2001 年度大阪市立大学インターネット講座「物性物理学における最近の話題」レポート

Miller-Rabin による素数の確率的判定法

深川　久

2002 年 1 月 13 日

1　はじめに

このレポートでは，講義の中で Rabin-Solovay-Strassen のアルゴリズムとして紹介された確率的素数判定法の有効性の証明を，必要な初等整数論の諸事実を準備しながら，極力 self-contained に記述することを目標にする。

講義は，およそ次のように進んだ。

- RSA 暗号の原理
- RSA 暗号の効率的な実現
- RSA 暗号が古典コンピュータで解読困難であること (素因数分解の困難さに依存)
- 量子コンピュータの概念
- 量子コンピュータでは素因数分解が効率的に行えること（Shor のアルゴリズム，1996）の要点

この中で，素数判定は主として 2 番目の「RSA 暗号の効率的な実現」にかかわる。すなわち，RSA 暗号の原理を古典コンピュータ上で実現するとき，その 1 ステップとして大きな素数を用意する必要があり，そのためには，大きな整数を与えたときにそれが素数かどうかを判定する必要が起こる。

効率的な素数判定法として，素数でない場合には確実に素数でないという結果を返すが，素数である場合にはおそらく素数であるだろう，という結果を返す，というものがある。ただし，判断を誤る確率を十分に小さくできるために，実用上素数判定に利用できる，という方法である。このような確率的判定法には幾つかのヴァリエーションがあるが，そのひとつが Solovay-Strassen の判定法であり，より精度の高い方法が Miller-Rabin 法である（参考文献 [3, pp. 181–184]）。講義で Rabin-Solovay-Strassen のアルゴリズムとして紹介されたものは後者にあたる。

第 2 節で，Miller-Rabin の判定法の内容を述べ，第 3 節で合同式・剰余類についての数学的準備を行い，第 4 節で Miller-Rabin の判定法が合成数であるという結果を返した場合には確実に合成数であることを示し，第 5 節で Miller-Rabin の判定法で合成数を素数と誤って判断してしまう確率が十分小さく抑えられることを証明する。

2　Miller-Rabin 法

ここでは，Miller-Rabin の判定法とはどのようなものかを述べる。奇数 n が与えられたとする。これが素数かどうかを判定したい。そのために，$0 < b < n$ なる整数 b をひとつ選び（「底」と呼ぶ），次のアルゴリズムにしたがって判定を行う。

Miller-Rabin のアルゴリズム

1.（入力）素数判定をしたい奇数 n と，$1 < b < n$ である整数 b をひとつ与える。
2. $n - 1 = 2^s t$，ただし t は奇数，となる s と t を求める（n を 2 で割れる限り繰り返し割ればよい）。
3. 判定条件「$b^t \equiv 1 \pmod{n}$ であるか，または，ある $0 \leqq r < s$ について $b^{2^r t} = -1 \pmod{n}$」を満たすかどうかを調べる。
4.（出力）判定条件を満たしていれば「Yes?」を，そうでなければ「No!」を返す。

この判定法について，次が成り立つ（第 4 節で示す）。

定理 1

n が奇素数であれば，このアルゴリズムは必ず「Yes?」を返す。

対偶をとれば，この判定法で「No!」という結果が返ってくれば，n は決して素数ではない。しかし，この逆は言えない。この判定法で「Yes?」が返ってきたからと言って，必ずしも n が素数であるとは言えない。

ではどうすればよいか。底を取り替えてもう一度 Miller-Rabin 法を適用するという手がある。ある底に対して「Yes?」が返ってきても，他の底に対しては「No!」が帰ってくるかも知れない。そうすれば，確実に合成数であるということが言えた事になる。多くの底に対して「Yes?」が返ってくるほど，n が素数であるという可能性が高くなるのではないか，と期待できる。

しかし，不安がある。可能なすべての底 b に対して Miller-Rabin 法を適用して，すべての結果が「Yes?」だったにもかかわらず，n が合成数である，といような事はないのだろうか。また，そのようなことが無いとしても，n が合成数であるにもかかわらず「Yes?」を返すような底 b があまりにも多いのであれば，結局可能な底ほとんどすべてにわたって Miller-Rabin の判定法を試してみなけらばならないことになり，効率的ではない。それなら，$0 < b < n$ であるすべての b に対して n を割り切るかどうか試してみるのと変わらないではないか。

この不安は払拭できる，というのが次の結果である（第 5 節で示す）。

定理 2

n が奇数の合成数であるにもかかわらず，Miller-Rabin のアルゴリズムが「Yes?」を返すような底 b の個数は，可能な底 $0 < b < n$ のうちの高々 $\frac{1}{4}$ である。

この結果より，n が奇合成数であるとき，底 $0 < b < n$ をひとつ選んで Miller-Rabin 法で判定した結果「Yes?」が返ってくる確率は高々 $\frac{1}{4}$ である。この試行を 2 回続けておこなったとき，連続して「Yes?」が返ってくる確率は高々 $\frac{1}{4^2}$ である。これを k 繰り返して，すべて「Yes?」が返ってくる確率は高々 $\frac{1}{4^k}$ であり，n が十分大きければ，k をある程度大きく取ることによって奇合成数であるにもかかわらず「Yes?」が続けて返ってくる確率を十分小さく抑えることができる。

以上が Miller-Rabin 法の内容である。上記 2 定理を証明するため，次節では数学的準備を行う。

3　合同式と剰余類群

3.1　合同式と剰余類群

整数全体の集合を $\mathbf{Z}$ と書く：$\mathbf{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$

定義 3.1. 2 つの整数 a と b が，整数 n を法として合同である $\Longleftrightarrow$ $a - b$ が n で割り切れる
このとき，$a \equiv b \pmod{n}$ と書く。

これは，a を n で割った余りと b を n で割った余りが一致する，と言っても同じである。法 n を固定したとき，各整数は $0, 1, 2, \cdots, n-1$ のうちのどれかひとつと合同であり，また，$0, 1, 2, \cdots, n-1$ の中のどの 2 数も n を法として合同ではない。今，整数 k と合同な整数の全体（すなわち，n で割ったときの余りが，k を n で割ったときの余りと一致する整数の全体）を一まとめにして $\overline{k}$ と表し，k を含む剰余類と呼ぶ事にする。すると，n を法とする剰余類は，$\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}$ で尽くされる。
n を法とする剰余類全体の集合を $\mathbf{Z}/n\mathbf{Z}$ で表す：$\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$。

例 3.2. $n = 3$ とする。剰余類の定義により，$\overline{0} = \overline{3} = \overline{6} = \cdots$ である。一般に，$a \equiv b \pmod{3} \Leftrightarrow \overline{a} = \overline{b}$ である。このとき，$\mathbf{Z}/3\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$ となる。

剰余類 $\overline{k}$ からひとつの整数を選んだとき，その整数をこの剰余類の代表元という。ひとつの剰余類には無限個の整数が含まれているので，代表元の選び方も無限にある。
次に，剰余類集合に足し算と引き算を定義しよう。

定義 3.3. $\overline{a}$，$\overline{b}$ を n を法とする剰余類とするとき，これらの和と差を次のように定義する。

$$\overline{a} + \overline{b} = \overline{a+b},\quad \overline{a} - \overline{b} = \overline{a-b}$$

すなわち，代表元の和と差で，剰余類の和と差を定義している。代表元の選び方によって和と差の結果が変わらないか，ということが気になるが，その心配はないということが次のようにしてわかる。

補題 3.4. $a \equiv a' \pmod{n}$ かつ $b \equiv b' \pmod{n}$ のとき，$a \pm b = a' \pm b' \pmod{n}$（複合同順）である。

証明. $a \equiv a' \pmod{n}$ より $a' = a + kn$，$b \equiv b' \pmod{n}$ より $b' = b + ln$ と表せる（k, l は整数）。このとき，$a' \pm b' = (a + kn) \pm (b + ln) = (a \pm b) + (k \pm l)n$ となるので，$a' \pm b' \equiv a \pm b \pmod{n}$ である。 □

従って，剰余類の和と差の定義は代表元の選び方によらない。剰余類の和 + は，次の性質を持つ。

1.（零元の存在）$\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$
2.（加法逆元の存在）$\overline{a} + \overline{-a} = \overline{-a} + \overline{a} = \overline{0}$
3.（結合法則）$(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
4.（可換）$\overline{a} + \overline{b} = \overline{b} + \overline{a}$

一般に，集合に上の 1 から 3 までの性質を満たす演算が定義されているものを群といい，さらに 4 も満たすときアーベル群という。剰余類の集合 $\mathbf{Z}/n\mathbf{Z}$ は演算 + に関してアーベル群である。この群を n を法とする剰余類群という。

3.2 剰余環

足し算，引き算の次は，掛け算について調べてみよう。

定義 3.5. $\overline{a}$，$\overline{b}$ を n を法とする剰余類とするとき，これらの積を次のように定義する。

$$\overline{a}\overline{b} = \overline{ab}$$

つまり，剰余類の積を代表元の積で定義した。和の場合と同じく，これが代表元の選び方によらないことを確かめておく。

補題 3.6. $a \equiv a' \pmod{n}$ かつ $b \equiv b' \pmod{n}$ ならば，$ab \equiv a'b' \pmod{n}$ である。

証明. $a \equiv a' \pmod{n}$ より $a' = a + kn$，$b \equiv b' \pmod{n}$ より $b' = b + ln$ と表せる（k, l は整数）。このとき，$a'b' = (a + kn)(b + ln) = ab + aln + knb + kln^2 = ab + (al + kb + kln)n$ なので，$ab \equiv a'b' \pmod{n}$ である。 □

こうして，剰余類群に積が定義された。和と積の間には，次の分配法則が成り立つ。

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a}\,\overline{b} + \overline{a}\,\overline{c}$$

このとき，$\mathbf{Z}/n\mathbf{Z}$ を n を法とする**剰余環**という。

さて，次は割り算について考える番だが，ここから少し注意が必要である。一旦，剰余類の話を離れて，通常の実数の計算を思い出そう。例えば，$2 \div 3$ は，掛け算を使って $2 \times \dfrac{1}{3}$ と表すことができる。すなわち，「3 で割ること」は「3 の逆数 $\dfrac{1}{3}$ を掛けること」と同じである。剰余類の計算でも，$\overline{b}$ の逆数にあたるものがあれば，「$\overline{b}$ で割ること」を「$\overline{b}$ の逆数を掛けること」と言い換えることで，割り算が実行できるだろう。割り算をどう定義するか，という問題を，逆数をどう定義するか，という問題に置き換えて考えよう。

実数では，3 の逆数は $\dfrac{1}{3}$ であった。剰余類は，整数の集まりなのだから，その中に実数の $\dfrac{1}{3}$ などもともとどこにもない。ここでは，逆数が乗法という演算においてどのような役割を持つ数だったか，という点に注目して剰余類における逆数にあたるものについて考えよう。

実数では，$\dfrac{1}{3}$ とは「$3x = 1$ となるような数 x」として，積だけを用いて言い表すことができた。剰余類の積に関する逆数も，同じように定義する。剰余類 $\overline{a}$ に対して，$\overline{a}\,\overline{x} = \overline{1}$ が成り立つような剰余類 $\overline{x}$ を $\overline{a}$ の逆元と呼ぶ。このように，「ある性質を満たすもの」という言い方で何かを定義したときには，本当にそのような性質をもつものが存在するのか，ということが気になる。また，存在するとしても，それはひとつに決まるのか，ということも気になる。これを調べていこう。

ここでは，少し一般的に $\overline{a}\,\overline{x} = \overline{b}$ という一次方程式を考える。合同式の形で書けば $ax \equiv b \pmod{n}$ である。以下，2 整数 a，n の最大公約数を (a, n) で表す。$(a, n) = 1$ とは，a と n が互いに素であること表す。また，整数 d が整数 b を割り切るとき，$d|b$ と表す。

補題 3.7. 合同式 $ax \equiv b \pmod{n}$ は，$(a, n) = 1$ のとき n を法として唯一つの解を持つ。また，$(a, n) = d$ のとき，$d|b$ ならば n を法として d 個の解を持ち，$d|b$ でないならば解を持たない。

証明. $(a, n) = 1$ の場合。n を法とする剰余類全体の集合を $\mathbf{Z}/n\mathbf{Z} = \{\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n}\}$ とする。この要素のちょうど一つが, 剰余類として b と同じものである。$ax_i \equiv ax_j \pmod{n} \Leftrightarrow a(x_i - x_j) \equiv 0 \pmod{n}$ であり, a と n が互いに素なのでこれは $x_i - x_j \equiv 0 \pmod{n}$ と同値である。従って, 集合として $\{\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n}\} = \{\overline{ax_1}, \overline{ax_2}, \cdots, \overline{ax_n}\}$。

よって，$\overline{ax_i}$ という形の剰余類の中に唯一つだけ $\overline{b}$ と一致するものがある。すなわち，$ax \equiv b \pmod{n}$ は，$(a,n)=1$ のとき n を法として唯一つの解を持つ。

$(a,n)=d$ の場合。$a=a'd$，$n=n'd$（a' と n' は互いに素）と表しておく。このとき，

$$ax \equiv b \pmod{n} \Longleftrightarrow a'dx \equiv b \pmod{n'd}$$

この方程式が解を持つならば，b も d で割り切れなければならない。対偶をとると，b が d で割り切れないならば，この方程式は解を持たない。そこで，$d|b$ である場合を考えよう。このとき，$b=b'd$ と表しておく。すると，

$$ax \equiv b \pmod{n} \Longleftrightarrow a'dx \equiv b'd \pmod{n'd}$$

整数 x がこの右辺の合同式を満たすことと，$a'x \equiv b' \pmod{n'}$ を満たすことは同値である。$(a',n')=1$ なので，前半の結果からこれは n' を法として唯一つの解をもつ。ここで，$n=n'd$ より，n' を法とした剰余類は，n を法とした剰余類を d 個含んでいる。すなわち，n を法とした解は d 個存在する。 □

さて，特に $b=1$ の場合を考えると，次が得られる。

系 3.7.1. 合同式 $ax \equiv 1 \pmod{n}$ が解を持つ $\Longleftrightarrow (a,n)=1$

また，このとき解は n を法として唯一つである。

証明. 上の補題において，$(a,n)=d>1$ の場合には $d|1$ とはなりえないことを考慮すれば直ちに得られる。 □

合同式の形で述べたが，これは n を法とした剰余類群において $\overline{a}\,\overline{x}=\overline{1}$ の解が存在するのは $(a,n)=1$ の場合に限られ，そのとき解は一意的に定まる，といっても同じである。つまり，$\overline{a}$ の乗法逆元が存在するのは $(a,n)=1$ の時に限られる。

3.3 既約剰余類群

前項で，剰余類の間に積を定義し，この積に関する逆元の存在について調べた。その結果，かならずしもすべての元に対して逆元が存在するわけではない，ということがわかった。その過程で，ここまで定義した剰余類の演算では，一次方程式が解を持たなかったり，また複数の解をもったりと，私たちが実数の世界で培ってきた直感にそぐわないような現象が起こることがわかった。

そこで，剰余類の乗法をもう少しうまく扱えるように，工夫をしよう。剰余類群の元の中から，乗法逆元を持つもの（これを既約剰余類という）だけを集めて，それを $(\mathbf{Z}/n\mathbf{Z})^\times$ と置く。

$$(\mathbf{Z}/n\mathbf{Z})^\times = \{\overline{a} \mid (a,n)=1\}$$

$\overline{a}$ と $\overline{b}$ がともに $(\mathbf{Z}/n\mathbf{Z})^\times$ の元であるとき，$(a,n)=1$ かつ $(b,n)=1$ より $(ab,n)=1$ となり，$\overline{ab}$ も $(\mathbf{Z}/n\mathbf{Z})^\times$ の元となる。すなわち，$(\mathbf{Z}/n\mathbf{Z})^\times$ は乗法に関して閉じている。さらに，$(\mathbf{Z}/n\mathbf{Z})^\times$ では，乗法に関して次の性質が成り立つ。

1. （乗法単位元の存在）$\overline{1} \in (\mathbf{Z}/n\mathbf{Z})^\times$ で，$\overline{1}\,\overline{a}=\overline{a}\,\overline{1}=\overline{a}$
2. （逆元の存在）$\overline{a} \in (\mathbf{Z}/n\mathbf{Z})^\times$ に対して，$\overline{a}\,\overline{b}=\overline{b}\,\overline{a}=\overline{1}$ となる $\overline{b}$ が存在する。
3. （結合法則）$(\overline{a}\,\overline{b})\overline{c}=\overline{a}(\overline{b}\,\overline{c})$
4. （可換性）$\overline{a}\,\overline{b}=\overline{b}\,\overline{a}$

すなわち，$(\mathbf{Z}/n\mathbf{Z})^\times$ は乗法に関してアーベル群になる。これを n を法とする既約剰余類群という。後の目的のためには，これら剰余環や既約剰余類群の元の個数を数える事が重要になる。

$(\mathbf{Z}/n\mathbf{Z})^\times$ に属する元の個数を $\varphi(n)$ と表す。これは，n 以下で n と互いに素な正の整数の個数に等しい。

例 3.8. $\varphi(1)=1, \varphi(2)=1, \varphi(3)=2, \varphi(4)=2, \varphi(5)=4, \cdots$

素数 p に対して，$\varphi(p)=p-1$，$\varphi(p^2)=p(p-1), \cdots, \varphi(p^k)=p^{k-1}(p-1)$

このとき，次の性質が成り立つ（フェルマの小定理）。

補題 3.9. $(a,n)=1$ であるとき，$a^{\varphi(n)} \equiv 1 \pmod{n}$ が成り立つ。

証明. 既約剰余類の全体を $\{\overline{x_1}, \overline{x_2}, \cdots, \overline{x_{\varphi(n)}}\}$ とする。$(a,n)=1$ のとき，$\{\overline{ax_1}, \overline{ax_2}, \cdots, \overline{ax_{\varphi(n)}}\}$ も既約剰余類の全体であるので，次の等式が成り立つ。

$$a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \equiv x_1 x_2 \cdots x_{\varphi(n)} \pmod{n}$$

ここで，$(x_i, n)=1$（$i=1,2,\cdots,\varphi(n)$）より $(x_1 x_2 \cdots x_{\varphi(n)}, n)=1$ なので，$a^{\varphi(n)} \equiv 1 \pmod{n}$ を得る。 □

とくに，p を素数とするとき $\varphi(p)=p-1$ なので，次を得る。

系 3.9.1. 素数 p に対し，a が p で割り切れないならば，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ。

素数 p を法とする場合，$1 \leqq a < p$ なる a はすべて p と互いに素であるので，既約剰余類群 $(\mathbf{Z}/p\mathbf{Z})^\times$ は剰余環から零元を除いたものに他ならない。すなわち，この場合剰余環 $\mathbf{Z}/p\mathbf{Z}$ は体になっている。

3.4 既約剰余類群の構造と 1 の累乗根

剰余環 $\mathbf{Z}/n\mathbf{Z}$ における一次方程式の解についてはすでに調べた。ここでは，高次方程式の中でもっとも単純な形のものとして $x^k \equiv 1 \pmod{n}$ の解について調べる。これもまた，Miller-Rabin 法に関わってくる。

そのために，既約剰余類群 $(\mathbf{Z}/n\mathbf{Z})^\times$ の構造に関する次の結果を利用する。

補題 3.10. 素数 p を法とする既約剰余類群 $(\mathbf{Z}/p\mathbf{Z})^\times$ は位数 p の巡回群である。

補題 3.11. 素数 p の平方 p^2 を法とする既約剰余類群 $(\mathbf{Z}/p^2\mathbf{Z})^\times$ は位数 $p(p-1)$ の巡回群である。

これら 2 つの補題の証明は付録にまわす。

一般に，群 G の元の個数を G の位数という。また，群 G の元 g に対して，$g^m=1$ となる最小の正整数 m をその元の位数という。位数 m の群 G の中にある元 g があって，$\mathrm{G}=\{1, g, g^2, g^3, \cdots, g^{m-1}\}$，$g^m=1$，となっているとき，G は巡回群であるといい，$g$ をその生成元という。巡回群では，群の位数と生成元の位数は一致する。

私たちは，Miller-Rabin 法に関わって，素数 p やその平方 p^2 を法とする既約剰余類群の中で方程式 $x^k=1$ がいくつ解を持つのかに興味がある。上の補題から，この場合には既約剰余類群が巡回群になるので，一般に巡回群の中での方程式 $x^k=1$ の解の個数について見ておこう（群の演算を乗法の形で書いたときの単位元を 1 で表している）。

補題 3.12. 位数 $m(>2)$ の巡回群 G において，方程式 $x^k=1$ の解の個数は $d=(k,m)$ 個である。

証明. 生成元 g をとる。$\mathrm{G} = \{1(=g^0), g, g^2, g^3, \cdots, g^{m-1}\}$ である。このとき，g^j が方程式 $x^k = 1$ の解であるための必要十分条件は，$(g^j)^k = 1 \Leftrightarrow g^{jk} = 1 \Leftrightarrow m|jk \Leftrightarrow (m/d)|(jk/d)$。ここで，$m/d$ と k/d は互いに素なので，これは $(m/d)|j$ と同値である。$0 \leqq j < m$ の範囲で m/d の倍数であるような j の個数は d 個なので，$x^k = 1$ の解の個数は d である。 □

これから，直ちに次が得られる。

系 3.12.1. 奇素数 p に対して，既約剰余類群 $(\mathbf{Z}/p\mathbf{Z})^\times$ における方程式 $x^k = \overline{1}$ の解の個数は $(k, p-1)$ であり，既約剰余類群 $(\mathbf{Z}/p^2\mathbf{Z})^\times$ における方程式 $x^k = \overline{1}$ の解の個数は $(k, p(p-1))$ である。

特に，1 の平方根について調べておこう。

系 3.12.2. 奇素数 p に対して，既約剰余類群 $(\mathbf{Z}/p\mathbf{Z})^\times$ における方程式 $x^2 = \overline{1}$ の解は $\overline{1}, \overline{-1}$ の 2 個である。

証明. $\overline{1}, \overline{-1}$ が解であることは明らか。補題より，解の個数は $(2, p-1) = 2$ であるので，この 2 つに限られる。 □

次に，異なる素数 p, q の積 pq を法とする剰余環や既約剰余類群の構造を調べておく。私たちが必要とするのは，特に剰余類の個数の数え上げである。少し一般的に，互いに素な 2 整数 m，n に対して次が成り立つ。

補題 3.13. m，n を互いに素な整数とする。写像 $f : \mathbf{Z}/mn\mathbf{Z} \longrightarrow (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$ を $f(\overline{x}) = (\overline{x}, \overline{x})$ と定めると，この写像は上への 1 : 1 写像である。

【注意】f の定義において，$\overline{x}$ が 3 通りの意味で使われていることに注意せよ。$f(\overline{x})$ における $\overline{x}$ は mn を法とする剰余類，$(\overline{x}, \overline{x})$ の第一成分は m を法とする剰余類，第二成分は n を法とする剰余類である。

この補題は，合同式の形で書けば次のようになる（中国剰余定理）。解の存在の部分が，上の補題の f が上への写像であることを示し，一意性の部分が，f が 1 : 1 の写像であることに対応する。

補題 3.14. m, n を互いに素な 2 つの整数とするとき，次の連立合同式は mn を法として唯一つの解を持つ。

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

証明.（解の存在）まず，$a = 1, b = 0$ の場合の解を一つ作ろう。$(m, n) = 1$ なので，補題 3.7 より $mx \equiv -1 \pmod{n}$ が解を持つ。この解を k とする。$x_0 = 1 + mk$ とおくと，m を法として $x_0 \equiv 1$ であり，n を法として $x_0 \equiv 1 - 1 \equiv 0$ である。同様にして，$a = 0, b = 1$ の場合の解 x_1，つまり $x_1 \equiv 0 \pmod{m}$，$x_1 \equiv 1 \pmod{n}$ となる x_1 がつくれる。このとき，一般の a, b に対し，$x = ax_0 + bx_1$ が連立合同式の解である。

（解の一意性）x と x' がともに連立合同式の解とすると，$x - x'$ は m と n のどちらを法としても 0 と合同であることになる。すなわち，$x - x'$ は m と n の両方で割り切れる。m と n が互いに素なので，$x - x'$ は mn で割り切れ，x と x' は mn を法として合同である。つまり，連立合同式の解は mn を法として唯一つしかない。 □

これで，補題 3.13 が示された。補題 3.13 の写像 f を既約剰余類群上に制限すると，「$(a, m) = 1$ かつ $(a, n) = 1 \Leftrightarrow (a, mn) = 1$」であることから，次の結果を得る。

補題 3.15. m, n を互いに素な 2 つの整数とするとき，補題 3.13 の写像 f を既約剰余類群上に制限して，次のような上への 1 : 1 写像が得られる。

$$f : (\mathbf{Z}/mn\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times$$

この 1 : 1 対応から，数え上げに際して基本的な次の結果が得られる。

補題 3.16. m, n を互いに素な 2 つの整数とする。$A \subset (\mathbf{Z}/m\mathbf{Z})^\times$ と $B \subset (\mathbf{Z}/n\mathbf{Z})^\times$ を，それぞれ s 個，t 個の元からなる部分集合とする。このとき，$(\mathbf{Z}/mn\mathbf{Z})^\times$ の元 $\overline{x}$ で，$x \pmod m \in A$ かつ $x \pmod n \in B$ となるようなものの個数は st 個である。

証明.「$(\mathbf{Z}/mn\mathbf{Z})^\times$ の元 $\overline{x}$ で，$x \pmod m \in A$ かつ $x \pmod n \in B$ となるようなもの」とは，補題 3.15 の写像 f を使えば「$f(\overline{x}) \in A \times B$」と同値。$A \times B$ の元の個数が st 個で，f が 1 : 1 対応だから，そのような $\overline{x}$ の個数は st 個である。 □

4　定理 1 の証明

準備が整った。この節では，奇素数に対して Miller-Rabin 法を適用した場合，必ず「Yes?」の結果が返ってくることを示す。

私たちは，ある整数が素数であるか合成数であるかを見分けたいのだから，整数の持つ性質のうちで特に素数の場合に成り立つようなタイプのものに注目しよう。そのようなものの筆頭は，フェルマの小定理である。奇数 n と底 b，$0 < b < n$，を与えたとき，もしも n が素数ならば，

$$b^{n-1} \equiv 1 \pmod n$$

が成り立つはずである（系 3.9.1）。しかし，これだけでは素数判定条件としてはまだ粗い。素数でないのに判定条件をクリアするようなものをできるだけ減らしたいのだから，もっと条件を精密にしてみよう。

今，n として奇数を取り上げているのだから，$n-1$ は偶数であり，$(n-1)/2$ は整数となる。そこで，$b^{(n-1)/2} \pmod n$ を考えてみよう。$b^{n-1} \equiv 1 \pmod n$ であるとき，$b^{(n-1)/2} \pmod n$ は 2 乗すると $1 \pmod n$ になる数である。法 n が素数ならば，そのような数は $\pm 1 \pmod n$ の 2 つしかない。法 n が素数でないならば，$\pm 1 \pmod n$ 以外の数であって 2 乗したら $1 \pmod n$ になるものがある。ここにも，素数と合成数を判別する手がかりがある。

例で観察してみよう。

例 4.1. $n = 15$ とする。このとき，$\overline{1}$ と $\overline{14} = \overline{-1}$ のほかに，$\overline{4}$，$\overline{11}$ も 2 乗すると $\overline{1}$ になる。実際，$\overline{4}^2 = \overline{16} = \overline{1}$，$\overline{11}^2 = \overline{121} = \overline{1}$ である。また，$n = 35$ では，$\overline{1}, \overline{6}, \overline{29}, \overline{34}$ の 4 個が 2 乗すると $\overline{1}$ となる。

これらの例のように，n が素数でない場合には，2 乗して $\overline{1}$ になる剰余類は $\pm\overline{1}$ とは限らない（このような実例は，補題 3.13 の 1 : 1 対応が環としての同型写像であることを利用して構成できる）。この事情を利用する。奇数 n に対して，$n-1$ を次々と割り切れる限り 2 で割りつづけて，$n - 1 = 2^s t$ と表しておく。ここで，q は奇数である。b^t から始めて，次々と 2 乗して得られる次の列を考える。

$$b^t, b^2 t, \cdots, b^{2^s t} = b^{n-1}$$

ここで，n が素数ならば，n を法として考えたとき最後の項は $\overline{1}$ である。その一つ前の項は，$\overline{1}$ か $\overline{-1}$ のどちらかである。もし $\overline{1}$ だとしらならば，もう一つ前の項にさかのぼればそれもまた $\overline{1}$ か $\overline{-1}$ のどちらかである。こうして，次々と遡って行けば，最後まで $\overline{1}$ であるかあるいは，どこか途中で $\overline{-1}$ になるかのどちらかでしかあ

りえない。n が素数でなければ，さかのぼる過程において，$\overline{1}$ の一つ前の段階に $\overline{1}$ でも $\overline{-1}$ でもない剰余類が現れるかも知れない。そうなったら，その数は素数ではないことがはっきりする。こうして，篩い分けがすこし精密化される。

以上をまとめると，n が奇素数で b が $0 < b < n$ であるような整数のとき，

1. $b^t \equiv 1 \pmod{n}$ であるか，または
2. ある r（$0 \leqq r \leqq s$）に対して $b^{2^r t} \equiv -1 \pmod{n}$

のいずれかが成り立つ。これが Miller-Rabin の判定条件である。n が素数の場合に成り立つ性質を取り出したものなのだから，この判定条件を満たさないような n は決して素数ではありえない。

単に列 $b^t, b^{2t}, \cdots, b^{2^s t} = b^{n-1}$ の末尾の項一つだけが $\overline{1}$ かどうかを見るよりは，精密な判定条件になっていることが期待される。

5　定理 2 の証明

前項で，Miller-Rabin の判定条件を満たさない奇数は，確実に合成数であることがわかった。本節では，合成数であるにも関わらず Miller-Rabin の判定条件を満たすような場合について調べる。Miller-Rabin の判定条件は，底 b に依存する。そこで，奇合成数 n に対して，Miller-Rabin の判定条件を満たすような底 b が何個程度あるのかを評価する。これが定理 2 の内容であった。

定理 2 を再掲しておく。

定理 2

> n が奇数の合成数であるにもかかわらず，Miller-Rabin のアルゴリズムが「Yes?」を返すような底 b の個数は，可能な底 $0 < b < n$ のうちの高々 $\dfrac{1}{4}$ である。

n のタイプによって場合わけして示す。

5.1　n が平方因子を持つ場合

n がある奇素数 p の平方 p^2 で割り切れる場合を考える。底 b に対して，n が Miller-Rabin の判定条件をみたすとする。このとき，$b^{n-1} \equiv 1 \pmod{n}$ である。$p^2 | n$ だから，法を p^2 で取り替えたとき，やはり $b^{n-1} \equiv 1 \pmod{p^2}$ となる。$(\mathbf{Z}/p^2\mathbf{Z})^\times$ は位数 $p(p-1)$ の巡回群なので，補題 3.12 よりこのような b は p^2 を法とする剰余類として $d = (n-1, p(p-1))$ 個である。$p | n$ より，p は $n-1$ の約数ではないので，p は d の約数ではない。従って，d は高々 $p-1$ である。以上より，条件を満たす b の個数が p^2 で割れない b 全体の中に占める割合は，p^2 を法とする剰余類の中で数えたとき，

$$\frac{p-1}{p^2-1} = \frac{1}{p+1} \leqq \frac{1}{4}$$

となる。n を法とした剰余類へ持ち上げたとき，$(p-1)/(p^2-1)$ の分母・分子がともに n/p^2 倍になるだけなので，割合としては同じである。

5.2 n が平方因子を持たない場合

この場合，$n = p_1 p_1 \cdots p_l$ と，異なる素数の積に素因数分解される。最初に，$n = pq$ と異なる 2 つの素数の積として表される場合を考えよう。

基本的なアイディアは，補題 3.13 の写像 f で $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ に移して考えるというものである。

まず，$p-1 = 2^{s'}t'$，$q-1 = 2^{s''}t''$（t', t'' は奇数）と表しておく。p と q に関して対称的なので，$s' \leqq s''$ と仮定しても一般性を失わない。これを二つの場合に分ける。

(i)$s' < s''$ の場合。

底 b に対して，n が次の Miller-Rabin の判定条件を満たしたとする。

1. $b^t \equiv 1 \pmod{n}$ であるか，または
2. ある r（$0 \leqq r < s$）に対して $b^{2^r t} \equiv -1 \pmod{n}$

$\overline{b} \in \mathbf{Z}/pq\mathbf{Z}$ を f で $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/q\mathbf{Z})$ に移すと，次が成り立たなければならないことがわかる。

1. $b^t \equiv 1 \pmod{p}$ かつ $b^t \equiv \pmod{q}$，または
2. ある r（$0 \leqq r < s$）に対して，$b^{2^r t} \equiv -1 \pmod{p}$ かつ $b^{2^r t} \equiv -1 \pmod{q}$

$b^t \equiv 1 \pmod{p}$ を満たすような b の p を法とした個数は，補題 3.12.1 によって，$(t, p-1)$ 個であり，また $b^t \equiv \pmod{q}$ を満たすような b の q を法とした個数は $(t, q-1)$ 個である。この両方を満たすような b の，pq を法とした剰余類の個数は，補題 3.16 によって積 $(t, p-1)(t, q-1)$ 個であることがわかる。ここで，$p-1 = 2^{s'}t'$，$q-1 = 2^{s''}t''$（t', t'' は奇数）と表しておくと，t が奇数であることから $(t, p-1) = (t, t')$，$(t, q-1) = (t, t'')$ であり，さらに $(t, t') \leqq t'$，$(t, t'') \leqq t''$ だから，最初の条件を満たすような b の pq を法とした剰余類の個数は高々 $t't''$ であることがわかる。

$0 \leqq r < s$ であるような r を一つ固定したときに，$b^{2^r t} \equiv -1 \pmod{p}$ かつ $b^{2^r t} \equiv -1 \pmod{q}$ であるような b の pq を法とした剰余類の個数を評価しよう。そのために次の補題を準備する。

補題 5.1. $(\mathbf{Z}/p\mathbf{Z})^\times$ において，方程式 $x^{2^r t} \equiv -1 \pmod{p}$ の解の個数は，$r \geqq s'$ のとき 0 であり，$r < s'$ のとき $2^r (t, t')$ である。

証明. $(\mathbf{Z}/p\mathbf{Z})^\times$ は巡回群であり，その生成元を g とする。この既約剰余類群の元を g^j（$0 \leqq g < p-1$）の形に書く。$g^{(p-1)/2} \equiv -1 \pmod{p}$ であることから，

$$\begin{aligned}(g^j)^{2^r t} \equiv -1 \pmod{p} &\iff (g^j)^{2^r t} \equiv g^{(p-1)/2} \pmod{p} \\ &\iff g^{2^r t j} \equiv g^{2^{s'-1}t'} \pmod{p} \\ &\iff 2^r t j \equiv 2^{s'-1}t' \pmod{2^{s'}t'}\end{aligned}$$

ここで, $r \geqq s'$ の場合, 最後の合同式は $2^{s'-1}(t' - 2^{r-s'+1}tj) \equiv 0 \pmod{2^{s'}t'}$ と同値であるが, t' が奇数で $2^{r-s'+1}tj$ が偶数より $2^{s'-1}(t' - 2^{r-s'+1}tj)$ が因数にもつ 2 の最大冪が $s'-1$ であるため，この合同式は解を持たない。

$r < s'$ の場合，$d = (t, t')$ とおくと，最後の合同式の両辺と法を $2^r d$ で割って $(t/d)j \equiv 2^{s'-1-r}(t'/d) \pmod{2^{s'-r}(t'/d)}$ を得る。これは，t/d と $2^{s'-r}(t'/d)$ が互いに素であることから，$2^{s'-r}(t'/d)$ を法として唯一つの解を持つ。$2^{s'-r}(t'/d)$ を法とする一つの剰余類の中には，$2^{s'}t'$ を法とする剰余類が $2^r d$ 個含まれるので，問題の合同式は $2^{s'}t'$ を法として $2^r d = 2^r (t, t')$ 個の解を持つ。 □

この補題と補題 3.16 より，$b^{2^r t} \equiv -1 \pmod{p}$ かつ $b^{2^r t} \equiv -1 \pmod{q}$ であるような b の pq を法とした剰余類の個数は，$2^r(t,t') \cdot 2^r(t,t'')$ である。これは，$2^r(t,t') \cdot 2^r(t,t'') \leqq 4^r t't''$ より，$4^r t't''$ を上界に持つ。

さて，条件 1 を満たす底が高々 $t't''$ 個，条件 2 を満たす底が各 r（$0 \leqq r < s$）ごとに高々 $4^r t't''$ 個ずつであり，また $n-1 = pq > (p-1)(q-1) = 2^{s'+s''}t't''$ だから，底 b（$0 < b < n$）のうち，$n = pq$ が Miller-Rabin の判定条件を満たすようなものの個数は次の値で上からおさえられる。

$$\frac{t't'' + t't'' + 4t't'' + 4^2 t't'' + \cdots + 4^{s'-1}t't''}{2^{s'+s''}t't''} = 2^{-s'-s''}\left(1 + \frac{4^{s'}-1}{4-1}\right)$$

この値が，1/4 以下であることを示せば証明が終わる。これは，次のようにしてわかる。

$$2^{-s'-s''}\left(1 + \frac{4^{s'}-1}{4-1}\right) \leqq 2^{-2s'-1}\left(\frac{2}{3} + \frac{4^{s'}}{3}\right) \leqq 2^{-3}\frac{2}{3} + \frac{1}{6} = \frac{1}{4}$$

(ii)$s' = s''$ の場合。

このとき，$(t,t') \leqq t'$，$(t,t'') \leqq t''$ の 2 つの不等式のうち，少なくとも一方の $\leqq$ は $<$ で置き換えることができる。なぜなら，もしも $(t,t') = t'$ かつ $(t,t'') = t''$ ならば，$t'|t$ かつ $t''|t$ となる。$t'|t$ ならば $t'|n-1$ であり，一方 $n-1 = pq-1 \equiv q-1 \pmod{t'}$ だから $t'|q-1$ を得る。従って，$t'|t''$ となる。まったく同様に $t''|t'$ が得られ，$t' = t''$ となる。よって $p = q$ となるが，これは p と q が異なる素数であるという仮定に反する。従って，$(t,t') < t'$ または $(t,t'') < t''$ である。今，$(t,t') < t'$ であるとすると，t' が奇数であることから $t'/(t,t') \geqq 3$。よって，$(t,t') \leqq t'/3$ である。従って，(i) のケースで $(t,t')(t,t'') \leqq t't''$ として評価した部分が，すべて $(t,t')(t,t'') \leqq t't''/3$ に置き換えることができる。従って，底 b の個数の割合の上界の評価は，

$$\frac{1}{3}2^{-s'-s''}\left(1 + \frac{4^{s'}-1}{4-1}\right) \leqq \frac{1}{3}2^{-2s'}\left(\frac{2}{3} + \frac{4^{s'}}{3}\right) \leqq \frac{1}{18} + \frac{1}{9} = \frac{1}{6} < \frac{1}{4}$$

となる。（$n = pq$ の場合の証明終わり）

最後に，n が異なる素数の 3 個以上の積の場合を示す。$n = p_1 p_2 \cdots p_k$，$k > 3$，とする。$p_i - 1 = 2^{s_i}t_i$（t_i は奇数）と表しておき，s_i の中で最小のものを s_1 としておく。このとき，$n = pq$ の場合とまったく同様に，可能な底の中で n が Miller-Rabin の判定条件を満たすような b の割合の上界が，次の値でおさえられることがわかる。

$$\begin{aligned}
2^{-s_1-s_2-\cdots-s_k}\left(1 + \frac{2^{ks_1}-1}{2^k-1}\right) &\leqq 2^{-ks_1}\left(\frac{2^k-2}{2^k-1} + \frac{2^{ks_1}}{2^k-1}\right) \\
&= 2^{-ks_1}\frac{2^k-2}{2^k-1} + \frac{1}{2^k-1} \\
&\leqq 2^{-k}\frac{2^k-2}{2^k-1} + \frac{1}{2^k-1} \\
&= 2^{1-k} \\
&\leqq \frac{1}{4}
\end{aligned}$$

以上で，定理 2 が証明された。

6　p および p^2 を法とする既約剰余類群が巡回群であることの証明

本文中で証明を与えなかった補題は，3.10 と 3.11 の 2 つだけである。それをここで与えておく。

まず，$(\mathbf{Z}/p\mathbf{Z})^\times$ が巡回群であることを示そう。$(\mathbf{Z}/p\mathbf{Z})^\times$ の中で位数最大の元を g とする。g の位数を m とおき，これが実は $p-1$ に一致することを示せばよい。

その為には，次の補題が必要である。

補題 6.1. 有限群 G とその部分群 H が与えられたとする。このとき，群 H の位数は群 G の位数の約数である。特に，元 $g \in \mathrm{G}$ の位数は，g の生成する巡回部部分群の位数に一致するので，群 G の位数の約数である。

証明. 元 $g \in \mathrm{G}$ に対して，$g\mathrm{H} = \{gh \mid h \in \mathrm{H}\}$ とおく。このとき，$g\mathrm{H} \cap g'\mathrm{H} \neq \emptyset$ ならば $g\mathrm{H} = g'\mathrm{H}$ が成り立つ。なぜなら，$gh = g'h'$ となるような $h \in \mathrm{H}$，$h' \in \mathrm{H}$ があるとすると，$g' = ghh' \in g\mathrm{H}$ より $g'\mathrm{H} \subset g\mathrm{H}$。まったく同様に，$g\mathrm{H} \subset g'\mathrm{H}$ である。従って，$g\mathrm{H} = g'\mathrm{H}$ である。このことから，ある $g_1, g_2, \cdots, g_k$ があって

$$\mathrm{G} = g_1\mathrm{H} \cup g_2\mathrm{H} \cup \cdots \cup g_k\mathrm{H}$$

と，共通部分をもたない異なる部分集合の和集合として G が表せる。各 $g_i\mathrm{H}$ と H は同じ個数だけ元を含むので，H の位数は G の位数の約数である。 □

補題 6.2. 素数 p に対して，m 次合同式 $x^m \equiv 1 \pmod{p}$ の解の個数は（法 p で合同なものを同一視して）高々 m 個である。

証明. 次数 m に関する帰納法によって証明する。$m = 1$ の場合は，補題 3.7 によって解は唯一つに定まる。

一般に，多項式 $f(x) = x^m - 1$ を一次式 $x - a$（a は整数）で割ったときの商を $g(x)$，余りを R とすると，$f(x) = (x-a)g(x) + R$ と表せる。a が $x^m - 1 \equiv 0 \pmod{p}$ の解であるとき，$R \equiv 0 \pmod{p}$ であり，合同式 $f(x) \equiv 0 \pmod{p}$ は合同式 $(x-a)g(x) \equiv 0 \pmod{p}$ と同値である。p が素数であるので，この合同式は「$x - a \equiv 0 \pmod{p}$ または $g(x) \equiv 0 \pmod{p}$」と同値であり，前者は補題 3.7 より唯一つの解を持ち，後者は $m-1$ 次なので帰納法の仮定により高々 $m-1$ 個の解を持つ。従って，$f(x) \equiv 0 \pmod{p}$ は高々 m 個の解を持つ。 □

もとに戻ろう。背理法によって $(\mathbf{Z}/p\mathbf{Z})^\times$ が巡回群であることを示す。$(\mathbf{Z}/p\mathbf{Z})^\times$ における最大位数の元を g とし，その位数を $m < p-1$ と仮定する。これは，$x^m - 1 \equiv 0 \pmod{p}$ の解である。このとき，$1, g, g^2, \cdots, g^{m-1}$ はすべて $x^m - 1 \equiv 0 \pmod{p}$ の解である。そしてこれら m 個の中には，p を法として合同になるものは含まれていない。なぜなら，$g^i \equiv g^j \pmod{p} \Rightarrow g^{i-j} \equiv 0 \pmod{p} \Rightarrow p-1 | i-j$（最後のところでは補題 6.1 を使った）となるが，$m < p-1$ で $0 \leqq i, j \leqq m-1$ ではこれは $i = j$ の時にしか起こりえない。従って，上にあげたものが $x^m - 1 \equiv 0 \pmod{p}$ の異なる m 個の解であり，補題 6.2 よりこれら以外に解は無い。$(\mathbf{Z}/p\mathbf{Z})^\times$ は $p-1$ 個の元を持つので，g^i 以外の元 h が存在する。h の位数を n とする（$n > 1$）。h は $x^m - 1 \equiv 0 \pmod{p}$ の解ではありえないので，n は m の約数ではない。ここで，二つの場合に分けて考える。

（i） $(m, n) = 1$ の場合。このとき，gh の位数が m よりも大きくなってしまうことを示そう。$(gh)^t \equiv 1 \pmod{p}$ とすると，$(gh)^{tm} \equiv g^{tm}g^{tm} \equiv g^{tm}$ より，$g^{tm} \equiv 1 \pmod{p}$ となる。g の位数が n だから，補題 6.1 より $n | tm$ である。n と m が互いに素の場合を考えているので，$n | t$。まったく同様に，$(gh)^{tn}$ から始めて $m | t$ を得る。すなわち，t は m と n の公倍数。$(m, n) = 1$ より，t は mn の倍数であり，$t > m$ となる。これは m が最大位数であったことと矛盾する。従って，$m = p-1$ でなければならず，このとき $(\mathbf{Z}/p\mathbf{Z})^\times$ は g を生成元とする巡回群である。

（ii） $(m, n) = d > 1$ の場合。このとき，m，n の最小公倍数を l とすると，$l = mn/d$ である。$(m/d, n/d) = 1$ より，$d = d_1^{e_1} d_2^{e_2} \cdots d_k^{e_k}$ と素因数分解したとき，各素因数 $d_i^{e_i}$ は m/d，n/d のうちせいぜいどちらか一方の因数にしかなっていない。そこで，もし $d_i^{e_i}$ が m/d，n/d のどちらかの因数になっていたらそちらに掛け，どちらの

因数にもなっていなければどちらか好きなほうを選んで掛けることで，二つの整数 m_0, n_0 を作り $(m_0, n_0) = 1$ かつ $m_0 n_0 = l$ となるようにできる。このとき，(i) より $g^{m/m_0} h^{n/n_0}$ の位数は $l = m_0 n_0$ である。n は m の約数ではないので，m，n の最小公倍数 l は m より大きい。これは，m が最大位数であったことと矛盾する。従って，$m = p - 1$ でなければならず，このとき $(\mathbf{Z}/p\mathbf{Z})^\times$ は g を生成元とする巡回群である。

以上より，$(\mathbf{Z}/p\mathbf{Z})^\times$ が巡回群であることが証明された。

次に，$(\mathbf{Z}/p^2\mathbf{Z})^\times$ も巡回群であることを示す。まず，$(\mathbf{Z}/p\mathbf{Z})^\times$ の生成元 $\overline{g}$ を一つ選ぶ。以下，同じ整数を法 p の元で考えたり，法 p^2 の元で考えたりするため，法を明示して $\overline{g}$ を $g \pmod p$ と書く。$g \pmod p$ は $g^{p-1} \equiv 1 \pmod p$ を満たし，$0 < i < p - 1$ のときには $g^i \equiv 1 \pmod p$ ではない。さて，この g を，法 p^2 のもとで考えよう。つまり，$g \pmod{p^2}$ を考える。すると，$g^{p(p-1)} \equiv 1 \pmod{p^2}$ であり，g の位数は $p(p-1)$ の約数である。今，$s | p - 1$ である $s < p - 1$ に対して，$g^s \equiv 1 \pmod{p^2}$ であったとすると，p^2 を法として合同な 2 数は p を法としても合同だから，$g^s \equiv 1 \pmod p$ となり，g の位数が $p - 1$ であることに反する。また $g^{ps} \equiv 1 \pmod p$ であったとすると，p を法として $1 \equiv g^{ps} \equiv (g^p)^s \equiv g^s \pmod p$ となり，やはり g の位数が $p - 1$ であることに反する。従って，$g \pmod{p^2}$ の位数となり得る候補は，$p - 1$ か $p(p-1)$ かのいずれかである。位数 $p(p-1)$ のときは，これが生成元となる。

では，もし $g \pmod{p^2}$ の位数が $p - 1$ のときはどうするか。このときは，$g' = (p+1)g$ とおき，g' が生成元となることを示す。まず，$g' \equiv (p+1)g \equiv g \pmod p$ であるから，$g' \pmod p$ は法 p のときの生成元である。さらに，$g'^{p-1} \equiv \{(p+1)g\}^{p-1} \equiv (p+1)^{p-1} \equiv 1 + (p-1)p + \binom{p-1}{2} p^2 + \cdots \equiv 1 - p \pmod{p^2}$ である。これは $1 - p \equiv 1 \pmod{p^2}$ となることはありえない（p が p^2 で割り切れることはありえない）ので，g' の位数は $p - 1$ ではない。よって前段と同様にこの g' が位数 $p(p-1)$ となり，生成元である。

以上により，$(\mathbf{Z}/p^2\mathbf{Z})^\times$ も巡回群であることが示された。

参考文献

[1] 高木貞治『初等整数論講義（第 2 版）』，共立出版，1971[初版 1931].

[2] 山本芳彦『数論入門 1』，岩波講座現代数学への入門，1996.

[3] N. コブリッツ『数論アルゴリズムと楕円暗号理論入門』，シュプリンガーフェアラーク東京，1997[原著初版 1987].