} \\
(u-y) \cdot t &\equiv xy \pmod{\delta} \\
(-x) \cdot -y &\equiv xy \pmod{\delta} \\
(z-s)z^{p-1} \cdot uy^{p-1} &\equiv y^p z^p \pmod{\delta} \\
(z-s) \cdot u &\equiv yz \pmod{\delta} \\
(y) \cdot z &\equiv yz \pmod{\delta}
\end{aligned}$$

(13)(16)(19) より (24) は解の条件および同値変換を満たす。

$$\begin{aligned}
x^p + y^p &\equiv z^p \pmod{\delta} \\
&\Leftrightarrow \\
x^p + yz^{p-1} &\equiv zy^{p-1} \pmod{\delta} \\
-xz^{p-1} + y^p &\equiv -zx^{p-1} \pmod{\delta} \\
-xy^{p-1} - yx^{p-1} &\equiv z^p \pmod{\delta}
\end{aligned}$$

1.4.2 $x + z \equiv y \pmod{\delta}$

- $x^p + zx^{p-1} \equiv yx^{p-1} \pmod{\delta}$
- $xy^{p-1} + zy^{p-1} \equiv y^p \pmod{\delta}$
- $xz^{p-1} + z^p \equiv yz^{p-1} \pmod{\delta}$

上式を並び替える。

Definition 12

$$R_1: \quad x^p + zx^{p-1} \equiv yx^{p-1} \pmod{\delta} \quad (25)$$

$$R_2: \quad -zy^{p-1} + y^p \equiv xy^{p-1} \pmod{\delta} \quad (26)$$

$$R_3: \quad yz^{p-1} - xz^{p-1} \equiv z^p \pmod{\delta} \quad (27)$$

$$\begin{aligned}
x^p + tx^{p-1} &\equiv (t+x)x^{p-1} \pmod{\delta} \\
(u-y)y^{p-1} + y^p &\equiv uy^{p-1} \pmod{\delta} \\
sz^{p-1} + (z-s)z^{p-1} &\equiv z^p \pmod{\delta}
\end{aligned}$$

Proposition 13

(14)(17)(20) より、以下は (24) と 2 項の位相が異なる組である。

$$\begin{aligned}
s &\equiv y \pmod{\delta} \\
t &\equiv z \pmod{\delta} \\
u &\equiv x \pmod{\delta}
\end{aligned}$$

1.4.3 共通 (Common)

(21)(25) より

$$\begin{aligned}x^p + zx^{p-1} &\equiv yx^{p-1} \pmod{\delta} \\zx^{p-1} \cdot yx^{p-1} &\equiv y^p z^p \pmod{\delta} \\(x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\delta}\end{aligned}\tag{28}$$

(22)(26) より

$$\begin{aligned}-zy^{p-1} + y^p &\equiv xy^{p-1} \pmod{\delta} \\-zy^{p-1} \cdot xy^{p-1} &\equiv x^p z^p \pmod{\delta} \\(y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta}\end{aligned}\tag{29}$$

(23)(27) より

$$\begin{aligned}yz^{p-1} - xz^{p-1} &\equiv z^p \pmod{\delta} \\yz^{p-1} \cdot -xz^{p-1} &\equiv x^p y^p \pmod{\delta} \\(z^{p-1})^2 &\equiv -x^{p-1} y^{p-1} \pmod{\delta}\end{aligned}\tag{30}$$

(28)(29)(30) より

$$-(x^{p-1})^3 \equiv (y^{p-1})^3 \equiv (z^{p-1})^3 \pmod{\delta}$$

$$0 \equiv (z^{p-1})^3 - (y^{p-1})^3 \equiv (z^{p-1} - y^{p-1})((z^{p-1})^2 + y^{p-1}z^{p-1} + (y^{p-1})^2) \pmod{\delta}$$

$$0 \equiv (x^{p-1})^3 + (z^{p-1})^3 \equiv (x^{p-1} + z^{p-1})((x^{p-1})^2 - x^{p-1}z^{p-1} + (z^{p-1})^2) \pmod{\delta}$$

$$0 \equiv (x^{p-1})^3 + (y^{p-1})^3 \equiv (x^{p-1} + y^{p-1})((x^{p-1})^2 - x^{p-1}y^{p-1} + (y^{p-1})^2) \pmod{\delta}$$

Definition 14

$$0 \equiv (z^{p-1})^3 - (y^{p-1})^3 \equiv (L_1)(R_1) \pmod{\delta}$$

$$0 \equiv (x^{p-1})^3 + (z^{p-1})^3 \equiv (L_2)(R_2) \pmod{\delta}$$

$$0 \equiv (x^{p-1})^3 + (y^{p-1})^3 \equiv (L_3)(R_3) \pmod{\delta}$$

$$A^3 - B^3 = (A - B)(3AB + (A - B)^2)$$

$$A^3 + B^3 = (A + B)(-3AB + (A + B)^2)$$

$$\delta \perp AB$$

$$x^p + y^p \equiv z^p \pmod{3}$$

$$3 \perp xyz \Rightarrow x + y \equiv z \pmod{3} \quad (\text{Fermat's little theorem})$$

$$x \equiv \pm 1 \pmod{3}$$

$$y \equiv \pm 1 \pmod{3}$$

$$z \equiv \mp 1 \pmod{3}$$

$$\delta \neq 3$$

よって

$$L \equiv 0 \pmod{\delta} \quad R \not\equiv 0 \pmod{\delta}$$

or

$$L \not\equiv 0 \pmod{\delta} \quad R \equiv 0 \pmod{\delta}$$

1.4.4 $L \equiv 0 \pmod{\delta}$

(12)(15)(18) より

$$L_1 : z^{p-1} \equiv y^{p-1} \pmod{\delta}$$

$$L_2 : -z^{p-1} \equiv x^{p-1} \pmod{\delta}$$

$$L_3 : -x^{p-1} \equiv y^{p-1} \pmod{\delta}$$

1.4.5 $R \equiv 0 \pmod{\delta}$

$$\begin{aligned}(x^{p-1})^2 + (y^{p-1})^2 + (z^{p-1})^2 &\equiv 0 \pmod{\delta} \\ (x^{p-1})^2 - x^{p-1}z^{p-1} - x^{p-1}y^{p-1} &\equiv 0 \pmod{\delta} \\ x^{p-1} - z^{p-1} - y^{p-1} &\equiv 0 \pmod{\delta} \\ x^{p-1} - y^{p-1} &\equiv z^{p-1} \pmod{\delta}\end{aligned}$$

- $x^p - xy^{p-1} \equiv xz^{p-1} \pmod{\delta}$
- $yx^{p-1} - y^p \equiv yz^{p-1} \pmod{\delta}$
- $zx^{p-1} - zy^{p-1} \equiv z^p \pmod{\delta}$

$$x^p - xy^{p-1} \equiv xz^{p-1} \pmod{\delta}$$

$$\begin{aligned}-xy^{p-1} &\equiv y^p \pmod{\delta} \\ xz^{p-1} &\equiv z^p \pmod{\delta} \Rightarrow\end{aligned}$$

$z^p y^p \perp \delta$ なのので

$$\begin{aligned}-x &\not\equiv y \pmod{\delta} \\ x &\not\equiv z \pmod{\delta}\end{aligned}$$

$$-yx^{p-1} + y^p \equiv -yz^{p-1} \pmod{\delta}$$

$$-yx^{p-1} \equiv x^p \pmod{\delta} \Rightarrow$$

$z^p \perp \delta$ なのので

$$-y \not\equiv x \pmod{\delta}$$

$$zx^{p-1} - zy^{p-1} \equiv z^p \pmod{\delta}$$

$$zx^{p-1} \equiv x^p \pmod{\delta} \Rightarrow$$

$y^p \perp \delta$ なのので

$$z \not\equiv x \pmod{\delta}$$

よって

$$x^p + y^p \equiv z^p \pmod{\delta}$$

\Leftrightarrow

$$R_3, R_2 : \quad x^p - xz^{p-1} \equiv xy^{p-1} \pmod{\delta} \quad (31)$$

$$R_3, R_1 : \quad yz^{p-1} + y^p \equiv yx^{p-1} \pmod{\delta} \quad (32)$$

$$R_2, R_1 : \quad -zy^{p-1} + zx^{p-1} \equiv z^p \pmod{\delta} \quad (33)$$

Definition 15

$$\begin{aligned} zx^{p-1} &= R_1^1, & yx^{p-1} &= R_1^2 \\ -zy^{p-1} &= R_2^1, & xy^{p-1} &= R_2^2 \\ yz^{p-1} &= R_3^1, & -xz^{p-1} &= R_3^2 \end{aligned}$$

$$\begin{aligned} (31) \text{ より } -xz^{p-1} \cdot xy^{p-1} &\equiv y^p z^p \pmod{\delta} \\ -x^2 &\equiv yz \pmod{\delta} \\ x^2 &\equiv -yz \pmod{\delta} \end{aligned}$$

$$\begin{aligned} (28) \text{ より } (x^{p-1})^2 &\equiv y^{p-1} z^{p-1} \pmod{\delta} \\ (x^2)^{p-1} &\equiv y^{p-1} z^{p-1} \pmod{\delta} \\ (-yz)^{p-1} &\equiv y^{p-1} z^{p-1} \pmod{\delta} \\ y^{p-1} z^{p-1} &\equiv y^{p-1} z^{p-1} \pmod{\delta} \\ R_3^2 \cdot R_2^2 &\equiv y^p z^p \pmod{\delta} \end{aligned}$$

$$\begin{aligned} (32) \text{ より } yz^{p-1} \cdot yx^{p-1} &\equiv x^p z^p \pmod{\delta} \\ y^2 &\equiv xz \pmod{\delta} \end{aligned}$$

$$\begin{aligned} (29) \text{ より } (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \\ (y^2)^{p-1} &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \\ (xz)^{p-1} &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \\ x^{p-1} z^{p-1} &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \end{aligned}$$

$$R_3^1 \cdot R_1^2 \not\equiv x^p z^p \pmod{\delta} \tag{34}$$

$$\begin{aligned} (33) \text{ より } -zy^{p-1} \cdot zx^{p-1} &\equiv x^p y^p \pmod{\delta} \\ -z^2 &\equiv xy \pmod{\delta} \\ z^2 &\equiv -xy \pmod{\delta} \end{aligned}$$

$$\begin{aligned} (30) \text{ より } (z^{p-1})^2 &\equiv -x^{p-1} y^{p-1} \pmod{\delta} \\ (z^2)^{p-1} &\equiv -x^{p-1} y^{p-1} \pmod{\delta} \\ (-xy)^{p-1} &\equiv -x^{p-1} y^{p-1} \pmod{\delta} \\ x^{p-1} y^{p-1} &\equiv -x^{p-1} y^{p-1} \pmod{\delta} \end{aligned}$$

$$R_2^1 \cdot R_1^1 \not\equiv x^p y^p \pmod{\delta} \tag{35}$$

Proposition 16

$e, d = \text{odd}$, $e \perp d$, $xz \perp \theta$

$$\begin{aligned} x^d &\equiv z^d \pmod{\theta} \\ x^e &\equiv z^e \pmod{\theta} \end{aligned} \tag{36}$$

\Rightarrow

$$x \equiv z \pmod{\theta} \tag{37}$$

Proof 17

d_n を d の素因数とすると、 $d = d_1 d_2 d_3 \cdots$

Fermat's little theorem より

$$\begin{aligned} e^{d_1-1} &\equiv 1 \pmod{d_1} \\ (e^{d_1-1})^{d_2-1} &\equiv 1 \pmod{d_2} \end{aligned}$$

$(e^{d_1-1})^{d_2-1} = d_1 d_2 m + 1$ とおけるので

$$(e^{d_1-1})^{d_2-1} \equiv 1 \pmod{d_1 d_2}$$

$$((e^{d_1-1})^{d_2-1})^{d_3-1} \equiv 1 \pmod{d_1 d_2 d_3}$$

\vdots

$$e^n \equiv 1 \pmod{d}$$

よって $e^n = dm + 1$ が存在する。

$$\begin{aligned} (x^e)^{e^{\cdots}} &\equiv (z^e)^{e^{\cdots}} \pmod{\theta} \\ x^{e^n} &\equiv z^{e^n} \pmod{\theta} \\ x^{dm+1} &\equiv z^{dm+1} \pmod{\theta} \end{aligned}$$

(36) より

$$\begin{aligned} x^{dm} &\equiv z^{dm} \pmod{\theta} \\ x &\equiv z \pmod{\theta} \end{aligned}$$

□

$$\begin{aligned}
x^{p-1} &\equiv -z^{p-1} \pmod{\delta} \\
(x^{p-1})^2 &\equiv (-z^{p-1})^2 \pmod{\delta} \\
x^{2p-2} &\equiv z^{2p-2} \pmod{\delta}
\end{aligned}$$

Fermat's little theorem より

$$\begin{aligned}
x^{\delta-1} &\equiv z^{\delta-1} \pmod{\delta} \\
(x^{\delta-1})^2 &\equiv (z^{\delta-1})^2 \pmod{\delta} \\
x^{2\delta-2} &\equiv z^{2\delta-2} \pmod{\delta}
\end{aligned}$$

$$\begin{aligned}
x^{2p-2\delta} &\equiv z^{2p-2\delta} \pmod{\delta} \\
(x^2)^{p-\delta} &\equiv (z^2)^{p-\delta} \pmod{\delta}
\end{aligned}$$

$p - \delta = 2^{n-1}d$ ($d \perp 2$, $n > 1$) とおくと

$$(x^{2^n})^d \equiv (z^{2^n})^d \pmod{\delta}$$

$\delta - 1 = 2k$ とおくと

$$\begin{aligned}
x^{2k} &\equiv z^{2k} \pmod{\delta} \\
(x^{2^n})^{2kj} &\equiv (z^{2^n})^{2kj} \pmod{\delta}
\end{aligned}$$

$2kj - d = e$, $e \perp d$ とおくと

$$(x^{2^n})^e \equiv (z^{2^n})^e \pmod{\delta}$$

(37) より

$$-x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \pmod{\delta} \text{ ならば}$$

$$\begin{aligned}
z^{2^n} &\equiv y^{2^n} \pmod{\delta} \\
x^{2^n} &\equiv z^{2^n} \pmod{\delta} \\
x^{2^n} &\equiv y^{2^n} \pmod{\delta}
\end{aligned} \tag{38}$$

Definition 18

$$\begin{aligned} -yx^{p-1} &= L_1^1, & -zx^{p-1} &= L_1^2 \\ -xy^{p-1} &= L_2^1, & zy^{p-1} &= L_2^2 \\ -xz^{p-1} &= L_3^1, & yz^{p-1} &= L_3^2 \end{aligned}$$

$$\begin{aligned} yz^{p-1} \cdot -yx^{p-1} &\equiv \pm x^p z^p \pmod{\delta} \\ &\Rightarrow \\ y^2 &\equiv \mp xz \pmod{\delta} \\ y^2 &\equiv x^2 z^2 \pmod{\delta} \\ &\vdots \\ y^{2^{n+1}} &\equiv x^{2^n} z^{2^n} \pmod{\delta} \end{aligned}$$

$$\begin{aligned} (29) \text{ より } (y^{p-1})^2 &\equiv -x^{p-1} z^{p-1} \pmod{\delta} \\ (y^{p-1})^4 &\equiv (x^{p-1} z^{p-1})^2 \pmod{\delta} \\ (y^4)^{p-1} &\equiv (x^2 z^2)^{p-1} \pmod{\delta} \end{aligned}$$

$$L_3^2 \cdot L_1^1 \not\equiv \pm x^p z^p \pmod{\delta} \Rightarrow y^2 \not\equiv \mp xz \pmod{\delta}$$

これは (38) に反するので

$$L_3^2 \cdot L_1^1 \not\equiv y^p \cdot y^p \pmod{\delta} \quad (39)$$

同様に

$$L_2^2 \cdot L_1^2 \not\equiv z^p \cdot z^p \pmod{\delta} \quad (40)$$

(34)(35),(39)(40) より

R と L は少なくとも 2 つの項が成立しないため同値変換は成り立たない。

$$\begin{aligned} sz^{p-1} + tx^{p-1} &\equiv uy^{p-1} \pmod{\delta} \\ &\not\equiv \\ (u-y)y^{p-1} + (z-s)z^{p-1} &\equiv (t+x)x^{p-1} \pmod{\delta} \end{aligned}$$

よって $\delta \perp 2$ のとき

$$x^p + y^p \not\equiv z^p \pmod{\delta}$$

1.4.6 $2 \mid x$, $2 \perp yz$

$S = 2^k$ のとき

$$x + z - y = p^n a 2^k$$

$$x^p = z^p - y^p = (z - y)(py^{p-1} + (z - y)(\dots))$$

$$2 \mid L = p^{pn-1} a^p$$

$$2 \mid a$$

$$2 \perp R = p\alpha^p$$

$$2 \perp \alpha$$

$$x + z - y = p^n a(\alpha + p^{(p-1)n-1} a^{p-1})$$

$$2^k = \alpha + p^{(p-1)n-1} a^{p-1} = \text{odd}$$

$$2^0 = 1$$

しかし、 $\alpha + p^{(p-1)n-1} a^{p-1} > 1$ なので矛盾する。

$S' = 2^k$ のとき

$$x + z - y = a' 2^k$$

$$x^p = z^p - y^p = (z - y)(py^{p-1} + (z - y)(\dots))$$

$$2 \mid L = a'^p$$

$$2 \mid a'$$

$$2 \perp R = \alpha'^p$$

$$2 \perp \alpha'$$

$$x + z - y = a'(\alpha' + a'^{p-1})$$

$$2^k = \alpha' + a'^{p-1} = \text{odd}$$

$$2^0 = 1$$

しかし、 $\alpha' + a'^{p-1} > 1$ なので矛盾する。

・ $2 \mid y$, $2 \perp xz$ のときは $y + z - x$

・ $2 \mid z$, $2 \perp xy$ のときは $z + x + y$ にて同様の結果を得る。

よって $\delta = 2$ のとき

$$x^p + y^p \not\equiv z^p \pmod{\delta}$$