ミラーラビン法とルーカスレーマー法による素数判定

岡垣祐二

2005年2月

大きな素数は正確な情報伝達手段の一つとして求められている。大きな数の素数性を調べる問題に対して、すべての自然数に適用できる判定法なのか、かなりたくさんの操作を必要としないかなどの問題がある。そこで、できるだけわずかな操作で、より短い時間で判定できる効率的な判定法を必要としている。ここでは、すべての自然数に適用できるミラーラビン法と、短い時間で判定できるルーカスレーマー法を紹介する。

その前に、単純な判定法の1つに次のものがある。

1 試行割算法

定理 1.1
$a \in Z, a > 1$ ならば a は素約数をもつ。
証明
$a \in Z, a > 1$ なので、a 自身が1より大きい約数である。a の1より大きい約数すべての中で一番小さい約数を p とする。もし p が約数 $b(\neq p)$ をもつなら、b は a の約数にもなり、p が a の一番小さい約数であることに反する。つまり、p は約数を持たないので素数である。(証明終)

定理 1.2
$n(\in N)$ が合成数ならば、n は $\sqrt{n} \geq p$ なる素約数 p をもつ。
証明
$n = ab \quad (a, b \in N)$ とする。$a > \sqrt{n}$ かつ $b > \sqrt{n}$ とすると $n = ab > \sqrt{n}\sqrt{n} = n$ となり矛盾する。つまり、$a \leq \sqrt{n}$ または $b \leq \sqrt{n}$ である。$a \leq \sqrt{n}$ のときを考える。定理1.1を使うと、a は素約数をもつ。この素約数を p とおく。この p は n の素約数である。また $p \leq a \leq \sqrt{n}$ でもある。(証明終)

定理1.2を用いると、$\sqrt{n}$ より小さいすべての素数に対して、n の約数である

かチェックすれば素数判定できる。しかし、nが大きいと$\sqrt{n}$より小さいすべての素数を知るのは大変で、この判定法は効率が悪い。大きな数に対する素数判定に有効なミラーラビン法を紹介する。

2　ミラーラビン法

準備として次の定理をしめす。
$\mathbb{Z}$を整数全体、$\mathbb{G}$を単位元1とする乗法群とする。$gcd(a,b)$はa,bの最大公約数とする。
定理 2.1
$g \in G, e \in Z$とする。$g^e = 1$となるのは、eがgの位数の倍数であるときまたはそのときに限る。
証明
$order \quad g = n$とする。$e = kn \quad (k \in Z)$ならば

$$g^e = g^{kn} = (g^n)^k = 1$$

となる。また、$g^e = 1$、$e = qn + r \quad (q, r \in Z, 0 \leq r < n)$と仮定する。

$$g^r = g^{e-qn} = g^e (g^n)^{-q} = 1$$

となる。nは$g^n = 1$を満たす、最小の正の整数であり、rの範囲は$0 \leq r < n$なので、$r = 0$となる。つまりeはnの倍数である。（証明終）

定理 2.2
$g(\in G)$の位数$e, n \in Z$とするならば、g^nの位数は$e/gcd(e,n)$となる。
証明
$order \quad g^n = k$とする。

$$(g^n)^{\frac{e}{gcd(e,n)}} = (g^e)^{\frac{n}{gcd(e,n)}} = 1$$

となるので、定理 2.1 より$e/gcd(e,n)$はkの倍数である。また

$$(g^n)^k = g^{nk} = 1$$

となるので、定理 2.1 よりnkはeの倍数である。nがeの倍数のとき$\forall k \in Z$でよいが、kはg^nの位数だから$k = 1$である。このとき、$gcd(e,n) = e$より、$k = e/gcd(e,n)$である。nがeの倍数でないとき、$n = gcd(e,n)a$、$e = gcd(e,n)b$ $(\exists a, b \in Z, b$はaを割り切らない$)$と表すことができる。nkがeの倍数であるためには、kは$b(= e/gcd(e,n))$の倍数でなければならない。また$e/gcd(e,n)$はkの倍数だから、$k = e/gcd(e,n)$となる。（証明終）

定理 2.3
G が位数 e の巡回群ならば、e の任意の正の約数 d に対して、G の位数 d の部分群をちょうど一つだけ持つ。
(理解不足のため証明無し)
$n(\in N)$ を奇数とする。

$$s = max\{r \in N : 2^r \mid (n-1)\}$$
$$d = \frac{n-1}{2^s}$$

定理 2.4
n を素数とする。$a \in Z$ に対して $gcd(a,n) = 1$ ならば

$$a^d \equiv 1 \mod n \tag{1}$$

を満たすか、$\exists r \in \{0,1,\cdots,s-1\}$ に対して

$$a^{2^r d} \equiv -1 \mod n \tag{2}$$

を満たす。
証明
n は素数なので、n を法とする剰余群 $(Z/n)^\times$ の位数は $n-1 = 2^s d$ である。
$a^d + nZ$ の位数を k とする。整数 2^s に対して定理 2.2 を用いると

$$(a^d)^{2^s} = \frac{k}{gcd(k,2^s)} = 1$$

$k = gcd(k,2^s)$ であるから、k は 2 のべき乗である。
$k = 1(= 2^0)$ とすると、$(a^d)^1 = 1$ なので

$$a^d \equiv 1 \mod n$$

$k > 1$ ならば、$(1 \leq \ell \leq s)$ に対して $k = 2^\ell$ と表せる。$a^{2^{\ell-1}d} + nZ$ の位数を m とする。整数 2 に対して定理 2.2 を用いると

$$(a^{2^{\ell-1}d})^2 = \frac{m}{gcd(m,2)} = a^{2^\ell d} = 1$$

$m = gcd(m,2)$ だから、m は 1 か 2 である。
$m = 1$ ならば

$$1 = a^{2^{\ell-1}d} = (a^d)^{2^{\ell-1}} = (a^d)^{\frac{1}{2}k}$$

であるが、k は a^d の位数であるのに、a^d が $\frac{1}{2}k$ 乗で 1 になることは矛盾している。m は 1 ではない。$m = 2$ ならば

$$1 = (a^{2^{\ell-1}d})^2 = (a^d)^{2^\ell} = (a^d)^k$$

条件にあう。$a^{2^{s-1}d}+nZ$ の位数は 2 である。定理 2.3 より、$(Z/n)^\times$ の位数 2 の部分群は $-1+nZ$ である。よって $r=\ell-1$ とおくと、$0\leq r<s$ となり

$$a^{2^r d}\equiv -1 \mod n$$

を満たす。(証明終)

n と互いに素な a が、(1),(2) をどちらも満たさないならば、n は合成数である。このようなときの a を n に対する $witness$(証言数) であるという。

定理 2.5
n が奇数かつ合成数ならば、$a\in\{1,2,\cdots,n-1\}$ に対して、$gcd(a,n)=1$ かつ n に対して $witness$ でない a の個数は、高々 $(n-1)/4$ である。
(証明)

$W=\{a\in\{1,2,\cdots,n-1\}\mid gcd(n,a)=1$ かつ定理 2.4 の (1)or(2) を満たす $\}$

$k=max\{r\in\{0,1,\cdots,s-1\}\mid \exists a\in\{1,2,\cdots,n-1\} s.t. a^{2^r d}\equiv -1 \pmod n\}$

$$m=2^k d,\qquad n=\prod_{p\mid n} p^{\nu(p)}$$

とおく。$(Z/nZ)^\times$ の部分群を次のように定義する。

$$J=\{a\in(Z/nz)^\times\mid gcd(a,n)=1, a^{n-1}\equiv 1 \pmod n\}$$

$$K=\{a\in(Z/nz)^\times\mid gcd(a,n)=1, a^m\equiv\pm 1 \pmod{p^{\nu(p)}}, \forall p\mid n\}$$

$$L=\{a\in(Z/nz)^\times\mid gcd(a,n)=1, a^m\equiv\pm 1 \pmod n\}$$

$$M=\{a\in(Z/nz)^\times\mid gcd(a,n)=1, a^m\equiv 1 \pmod n\}$$

これらの部分群について考える。明らかに $M\subset L$ である。L,K について $\forall a\in L$ とすると $n\mid a^m\pm 1$ であり、$\forall p\mid n$ で $p^{\nu(p)}\mid n$ なので、$p^{\nu(p)}\mid a^m\pm 1$ となる。よって、$L\subset K$. K,J について、$\forall a\in K$ とする. $a^m\equiv\pm 1 \pmod{p^{\nu(p)}}\forall p\mid n$ を 2^{s-k} 乗すると $a^{n-1}\equiv 1 \pmod{p^{\nu(p)}}, \forall p\mid n$ となる。これは $a^{n-1}\equiv 1 \pmod n$ と同じ. よって $K\subset J$. まとめると

$$M\subset L\subset K\subset J\subset(Z/nZ)^\times$$

次に $W\subset L$ になることを示す。
$W\ni\forall a$ に対して

$$a^d\equiv 1 \pmod n \qquad \text{を } 2^k \text{乗すると} \qquad a^m\equiv 1 \pmod n$$

$\exists r \in \{0,1,\cdots,s-1\} \quad s.t. \quad a^{2^r d} \equiv -1 \pmod{n}$. $a^{2^{r+1} d} \equiv -1 \pmod{n}$を$2^{k-r}$乗すると

$$a^{2^n} \equiv \begin{cases} 1 & (\mathrm{mod}\ n) \quad (\mathrm{k} \neq \mathrm{r}) \\ -1 & (\mathrm{mod}\ n) \quad (\mathrm{k} = \mathrm{r}) \end{cases}$$

よって$a \in L$.つまり,$W \subset L$.
$(Z/nZ)^\times$ における L の指数が少なくとも 4 であることを示すことにより定理を証明する。つまり

$$\sharp\left(\frac{(Z/nZ)^\times}{L}\right) \geq 4 \quad \Rightarrow \quad \sharp L \leq \frac{n-1}{4}$$
$$\Rightarrow \quad \sharp W \leq \frac{n-1}{4} \quad (W \subset L \text{であるから})$$

を示す。
まず、$\sharp((Z/nZ)^\times/L) \geq 4 \quad \Rightarrow \sharp L \leq \frac{n-1}{4}$ について示す。
準備としてつぎの定理を示す。
定理 2.5.1

$$G:\text{群}, H < G, \sharp G < \infty \Rightarrow \sharp(G/H) = \frac{\sharp G}{\sharp H}$$

証明
$G \ni \forall g$
$H \to gH \qquad h \to gh$
に対して,$h,h' \in H$ とするとき,$gh = gh'$ならば,G は群だから $G \ni \exists g^{-1}$なので、$h = h'$.よって単射である。従って、$\sharp H = \sharp gH$
H を法とする左合同関係によって,Gは$\sharp(G/H)$ 個の左剰余類に分割されるが各々の左剰余類は$\sharp H$ 個の元を持つ。よって$\sharp G = \sharp H \times \sharp(G/H)$.したがって $\sharp(G/H) = \frac{\sharp G}{\sharp H}$. (証明終)
定理 2.5.1 より

$$\sharp\left(\frac{(Z/nZ)^\times}{L}\right) \geq 4 \quad \Rightarrow \quad \frac{\sharp(Z/nZ)^\times}{\sharp L} \geq 4$$
$$\Rightarrow \quad \frac{n-1}{\sharp L} \geq 4$$
$$\Rightarrow \quad \sharp L \leq \frac{n-1}{4}$$

次に $\sharp(K/M) = 2$ のべき乗 であることを示す。
準備として $K \ni \forall a \Rightarrow a^2 \in M$ を示す。
証明
中国式剰余定理から $n = \prod_{p_i | n}^{t} p_i^{v(p_i)}$

$$\Rightarrow (Z/nZ)^\times \simeq (Z/p_1^{v(p_1)}Z)^\times \times (Z/p_2^{v(p_2)}Z)^\times \times \cdots \times (Z/p_t^{v(p_t)}Z)^\times$$

$$a^m = \pm 1 \leftrightarrow a^m = \pm(1,\cdots,1)$$

$\ell : n$ を素因数分解したときの素数の数とする

$$\begin{aligned}
a \in K &\Leftrightarrow a^m \equiv \begin{cases} 1 & (\mathrm{mod}\ p_i^{e(p_i)}) \\ -1 & (\mathrm{mod}\ p_i^{e(p_i)}) \end{cases} \quad (\text{各々} p_i) \\
a^m &= (\pm 1,\cdots,\pm 1) \\
a \in L &\Leftrightarrow a^m \equiv \begin{cases} 1 & (\mathrm{mod}\ n) \\ -1 & (\mathrm{mod}\ n) \end{cases} \\
a^m &= \pm(1,\cdots,1) \\
a \in M &\Leftrightarrow a^m \equiv 1 \pmod{n} \\
a^m &= (1,\cdots,1)
\end{aligned}$$

$K \ni a \Rightarrow a^{2m} = (1,\cdots,1)$ よって $a^2 \in M$

(証明終)

このことにより $(K/M) \ni \forall a+M \Rightarrow (a+M)^2 = 1$ である。つまり $(K/M) \ni a+M$ の位数は 2 以下である。

アーベル群の基本定理より

$$(K/M) \simeq \prod (Z/p_i^{e(p_i)}Z)$$

$(K/M) \ni a+M$ の位数は 2 以下であるので

$$(K/M) \simeq \prod (Z/2Z)$$

よって $\sharp(K/M) = 2$ のべき乗である。

次に $\sharp(K/L)$ について考える。$n = \prod_{p_i \mid n, i=1}^{l} p_i\, e(p_i)$ のとき

$$\sharp(K/L) = 2^{l-1} \qquad (\ell : n \text{を素因数分解したときの素数の数})$$

を示す。

その前に次の定理を示す。

定理 2.5.2

G_1, G_2;群, $H < G_2$ とする

$$\begin{array}{rcl}
\varphi : G_1 & \to & G_2 \\
\cup & & \cup \\
\varphi' : \varphi^{-1}(H) & \to & H
\end{array}$$

φ, φ' が全射準同型ならば $\sharp(G_2/H) = \sharp(G_1/\varphi^{-1}(H))$
(証明)
$(Ker\varphi' \ni) \forall g_1 \quad s.t. \quad \varphi'(g_1) = e_H$に対して,$\varphi^{-1}(e_H) \ni g_1$より$\varphi(g_1) = e_H$.
つまり $g_1 \in Ker\varphi$.よって $Ker\varphi' \subset Ker\varphi$
$Ker\varphi = \varphi^{-1}(e_H) \subset \varphi^{-1}(H)$.よって $\quad Ker\varphi \subset Ker\varphi'$
従って,$Ker\varphi = Ker\varphi'$ 群準同型定理から

$$G_2 \simeq G_1/Ker\varphi, H \simeq \varphi^{-1}(H)/Ker\varphi'$$

定理 2.5.1 より

$$\sharp G_2 = \frac{\sharp G_1}{\sharp Ker\varphi}, \sharp H = \frac{\sharp \varphi^{-1}(H)}{\sharp Ker\varphi'}$$

よって、$\sharp(G_2/H) = \sharp(G_1/\varphi^{-1}(H))$

(証明終)

$$(Z/nZ)^\times \simeq (Z/p_1^{e(p_1)}) \times (Z/p_2^{e(p_2)}) \times \cdots \times (Z/p_l^{e(p_l)})$$

$$\begin{array}{ccc} K & \longrightarrow & \{(\pm 1, \pm 1, \cdots, \pm 1)\} \\ \cup & & \\ L & \longrightarrow & \{\pm(1, 1, \cdots, 1)\} \end{array}$$

定理 2.5.1, 定理 2.5.2 より

$$\sharp(K/L) = \sharp(2^l/2) = 2^{l-1}$$

$\sharp(K/L) = 2^j$ とおく。

1. $j \geq 2$ のとき

$$2^j = \sharp(K/L) = \frac{\sharp K}{\sharp L} \text{より、} \sharp L = \frac{\sharp K}{2^j} \leq \frac{\sharp K}{4} \leq \frac{\sharp(Z/nZ)^\times}{4}$$

よって $\sharp L \leq \frac{n-1}{4}$ となり、定理を満たす。

2. $j = 1$ のとき
$2^1 = \sharp(K/L) = 2^{l-1}$ よって $l = 2$. $\quad n$ は 2 つの素因数をもつ。
ここで次の定理を示す。
n が Carmichael 数であるとは、$\forall a \in Z \quad s.t. \quad gcd(a, n) = 1,$ に対し

て $a^{n-1} \equiv 1 \pmod{n}$ が成立
定理 2.5.3
$n : Carmichael$ 数 $\Rightarrow n$ は少なくとも 3 つの異なった素因数を持つ
(理解不足のため証明無し)
定理 2.5.3 より n は Carmichael 数ではない。よって
$\exists a \in (Z/nZ)^{\times} \quad s.t. \quad a^{n-1} \neq 1 \pmod{n}$
であるので,$J \neq (Z/nZ)^{\times}$.$(J \subset (Z/nZ)^{\times})$
従って

$$\sharp((Z/nZ)^{\times}/J) \geq 2$$

よって

$$\begin{aligned} \sharp((Z/nZ)^{\times}/L) &= \sharp((Z/nZ)^{\times}/J) \times \sharp(J/K) \times \sharp(K/L) \\ &\geq 2 \times \sharp(J/K) \times 2 \\ &\geq 4 \end{aligned}$$

よって $\sharp L \leq \frac{n-1}{4}$ となり定理を満たす。

3. j=0 のとき
$2^0 = \sharp(K/L) = 2^{l-1}$ よって $l = 1$. つまり n は 1 の素因数をもつ。
$n = p^e$ とおく。

$$J = \{a \in (Z/nz)^{\times} \mid gcd(a,n) = 1, a^{p^e-1} \equiv 1 \pmod{p^e}\}$$

$\psi(n)$ を n と互いに素で n より小さいものの個数とする。
$\sharp(Z/p^e Z)^{\times} = \psi(p^e) = (p-1)p^{e-1}$ より

$$\begin{aligned} a \in J &\Leftrightarrow a^{\psi(p^e)} \equiv 1 \pmod{p^e}, a^{p^e-1} \equiv 1 \pmod{p^e} \\ &\Leftrightarrow a^{gcd(\psi(p^e), p^e-1)} \equiv 1 \pmod{p^e} \\ &\Leftrightarrow a^{p-1} \equiv 1 \pmod{p^e} \end{aligned}$$

定理 2.5.4
$(Z/p^e Z)^{\times} = (Z/(p-1)Z) \times (Z/p^{e-1}Z)$
(理解不足のため証明無し)
これにより $(Z/p^e Z)^{\times}$ の中に位数 $p-1$ を割り切るものはちょうど $p-1$ 個である。よって、$\sharp J = p-1$.
$n = p^e$ において n は奇数の合成数なので最小のものは $n = 9$ である。
$\{1,2,\cdots,8\}$ のなかで 9 と互いに素で witness でないものは、1,8 である。1 と 8 の 2 個なので、定理の $\frac{n-1}{4} = \frac{8}{4} = 2$ を満たす。
つぎに小さい数は $p = 5, e = 2$. よって、$p^{e-1} \geq 5$.

$$\sharp\frac{(Z/nZ)^{\times}}{J} = \frac{\sharp(Z/nZ)^{\times}}{\sharp J} = \frac{(p-1)p^{e-1}}{p-1} = p^{e-1} \geq 4$$

$L \subset J$ より　$\sharp\frac{(\mathbb{Z}/n\mathbb{Z})^\times}{L} \geq 4$

(証明終)

　ミラーラビン法
奇数 n に対して判定する。
ランダムに $a \in 1,2,\cdots,n-1$ を選ぶ。
$gcd(a,n) > 1$　$\Rightarrow n$ は合成数。
$gcd(a,n) = 1$　$\Rightarrow (1),(2)$ を満たすかチェックする。
$(1),(2)$ をともに満たさない場合、定理 2.4 により n は合成数。
(1) か (2) を満たす場合、定理 2.5 により n が合成数である確率は高々 $1/4$。
この作業を i 回繰り返して、(1) か (2) を満たす場合ばかりなら高々 $(1/4)^i$ の確率で n は合成数である。つまり、$1-(1/4)^i$ の確率で n は素数である。i を大きくすれば高い確率で n は素数である。
つぎに確率的ではない判定法のルーカスレーマー法を紹介する。

3　ルーカスレーマー法

　準備としてヤコビ記号、ルーカス数列の定義する。

3.1　ヤコビ記号

　pを奇素数とする。p と互いに素な a に対して $a \equiv b^2 mod \quad p$ なる整数 b が存在するならば a は法 p に関して平方剰余という。
定義 3.1（ルジャンドルの記号）

$$(\frac{a}{p}) = \begin{cases} 1 & (a\text{が法}\ p\text{で平方剰余}) \\ -1 & (\text{その他}) \end{cases}$$

　定義 3.2（ヤコビ記号）
a は 0 でない整数、b は奇数で $gcd(a,b) = 1$ とする。

$$|b| = \prod_{p|b} p^{e_p} \quad (\text{各}\ p\ \text{は}\ b\ \text{を割り切る異なる素数}, e_p \geq 1)$$

このとき

$$(\frac{a}{b}) = (\frac{a}{-b}) = \prod_{p|b} (\frac{a}{p})^{e_p}$$

と定義する。
定理 3.1(オイラー規準)
pを奇素数とする。p と a は互いに素ならば

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} mod \quad p$$

証明
まず、次の 2 つの定理を示す。
定理 3.1.1

$$ax \equiv b \pmod{p}$$

$gcd(a,p) = 1$ のときただ一つ解がある。$gcd(a,p) = d > 1$ のときは b が d で割り切れるときに限って解がある。その解の個数は d である。
証明
$gcd(a,p) = 1$ のとき,$\{x_1,x_2,\cdots,x_p\}$ を p を法とする剰余系とする。このとき $\{ax_1,ax_2,\cdots,ax_p\}$ も p を法とする剰余系である。
なぜなら $\{ax_1,ax_2,\cdots,ax_p\} \ni ax_i,ax_j$ に対して

$$ax_i \equiv ax_j \pmod{p}$$

なら、$gcd(a,p) = 1$ であるので

$$x_i \equiv x_j \pmod{p}$$

となる。それは $i = j$ のときに限るからである。ゆえに任意の b に対して $\{x_1,x_2,\cdots,x_p\}$ のなかのただ一つ

$$ax_i \equiv b \pmod{p}$$

となる x_i が存在する。
$gcd(a,p) = d > 1$ のとき
解があると仮定すると、$ax - b = pN \quad (N \in Z)$ と表される。ゆえに $b = ax - pN$ は $d = gcd(a,p)$ で割り切れる。そこで

$$a = da' \quad p = dp' \quad b = db'$$

とおく。このとき

$$ax \equiv b \pmod{p} \Leftrightarrow a'x \equiv b' \pmod{p'}$$

となる。$gcd(a',p') = 1$ なので,$a'x \equiv b' \pmod{p'}$ を満たす x は p' を法とする一つの類である。それを $x \equiv x_0 \pmod{p}$ とする。$a'x \equiv b' \pmod{p'}$ の解は

$$x = x_0 + p't \quad t \text{ は任意の整数}$$

によって与えられる。t_1とt_2に対するxがpを法として合同になるのは

$$x_0+p^lt_1 \equiv x_0+p^lt_2 \pmod{p}$$

$$p^l(t_1-t_2) \equiv 0 \pmod{p}$$

$p^l(t_1-t_2)=pS \quad S \in Z$と表されるので,$(t_1-t_2)=dS$.つまり

$$t_1-t_2 \equiv 0 \pmod{d}$$

となるときに限る。したがってtにdを法とする剰余系$\{0,1,\cdots,d-1\}$の値を与えるとき、mを法とする$ax \equiv b \pmod{p}$のすべての解が得られる。その解の個数はdである。
(証明終)
定理 3.1.2
p:素数,$a \not\equiv 0 \pmod{p}$とする。

$$x^n \equiv a \pmod{p}$$

に解があるための必要十分条件は$f=\frac{p-1}{gcd(n,p-1)}$とするとき

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

である。
(証明)
$(Z/p)^\times$の原始根をrとする。rを底としてのaの指数をInd_raと表す。x^n,aに対して

$$r^{Ind_rx^n} \equiv x^n \pmod{p} \qquad r^{Ind_ra} \equiv a \pmod{p}$$

となる。$x^n \equiv a$なので

$$r^{Ind_rx^n} \equiv r^{Ind_ra} \pmod{p}$$

$$Ind_rx^n \equiv Ind_ra \pmod{p-1}$$

$$n \cdot Ind_rx \equiv Ind_ra \pmod{p-1}$$

この合同式を解くことは$x^n \equiv a \pmod{p}$を解くことと等しい。
$(\Rightarrow) \quad x^n \equiv a \pmod{p}$が解を持つとする。
$gcd(n,p-1)=c$とする。定理3.1.1より、解を持つから$c \mid Ind_ra$. $Ind_ra=qc \quad (q \in Z)$とする。このとき

$$a \equiv r^{Ind_ra} \pmod{p}.$$

両辺をf乗すると

$$a^f \equiv r^{f \cdot Ind_ra} \equiv r^{\frac{p-1}{c} \cdot qc} \equiv r^{(p-1)q} \equiv 1 \pmod{p}.$$

($\Leftarrow$)　$a^f \equiv 1 \pmod{p}$ ならば

$$r^{Ind_r a} \equiv a \pmod{p}$$

を両辺 f 乗して

$$r^{f \cdot Ind_r a} \equiv a^f \equiv 1 \pmod{p}$$

よって $f \cdot Ind_r a = \frac{p-1}{c} Ind_r a = (p-1)t \quad (t \in Z)$. つまり

$$Ind_r a = ct.$$

$c \mid Ind_r a$ が示せたので $n \cdot Ind_r x \equiv Ind_r a \pmod{p-1}$ は解をもつ。
(証明終)
定理 3.1.2 より, $a \equiv x^2 \pmod{p}$ が解をもつ、つまり平方剰余であること
$\Leftrightarrow$

$$a^{\frac{p-1}{gcd(2,p-1)}} \equiv 1 \pmod{p}$$

$p-1$ は偶数だから

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

である。ゆえに $(\frac{a}{p}) = 1$ ならば、$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ で $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
また $(\frac{a}{p}) = -1$ ならば、$a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ である。フェルマーの小定理より

$$(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$$

であるから、$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ となり、$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
(証明終)
ルジャンドル記号の性質
$a \equiv a' mod \quad p$

$$(\frac{a}{p}) = (\frac{a'}{p})$$

任意の整数 a, a' に対して、

$$(\frac{aa'}{p}) = (\frac{a}{p})(\frac{a'}{p}).$$

(証明)
$(Z/pZ)^\times$ の原始根を r とする。まず、平方剰余であるなら $Ind_r a$ が偶数、平方剰余でないなら $Ind_r a$ が奇数であることを示す。
平方剰余であるなら、定理 3.1.2 の議論から $c \mid Ind_r a$.　今、$c = gcd(2, p-1) = 2$ なので, $Ind_r a$ は偶数。平方剰余でないなら $2 \nmid Ind_r a$ なので $Ind_r a$ は奇数。
従って

$$(\mathrm{i}) \quad (\frac{a}{p}) = (-1)^{Ind_r a}.$$

$a \equiv a' mod \quad p$ のとき $Ind_r a \equiv Ind_r a' \pmod{p-1}$. $p-1$ は偶数なので、$Ind_r a$ が偶数なら $Ind_r a'$ もっ偶数。$Ind_r a$ が奇数なら $Ind_r a'$ も奇数。従って (i) より

$$(\frac{a}{p}) = (\frac{a'}{p})$$

任意の整数 a, a' に対して、(i) より

$$\begin{aligned}(\frac{aa'}{p}) &= (-1)^{Ind_r aa'} = (-1)^{Ind_r a + Ind_r a'} \\ &= (-1)^{Ind_r a}(-1)^{Ind_r a'} = (\frac{a}{p})(\frac{a'}{p})\end{aligned}$$

補足

$$r^{Ind_r a} \equiv a \pmod{p} \qquad r^{Ind_r a'} \equiv a' \pmod{p}$$

ゆえに両辺それぞれ掛けると

$$aa' \equiv r^{Ind_r a + Ind_r a'} \pmod{p}$$

また

$$aa' \equiv r^{Ind_r aa'} \pmod{p}$$

でもある。従って

$$Ind_r aa' \equiv Ind_r a + Ind_r a' \pmod{p-1}$$

(証明終)

定理 3.2
p, q を相異なる奇素数とする。

$$(1) \qquad (\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

$$(2) \qquad (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & (p \equiv 1 \mod 4) \\ -1 & (p \equiv 3 \mod 4) \end{cases}$$

$$(3) \qquad (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & (p \equiv 1, 7 \mod 8) \\ -1 & (p \equiv 3, 5 \mod 8) \end{cases}$$

(1) の証明は理解不足のため無し
(2) の証明
オイラー規準を $a = -1$ で用いると

$$(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

pは奇数であるから

$$(\frac{-1}{p})=(-1)^{\frac{p-1}{2}}$$

(証明終)
(3)の証明
まず次の定理を示す。
定理 3.2.1
aがpで割り切れないならば

$$1a,2a,3a,\cdots,\frac{p-1}{2}a \qquad (\mathrm{i})$$

をpで割るとき、その剰余の中に$\frac{p}{2}$より大きいものがn個あれば

$$(\frac{a}{p})=(-1)^n$$

(証明)
法pに関する剰余のうち$\frac{p}{2}$より大きいものについて、それからpを引くと、絶対値において$\frac{p}{2}$より小さい剰余を得る。pを法とする剰余をこのように絶対値で最小になるようにとると、nはそのうち負な剰余の個数である。(i)の数の絶対値最小な剰余は

$$\pm1,\pm2,\cdots,\pm\frac{p-1}{2}$$

の中にある。(i)のなかのどの二つの和も差もpで割り切れない(つまり、どの二つも同じ剰余類ではない)ので、(i)の絶対値最小剰余はすべて異なるのみでなく、(i)のなかに絶対値が等しいものもない。(i)の$\frac{p-1}{2}$個の数は絶対値をとると$1,2,\cdots,\frac{p-1}{2}$と1対1に対応し、そのうちn個が負である。よって

$$1a,2a,3a,\cdots,\frac{p-1}{2}a\equiv(-1)^n1\cdot2\cdot\cdots\cdot\frac{p-1}{2} \pmod p$$

従って

$$a^{\frac{p-1}{2}}\equiv(-1)^n \pmod p.$$

オイラー規準より

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

である。pは奇数なので

$$(\frac{a}{p})=(-1)^n$$

(証明終)
定理 3.2.1 を$a=2$で用いる。つまり

$$2,4,6,\cdots,p-5,p-3,p-1$$

となる。このうち $\frac{p}{2}$ より大きいものの個数が n である。(ⅰ)の左から k 番目の数は $2k$ であるとする。$\frac{p}{2}<2k$ は $p-2k<\frac{p}{2}$ と同値であるから、$p-2k<\frac{p}{2}$ を満たす k のうち最小のものを k' とすると、その個数は $p-2k', \cdots, 5, 3, 1$ の個数である。$\frac{p-1}{2}$ が奇数なら $\frac{p-1}{2}$ まで、$\frac{p-1}{2}$ が偶数なら $\frac{p-1}{2}-1$ までである。
いずれにせよ

$$\begin{aligned} n &\equiv 1+3+\cdots+(\frac{p}{2}\text{より小さい奇数}) \pmod 2 \\ &\equiv 1+2+3+\cdots+\frac{p-1}{2} \pmod 2 \end{aligned}$$

すなわち

$$n \equiv \frac{1}{2}\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)=\frac{p^2-1}{8} \pmod 2$$

よって

$$(\frac{2}{p})=(-1)^n=(-1)^{\frac{p^2-1}{8}}$$

(証明終)
定義 3.3(ルーカス数列)
P,Q を 0 でない整数として、2 次多項式 X^2-PX+Q を考える。判別式は $D=P^2-4Q$ であり、解は

$$a=\frac{P+\sqrt{D}}{2}, \quad b=\frac{P-\sqrt{D}}{2}$$

であるから、$a+b=P, \quad ab=Q, \quad a-b=\sqrt{D}$.

$$U_n(P,Q)=\frac{a^n-b^n}{a-b}, \quad V_n(P,Q)=a^n+b^n$$

$$U(P,Q)=(U_n(P,Q))_{n\geq 0}, \quad V(P,Q)=(V_n(P,Q))_{n\geq 0}$$

と定義する。$U(P,Q)$ と $V(P,Q)$ を同伴ルーカス数列という。
ルーカス数列の関係式

3.3.1 $$U_n=PU_{n-1}-QU_{n-2} \quad (n\geq 2) \quad U_0=0, U_1=1,$$

$$V_n=PV_{n-1}-QV_{n-2} \quad (n\geq 2) \quad V_0=2, V_1=P$$

3.3.2 $$U_{2n}=U_nV_n \qquad V_{2n}=V_n^2-2Q^n$$

3.3.3 $$U_{m+n}=U_mV_n-Q^nU_{m-n}$$

$$V_{m+n}=V_mV_n-Q^nV_{m-n} \quad (m\geq n)$$

3.3.4
$$U_{m+n} = U_m U_{n+1} - QU_{m-1}U_n$$
$$2V_{m+n} = V_m V_n + DU_m U_n \quad (m \geq n)$$

3.3.5
$$DU_n = 2V_{n+1} - PV_n$$
$$V_n = 2U_{n+1} - PU_n$$

3.3.6
$$U_n^2 = U_{n-1}U_{n+1} + Q^{n-1}$$
$$V_n^2 = DU_n^2 + 4Q^n$$

(3.3.1) ~ (3.3.6) の証明は具体的に代入することで示せる。

3.3.7
$$2^{n-1}U_n = \binom{n}{1}P^{n-1} + \binom{n}{3}P^{n-3}D + \binom{n}{5}P^{n-5}D^2 + \cdots$$
$$2^{n-1}V_n = P^n + \binom{n}{2}P^{n-2}D + \binom{n}{4}P^{n-4}D^2 + \cdots$$

証明

(1) $2^{n-1}V_n + \sqrt{D}2^{n-1}U_n = (P + \sqrt{D})^n$
(2) $2^{n-1}V_n - \sqrt{D}2^{n-1}U_n = (P - \sqrt{D})^n$

を示す。

$$\begin{aligned} 2^{n-1}(V_n + \sqrt{D}U_n) &= 2^{n-1}(a^n - b^n + a^n + b^n) \\ &= 2^{n-1}(2a^n) = (2a)^n = (a+b+a-b)^n \\ &= (P + \sqrt{D})^n \end{aligned}$$

$2^{n-1}V_n - \sqrt{D}2^{n-1}U_n = (P - \sqrt{D})^n$ も同様にして示せる。(1),(2) を両辺それぞれたすと

$$\begin{aligned} 2^n V_n &= 2\{P^n + \binom{n}{2}P^{n-2}D + \binom{n}{4}P^{n-4}D^2 + \cdots\} \\ 2^{n-1}V_n &= P^n + \binom{n}{2}P^{n-2}D + \binom{n}{4}P^{n-4}D^2 + \cdots \end{aligned}$$

また

$$2^{n-1}U_n = \binom{n}{1}P^{n-1} + \binom{n}{3}P^{n-3}D + \binom{n}{5}P^{n-5}D^2 + \cdots$$

(証明終)

3.3.8 m は奇数で $k \geq 1$ のとき

$$D^{\frac{m-1}{2}}U_k^m = U_{km} - \binom{m}{1}Q^k U_{k(m-2)} - \binom{m}{2}Q^{2k}U_{k(m-4)}$$
$$- \cdots \pm \binom{m}{\frac{m-1}{2}}Q^{\frac{m-1}{2}k}U_k$$
$$V_k^m = V_{km} - \binom{m}{1}Q^k V_{k(m-2)} - \binom{m}{2}Q^{2k}V_{k(m-4)}$$
$$+ \cdots + \binom{m}{\frac{m-1}{2}}Q^{\frac{m-1}{2}k}V_k$$

m は偶数で $k \geq 1$ のとき

$$D^{\frac{m}{2}}U_k^m = V_{km} - \binom{m}{1}Q^k V_{k(m-2)} - \binom{m}{2}Q^{2k}V_{k(m-4)}$$
$$+ \cdots + \binom{m}{\frac{m}{2}}Q^{\frac{m}{2}k}2$$
$$V_k^m = V_{km} - \binom{m}{1}Q^k V_{k(m-2)} - \binom{m}{2}Q^{2k}V_{k(m-4)}$$
$$+ \cdots + \binom{m}{\frac{m}{2}}Q^{\frac{m}{2}k}2$$

(理解不足のため証明無し)

3.3.9 (1) $U_m = V_{m-1} + QV_{m-3} + Q^2V_{m-5} + \cdots +$ (最終項)

$$\text{最終項} = \begin{cases} Q^{\frac{m-2}{2}}P & (m\text{：偶数のとき}) \\ Q^{\frac{m-1}{2}} & (m\text{：奇数のとき}) \end{cases}$$

(2) $P^m = V_m + \binom{m}{1}QV_{m-2} + \binom{m}{2}Q^2V_{m-4} + \cdots +$ (最終項)

$$\text{最終項} = \begin{cases} \binom{m}{\frac{m}{2}}Q^{\frac{m}{2}} & (m\text{：偶数のとき}) \\ \binom{m}{\frac{m-1}{2}}Q^{\frac{m-1}{2}}P & (m\text{：奇数のとき}) \end{cases}$$

(証明)
(1)

$$
\begin{aligned}
\text{右辺} &= a^{n-1}+b^{n-1}+ab(a^{n-3}+b^{n-3})+a^2b^2(a^{n-5}+b^{n-5})+\cdots \\
&= a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+a^2b^{n-3}+ab^{n-2}+b^{n-1} \\
&\quad \text{初項 } a^{n-1}\text{,公比 } b/a \text{ の等比数列の和だから} \\
&= \frac{a^{n-1}(1-(\frac{b}{a})^n)}{1-\frac{b}{a}}=\frac{a^n-b^n}{a-b}=U_n
\end{aligned}
$$

(2)

$$
\begin{aligned}
P^m &= (a+b)^m=a^m+\binom{m}{1}a^{m-1}b+\cdots+\binom{m}{m-1}ab^{m-1}+b^m \\
&= \{a^m+b^m\}+\{\binom{m}{1}a^{m-1}b+\binom{m}{m-1}ab^{m-1}\}+\cdots \\
&\quad +\begin{cases} \binom{m}{\frac{m}{2}}(ab)^{\frac{m}{2}} & (m:\text{偶数のとき}) \\ \{\binom{m}{\frac{m-1}{2}}a^{m-\frac{m-1}{2}}b^{\frac{m-1}{2}}+\binom{m}{\frac{m+1}{2}}a^{m-\frac{m+1}{2}}b^{\frac{m+1}{2}}\} & (m:\text{奇数のとき}) \end{cases} \\
&= V_m+\binom{m}{1}QV_{m-2}+\binom{m}{2}Q^2V_{m-4}+\cdots \\
&\quad +\begin{cases} \binom{m}{\frac{m}{2}}Q^{\frac{m}{2}} & (m:\text{偶数のとき}) \\ \binom{m}{\frac{m-1}{2}}Q^{\frac{m-1}{2}}P & (m:\text{奇数のとき}) \end{cases}
\end{aligned}
$$

(証明終)

3.3.10

$$U_n=V_{n-1} \mod Q$$

$$V_n=P^n \mod Q$$

(証明)
(3.3.9) より

$$
V_{n-1}-U_n=-QV_{m-3}-Q^2V_{m-5}-\cdots-\begin{cases} Q^{\frac{m-2}{2}}P & (m:\text{偶数のとき}) \\ Q^{\frac{m-1}{2}} & (m:\text{奇数のとき}) \end{cases}
$$

$$
P^n-V_n=\binom{m}{1}QV_{m-2}+\binom{m}{2}Q^2V_{m-4}+\cdots+\begin{cases} \binom{m}{\frac{m}{2}}Q^{\frac{m}{2}} & (m:\text{偶数のとき}) \\ \binom{m}{\frac{m-1}{2}}Q^{\frac{m-1}{2}}P & (m:\text{奇数のとき}) \end{cases}
$$

(証明終)

3.3.11

p : 奇素数

$$U_{kp}\equiv D^{\frac{p-1}{2}}U_k \mod p$$

そして各 $c \geq 1$ に対して

$$U_{p^c} \equiv D^{\frac{p^c-1}{2}} \mod p$$

特に

$$U_p \equiv (\frac{D}{p}) \mod p$$

(証明) (3.3.8) より

$$D^{\frac{p-1}{2}}U_k^p - U_{kp} = -\binom{p}{1}Q^k U_{k(p-2)} - \binom{p}{2}Q^{2k}U_{k(p-4)}$$
$$- \cdots \pm \binom{p}{\frac{p-1}{2}}Q^{\frac{p-1}{2}k}U_k.$$

二項係数は p の倍数なので $D^{\frac{p-1}{2}}U_k^p - U_{kp}$ は p の倍数である。よって、

$$U_{kp} \equiv D^{\frac{p-1}{2}}U_k^p \mod p$$

また、p は素数なので

$$U_k^p \equiv U_k \mod p.$$

従って、

$$U_{kp} \equiv D^{\frac{p-1}{2}}U_k \mod p.$$

$c \geq 1$ に対して

$$\begin{aligned} U_{p^c} = U_{p^{c-1}p} &\equiv D^{\frac{p-1}{2}}U_{p^{c-1}} \equiv D^{\frac{p-1}{2}}\left(D^{\frac{p-1}{2}}U_{p^{c-2}}\right) \equiv \cdots \\ &\equiv D^{\frac{p-1}{2}c}U_{p^0} = D^{\frac{p-1}{2}c}U_1 = D^{\frac{p-1}{2}c} \mod p. \end{aligned}$$

特に $c = 1$ のとき、オイラー規準を用いると

$$(\frac{D}{p}) \equiv D^{\frac{p-1}{2}} \equiv U_p \mod p$$

(証明終)

3.3.12 p : 奇素数とするとき、$V_p \equiv P \mod p$

(証明)
(3.3.9) の (2) より

$$P^p - V_p = \binom{p}{1}QV_{p-2} + \binom{p}{2}Q^2V_{p-4} + \cdots + \binom{p}{\frac{p-1}{2}}Q^{\frac{p-1}{2}}P.$$

よって $F^p - V_p$ は p の倍数。また、p は素数なので $F^p \equiv P \mod p$. 従って

$$V_p \equiv P \mod p$$

(証明終)

3.3.13 $n, k \leq 1$ のとき U_n は U_{kn} を割り切る。

(3.3.3) を用いて帰納法で示す。

1. $U_n \mid U_n$, $U_{2n} = U_n V_n$ より $U_n \mid U_{2n}$ は成り立つ。
2. $U_n \mid U_{(k-1)n}, U_n \mid U_{kn}$ が成り立つと仮定する。(3.3.3) より $U_{(k+1)n} = U_{kn}V_n - Q^n U_{(k-1)n}$ なので

$$U_n \mid U_{(k+1)n}$$

(証明終)

3.3.14

(1) Q、P が偶数ならば、$U_n (n \geq 2)$ と $V_n (n \geq 1)$ は偶数
(2) Q が偶数、P が奇数ならば、$U_n (n \geq 1)$ と $V_n (n \geq 1)$ は偶数
(3) Q が奇数、P が偶数ならば、$U_n \equiv n \mod 2$ かつ V_n は奇数
(4) Q、P が奇数ならば、U_n と V_n は $3 \mid n$ のとき偶数、その他のときは奇数
(5) 特に U_n が偶数ならば、V_n は偶数
(理解不足のため証明無し)

3.3.15 p : 奇素数

(1) $p \mid P$ かつ $p \mid Q$ ならば、任意の $k > 1$ に対して $p \mid U_k$
(2) $p \mid P$ かつ $p \nmid Q$ ならば、k が偶数の時に限り $p \mid U_k$
(3) $p \nmid P$ かつ $p \mid Q$ ならば、任意の $k \geq 1$ に対して $p \nmid U_k$.
(4) $p \mid D$ かつ $p \nmid P$、$p \nmid Q$ ならば、$p \mid k$ のときに限り $p \mid U_k$
(5) $p \nmid PQD$ ならば、$p \mid D_{\psi(p)}$.ただし $\psi(p) = p - (D/p)$
(理解不足のため証明無し)

3.3.16 $m \geq 1$ で g が奇数のとき

$$U_{mq}=D^{\frac{q-1}{2}}U_m^q+\frac{q}{1}Q^mD^{\frac{q-2}{2}}U_m^{q-2}+\frac{q}{2}\binom{q-3}{1}Q^{2m}D^{\frac{q-3}{2}}U_m^{q-4}$$
$$+\cdots+\frac{q}{r}\binom{q-r-1}{r-1}Q^{rm}D^{\frac{q-2r-1}{2}}U_m^{q-2r}+\cdots+(\text{最終項})$$
$$\text{最終項}=\frac{q}{(q-1)/2}\binom{\frac{q-1}{2}}{\frac{q-3}{2}}Q^{\frac{q-1}{2}-m}U_m=qQ^{\frac{q-1}{2}-m}U_m.$$

(証明)
Lagrange(1741 年) による次の恒等式を使う。

$$\begin{aligned}X^n+Y^n &= (X+Y)^n-\frac{n}{1}XY(X+Y)^{n-2}\\ &+ \frac{n}{2}\binom{n-3}{1}X^2Y^2(X+Y)^{n-4}\\ &- \frac{n}{3}\binom{n-4}{2}X^3Y^3(X+Y)^{n-6}+\cdots\\ &+ (-1)^r\frac{n}{r}\binom{n-r-1}{r-1}X^rY^r(X+Y)^{n-2r}\pm\cdots\end{aligned}$$

ここで右辺の和は $2r\le n$ なる最大整数 r までわたる。各係数は整数である。

$$\begin{aligned}(3.3.16)\text{ の右辺} &= \frac{(a^m-b^m)^q}{a-b}+\frac{q}{1}(ab)^m\frac{(a^m-b^m)^{q-2}}{a-b}\\ &+ \frac{q}{2}\binom{q-3}{1}(ab)^{2m}\frac{(a^m-b^m)^{q-4}}{a-b}+\cdots\\ &+ \frac{q}{r}\binom{q-r-1}{r-1}(ab)^{rm}\frac{(a^m-b^m)^{q-2r}}{a-b}+\cdots\\ &+ \frac{q}{(q-1)/2}\binom{\frac{q-1}{2}}{\frac{q-3}{2}}(ab)^{\frac{q-1}{2}-m}\frac{a^m-b^m}{a-b}\\ &= \frac{1}{a-b}\Bigg\{(a^m-b^m)^q+\frac{q}{1}(ab)^m(a^m-b^m)^{q-2}\\ &\quad+ \frac{q}{2}\binom{q-3}{1}(ab)^{2m}(a^m-b^m)^{q-4}+\cdots\\ &\quad+ \frac{q}{r}\binom{q-r-1}{r-1}(ab)^{rm}(a^m-b^m)^{q-2r}+\cdots\\ &\quad+ \frac{q}{(q-1)/2}\binom{\frac{q-1}{2}}{\frac{q-3}{2}}(ab)^{\frac{q-1}{2}-m}(a^m-b^m)\Bigg\}\end{aligned}$$

$X=a^m, Y=-b^m$ で、上の恒等式を用いると

$$(3.3.16)\text{ の右辺}=\frac{1}{a-b}\left((a^m)^q+(-b^m)^q\right)$$

qは奇数なので

$$(3.3.16)\text{の右辺} = \frac{(a^m)^q - (b^m)^q}{a-b} = U_{mq}$$

(証明終)

3.3.17

$c \leq 1$としてp^gはU_mを割り切るpの最高べきとする。$p \nmid k, f \leq 1$ならばp^{g+f}はU_{mkp^f}を割り切る。さらに$p \nmid Q$かつ$p^g \neq 2$ならば、p^{g+f}はU_{mkp^c}を割り切るpの最高べきであり$p^g = 2$ならば$\frac{U_{mk}}{2}$は奇数
(理解不足のため証明無し)

定義 3.4(Carmichael 関数)
Carmichael 関数$\lambda(n)$を次のように定義する。
$\lambda(1) = 1, \quad \lambda(2) = 1, \quad \lambda(2^2) = 2, \quad \lambda(2^r) = 2^{r-2}, \quad (r \leq 3)$
$\lambda(p^r) = p^{r-1}(p-1) = \phi(p^r), \quad (p\text{は奇素数}, r \leq 1)$
$\lambda(2^r p_1^{s_1} \cdots p_g^{s_g}) = lcm\lambda(2^r), \lambda(p_1^{s_1}), \cdots, \lambda(p_g^{s_g}), \quad (lcm\text{は最小公倍数を表す})$

定義 3.5(オイラー関数)
α, βを多項式$X^2 - PX + Q$の解として

$$(\frac{\alpha,\beta}{2}) = \begin{cases} 1 & \text{Q:偶数} \\ 0 & \text{Q:奇数,P:偶数} \\ -1 & \text{Q,P:奇数} \end{cases}$$

$p \neq 2$のとき

$$(\frac{\alpha,\beta}{p}) = (\frac{D}{p})$$

とおく。すべての素数pに対して

$$\psi_{\alpha,\beta}(p) = P - (\frac{\alpha,\beta}{p})$$

そしてまた

$$\psi_{\alpha,\beta}(p^s) = P^{s-1}\psi_{\alpha,\beta}(p) \ (c \leq 1)$$

とおく。$n = \Pi_{p|n} p^s$のとき Carmichael 関数を

$$\lambda_{\alpha,\beta}(n) = lcm\{\psi_{\alpha,\beta}(p^s)\} \qquad (lcm\text{は最小公倍数})$$

により定義し、Euler 関数を

$$\psi_{\alpha,\beta}(n) = \Pi_{p|n}\psi_{\alpha,\beta}(p^{\delta})$$

と定義する。

3.3.18
$gcd(n,Q) = 1$ ならば、$nU_{\lambda_{\alpha,\beta}(n)}$を割り切る。よって $nU_{psi_{\alpha,\beta}(n)}$も割り切る。

(理解不足のため証明無し)

3.3.19　　$gcd(P,Q) = 1 \quad \Rightarrow \quad gcd(U_n,Q) = 1 \qquad gcd(V_n,Q) = 1$

(証明)
$gcd(P,Q) = 1$ より $gcd(P^n,Q) = 1$.(3.3.10) より

$$V_n = P^n \mod Q.$$

$P^n = V_n + kQ \quad (k \in Z)$ とおく。$gcd(P^n,Q) = gcd(V_n + kQ,Q) = 1$ だから、

$$gcd(V_n,Q) = 1$$

また (3.3.10) より

$$U_n = V_{n-1} \mod Q$$

$V^{n-1} = U_n + kQ \quad (k \in Z)$ とおく。$gcd(V^{n-1},Q) = gcd(U_n + kQ,Q) = 1$ だから、

$$gcd(U_n,Q) = 1$$

(証明終)

$n \leq 2$ に対し n が U_r を割り切る $r \leq 1$ が存在したとき、このような r の中で最小のものを $\rho(n) = \rho(n,U)$ で表す。

3.3.20　　$gcd(P,Q) = 1$ とする。

$\rho(n)$ が存在したと仮定する。$n|U_k$ となるのは $\rho(n)|k$ のときでありまたそのときに限る。
(証明)
(ⅰ)$\rho(n) \mid k$ であるとする。$k = m\rho(n) \quad (m \in N)$ とおく。(3.3.13) より、$U_{\rho(n)} \mid U_{m\rho(n)}$. つまり $U_{\rho(n)} \mid U_k$ である。また、$n \mid U_{\rho(n)}$ なので $n \mid U_k$.
(ⅱ)$\rho(n) \nmid k$ とする。$k = m\rho(n) + \ell \quad (m \in N) \quad (0 < \ell < \rho(n))$ とおく。

(3.3.19) より $gcd(U_{\rho(n)}, Q) = 1$.(3.3.3) より
(1)m が偶数のとき,

$$U_k = U_{m\rho(n)+t} = U_{\{\frac{m}{2}\rho(n)+t\}+\{\frac{m}{2}\rho(n)\}} = U_{\frac{m}{2}\rho(n)+t}V_{\frac{m}{2}\rho(n)} - Q^{\frac{m}{2}\rho(n)}U_t$$

$n \nmid U_t$ なので $n \nmid U_k$.
(2)m が奇数のとき,

$$\begin{aligned} U_k = U_{m\rho(n)+t} &= U_{\{\frac{m+1}{2}\rho(n)+t\}+\{\frac{m-1}{2}\rho(n)\}} \\ &= U_{\frac{m+1}{2}\rho(n)+t}V_{\frac{m-1}{2}\rho(n)} - Q^{\frac{m-1}{2}\rho(n)}U_{\rho(n)} + t \\ U_{\rho(n)+t} &= U_{\rho}(n)V_t - Q^t U_{\rho(n)-t} \end{aligned}$$

$n \nmid U_{\rho(n)-t}$ なので $n \nmid U_{\rho(n)+t}$.従って $n \nmid U_k$.
(i),(ii) より $n|U_k$となるのは$\rho(n) \mid k$ のときでありまたそのときに限る。
(証明終)

ルーカスレーニー法の証明に必要ないくつかの定理を示す。

すべての整数 $D > 1$ に対して、次のように定義される関数 ψ_D を導入する。$N = \Pi_{i=1}^{s} p_i^{e_i}$ に対して、

$$\psi_D(N) = \frac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i-1} \left\{ p_i - (\frac{D}{p_i}) \right\}$$

定理 3.5
N は奇数で $gcd(N, D) = 1$ ならば、$\psi_D(N) = N - (D/N)$ となるのは N が素数のときでありまたそのときに限る。
証明
N が素数ならば定義より、$\psi_D(N) = N - (D/N)$.N=p^e(p は素数、$e \leq 2$) ならば $\psi_D(N)$ は $\psi_D(N) = p^e - p^{e-1}(D/p)$ より pの倍数であるが、$N-(D/N)$ は p の倍数ではない。よって $\psi_D(N) \neq N - (D/N)$.$N = \Pi_{i=1}^{s} p_i^{e_i}$(各 p^i は素数、$e_i \leq 1, s \leq 2$) ならば、$N > 5$

$$\begin{aligned} \psi_D(N) &\leq \frac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i-1}(p_i+1) \\ &= 2\prod_{i=1}^{s} \frac{1}{2}(1+\frac{1}{p_i}) \\ &\leq 2N \times \frac{2}{3} \times \frac{3}{5} \times \cdots \\ &\leq \frac{4}{5}N < N-1 \qquad \text{(証明終)} \end{aligned}$$

定理 3.7
N を奇数、$gcd(N,D)=1$、$N-(\frac{D}{N})$ は$\psi_D(N)$ を割り切るとする。このとき N は素数である。
証明
N は合成数であると仮定する。まず $N=p^e$(p は素数、$e\geq 2$) とすれば $\psi_D(N)=p^e-p^{e-1}(D/p)$. したがって

$$p^e-p^{e-1}<p^e-1\leq p^e-(D/N)\leq p^e-p^{e-1}(D/p).$$

よって $(D/p)=-1$ なので、$\psi_D(N)=p^e+p^{e-1}$ である。$N-(D/N)=p^e\pm 1$ は $\psi_D(N)=p^e+p^{e-1}$ を割り切らなければならないが、$p^e+p^{e-1}<2(p^e-1)$ なので不可能である。

また、N が少なくとも 2 つの異なる素因数をもつ場合、定理 3.6 で考察したように、$\psi_D(N)<N-1\leq N-(D/N)$ となるが、$N-(\frac{D}{N})$ が$\psi_D(N)$ を割り切ることに反する。よって N は素数でなければならない。

定理 3.8
N を奇数、$U=U(P,Q)$ を判別式 D をもつ Lucas 数列とする。$gcd(N,Q)=1$ ならば、$N \mid U_{\psi_D(N)}$ が成り立つ。
証明
$gcd(N,Q)=1$ であるから、(3.3.17) より N は $U_{\lambda_{\alpha,\beta}(N)}$ を割り切る。α,β は X^2-PX+Q の解とする。$N=\Pi_{i=1}^{s}p_i^{e_i}$ とすれば

$$\lambda_{\alpha,\beta}(N)=lcm\left\{p_i^{e_i-1}\left(p_i-(\frac{D}{p_i})\right)\right\} \quad = \quad 2lcm\left\{\frac{1}{2}p_i^{e_i-1}\left(p_i-(\frac{D}{p_i})\right)\right\}$$

となり、$\lambda_{\alpha,\beta}(N)$ は

$$\psi_D(N)=\frac{1}{2^{s-1}}\prod_{i=1}^{s}p_i^{e_i-1}\left\{p_i-(\frac{D}{p_i})\right\} \quad = \quad 2\prod_{i=1}^{s}\frac{1}{2}p_i^{e_i-1}\left(p_i-(\frac{D}{p_i})\right)$$

を割り切る。よって (3.3.12) より $U_{\lambda_{\alpha,\beta}(N)} \mid U_{\psi_D}(N)$ である。$N \mid U_{\lambda_{\alpha,\beta}(N)}$ でもあったので、$N \mid U_{\psi_D}(N)$ である。(証明終)

定理 3.9
N を奇数、$U=U(P,Q)$ を $(\frac{D}{N})=-1$ なる判別式 D をもつ Lucas 数列とし、N は U_{N+1} を割り切るとする。このとき $gcd(N,Q)=1$.
証明
$(D/N)\neq 0$ より $gcd(N,D)=1$. $p \mid N$ かつ $p \mid Q$ なる素数 p が存在すれば、$p \mid N$ より、$p \nmid D=P^2-4Q$ である。よって $p \nmid P$.(3.3.14.(3)) よりすべての $n\geq 1$ に対して $p \nmid U_n$ となるが, これはかていに反する。よって gcd(N,Q)=1 (証明終)

定理 3.10
$N > 1$ を奇数とし、$N+1 = \Pi_{i=1}^{s} q_i^{f_i} (q_i$: 素数, $f_i \geq 1, s \geq 2)$ とする。$(\frac{D}{N}) = -1$ なる整数 D が存在し、また $N+1$ のすべての素因数 q_i に対して判別式 $D = P_i^2 - 4Q_i (gcd(P_i, Q_i) = 1$ または $gcd(N, Q_i) = 1)$ をもつ Lucas 数列 $(U_n^{(i)})_{n \geq 0}$ が存在して、$N \mid U_{N+1}^{(i)}$ かつ $N \nmid U_{\frac{N+1}{q_i}}^{(i)}$ が成立すると仮定する。このとき N は素数である。
証明
定理 3.9 より各 $i = 1, 2, \cdots, s$ に対して $gcd(N, Q_i) = 1$. また定理 3.8 より各 $i = 1, 2, \cdots, s$ に対して $N \mid U_{\psi_D(N)}^{(i)}$. ここで $\rho^{(i)}(N)$ を $N \mid U_r^{(i)}$ となる最小の整数 r とする. (3.3.19)、仮定より $\rho^{(i)}(N) \mid (N+1)$, $\rho^{(i)}(N) \nmid (N+1)/q_i$, $\rho^{(i)}(N) \mid \psi_D(N)$ である。$\rho^{(i)}(N) \mid (N+1)$, $\rho^{(i)}(N) \nmid (N+1)/q_i$ より, $\rho^{(i)}(N)$ の素因数 q_i の数と、$N+1$ の素因数 q_i の数は等しいから、$q_i^{(i)} \mid \rho^{(i)}(N)$. 結局 $(N+1) \mid \psi_D(N)$ となる. $(D/N) = -1$ だから $gcd(N, D) = 1, N - (D/N) = N+1$ で, 定理 3.7 より N は素数である.

$P = 2, Q = -2, D = 12$ をもつ、Lucas 数列 $(U_n), (V_n)$ を考える。
p : 素数、$M_p = 2^p - 1$(Mersenne 数) とする。
定理 3.11
$N = M_p$が素数であるためには、N が $V_{\frac{N+1}{2}}$ を割り切ることが必要十分である。
証明
($\Rightarrow$)N を素数とする。
$3 - (2^p - 1) = 4 - 2^p$だから $\quad N \equiv 3 mod \quad 4$
$7 - (2^p - 1) = 8 - 2^p$だから $\quad N \equiv 7 mod \quad 8$
であるから, 定理 3.2 より

$$(\frac{-2}{N}) = (\frac{-1}{N})(\frac{2}{N}) = -1$$

(3.3.2), 定理 3.1(オイラー規準) より

$$\begin{aligned} V_{\frac{N+1}{2}}^2 &= V_{N+1} + 2Q^{\frac{N+1}{2}} = V_{N+1} - 4(-2)^{\frac{N-1}{2}} \\ &\equiv V_{N+1} - 4(\frac{-2}{N}) \\ &\equiv V_{N+1} + 4 \quad mod \quad N. \end{aligned}$$

$V_{N+1} \equiv -4 \quad mod \quad N$ を示せば、N が $V_{\frac{N+1}{2}}$ を割り切る.
(3.3.4),(3.3.11),(3.3.12) より

$$\begin{aligned} 2V_{N+1} &= V_N V_1 + DU_N U_1 = 2V_N + 12U_N \\ V_{N+1} &= V_N + 6U_N \equiv 2 + 6(\frac{12}{N}) \equiv 2 + 6(\frac{2}{N})^2(\frac{3}{N}) \quad mod \quad N \end{aligned}$$

$(\frac{N}{3})$ について, まず $N \equiv 7 \pmod{12}$ となることを示す。
p は素数なので奇数.$p = 2\ell + 1 \quad (\ell \geq 1)$ とおく.

$$7 - N = 8 - 2^{2\ell+1} = 2^3(1 - 2^{2(\ell-1)})$$

$1 - 2^{2(\ell-1)}$ が 3 の倍数なら $N \equiv 7 \pmod{12}$
帰納法で示す。
$\ell = 1$ のとき
$N \equiv 7 \pmod{12}$ を満たす。
$\ell = k$ のとき、$1 - 2^{2(k-1)} = 1 - 4^{k-1} = 3m$ と仮定する。
$\ell = k + 1$ のとき
$1 - 4^k = 1 - 4 \times 4^{k-1} = 1 - 4 \times (1 - 3m) = 12m - 3 = 3(4m - 1)$.
であるので、$N \equiv 7 \pmod{12}$ を満たす。

$$\begin{aligned} N &\equiv 7 \pmod{12} \\ N &\equiv 7 \pmod{3} \\ N &\equiv 1 \pmod{3} \\ (\frac{N}{3}) &= 1 \end{aligned}$$

定理 3.2 より

$$\begin{aligned} (\frac{3}{N}) &= (\frac{N}{3})(-1)^{\frac{N-1}{2}} \\ &= 1 \times (-1)^{\frac{p'-2}{2}} = -1 \end{aligned}$$

$$\begin{aligned} V_{N+1} &\equiv 2 + 6(1)^2(-1) \mod N \\ &\equiv 2 - 6 \equiv -4 \mod N \end{aligned}$$

$(\Leftarrow)$ N が $V_{\frac{N+1}{2}}$ を割り切るとする.(3.3.2) より $U_{N+1} = U_{\frac{N+1}{2}} V_{\frac{N+1}{2}}$ で U_{N+1} を N が割り切る. また (3.3.6) より

$$V^2_{\frac{N+1}{2}} - 12U^2_{\frac{N+1}{2}} = 4(-2)^{\frac{N+1}{2}}$$

また、$4(-2)^{\frac{N+1}{2}}$ の因数は 2 だけなので奇数の N とは $gcd(N, 4(-2)^{\frac{N+1}{2}}) = 1$ である。つまり

$$gcd(N, V^2_{\frac{N+1}{2}} - 12U^2_{\frac{N+1}{2}}) = 1$$

N は $V^2_{\frac{N+1}{2}}$ を割り切るので,$gcd(N, U_{\frac{N+1}{2}}) = 1$. また、$gcd(N, Q) = gcd(N, -2) = 1$, $(D/N) = (12/N) = (2/N)^2(3/N) = -1$ であるので、定理 3.10 より N は

素数である。(証明終)

ルーカスレーマー法
S_k を次のように定義する。

$$S_0 \equiv 4$$
$$S_k \equiv S_{k-1}^2 - 2 \mod M_p$$

このとき $N = M_p$ が素数であるためには、N が S_{p-2} を割り切ることが必要十分である。
証明
$S_0 = 4 = \frac{V_2}{2}$ である。$S_{k-1} = V_{2^k}/2^{2^k+1}$ と仮定すれば、(3.3.2) より

$$\begin{aligned} S_k &= S_{k-1}^2 - 2 = \frac{V_{2^k}^2}{2^{2^k}} - 2 \\ &= \frac{V_{2^{k+1}} + 2(-2)^{2^k}}{2^{2^k}} - 2 \\ &= \frac{V_{2^{k+1}} + (2)^{2^k+1}}{2^{2^k}} - 2 \\ &= \frac{V_{2^{k+1}}}{2^{2^k}} + 2 - 2 = \frac{V_{2^{k+1}}}{2^{2^k}} \end{aligned}$$

$V_{2^{p-1}} = V_{\frac{M_p+1}{2}} = 2^{2^{p-2}} S_{p-2}$, $2^{2^{p-2}} \nmid N$ であるから、

N が S_{p-2} を割り切ること $\iff$ N が $V_{\frac{N+1}{2}}$ を割り切ること

である。定理 3.11 より

N が素数であること $\iff$ N が S_{p-2} を割り切ること

(証明終)

参考文献
Johannes A.Buchmann 著、「INTRODUCTION TO CRYPTOGRAPHY」(Springer,2000 年)
Paulo Ribenecim 著、吾郷孝視　訳編「素数の世界その探索と発見 第 2 版」(共立出版、2001 年)
青空学園数学科　「初等整数論」
(address, http://www33.ocn.ne.jp/~aozora_gakuen/index.html)
松坂和夫　著、「代数系入門」(岩波書店、1976 年)

松本眞先生にたいへんお世話になりました。厚くお礼申し上げます。