放送大学東京文京学習センター
平成30年度第1学期面接授業

「素数と素因数分解」

講義資料

縫田 光司
（東京大学大学院情報理工学系研究科）
nuida@mist.i.u-tokyo.ac.jp

初版：2018年4月11日
最終更新：2018年4月25日

放送大学平成 30 年度面接授業資料（縫田 光司）2018.4.25 版

目 次

1 素数の性質

まず、いくつかの記号を導入します。$\mathbb{Z}$ を整数全体の集合とし、$\mathbb{Z}_{\geq 0}$ と $\mathbb{Z}_{>0}$ をそれぞれ非負整数全体の集合と正整数全体の集合とします。また、$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ をそれぞれ有理数全体の集合、実数全体の集合、複素数全体の集合とします。

整数 a, b について、a が b の **倍数** であるということを、$a = bc$ を満たす整数 c が存在することと定義します。特に、0 はすべての整数の倍数です。また、a が b の倍数であるときに、b は a の **約数** であるといい、記号 $b \mid a$ で表わします。なお、「倍数の倍数はまた倍数である」、すなわち整数 a, b, c について $a \mid b$ かつ $b \mid c$ であれば $a \mid c$ である、という性質が成り立ちます。

以下に素数の定義を述べます。ここで、a を整数とすると、a 自身および 1 は常に a の約数であることに注意してください。

定義 1.1 (素数)**.** 正の整数 $p \in \mathbb{Z}_{>0}$ が **素数** であるとは、$p \neq 1$ であり、かつ p が 1 と p 以外の正の約数を持たないことと定義する。1 より大きな整数が素数でないとき、その数を **合成数** と呼ぶ。

小さい方からいくつかの素数は、$2, 3, 5, 7, 11, 13, 17, \ldots$ と並びます。

ある整数 a を一つ決めたとき、a の倍数同士の和と差、および a の倍数を何らかの整数倍した結果もまた a の倍数となります。（代数学の言葉では、この性質を「a の倍数全体は環 $\mathbb{Z}$ のイデアルをなす」などと言い表します。）この性質の対偶を考えることで、以下の性質が示されます。

補題 1.1. a, b, c を整数とし、b は a の倍数であり、一方で c は a の倍数でないとする。このとき $b + c$ は a の倍数でない。

証明. もし b のみならず $b + c$ も a の倍数であったなら、前述の性質により $c = (b + c) - b$ も a の倍数となるはずであるが、これは c が a の倍数でないという前提と矛盾する。よって $b + c$ は a の倍数ではあり得ない。 □

一方で、以下の性質が成り立ちます。

補題 1.2. n を 2 以上の整数とすると、n は何らかの素数を約数に持つ。

証明. n についての数学的帰納法を用いる。n が素数であれば（特に、$n = 2$ であれば）、n 自身が n の約数なので目標の性質が成り立つ。以下、n が素数でないとすると、n は 1 でも n でもない正の約数を持つ。これを d と書く。すると

$2 \leq d < n$ なので、数学的帰納法の仮定により d は何らかの素数を約数に持つ。この素数は n の約数でもあるので、この場合にも目標の性質が成り立つ。よって主張が成り立つ。 □

これらの性質を用いて、以下の最も基本的かつ重要な事実が示されます。

定理 1.1. 無限に多くの素数が存在する。

証明. 素数が有限個 $p_1, p_2, \ldots, p_k$ しかないと仮定して矛盾を導く。2 が素数であることは直接確かめられるので、$k \geq 1$ であり $p_1, \ldots, p_k$ のどれかは 2 である。$n = p_1 p_2 \cdots p_k + 1$ と定めると、直前の注意により $n \geq 3$ である。ここで各 p_i について、$p_1 p_2 \cdots p_k$ は p_i の倍数であるが 1 は p_i の倍数ではない（$p_i \geq 2$ より）ので、補題 1.1 により n は p_i の倍数ではない。一方で、補題 1.2 により、n は何らかの素数を約数に持つが、直前の議論によりこの素数は $p_1, \ldots, p_k$ のどれとも異なることになる。これは $p_1, \ldots, p_k$ が素数のすべてであるという仮定に矛盾する。よって主張が成り立つ。 □

整数 a が整数 b と c の両方の約数であるとき、a を b と c の **公約数** と呼びます。整数 a が整数 b と c の両方の倍数であるとき、a を b と c の **公倍数** と呼びます。三つ以上の整数の公約数や公倍数も同様に定義されます。

定義 1.2 (最大公約数)**.** 整数 a と b の **最大公約数**（$\gcd(a, b)$ で表わす）を以下のように定義する：

- $a = 0$ かつ $b = 0$ のときは、$\gcd(a, b) = 0$ とする。
- $a \neq 0$ または $b \neq 0$ のときは、a と b の正の公約数のうち最大のもの（これは確かに存在する、なぜなら正の公約数は常に存在し（例えば 1）、また公約数は a と b のうち 0 でないもの以下なので）を $\gcd(a, b)$ とする。

また、$\gcd(a, b) = 1$ のとき、a と b は **互いに素** であるという。

定義 1.3 (最小公倍数)**.** 整数 a と b の **最小公倍数**（$\mathrm{lcm}(a, b)$ で表わす）を以下のように定義する：

- $a = 0$ または $b = 0$ のときは、$\mathrm{lcm}(a, b) = 0$ とする。

- $a \neq 0$ かつ $b \neq 0$ のときは、a と b の正の公倍数のうち最小のもの（これは確かに存在する、なぜなら正の公倍数は常に存在し（例えば $|ab|$）、また正の公倍数は a 以上なので）を $\mathrm{lcm}(a,b)$ とする。

定義より $\gcd(a,b) = \gcd(b,a)$ かつ $\mathrm{lcm}(a,b) = \mathrm{lcm}(b,a)$ であることを注意しておきます。最大公約数を計算するアルゴリズムとして、**ユークリッドの互除法**が有名です。その中核をなすのが以下の性質です。

補題 1.3. a と b を正の整数とし、a を b で割った余りを r とする（したがって $0 \leq r < b$）と、$\gcd(a,b) = \gcd(r,b)$ が成り立つ。

証明. 最大公約数の定義により、主張が成り立つためには、a と b の正の公約数の集合と、r と b の正の公約数の集合が一致すれば充分である。そのためには、d を b の正の約数としたとき、条件 $d \mid a$ と $d \mid r$ が同値であればよい。ここで、r は a を b で割った余りなので、ある整数 q を用いて $a = qb + r$ と表わせる。すると、上記のような d について、b と同様に qb も d の倍数であるから、r が d の倍数ならば $a = qb + r$ も d の倍数であり、逆に a が d の倍数ならば $r = a - qb$ も d の倍数である。よって主張が成り立つ。 □

補題 1.3 により、整数 a, b（ただし $a > b > 0$ とします）について、a を b で割った余りを r とすると、$\gcd(a,b) = \gcd(b,r)$ が成り立ちます。ここで $r = 0$ であれば $\gcd(b,r) = b$ すなわち $\gcd(a,b) = b$ として $\gcd(a,b)$ が求まります。一方 $r \neq 0$ のときは、$\gcd(a,b)$ の計算が $\gcd(b,r)$（$b > r > 0$）の計算に帰着されます。r は a よりも小さくなっていますので、この手順を繰り返すことで、有限の手数で $\gcd(a,b)$ を計算することができます。これがユークリッドの互除法です。

また、ユークリッドの互除法を少々拡張することで、整数 a と b の最大公約数を計算するだけでなく、$ca+db = \gcd(a,b)$ を満たす整数 c, d も同時に計算することが可能になります。実際、前の段落の状況で、もし $cb+dr = \gcd(b,r) = \gcd(a,b)$ となる整数 c, d が計算できたとすると、割り算の結果 $a = bq + r$（$q \in \mathbb{Z}$）と合わせて、

$$\gcd(a,b) = cb + dr = cb + d(a - bq) = da + (c - dq)b$$

として、$c'a + d'b = \gcd(a,b)$ を満たす整数 $c' = d$ と $d' = c - dq$ が求まります。このように、ユークリッドの互除法の最終段階（そこでは $r = 0$ となっているので、$\gcd(a,b) = b$ すなわち $0 \cdot a + 1 \cdot b = \gcd(a,b)$ です）から遡ることで上記

のような係数 c, d を計算できます。この計算の部分を割愛して、係数の存在だけを抜き出すと以下の結果となります。

定理 1.2. a, b を整数とすると、$ca+db = \gcd(a, b)$ を満たす整数 c, d が存在する。

本稿では、整数 a, b および m について、$a - b$ が m の倍数であることを記号 $a \equiv_m b$ で表わします。（これは $a \equiv b \pmod{m}$ などと表わすのが一般的ですが、この一般的な記法は不便だと筆者は常々思っているので上記の記号を使うことにします。）さて、定理 1.2 を用いると以下の性質が示されます。

命題 1.1. a と m を整数とする。このとき、$ba \equiv_m \gcd(a, m)$ を満たす整数 b が存在する。特に、a と m が互いに素であるとき、$ba \equiv_m 1$ を満たす整数 b が存在する。

証明. 後半部は前半部の特別な場合なので、前半部を示せばよい。定理 1.2 を a と m に適用すると、$ba + cm = \gcd(a, m)$ を満たす $b, c \in \mathbb{Z}$ が存在することがわかる。このとき cm は m の倍数なので $\gcd(a, m) = ba + cm \equiv_m ba$ となり、主張が成り立つ。 □

素数にまつわる概念としては素因数分解が重要ですが、素因数分解に関係する素数の性質として以下が挙げられます。

命題 1.2. p を 2 以上の整数とするとき、以下は互いに同値である。

1. p は素数である。
2. 整数 a, b が $p \nmid a$ かつ $p \nmid b$ を満たすならば $p \nmid ab$ である。

証明. まず、条件 1 を仮定して条件 2 を示す。p が素数なので、p と a の正の公約数の候補は 1 と p だけであるが、$p \nmid a$ という前提より p は公約数ではなく、p と a の正の公約数は 1 のみである。よって $\gcd(a, p) = 1$ であり、定理 1.2 により $ca + dp = 1$ を満たす $c, d \in \mathbb{Z}$ が存在する。b についても同様に、$c'b + d'p = 1$ を満たす $c', d' \in \mathbb{Z}$ が存在する。すると両辺をそれぞれ掛け合わせて、

$$(ca + dp)(c'b + d'p) = 1$$

が成り立つ。左辺を展開すると

$$(ca + dp)(c'b + d'p) = cc' \cdot ab + (cad' + dc'b + dd'p) \cdot p$$

となり、これを用いると

$$cc' \cdot ab = -(cad' + dc'b + dd'p) \cdot p + 1$$

となる。右辺の第 1 項は p の倍数であり第 2 項は p の倍数ではないので、補題 1.1 により左辺 $cc' \cdot ab$ は p の倍数ではなく、したがって ab も p の倍数ではない。こうして条件 2 が示された。

逆に、条件 2 を仮定して条件 1 を示す。a を p の正の約数とする、つまり $ab = p$ を満たす整数 b が存在するとする。この b も p の正の約数である。このとき、$p \mid p = ab$ であるから、条件 2 の前提 $p \nmid a$ および $p \nmid b$ のうちどちらかは成り立たないことになる。$p \mid a$ であるとすると、正の整数 a と p が互いにもう一方の約数であることになり、したがって $a = p$ である。一方 $p \mid b$ であるとすると、上と同じ議論により $b = p$ となり、$ap = p$ したがって $a = 1$ となる。よって、p の正の約数は p または 1 しかないことになり、p は素数であり条件 1 が成り立つ。以上より主張が成り立つ。 □

この性質を用いると、整数に対する「素因数分解の存在と一意性」が示されます。より詳しくは以下の性質が成り立ちます。

定理 1.3. n を正の整数とすると、

1. ある整数 $k \geq 0$ と互いに異なる素数 $p_1, \ldots, p_k$、および正整数 $e_1, \ldots, e_k$ で、等式 $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ を満たすものが存在する。（$k = 0$ のときは右辺は「空っぽの積」になるが、この「空っぽの積」は 1 であるとみなす。）この等式 $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ を n の **素因数分解** と呼ぶ。さらに、

2. $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ および $n = {q_1}^{f_1} \cdots {q_\ell}^{f_\ell}$ をともに n の素因数分解とすると、$k = \ell$ であり、対 $(q_1, f_1), \ldots, (q_k, f_k)$ たちを適切に並べ替えることで、$p_i = q_i$ かつ $e_i = f_i$ がすべての $i = 1, \ldots, k$ について成り立つ。

証明. まず主張 1、つまり n の素因数分解の存在を n に関する数学的帰納法によって示す。$n = 1$ のときは、主張の中で述べた注意により、「空っぽの積」が n の素因数分解となる。以降では $n \geq 2$ のときを考える。もし n 自身が素数であれば、$n = n^1$ が n の素因数分解である。よって、n が合成数の場合を考えればよい。このとき、n よりも小さい正の整数 a, b を用いて $n = ab$ と表わせる。数学的帰納法の仮定により、a と b はそれぞれ素因数分解を持つ、つまり

$a = {p_1}^{e_1} \cdots {p_k}^{e_k}$ および $b = {p'_1}^{e'_1} \cdots {p'_{k'}}^{e'_{k'}}$ という形に素因数分解される。これらを両辺ごとに掛け合わせることで $n = ab$ の素因数分解が得られる。より厳密には、重複を省いて素数 $p_1, \ldots, p_k, p'_1, \ldots, p'_{k'}$ を並べ直したものを $q_1, \ldots, q_\ell$ と書き、$i = 1, \ldots, \ell$ について整数 f_i を、

- $q_i = p_j$ かつ $q_i \notin \{p'_1, \ldots, p'_{k'}\}$ のとき $f_i = e_j$
- $q_i = p'_j$ かつ $q_i \notin \{p_1, \ldots, p_k\}$ のとき $f_i = e'_j$
- $q_i = p_j = p'_{j'}$ のとき $f_i = e_j + e'_{j'}$

で定めると、$n = {q_1}^{f_1} \cdots {q_\ell}^{f_\ell}$ が n の素因数分解となる。

次に主張 2、つまり n の素因数分解の一意性を n に関する数学的帰納法で示す。$n = 1$ のときは、n の素因数分解は「空っぽの積」以外にあり得ない（素数は 1 より大きいので）ため、主張が確かに成り立つ。以降では $n \geq 2$ のときを考える。このとき、前提にある素因数分解 $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ および $n = {q_1}^{f_1} \cdots {q_\ell}^{f_\ell}$ は「空っぽの積」ではない。前者の素因数分解により $p_k \mid n$ であるので、後者の素因数分解により $p_k \mid {q_1}^{f_1} \cdots {q_\ell}^{f_\ell}$ である。ここで命題 1.2 を繰り返し用いると、どれかの q_i について $p_k \mid q_i$ が成り立つことになる。q_i は素数であり $p_k \geq 2$ であるから、これは $p_k = q_i$ を意味する。ここで、n の素因数分解 $n = {q_1}^{f_1} \cdots {q_\ell}^{f_\ell}$ の右辺の積の順番を適当に並べ替えても目標の性質には影響しないので、$i = \ell$ となるように並べ替えておく。

以下、$e_k \leq f_\ell$ か $e_k \geq f_\ell$ かに応じて場合分けをするが、後者の場合も前者の場合と同様に議論が進むので、$e_k \leq f_\ell$ の場合のみを考えることにする。$n' = n/{p_k}^{e_k}$ $(= n/{q_\ell}^{e_k})$ とおくと、

$$n' = {p_1}^{e_1} \cdots {p_{k-1}}^{e_{k-1}} = {q_1}^{f_1} \cdots {q_{\ell-1}}^{f_{\ell-1}} {p_k}^{f_\ell - e_k}$$

が成り立つ。ここで、もし $f_\ell - e_k > 0$ とすると、上の式により $p_k \mid n'$ なので、先程の議論と同様に $p_k \in \{p_1, \ldots, p_{k-1}\}$ となるが、これは $p_1, \ldots, p_k$ がどれも異なるという素因数分解の前提に矛盾する。よって $f_\ell - e_k = 0$ となり、

$$n' = {p_1}^{e_1} \cdots {p_{k-1}}^{e_{k-1}} = {q_1}^{f_1} \cdots {q_{\ell-1}}^{f_{\ell-1}}$$

が成り立つ。これらは n' の二通りの素因数分解であるが、$n' < n$ なので、数学的帰納法の仮定により主張 2 が n' について成り立つ。つまり、$k - 1 = \ell - 1$（すな

わち $k = \ell$）であり、$(q_1, f_1), \ldots, (q_{k-1}, f_{k-1})$ たちを適切に並べ替えると $p_j = q_j$ かつ $e_j = f_j$ がすべての $j = 1, \ldots, k-1$ について成り立つ。さらに（$k = \ell$ なので）上の議論により $p_k = q_k$ かつ $e_k = f_k$ でもある。これは主張 2 が n について成り立つことを意味する。以上より主張が成り立つ。 □

2 素数で割った余りの世界

n を正整数とするとき、前述のように、整数 a, b について $n \mid a-b$ であることを $a \equiv_n b$ と表わします。また、整数 a を n で割った余りを $a \bmod n$ で表わします。つまり、a を n で割った商 $q \in \mathbb{Z}$ について、$a = qn + (a \bmod n)$ および $a \bmod n \in \{0, 1, \ldots, n-1\}$ が成り立ちます。定義より $a \equiv_n (a \bmod n)$ であることを注意しておきます。

関係 $\equiv_n$ については以下の性質が成り立ちます。

命題 2.1. n を正整数、a_1, a_2, b_1, b_2 を整数とする。もし $a_1 \equiv_n b_1$ かつ $a_2 \equiv_n b_2$ であれば、

$$a_1 + a_2 \equiv_n b_1 + b_2\,,\ a_1 - a_2 \equiv_n b_1 - b_2\,,\ a_1 a_2 \equiv_n b_1 b_2$$

が成り立つ。

証明. 前提より、$a_1 - b_1 = cn$ となる整数 c と、$a_2 - b_2 = dn$ となる整数 d が存在する。すると、足し算に関する主張については、

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) = cn + dn = (c+d)n$$

より $a_1 + a_2 \equiv_n b_1 + b_2$ が成り立つ。同様に、引き算についても

$$(a_1 - a_2) - (b_1 - b_2) = (a_1 - b_1) - (a_2 - b_2) = cn - dn = (c-d)n$$

より $a_1 - a_2 \equiv_n b_1 - b_2$ が成り立ち、掛け算についても

$$a_1 a_2 - b_1 b_2 = a_1(a_2 - b_2) + (a_1 - b_1)b_2 = a_1 dn + cnb_2 = (a_1 d + cb_2)n$$

より $a_1 a_2 \equiv_n b_1 b_2$ が成り立つ。よって主張が成り立つ。 □

命題 2.1 により、整数の加減乗算を繰り返した結果について n で割った余りを計算したい場合、加減乗算の繰り返しの最中に途中経過を適宜 n で割った余りに置き換えても結果に影響がないことがわかります。これを用いると、途中経過に現れる数を不必要に大きくすることを避けられて便利です。例えば、$n = 7$ として $(3 \cdot 4^3 + 2 \cdot 6) \bmod 7$ を計算したい場合、

$$4^2 = 16 \equiv_7 2\ ,$$

$$4^3 = 4^2 \cdot 4 \equiv_7 2 \cdot 4 = 8 \equiv_7 1 \ ,$$

$$3 \cdot 4^3 \equiv_7 3 \cdot 1 = 3 \ ,$$

$$2 \cdot 6 = 12 \equiv_7 5 \ ,$$

$$3 \cdot 4^3 + 2 \cdot 6 \equiv_7 3 + 5 = 8 \equiv_7 1$$

として、$(3 \cdot 4^3 + 2 \cdot 6) \bmod 7 = 1$ が得られます。

なお、べき乗の高速計算法の一つである **バイナリ法** と、命題 2.1 の性質を合わせると、整数のべき乗を n で割った余りを効率的に計算できます。例えば、$n = 11$ として $7^{29} \bmod 11$ を計算してみます。ここでべき指数 29 を二進数表示すると $29 = (11101)_2$ となりますが、この二進数表示の先頭からの部分列に対応する整数は、それぞれ $(1)_2 = 1$、$(11)_2 = 3$、$(111)_2 = 7$、$(1110)_2 = 14$、$(11101)_2 = 29$、となります。この結果を基に、$7^{29} \bmod 11$ を以下のように計算します。

$$7^1 \equiv_{11} 7 \, ,$$

$$7^3 = (7^1)^2 \cdot 7 \equiv_{11} 7^2 \cdot 7 = 49 \cdot 7 \equiv_{11} 5 \cdot 7 = 35 \equiv_{11} 2 \, ,$$

$$7^7 = (7^3)^2 \cdot 7 \equiv_{11} 2^2 \cdot 7 = 4 \cdot 7 \equiv_{11} 4 \cdot 7 = 28 \equiv_{11} 6 \, ,$$

$$7^{14} = (7^7)^2 \equiv_{11} 6^2 = 36 \equiv_{11} 3 \, ,$$

$$7^{29} = (7^{14})^2 \cdot 7 \equiv_{11} 3^2 \cdot 7 = 9 \cdot 7 \equiv_{11} 9 \cdot 7 = 63 \equiv_{11} 8 \ .$$

集合 $\mathbb{Z}/n\mathbb{Z}$ を $\mathbb{Z}/n\mathbb{Z} = \{a \bmod n \mid a \in \{0, 1, \ldots, n-1\}\}$ と定めます。命題 2.1 により、この集合 $\mathbb{Z}/n\mathbb{Z}$ には足し算、引き算、掛け算がそれぞれ

$$(a \bmod n) + (b \bmod n) = (a + b) \bmod n \, ,$$

$$(a \bmod n) - (b \bmod n) = (a - b) \bmod n \, ,$$

$$(a \bmod n) \cdot (b \bmod n) = (a \cdot b) \bmod n$$

として定まり、これらの演算は整数の加減乗算と同様の性質（例えば足し算の結合法則や掛け算と足し算の分配法則など）を持ちます。代数学の言葉では、$\mathbb{Z}/n\mathbb{Z}$ は乗法単位元を持つ可換環である、などと言い表します。$\mathbb{Z}/n\mathbb{Z}$ という形の集合のことを **整数剰余環** と呼びます。紛らわしさのない場合には、$\mathbb{Z}/n\mathbb{Z}$ の元 $a \bmod n$ のことを単に a と書き表します。

ここで代数学に現れる概念を少し述べておきます。

定義 2.1 (群)**.** G を集合とし、$*$ を G 上の二項演算とする（つまり、G の元 a, b に応じて G の元 $a * b$ が定まっているとする）。これらが以下の条件を満たすとき、G は（演算 $*$ に関する）**半群** であるという。

1. 演算 $*$ は結合法則を満たす、すなわち G の元 a, b, c について常に $(a*b)*c = a*(b*c)$ が成り立つ。

G の元 a, b について常に $a*b = b*a$ が成り立つとき、G は **可換** であるといい、そうでない G は **非可換** であるという。半群 G が以下の条件も満たすとき、G は単位元を持つ半群、あるいは **モノイド** であるという。

2. 以下の条件を満たす G の元 e が存在する：G の元 a について常に $a*e = a$ かつ $e*a = a$ が成り立つ。このような e を G の **単位元** と呼ぶ。

さらに、モノイド G が以下の条件も満たすとき、G は **群** であるという。

3. e を G の単位元とする。このとき、a が G の元であれば、$a*b = e$ かつ $b*a = e$ を満たす G の元 b が存在する。この b を a の **逆元** と呼ぶ。

証明は割愛しますが、モノイドにおける単位元はただ一つに定まることと、群におけるある元の逆元はただ一つに定まることがわかります。

定義 2.2 (環)**.** 集合 R が以下の条件を満たすとき、R は（加法 $+$ と乗法 $\times$ に関する）**環** であるという。

1. R は演算 $+$ に関して可換群である。以下、特に断りの無い限り、その単位元を 0 で表わす。また、a の逆元を $-a$ で表わし、$a + (-b)$ のことを $a - b$ で表わす。

2. R は演算 $\times$ に関して半群である。以下、$a \times b$ の代わりに $a \cdot b$ や ab などとも書き表す。

3. 加法 $+$ と乗法 $\times$ は分配法則を満たす、つまり R の元 a, b, c について $a \times (b + c) = (a \times b) + (a \times c)$ および $(b + c) \times a = (b \times a) + (c \times a)$ が成り立つ。

R の演算 $\times$ が可換であるとき R は **可換** であるという。さらに、R が以下の条件も満たすとき、R は単位元を持つ環であるという（以降では、環といえば単位元を持つ環のことを指し表わすことが多い）。

4. $R \setminus \{0\}$ はモノイドである。以下、特に断りの無い限り、その単位元を 1 で表わす。

R が単位元を持つ環であるとき、モノイド $R \setminus \{0\}$ において可逆な元のことを R において **可逆** であるといい、モノイド $R \setminus \{0\}$ における逆元を R における **逆元** と呼ぶ。R の可逆な元全体の集合を $R^\times$ もしくは R^* と書く。

環について、一般に $0 \cdot a = 0$ および $a \cdot 0 = 0$ が成り立つことがわかります。例えば、$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ はすべて単位元を持つ可換環で、0 が加法の単位元、1 が乗法の単位元です。これらについての「逆元」は通常の用語でいう「逆数」にあたります。また、前述の集合 $\mathbb{Z}/n\mathbb{Z}$ は上で定めた加法と乗法に関する可換環であり、$0 = 0 \bmod n$ が加法に関する単位元です。さらに $n \geq 2$ であれば $\mathbb{Z}/n\mathbb{Z}$ は乗法の単位元 $1 = 1 \bmod n$ を持ちます。（$n = 1$ のときは、$\mathbb{Z}/n\mathbb{Z}$ は唯一の元 0 を持つ環となります。このような環は「零環」と呼ばれます。）

整数環 $\mathbb{Z}$ については、± 1 以外の元 $a \in \mathbb{Z}$ は $\mathbb{Z}$ の中に逆元を持ちません（$a = 0$ であるか、$a^{-1} \in \mathbb{Q}$ が存在してもそれが整数になりません）。一方で、整数剰余環 $\mathbb{Z}/n\mathbb{Z}$ においては、1 や $(-1 \bmod n) = n - 1$ 以外にも逆元を持つ元が存在し得ます。$\mathbb{Z}/n\mathbb{Z}$ の元の逆元のことを「n を法とする逆元」などとも呼びます。

命題 2.2. n を 2 以上の整数とする。$a \in \mathbb{Z}/n\mathbb{Z}$ について、a が可逆であることと $\gcd(a, n) = 1$ であることは同値である。

証明. まず、$\gcd(a, n) = 1$ とすると、命題 1.1 により $ab \equiv_n 1$ を満たす整数 b が存在する。この b（より正確には $b \bmod n$）が a の逆元となる。逆に、b が n を法とする a の逆元であるとすると、$ab \equiv_n 1$ なので、$ab + cn = 1$ を満たす $c \in \mathbb{Z}$ が存在する。すると、$\gcd(a, n)$ は ab と cn の公約数なので 1 の約数でもある。したがって $\gcd(a, n) = 1$ となる。よって主張が成り立つ。 □

命題 2.2 を n が素数 p である場合に適用すると、$(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$、つまり $\mathbb{Z}/p\mathbb{Z}$ の 0 以外の元はすべて可逆であることがわかります。以下に述べる用語を用いると、素数 p について $\mathbb{Z}/p\mathbb{Z}$ は体になる、ということです。この $\mathbb{Z}/p\mathbb{Z}$ のことを $\mathbb{F}_p$ とも書きます。

定義 2.3 (体)**.** 単位元を持つ可換環 K について、$K^\times = K \setminus \{0\}$ が成り立つとき、K は **体** であるという。

$\mathbb{F}_p$ たち以外に、$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ も体となります。一方 $\mathbb{Z}$ は体ではありません。なお、単位元を持つ環については以下の性質が成り立ちます。

命題 2.3. R を単位元を持つ環とすると、$R^\times$ は R の乗法（を部分集合 $R^\times$ に制限したもの）に関して群となる。この $R^\times$ を環 R の **乗法群** と呼ぶ。

証明. まず、$a, b \in R^\times$ のとき $ab \in R^\times$ であることを示す。このことにより、R の乗法を $R^\times$ に制限したものが実際に $R^\times$ 上の演算となることがわかる。さて、$a, b \in R^\times$ よりこれらの元の（R における）逆元 a^{-1}, b^{-1} が存在する。すると

$$(ab) \cdot (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$$

となるので、$b^{-1}a^{-1}$ が ab の逆元であり、確かに $ab \in R^\times$ となる。

乗法が結合法則を満たすことは環の定義より直ちに成り立ち、$R^\times$ もまた半群となる。また、$1 = 1 \cdot 1$ であることから $1 \in R^\times$ であり、この 1 が $R^\times$ の単位元となる。よって $R^\times$ はモノイドである。さらに $a \in R^\times$ について、$aa^{-1} = a^{-1}a = 1$ より a^{-1} も可逆（a が a^{-1} の逆元）であり、$a^{-1} \in R^\times$ である。この a^{-1} が $R^\times$ における a の逆元でもあるので、a は $R^\times$ においても可逆である。よって $R^\times$ は群であり、主張が成り立つ。 □

定義 2.4 (群の準同型写像)**.** G_1, G_2 を群とする。写像 $\varphi\colon G_1 \to G_2$ が、以下の条件

- $g_1, g_2 \in G_1$ のとき $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$

を満たすとき、φ を G_1 から G_2 への **群準同型写像**（あるいは単に、準同型写像）と呼ぶ。また、群準同型写像が全単射であるとき、**群同型写像**（あるいは単に、同型写像）と呼ぶ。

定義 2.5 (環の準同型写像)**.** R_1, R_2 を単位元を持つ環とする。写像 $\varphi\colon R_1 \to R_2$ が、以下の条件

- $r_1, r_2 \in R_1$ のとき $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$
- $r_1, r_2 \in R_1$ のとき $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$
- 1_{R_1} と 1_{R_2} をそれぞれ R_1 と R_2 の乗法の単位元とすると、$\varphi(1_{R_1}) = 1_{R_2}$

を満たすとき、φ を R_1 から R_2 への **環準同型写像**（あるいは単に、準同型写像）と呼ぶ。また、環準同型写像が全単射であるとき、**環同型写像**（あるいは単に、同型写像）と呼ぶ。

$m_1, \ldots, m_k$ を正の整数とするとき、$\mathbb{Z}/m_i\mathbb{Z}$ の元 a_i たちを $i = 1, \ldots, k$ について並べた列 $(a_1, \ldots, a_k)$ 全体の集合を $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ で表わします。代数的には、この $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ は環 $\mathbb{Z}/m_1\mathbb{Z}, \ldots, \mathbb{Z}/m_k\mathbb{Z}$ の直和に相当します。この $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ における和、差、積を、成分ごとの和、差、積によって定めます。つまり

$$(a_1, \ldots, a_k) + (b_1, \ldots, b_k) = (a_1 + b_1, \ldots, a_k + b_k)\,,$$

$$(a_1, \ldots, a_k) - (b_1, \ldots, b_k) = (a_1 - b_1, \ldots, a_k - b_k)\,,$$

$$(a_1, \ldots, a_k) \cdot (b_1, \ldots, b_k) = (a_1 \cdot b_1, \ldots, a_k \cdot b_k)$$

と定めます。このとき $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ は単位元を持つ可換環であり、加法の単位元は $(0, 0, \ldots, 0)$、乗法の単位元は $(1, 1, \ldots, 1)$ であることがわかります。さらに、以下の事実が成り立ちます。

定理 2.1 (中国式剰余定理)**.** $m_1, \ldots, m_k$（$k \geq 1$）を、どの二つも互いに素であるような 2 以上の整数とし、$m = m_1 \cdots m_k$ とする。このとき、$\mathbb{Z}/m\mathbb{Z}$ の元 a を $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ の元 $(a \bmod m_1, \ldots, a \bmod m_k)$ に対応させる写像を f で表わすと、

1. f は環 $\mathbb{Z}/m\mathbb{Z}$ から環 $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ への同型写像である。
2. $a \in \mathbb{Z}/m\mathbb{Z}$、$f(a) = (a_1, \ldots, a_k)$ とすると、$a \in (\mathbb{Z}/m\mathbb{Z})^\times$ であることと、$a_i \in (\mathbb{Z}/m_i\mathbb{Z})^\times$ がすべての $i = 1, \ldots, k$ について成り立つことが同値である。特に、f は群 $(\mathbb{Z}/m\mathbb{Z})^\times$ から群 $(\mathbb{Z}/m_i\mathbb{Z})^\times$ たちの直積群への同型写像を定める。

証明. まず、写像 f が well-defined であること、すなわち、$a \equiv_m a'$ であれば常に $f(a) = f(a')$ であることを確かめておく。これは、$a - a' = cm$ となる整数 c をとると、各 i について $a - a' = cm_1 \cdots m_{i-1}m_{i+1} \cdots m_k \cdot m_i$ であり、したがって $a \equiv_{m_i} a'$ つまり $a \bmod m_i = a' \bmod m_i$ でもあることから成り立つ。

条件 $f(a + b) = f(a) + f(b)$ および $f(ab) = f(a)f(b)$ は、環 $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ における加法と乗法の定義より直ちに成り立つ。条件 $f(1) = (1, 1, \ldots, 1)$

も定義より直ちに成り立つので、f は環準同型写像である。また、$\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_k\mathbb{Z}$ の元の個数は定義より $m_1\cdots m_k = m$ であり、これは $\mathbb{Z}/m\mathbb{Z}$ の元の個数に等しい。このことから、あとは f が全射であることを示せば f は全単射でもあり、主張 1 が示される。

f が全射であることを示す。まず、$m_1,\ldots,m_k$ がどの二つも互いに素であることから、各 i について m_i と m/m_i は互いに素である。命題 2.2 により、m_i を法とする m/m_i の逆元が存在するので、それを c_i で表わす。ここで、各 i について $a_i\in\mathbb{Z}/m_i\mathbb{Z}$ が与えられているとき、$a\in\mathbb{Z}/m\mathbb{Z}$ を

$$a = (m/m_1)\cdot c_1a_1 + (m/m_2)\cdot c_2a_2 + \cdots + (m/m_k)\cdot c_ka_k$$

で定める。各 i について、$j\neq i$ であれば m/m_j は m_i の倍数なので、$(m/m_j)\cdot c_ja_j \equiv_{m_i} 0$ である。よって $a\equiv_{m_i}(m/m_i)\cdot c_ia_i$ である。さらに c_i は $\mathbb{Z}/m_i\mathbb{Z}$ における m/m_i の逆元なので、$a\equiv_{m_i}a_i$ となり、$a \bmod m_i = a_i$ が成り立つ。よって $f(a) = (a_1,\ldots,a_k)$ となることから、f は全射であり、主張 1 が成り立つ。

主張 2 について、まず、$a\in(\mathbb{Z}/m\mathbb{Z})^\times$ とすると、命題 2.2 により a は m と互いに素である。すると各 i について a は m_i とも互いに素であり、再び命題 2.2 により a は m_i を法として可逆なので、$a_i = a \bmod m_i\in(\mathbb{Z}/m_i\mathbb{Z})^\times$ が確かに成り立つ。

逆に、各 i について $a_i\in(\mathbb{Z}/m_i\mathbb{Z})^\times$ であるとする。$\mathbb{Z}/m_i\mathbb{Z}$ における a_i の逆元を b_i とおく。主張 1 により f は全射なので、$f(b) = (b_1,\ldots,b_k)$ を満たす $b\in\mathbb{Z}/m\mathbb{Z}$ が存在する。このとき

$$f(ab) = f(a)f(b) = (a_1,\ldots,a_k)\cdot(b_1,\ldots,b_k) = (a_1b_1,\ldots,a_kb_k) = (1,\ldots,1)$$

であり、一方で $f(1) = (1,\ldots,1)$ でもある。よって $f(ab) = f(1)$ であり、主張 1 により f は単射なので、$ab = 1$ となり、$a\in(\mathbb{Z}/m\mathbb{Z})^\times$ が成り立つ。以上より主張が成り立つ。 □

正の整数 n について、**オイラーの totient 関数** $\varphi(n)$（あるいは単にオイラー関数）を

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

で定義します。この関数について以下の性質が成り立ちます。

定理 2.2. $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ を n の素因数分解とすると、

$$\varphi(n) = (p_1 - 1){p_1}^{e_1 - 1} \cdots (p_k - 1){p_k}^{e_k - 1}$$

が成り立つ。

証明. 定理 2.1 により、

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/{p_1}^{e_1}\mathbb{Z})^\times| \cdots |(\mathbb{Z}/{p_k}^{e_k}\mathbb{Z})^\times| = \varphi({p_1}^{e_1}) \cdots \varphi({p_k}^{e_k})$$

が成り立つので、n が素数 p と整数 $e \geq 1$ について p^e という形のときに目標の性質が成り立てば一般の n についても目標の性質が成り立つ。

上記のように $n = p^e$ という形のとき、命題 2.2 より、$\varphi(p^e)$ は p^e と互いに素である整数 $a \in \{0, 1, \ldots, p^e - 1\}$ の個数に等しい。ここで、上記の範囲にある整数 a について、a が p^e と互いに素であることは a が p の倍数でないことと同値であるので、p^e と互いに素である a の個数は全体の $1 - 1/p$ 倍である。その個数は $p^e \cdot (1 - 1/p) = p^e - p^{e-1} = (p-1)p^{e-1}$ であるから、$\varphi(p^e) = (p-1)p^{e-1}$ であり、$n = p^e$ の形のときには目標の性質が成り立つ。以上より主張が成り立つ。 □

以下、オイラー関数 φ についてのオイラーの定理を証明しますが、その準備として群に関する以下の性質を示しておきます。

定理 2.3 (ラグランジュの定理)**.** G を有限群とし、H をその部分群（すなわち、部分集合 $H \subset G$ であって、G の演算を制限した演算によって群をなすもの）とすると、$|H|$ は $|G|$ の約数である。

証明. G の元 a について、集合 aH を $aH = \{ah \in G \mid h \in H\}$ と定義する。まず、$aH \cap bH \neq \emptyset$ であれば $aH = bH$ であることを示す。$aH \cap bH$ の元 g をとると、$g = ah_1$ および $g = bh_2$（$h_1, h_2 \in H$）という形で表わせる。$g = ah_1 = bh_2$ より、$a = bh_2{h_1}^{-1}$ および $b = ah_1{h_2}^{-1}$ が成り立つ。ここで、aH の元 ah（$h \in H$）について、$ah = bh_2{h_1}^{-1}h$ となり、また H が G の部分群であることから $h_2{h_1}^{-1}h \in H$ となる。よって $ah \in bH$ が成り立つ。逆に、bH の元 bh（$h \in H$）について、$bh = ah_1{h_2}^{-1}h$ となり、また H が G の部分群であることから $h_1{h_2}^{-1}h \in H$ となる。よって $bh \in aH$ も成り立ち、確かに $aH = bH$ となる。

前の段落の結果から、$a \in G$ について aH という形をしている G の部分集合たちは、互いに一致するか交わりを持たないかのいずれかである。そして、G

の元はどれも何らかの集合 aH に属するため、G は aH という形をしている互いに交わらない部分集合いくつかの和集合となっている。さらに aH の元の個数はどれも $|H|$ に等しいことから、G の元の個数 $|G|$ は $|H|$ の倍数となることがわかる。よって主張が成り立つ。 □

定理 2.3 を用いると以下の性質が示されます。

定理 2.4 (オイラーの定理)**.** n を 2 以上の整数とし、a を n と互いに素な整数とすると、$a^{\varphi(n)} \equiv_n 1$ が成り立つ。

証明. a の代わりに $a \bmod n$ を考えることで a を $\mathbb{Z}/n\mathbb{Z}$ の元とみなす。命題 2.2 より $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ が成り立つ。a^k（$k \in \mathbb{Z}$）という形に表わせる $(\mathbb{Z}/n\mathbb{Z})^\times$ の元全体の集合を $\langle a \rangle$ で表わす（これを a が生成する $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群という）。定義より $\langle a \rangle$ は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群である。また、$a^k = a^\ell$ を満たす整数 $k \geq 0$ と $\ell > k$ の組 (k, ℓ)（$(\mathbb{Z}/n\mathbb{Z})^\times$ は有限集合なのでこのような組は必ず存在する）のうち ℓ が最小になるものをとると、$k = 0$ であり（もし $k > 0$ とすると $(k-1, \ell-1)$ も条件を満たすため）、したがって $a^\ell = a^0 = 1$ である。すると整数 m について $a^m = a^{m \bmod \ell}$ となることから $\langle a \rangle = \{1 = a^0, a^1, \ldots, a^{\ell-1}\}$ であり、ℓ の選び方よりこれら ℓ 個の元はすべて異なる。よって $|\langle a \rangle| = \ell$ であり、定理 2.3 より $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ は $|\langle a \rangle| = \ell$ の倍数である。これと $a^\ell = 1$ より、$a^{\varphi(n)} = 1$ が $\mathbb{Z}/n\mathbb{Z}$ において成り立つ。よって主張が成り立つ。 □

系 2.1 (フェルマーの小定理)**.** p を素数とすると、p と互いに素な整数 a について $a^{p-1} \equiv_p 1$ が成り立つ。

証明. 定理 2.4 と $\varphi(p) = p - 1$ より成り立つ。 □

体の乗法群は以下の性質を持ちます。

命題 2.4. K を体とし、G を $K^\times$ の有限部分群とすると、G は巡回群である、すなわち以下の条件を満たす G の元 a が存在する：G の元はどれも a^k（$k \in \mathbb{Z}$）という形に表わせる。この a を G の **生成元** という。

証明. $a \in G$ について、$\mathrm{ord}(a) = \min\{k \in \mathbb{Z}_{>0} \mid a^k = 1\}$ と定める（これを a の G における位数という）。定理 2.4 の証明と同様の議論により、a が生成する G の部分群 $\langle a \rangle$ について $|\langle a \rangle| = \mathrm{ord}(a)$ が成り立つ。よって、$\mathrm{ord}(a) = |G|$ を満たす $a \in G$ が存在することを示せばよい。$\mathrm{ord}(a)$ を最大にする G の元の一つを a

とする。$\mathrm{ord}(a) = |G|$ であれば主張が成り立つので、$\mathrm{ord}(a) < |G|$ と仮定して矛盾を導く。

多項式に対する剰余定理により、多項式 $x^{\mathrm{ord}(a)} - 1$ は K において $\mathrm{ord}(a)$ 個以下の根しか持たない。つまり、$b^{\mathrm{ord}(a)} = 1$ を満たす K の元 b は $\mathrm{ord}(a)$ 個以下、したがって $|G|$ 個未満である。このことから、$b^{\mathrm{ord}(a)} \neq 1$ を満たす $b \in G$ が存在する。

$b^{\mathrm{ord}(a)} \neq 1$ と $b^{\mathrm{ord}(b)} = 1$ より、$\mathrm{ord}(b)$ は $\mathrm{ord}(a)$ の約数ではない。したがって、$\mathrm{ord}(a)$ と $\mathrm{ord}(b)$ の素因数分解を考えると、ある素数 p については、$\mathrm{ord}(a)$ における p の指数 e よりも $\mathrm{ord}(b)$ における p の指数 f の方が大きくなる。ここで、$a' = a^{p^e}$ および $b' = b^{\mathrm{ord}(b)/p^f}$ とおくと、$\mathrm{ord}(a') = \mathrm{ord}(a)/p^e$ および $\mathrm{ord}(b') = p^f$ が成り立つ。

$k = \mathrm{ord}(a'b')$ とおくと、$k \geq 1$ かつ $(a'b')^k = (a')^k(b')^k = 1$ が成り立ち、$(a')^k = (b')^{-k} \in \langle a' \rangle \cap \langle b' \rangle$ となる。ここで定理 2.3 より、$\langle a' \rangle$ のどの元の位数も $\mathrm{ord}(a') = \mathrm{ord}(a)/p^e$ の約数であり、$\langle b' \rangle$ のどの元の位数も $\mathrm{ord}(b') = p^f$ の約数である。今、$\mathrm{ord}(a)/p^e$ と p^f は互いに素であるから、$\langle a' \rangle \cap \langle b' \rangle$ の元の位数は 1、すなわちその元は単位元である。よって $(a')^k = (b')^{-k} = 1$、したがって $(b')^k = 1$ である。このことから k は $\mathrm{ord}(a') = \mathrm{ord}(a)/p^e$ と $\mathrm{ord}(b') = p^f$ の公倍数であり、$\mathrm{ord}(a')$ と $\mathrm{ord}(b')$ は互いに素なので、k は $\mathrm{ord}(a')\mathrm{ord}(b') = \mathrm{ord}(a) \cdot p^{f-e}$ の倍数である。特に $\mathrm{ord}(a'b') = k \geq \mathrm{ord}(a) \cdot p^{f-e} > \mathrm{ord}(a)$ である（$f > e$ なので）。しかしながら、定義より $a', b' \in G$ したがって $a'b' \in G$ であるので、これは $\mathrm{ord}(a)$ が最大になるように $a \in G$ を選んだことに矛盾する。以上より主張が成り立つ。 □

系 2.2. K を有限体とすると、その乗法群 $K^\times$ は巡回群である。$K^\times$ の生成元を K の **原始元** と呼ぶ。

以降では、平方剰余の定義や性質について述べます。

定義 2.6 (平方剰余)**.** n を正の整数とする。n と互いに素な整数 a について、a が n を法とする **平方剰余** であるとは、$b^2 \equiv_n a$ を満たす $b \in \mathbb{Z}$ が存在することと定義する。n と互いに素な整数 a が平方剰余でないときに a は **平方非剰余** であるという。

定義 2.7 (ルジャンドル記号)**.** p を素数、a を整数とするとき、**ルジャンドル記号**

$\left(\dfrac{a}{p}\right) \in \{-1, 0, 1\}$ を

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & (\gcd(a,p) \neq 1 \text{ のとき}) \\ 1 & (\gcd(a,p) = 1 \text{ かつ、} a \text{ が } p \text{ を法とする平方剰余のとき}) \\ -1 & (\gcd(a,p) = 1 \text{ かつ、} a \text{ が } p \text{ を法とする平方非剰余のとき}) \end{cases}$$

で定義する。また、$n > 1$ を整数、$n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ を素因数分解とするとき、**ヤコビ記号** $\left(\dfrac{a}{n}\right)$ を

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & (\gcd(a,n) \neq 1 \text{ のとき}) \\ \left(\dfrac{a}{p_1}\right)^{e_1} \cdots \left(\dfrac{a}{p_k}\right)^{e_k} & (\gcd(a,n) = 1 \text{ のとき}) \end{cases}$$

で定義する。

補題 2.1. p を奇素数、a を p と互いに素な整数とすると、$\left(\dfrac{a}{p}\right) \equiv_p a^{(p-1)/2}$ が成り立つ。

証明. b を有限体 $\mathbb{F}_p$ の原始元の一つとする。定義より $\mathrm{ord}(b) = p - 1$ であり、これは偶数である。これより、${\mathbb{F}_p}^\times$ の元 c はすべて $c = b^k$（$k \in \mathbb{Z}$）という形に表わせて、しかも、k 自体は複数の選び方があるものの「k が偶数か奇数か」は c だけから一通りに定まる。そして、c が平方剰余であることと、$c = b^k$ という表示において k が偶数であることは等価である。さて、a が平方剰余、すなわち $\left(\dfrac{a}{p}\right) = 1$ であるとき、上の議論により p を法として $a = b^{2k}$（$k \in \mathbb{Z}$）という形に表わせるので、$a^{(p-1)/2} = b^{(p-1)k} = (b^{p-1})^k = 1^k = 1$ である（途中で系 2.1 を用いた）。一方、a が平方非剰余、すなわち $\left(\dfrac{a}{p}\right) = -1$ であるとき、上の議論により p を法として $a = b^{2k+1}$（$k \in \mathbb{Z}$）という形に表わせるので、$a^{(p-1)/2} = b^{(p-1)k+(p-1)/2} = (b^{p-1})^k b^{(p-1)/2} = b^{(p-1)/2}$ である。ここで、b が原始元であることから $b^{(p-1)/2} \neq 1$ であり、一方で $(b^{(p-1)/2})^2 = b^{p-1} = 1$ であるから、$b^{(p-1)/2} = -1$ である。よって $a^{(p-1)/2} = b^{(p-1)/2} = -1$ である。以上より主張が成り立つ。 □

命題 2.5. a, b および $n > 1$ を整数とすると、$\left(\dfrac{ab}{n}\right) = \left(\dfrac{a}{n}\right)\left(\dfrac{b}{n}\right)$ が成り立つ。

証明. ab が n と互いに素でない場合には、a または b が n と互いに素でないので、ヤコビ記号の定義により両辺ともに 0 となり一致する。以下、ab が n と互いに素である場合を考える。このとき、a も b も n と互いに素である。$n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ を n の素因数分解とすると、ヤコビ記号の定義より

$$\left(\frac{ab}{n}\right) = \left(\frac{ab}{p_1}\right)^{e_1} \cdots \left(\frac{ab}{p_k}\right)^{e_k}$$

である。このことから、各 i について $\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)$ を示せばよい。なお、ab が n と互いに素であることから a も b も p_i と互いに素である。$p_i = 2$ のとき、上の注意より a も b も奇数であり、定義よりすべての奇数は 2 を法として平方剰余なので、$\left(\frac{ab}{p_i}\right) = 1 = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)$ が確かに成り立つ。一方、p_i が奇素数のときは、補題 2.1 により

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

であり、$\left(\frac{ab}{p_i}\right) \equiv_{p_i} \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)$ である。さらに両辺は ± 1 であるから、$\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)$ が確かに成り立つ。よって主張が成り立つ。 □

証明は割愛しますが、ルジャンドル記号やヤコビ記号については以下の有名な事実が成り立ちます。

定理 2.5 (平方剰余の相互法則). *1.* a と b を互いに素な 1 より大きい奇数とすると、

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

が成り立つ。

2. a を 1 より大きな奇数とすると、

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}} = \begin{cases} 1 & (a \equiv_4 1 \text{ のとき}) \\ -1 & (a \equiv_4 3 \text{ のとき}) \end{cases}$$

が成り立つ。

3. a を 1 より大きな奇数とすると、

$$\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}} = \begin{cases} 1 & (a \equiv_8 1, 7 \text{ のとき}) \\ -1 & (a \equiv_8 3, 5 \text{ のとき}) \end{cases}$$

が成り立つ。

ルジャンドル記号やヤコビ記号の値を定義に従って直接計算するのは一般に大変ですが、定理 2.5 と命題 2.5 を用いると大変さが多少緩和されます。例えば、

$$\left(\frac{38}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{19}{127}\right) = (-1)^{(127^2-1)/8} \cdot (-1)^{\frac{19-1}{2}\frac{127-1}{2}} \left(\frac{127}{19}\right)$$

$$= 1 \cdot (-1)\left(\frac{13}{19}\right) = (-1) \cdot (-1)^{\frac{13-1}{2}\frac{19-1}{2}} \left(\frac{19}{13}\right) = (-1) \cdot 1 \cdot \left(\frac{6}{13}\right)$$

$$= (-1)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = (-1) \cdot (-1)^{(13^2-1)/8} \cdot (-1)^{\frac{3-1}{2}\frac{13-1}{2}} \left(\frac{13}{3}\right)$$

$$= (-1) \cdot (-1) \cdot 1 \cdot \left(\frac{1}{3}\right) = 1 \cdot 1 = 1$$

より $\left(\frac{38}{127}\right) = 1$ となります。

3　素数であることの証明（1）

何らかの理由で（大きな）素数を見つけたいとき、まずランダムに整数を選び、その数が素数であるかどうかを何らかの手段で確認する（素数でなければ、ランダムに整数を選び直す）という方法が考えられます。そのためには、与えられた整数が素数であるか合成数であるかを特定する手段（primality test などと呼ばれます）が必要となります。また、この問題と密接に関連する問題として、与えられた整数が素数であることを示す「証拠」を確認する手段（primality certificate や primality proof などと呼ばれます）や、逆に合成数である「証拠」を確認する手段も問題として考えられます。ここで、後者の問題においては、ある数が素数である「証拠」が与えられた状況でその「証拠」の正しさを確認する手続きのみを考慮しており、その「証拠」をどのように（効率的に）見つけるかは考慮していないことを注意しておきます。一方、前者の問題においては、そもそも与えられた数が素数かどうかがわからない（上記のような「証拠」が得られていない）状況から始めて、その数が素数であるかどうかを特定することを目標としています。

ある整数 $n > 1$ が素数であるかどうかを特定する、素数の定義に基づいた最も素朴な方法は、2 から $n-1$ までの整数で n を順番に割り算してみるという方法でしょう。このとき、どれかの数で n が割り切れれば n は合成数であり、どの数でも割り切れなければ n は素数であることがわかります。この総当たり的な方法は、n が素数かどうかを確実に判定できるものの、n が大きな数になると試すべき割り算の数が膨大になるため、実用的な方法とはいえません。（2 から $n-1$ までのすべての整数で割り算してみなくても、$\sqrt{n}$ 以下の範囲でだけ割り算を試せばよいとか、合成数であることがわかっている数での割り算は試す必要がないなどのささやかな効率化は可能ですが、n が巨大な場合には焼け石に水です。）とはいえ、n が小さな範囲、例えば（十進数で）2 桁程度の数が素数であるかを確認するぐらいであれば、後述するより高度な方法を使うよりもこの素朴な方法が一番使いやすいでしょう。

上記の総当たり的な方法は、ある一つの数が素数かどうかを調べる場面よりも、ある数以下の素数をすべて調べ上げたいといった場面の方がより効果を発揮します。**エラトステネスのふるい** は、この目的に沿った、単純ながら古代ギリシアより伝わる由緒正しい（？）方法です。

定義 3.1 (エラトステネスのふるい)**.** $n > 1$ を整数とする。1 から n までの整数を小さい順に並べた表を用意しておき、以下の手順に従って各々の数字に「○」または「×」を付けていく。

1. 1 に「×」を付ける。
2. $\sqrt{n}$ 以下の整数のうち、まだ「○」も「×」も付いていない最小の数 k をとる（このような数が無くなったら手順 3 に進む)。k に「○」を付けて、そこから k 個おきに数に「×」を付けていく（既に「×」が付いているときはそのままにしておく)。以下この手順を繰り返す。
3. まだ「○」も「×」も付いていないすべての数に「○」を付ける。

以上の手順の後に「○」が付いている数が素数であり、「×」が付いている数は素数ではない。

ある整数 $n > 1$ が素数である、もしくは素数でない「証拠」の話をします。素数の定義を思い起こせば、素数である「証拠」を示すよりも、素数でない「証拠」を示す方が簡単そうに思えます。というのも、素数の定義に従えば、n が合成数である「証拠」としては 1 でも n でもない n の正の約数を一つだけ与えれば（そして、その数で n を実際に割り算してみせれば）充分であるのに対して、n が素数である「証拠」としてはそういった正の約数が一つも存在しないことを示す必要があるように思われるからです。ただ、いくら「証拠」を確認する方法だけを考慮し「証拠」をどうやって見つけるかは一旦考慮から外しているとはいっても、できることなら「証拠」を実際に見つける方法のことも少しは考慮したいものです。その観点では、合成数 n の「証拠」として 1 でも n でもない正の約数を採用するのは、その約数を実際に見つけるために n の素因数分解という（現時点では）非常に時間のかかる計算が必要となるため、あまり好ましくありません。

合成数の「証拠」の候補を探すために、フェルマーの小定理（系 2.1）に注目します。整数 $n > 1$ について、もし n が素数であれば、n と互いに素な整数 a については常に $a^{n-1} \equiv_n 1$ が成り立つはずです。逆に言えば、$a^{n-1} \equiv_n 1$ とならない a が見つかったならば、その a を n が合成数である「証拠」として用いることができます。この方法は **フェルマーテスト** などと呼ばれます。その手順を改めて以下に記しておきます。

定義 3.2 (フェルマーテスト)**.** 整数 $n > 1$ について、以下の手順を考える。

1. 整数 a を 1 から $n-1$ までの範囲でランダムに選ぶ。ユークリッドの互除法を用いて $\gcd(a, n)$ を計算し、もし $\gcd(a, n) \neq 1$ であれば「n は合成数」と判定し終了する。

2. $a^{n-1} \not\equiv_n 1$ であれば「n は合成数」と判定する。そうでなければ何の判定も下さない。

フェルマーテストの利点として、「n は合成数」と判定された場合にはその結果は確実に正しいということが挙げられます。なお、手順 2 におけるべき乗 a^{n-1} の計算には一見すると膨大な手間が掛かりそうですが、前述のバイナリ法を用いると n の二進法での桁数（およそ $\log_2 n$）の定数倍程度の回数の掛け算と割り算だけで済むので、見た目よりは手数が少なくて済みます。また、厳密な評価は難しいので割愛しますが、大抵の合成数 n については、ランダムに選んだ a がそれなりに高い確率で上記手順中の条件を満たし、n が合成数であることを確認できると期待できます。しかしながら、フェルマーテストの最大の欠点として、どのような合成数 n についても「n は合成数」という判定が高い確率で得られるわけではないことが挙げられます。さらに言えば、上記手順を成立させる n と互いに素な整数 a が一つも存在しないような合成数 n も存在します。このような整数 n は、その具体例を最初に発見した人物[1] の名前にちなんで **カーマイケル数** と呼ばれています。すなわち、整数 $n > 1$ がカーマイケル数であるとは、n と互いに素なすべての整数 a が $a^{n-1} \equiv_n 1$ を満たすことと定義されます。最小のカーマイケル数は 561 であり、また無限に多くのカーマイケル数が存在することが知られています。もしカーマイケル数が有限個しかなければ、「最大のカーマイケル数よりも大きな入力値 n についてはフェルマーテストを行い、それ以外の入力値については別の手段で素数かどうか判定する」といった作戦も考えられましたが、残念ながらそのような作戦は通用しません。

合成数の「証拠」を見つける方法として、現在知られている中で最も実用的と考えられているのが、以下で紹介する **ミラー・ラビン法** です。この手法もフェルマーテストと同様にフェルマーの小定理に基づく手法ですが、フェルマーテストよりは若干込み入っています。

[1] R. D. Carmichael: Note on a new number theory function. Bulletin of the American Mathematical Society, vol.16, no.5, pp.232–238 (1910). doi:10.1090/s0002-9904-1910-01892-9

定義 3.3 (ミラー・ラビン法)**.** 奇数 $n > 1$ について以下の手順を考える（n が偶数の場合には素数かどうかの判定は容易なので省略する）。

1. $n-1$ を 2 で割り切れるだけ割り続けて、$n-1 = 2^s d$、$s \geq 1$、d は奇数、という形に表わす。

2. 整数 a を 1 から $n-1$ の範囲でランダムに選ぶ。$\gcd(a, n) \neq 1$ であれば「n は合成数」と判定して終了する。

3. もし、$a^d \not\equiv_n 1$ かつ、すべての $i = 0, 1, \ldots, s-1$ について $a^{2^i d} \not\equiv_n -1$ であれば、「n は合成数」と判定する。そうでなければ何の判定も下さない。

フェルマーテストと同様に、ミラー・ラビン法でも「n は合成数」と判定されればその結果は常に正しいものです。言い換えると下記が成り立ちます。

命題 3.1. 入力値 n が素数の場合にはミラー・ラビン法は何の判定も下さない。

証明. n が素数のとき、$1 \leq a \leq n-1$ とすると $\gcd(a, n) = 1$ である。また、フェルマーの小定理より $a^{2^s d} = (a^{2^{s-1} d})^2 \equiv_n 1$ である。ここで、$\mathbb{F}_n$ は体なので、多項式の剰余定理により $\mathbb{F}_n$ における 1 の平方根は 1 と -1 のみである。よって $a^{2^{s-1} d} \equiv_n \pm 1$ が成り立つ。手順 3 の定義により、$a^{2^{s-1} d} \equiv_n -1$ であれば「n は合成数」とは判定されないので、以降では $a^{2^{s-1} d} \equiv_n 1$ の場合を考える。ここで、$s-1 = 0$ であればやはり「n は合成数」とは判定されないので、$s-1 > 0$ の場合を考えればよい。すると上の議論と同様に $a^{2^{s-2} d} \equiv_n \pm 1$ が成り立つので、以下同様に繰り返すことで、ある i について $a^{2^i d} \equiv_n -1$ であるかもしくは $a^d \equiv_n 1$ であるかのいずれかの結論に到達する。よって「n は合成数」とは判定されないことがわかり、主張が成り立つ。 □

フェルマーテストと比較したミラー・ラビン法の顕著な利点は、n が合成数であれば、どの n についてもある一定値以上の確率で「n は合成数」という判定結果を返してくれる点です。そのため、ランダムな a に対するテストを充分な回数だけ繰り返すことで、n が合成数であればほぼ確率 1 で「n は合成数」という正しい判定を得ることができます（したがって、「n は合成数」という判定が出ない場合にはほぼ間違いなく n は素数と考えられます）。具体的には n が合成数のとき確率 3/4 以上で「n は合成数」と判定されることが知られていますが、ここでは証明を簡略化する都合上、少しだけ弱い（けれども実用上はまだ役立つ）結果を述べます。

定理 3.1. ミラー・ラビン法の入力値 n が合成数であるが、2 乗以上のべき乗の形はしていないと仮定する。このとき確率 $1/2$ 以上で「n は合成数」と判定される。

証明. 前提より、n は $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ かつ $k \geq 2$ という形に素因数分解される。中国式剰余定理により、同型写像

$$f\colon (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/{p_1}^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/{p_k}^{e_k}\mathbb{Z})^\times$$

が得られる。

$n-1 = 2^s d$ という表示を考える。d は奇数なので、$(-1)^d \equiv_n -1$ である。このことから、$i = 0$ については、$b^{2^i d} \equiv_n -1$ を満たす $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ が存在する。そこで、$b^{2^i d} \equiv_n -1$ を満たす $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ が存在するような $s-1$ 以下の整数 i のうち最大のものをとる。すると、「n は合成数」という判定が得られないような a は、$a^d \equiv_n 1$ もしくはある $j = 0, 1, \ldots, i$ について $a^{2^j d} \equiv_n -1$ を満たすものである。このような a は、少なくとも $a^{2^i d} \equiv_n 1$ か $a^{2^i d} \equiv_n -1$ のどちらかを満たす。そこで、$A_1 = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid b^{2^i d} \equiv_n 1\}$、$A_{-1} = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times \mid b^{2^i d} \equiv_n -1\}$ と定義した上で、$A_1 \cup A_{-1}$ の元の個数が全体の $1/2$ 以下であることを示せば目標の性質が成り立つ。

上の議論により $A_{-1} \neq \emptyset$ であることに注意して、A_{-1} の元 b を一つ選ぶ。$f(b) = (b_1, \ldots, b_k)$ と書く。$b^{2^i d} \equiv_n -1$ なので $f(b^{2^i d}) = f(-1) = (-1, \ldots, -1)$ であり、したがって $(b_1, \ldots, b_k)^{2^i d} = ({b_1}^{2^i d}, \ldots, {b_k}^{2^i d}) = (-1, \ldots, -1)$ である。ここで、$f(c) = (b_1, 1, \ldots, 1)$ を満たす $c \in (\mathbb{Z}/n\mathbb{Z})^\times$ をとると、$a \in A_1$ のとき

$$f((ac)^{2^i d}) = f(a^{2^i d}) f(c^{2^i d}) = f(1) \cdot (b_1, 1, \ldots, 1)^{2^i d} = (-1, 1, \ldots, 1)$$

より $ac \notin A_1 \cup A_{-1}$ である（$k = 2$ であることに注意）。同様に、$a \in A_{-1}$ のとき

$$f((ac)^{2^i d}) = f(a^{2^i d}) f(c^{2^i d}) = f(-1) \cdot (b_1, 1, \ldots, 1)^{2^i d} = (1, -1, \ldots, -1)$$

より $ac \notin A_1 \cup A_{-1}$ である。こうして、$A_1 \cup A_{-1}$ の元 a と少なくとも同じ個数だけ $A_1 \cup A_{-1}$ 以外の元 ac が存在することがわかったので、

$$|A_1 \cup A_{-1}| \leq |(\mathbb{Z}/n\mathbb{Z})^\times|/2 \leq (n-1)/2$$

であり、「n は合成数」と判定されないような a が選ばれる確率は $1/2$ 以下である。よって主張が成り立つ。 □

ちなみに、ミラー・ラビン法では a の候補をランダムに選んでいますが、a の候補をランダムに選ぶ代わりに小さい値から順に試していくという変種も考えられます。実は、現時点では未解決である一般化されたリーマン予想（generalized Riemann hypothesis、GRH）を仮定すると、このミラー・ラビン法の変種において「n は合成数」と判定されるまでに試すべき a の個数がわりと少なくて済む（より詳しくは、n の二進法表示の桁数を 2 乗した数の定数倍以下の個数で済む）ことが知られています。ミラー・ラビン法の名前は二人の人物名にちなんだものですが、歴史的には、まず GRH を仮定した上記の結果が 1976 年に Miller によって得られ [2]、その結果を 1980 年に Rabin が（GRH を仮定しない）確率的アルゴリズムへと変形させた [3]、という経緯があります。

上記の方式はいずれも、合成数である入力値についてそれが合成数である「証拠」を（ある確率で）与えるというものです。これとは反対に、素数であることを保証する「証拠」について考えます。一例として、Pratt によって 1975 年に示された以下の結果 [4] を紹介します。

定理 3.2. 整数 $n > 2$ と整数 a について、以下の条件が成り立つとする：

1. $a^{n-1} \equiv_n 1$ が成り立つ。
2. p を $n-1$ の素因数とすると、常に $a^{(n-1)/p} \not\equiv_n 1$ である。

このとき n は素数である。

証明. n が合成数であると仮定して矛盾を導く。条件 1 より $a^{n-1} \equiv_n 1$ であるから $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ であり、オイラーの定理より $a^{\varphi(n)} \equiv_n 1$ となる。n は合成数なので $\varphi(n) < n-1$ であり、したがって n を法とする a の位数 $\mathrm{ord}(a)$ は $n-1$ の約数であり $\mathrm{ord}(a) < n-1$ を満たす。このことから、$n-1$ のある素因数 p について $\mathrm{ord}(a)$ は $(n-1)/p$ の約数でもある。すると $a^{(n-1)/p} \equiv_n 1$ となるが、これは条件 2 に矛盾する。よって主張が成り立つ。 □

定理 3.2 により、n が素数である「証拠」として、

[2] G. L. Miller: Riemann's Hypothesis and Tests for Primality. Journal of Computer and System Sciences, vol.13, no.3, pp.300–317 (1976). doi:10.1145/800116.803773

[3] M. O. Rabin: Probabilistic algorithm for testing primality. Journal of Number Theory, vol.12, no.1, pp.128–138 (1980). doi:10.1016/0022-314X(80)90084-0

[4] V. Pratt: Every prime has a succinct certificate. SIAM Journal on Computing, vol.4, pp.214–220 (1975)

- $n-1$ の素因数分解 $n-1 = {p_1}^{e_1} \cdots {p_k}^{e_k}$
- $p_1, \ldots, p_k$ たちが実際に素数である「証拠」
- $a^{n-1} \equiv_n 1$ および各 i について $a^{(n-1)/p_i} \not\equiv_n 1$ が成り立つ整数 a

を用いることができます。ただし、これは「証拠」が与えられていればその正しさを効率的に確認できるという話であり、上記のような「証拠」を実際に見つけるためには $n-1$ の素因数分解を行う必要があるため、一般の素数 n についてその「証拠」を効率的に見つけられるとは限らないことを注意しておきます。

4 素数であることの証明（2）

前の節で紹介したミラー・ラビン法（を充分な回数だけ繰り返す方法）は、与えられた整数が素数かどうかを効率的に判定できますが、ごく小さい確率で合成数を素数と誤判定してしまう可能性が残っています。このような誤判定の可能性を排除し、入力値が素数かどうかを常に正しく判定できる方法が、2002 年に Agrawal, Kayal, Saxena により発表されました（2004 年に論文誌で正式に公表されました [5]）。この方法は、考案者のイニシャルを取って、AKS アルゴリズムや AKS 素数判定法などと俗に呼ばれています。AKS 素数判定法は、入力値 n の桁数に関する多項式以下の実行手数を持つ確定的な（常に正しい結果を返す）素数判定法として初めてのもので、長年の未解決問題を解決した結果として大きな話題となりました。このように理論的には非常に重要な結果なのですが、実用上は n が大きくなると実行時間が大きくなりすぎるため、現在でも AKS 素数判定法ではなくミラー・ラビン法が実用的な（確率的）素数判定法として広く用いられています。

AKS 素数判定法（を、本質的な仕組みを変えずに少々書き換えたもの）を以下に記します。なお、ステップ 4 で $(X+a)^n \neq_{X^{r_0}-1,n} X^n + a$ という記法が使われていますが、これは「$\mathbb{Z}/n\mathbb{Z}$ の元を係数とする多項式として、両辺の差が多項式 $X^{r_0}-1$ で割り切れない」という意味です。

定義 4.1 (AKS 素数判定法)**.** 整数 $n > 1$ について以下の手順を考える。

1. n が a^k の形（$a > 0$ と $k \geq 2$ は整数）をしていれば「n は合成数」と判定して終了する。

2. $r = 2, 3, \ldots, n-1$ について以下を行う：

   (a) $\gcd(r, n) > 1$ であれば「n は合成数」と判定して終了する。

   (b) $i = 1, 2, \ldots, \lfloor (\log_2 n)^2 \rfloor$ のすべてについて $n^i \neq_r 1$ が成り立つならば、この r を r_0 としてループを終了する。

3. 先のループで r_0 が見つからなかったならば「n は素数」と判定して終了する。

[5] M. Agrawal, N. Kayal, N. Saxena: PRIMES Is in P. Annals of Mathematics, vol.160, pp.781–793 (2004)

4. $a = 1, 2, \ldots, \lfloor \sqrt{\varphi(r_0)} \log_2 n \rfloor$ の各々について、$(X+a)^n \not\equiv_{X^{r_0}-1,n} X^n + a$ ならば「n は合成数」と判定して終了する。

5. 「n は素数」と判定する。

以下では、このアルゴリズムの判定結果の正しさと必要な計算量について考察します。まず、いくつかの簡単な場合を考えます。

- ステップ 1 のように $n = a^k$ という形をしている n は合成数ですから、この場合には正しい判定結果となります。計算量理論のオーダー記法を用いると、このステップは計算量 $O((\log n)^3 \cdot poly(\log \log n))$ で実行可能であることが知られています。

- ステップ 2(a) について、$\gcd(r, n) > 1$ となった場合には、$r < n$ であることから $1 < \gcd(r, n) < n$ であり、この場合には確かに n は合成数なので正しい判定結果となります。ここの計算にはユークリッドの互除法を用いれば効率的に実行可能です。

- ステップ 3 について、まだアルゴリズムが終了していない上に「先のループで r_0 が見つからなかった」とすると、$r = 2, 3, \ldots, n-1$ のすべてについて $\gcd(r, n) = 1$ であったことになります。これは n が素数であることを意味するため、この場合には正しい判定結果となります。

- ステップ 4 について、二項定理により

  $$(X+a)^n = X^n + \binom{n}{1} aX^{n-1} + \binom{n}{2} a^2 X^{n-2} + \cdots + \binom{n}{n-1} a^{n-1} X + a^n$$

  です。もし n が素数ならば、途中の二項係数 $\binom{n}{1}, \ldots, \binom{n}{n-1}$ たちはすべて n の倍数であることが知られており、またフェルマーの小定理より $a^n \equiv_n a$ が成り立ちます。よってこの場合には、$\mathbb{Z}/n\mathbb{Z}$ 係数の多項式として $(X+a)^n = X^n + a$ ですから、特に $(X+a)^n \equiv_{X^{r_0}-1,n} X^n + a$ が成り立ちます。逆に、ある a について条件 $(X+a)^n \equiv_{X^{r_0}-1,n} X^n + a$ が成り立たない場合には n は素数ではありません。したがって、この場合には正しい判定結果となります。なお、一見すると上記の条件に n 次多項式が現れることから、条件の確認には n に比例する程度の計算量が必要そうに思えますが、実際には多項式のべき乗をバイナリ法で計算する過程で多項式 $X^{r_0} - 1$ で割った余

りに順次置き換えていけばよいので、r_0 次以下の多項式だけを扱えば済みます。そのため、r_0 が大きすぎない限りは、このステップの計算量もあまり大きくない範囲で収まります。また、ループの終了条件の判定に $\varphi(r_0)$ の計算が必要で、それには r_0 の素因数分解が必要となるように思われますが、後述する通り実際には r_0 はそこまで大きな値にはならないので、少なくとも理論的な観点では r_0 の素因数分解が障害となることはありません。ただ、ループの終了条件をもっと大きな値に取り替えても冗長になるだけで判定結果の正しさには影響しませんので、もし素因数分解を行いたくない場合には、$\varphi(r_0)$ をより大きな値 r_0 に取り替えても構いません。

残された（本質的に難しい）考慮すべきことは、ステップ 2 について r_0 がどの程度の範囲に見つかるかの解析と、ステップ 4 で「n は合成数」と判定されなかった場合に n が素数であることの証明です。

命題 4.1. $n > \lceil(\log_2 n)^5\rceil + 1$ と仮定すると、このアルゴリズムがステップ *1* で終了しなかった場合、$r \le \lceil(\log_2 n)^5\rceil$ の範囲の r について、ステップ *2(a)* で「n は合成数」と判定されるかステップ *2(b)* で r_0 が見つかるかのいずれかが起こる。

証明. $B = \lceil(\log_2 n)^5\rceil$ とおく。n が 2 以上 B 以下の約数（仮に d と書く）を持つ場合には、もし r_0 が見つからないとしても、r が d もしくはその約数となった段階でステップ 2(a) において「n は合成数」と判定される。よってこの場合には目標の性質が成り立つので、以降では n は 2 以上 B 以下の約数を持たないとする。この場合には、主張にある r の範囲においては、ステップ 2(a) の条件が満たされることはないことを注意しておく。

この範囲に r_0 が見つからないと仮定して矛盾を導く。このとき、$2 \le r \le B$ の各々について、r が $n^i - 1$ を割り切るような $i \le \lfloor(\log_2 n)^2\rfloor$ が存在する。よって、$P = \prod_{i=1}^{\lfloor(\log_2 n)^2\rfloor} (n^i - 1)$ とおくと、P は 2 から B までの整数の公倍数である。また、

$$P < \prod_{i=1}^{\lfloor(\log_2 n)^2\rfloor} n^{(\log_2 n)^2} \le n^{(\log_2 n)^4} = 2^{(\log_2 n)^5} \le 2^B$$

である。よって $\mathrm{lcm}(2,\ldots,B) \le P < 2^B$ となるが、一方で論文 [Nai][6] によると、整数 $m \ge 7$ について $\mathrm{lcm}(2,\ldots,m) \ge 2^B$ が成り立つ。今、仮定 $n > \lceil(\log_2 n)^5\rceil + 1$

[6] M. Nair: On Chebyshev-Type Inequalities for Primes. Amer. Math. Monthly, vol.89, pp.126–129 (1982)

より $n > 2$、したがって $B \geq \lceil (\log_2 3)^5 \rceil \geq (\log_2 2\sqrt{2})^5 = (3/2)^5 = 243/32 > 7$ であるので、これは矛盾である。よって主張が成り立つ。 □

アルゴリズムのステップ 2 は、見掛け上は n 個程度の r について実行される可能性があるように見えますが、実際には命題 4.1 より $r \leq \lceil (\log_2 n)^5 \rceil$ の範囲でしか実行されないことがわかります。

以下では、ステップ 4 で「n は合成数」と判定されなかった場合について考えます。r_0 の選び方より、n は $(\mathbb{Z}/r_0\mathbb{Z})^\times$ の要素でありその位数 $\mathrm{ord}(n)$ は $(\log_2 n)^2$ より大きいことがわかります。よって、n の素因数 p のいずれかは、$p \in (\mathbb{Z}/r_0\mathbb{Z})^\times$ かつ $\mathrm{ord}(p) > 1$ を満たします。この p を一つ固定しておきます。なお、ステップ 2(a) でアルゴリズムが終了しなかったことから、$p > r_0$ が成り立ちます。

ここで以下の（一時的な）用語を導入しておきます。

定義 4.2 (introspective)**.** 整数係数の多項式 $f(X)$ と整数 $m > 0$ について、m が $f(X)$ に関して **introspective** であるとは、$f(X)^m \equiv_{X^{r_0}-1,p} f(X^m)$ であることと定義する。

このとき以下の性質が成り立ちます。

補題 4.1. *1.* 正の整数 m と m' が多項式 $f(X)$ に関して *introspective* ならば、mm' も $f(X)$ に関して *introspective* である。

2. 正の整数 m が多項式 $f(X)$ と $g(X)$ の両方に関して *introspective* ならば、m は $f(X)g(X)$ に関しても *introspective* である。

証明. 主張 1 について、m が introspective であることから $f(X)^{mm'} \equiv_{X^{r_0}-1,p} f(X^m)^{m'}$ が成り立つ。また、m' が introspective であることから $f(X)^{m'} \equiv_{X^{r_0}-1,p} f(X^{m'})$ である。後者の式の X に X^m を代入することで、

$$f(X^m)^{m'} \equiv_{X^{mr_0}-1,p} f(X^{mm'})$$

となる。さらに、多項式 $X^{r_0} - 1$ は $X^{mr_0} - 1$ を割り切ることから、

$$f(X^m)^{m'} \equiv_{X^{r_0}-1,p} f(X^{mm'})$$

となり、以上をまとめると

$$f(X)^{mm'} \equiv_{X^{r_0}-1,p} f(X^{mm'})$$

となる。よって確かに mm' も $f(X)$ に関して introspective である。

主張 2 については、m が $f(X)$ および $g(X)$ に関して introspective であることから、

$$(f(X)g(X))^m = f(X)^m g(X)^m \equiv_{X^{r_0}-1,p} f(X^m)g(X^m)$$

となるので、m は確かに多項式 $f(X)g(X)$ に関しても introspective である。よって主張が成り立つ。 □

$\ell = \lfloor \sqrt{\varphi(r_0)} \log_2 n \rfloor$ とおくと、さらに以下の性質が成り立ちます。

補題 4.2. $1 \le a \le \ell$ のとき、$n, p, n/p$ はいずれも多項式 $X + a$ に関して *introspective* である。

証明. アルゴリズムがステップ 4 で終了していないという前提により、$(X + a)^n \equiv_{X^{r_0}-1,n} X^n + a$ である。さらに p は n の素因数なので、$(X + a)^n \equiv_{X^{r_0}-1,p} X^n + a$ が成り立つ。よって n は多項式 $X + a$ に関して introspective である。

p は素数なので、フェルマーの小定理より $(X + a)^p \equiv_p X^p + a$ であり、したがって $(X + a)^p \equiv_{X^{r_0}-1,p} X^p + a$ が成り立つ。よって p も多項式 $X + a$ に関して introspective である。

以降では n/p について考える。$c_i = \binom{n/p}{i} a^{n/p-i}$ とおくと、二項定理より $(X + a)^{n/p} = X^{n/p} + \sum_{i=0}^{n/p-1} c_i X^i$ である。前述の通り $(X + a)^p \equiv_{X^{r_0}-1,p} X^p + a$ なので、

$$(X + a)^n = ((X + a)^p)^{n/p} \equiv_{X^{r_0}-1,p} (X^p + a)^{n/p} = X^n + \sum_{i=0}^{n/p-1} c_i X^{pi}$$

となる。一方、前述の通り $(X + a)^n \equiv_{X^{r_0}-1,p} X^n + a$ である。よって

$$X^n + \sum_{i=0}^{n/p-1} c_i X^{pi} \equiv_{X^{r_0}-1,p} X^n + a$$

したがって

$$\sum_{i=0}^{n/p-1} c_i X^{pi} \equiv_{X^{r_0}-1,p} a$$

が成り立つ。これは、各 $0 \le j \le r_0 - 1$ について

$$\sum_{\substack{0 \le i < n/p \\ pi \bmod r_0 = j}} c_i \equiv_p \begin{cases} a & (j = 0 \text{ のとき}) \\ 0 & (j > 0 \text{ のとき}) \end{cases}$$

を意味する。ここで、$p \in (\mathbb{Z}/r_0\mathbb{Z})^\times$ より r_0 を法とする p の逆元が存在するので、それを p' とおくと、$pi \bmod r_0 = j$ は $i \bmod r_0 = p'j \bmod r_0$ と同値である。さらに、$j = 0$ と $p'j \bmod r_0 = 0$ が同値であるから、上の式より各 $0 \le j' \le r_0 - 1$ について

$$\sum_{\substack{0 \le i < n/p \\ i \bmod r_0 = j'}} c_i \equiv_p \begin{cases} a & (j' = 0 \text{ のとき}) \\ 0 & (j' > 0 \text{ のとき}) \end{cases}$$

が成り立つ。これより

$$(X + a)^{n/p} = X^{n/p} + \sum_{i=0}^{n/p-1} c_i X^i \equiv_{X^{r_0}-1,p} X^{n/p} + a$$

が成り立つので、n/p も多項式 $X + a$ に対して introspective である。よって主張が成り立つ。 □

$I = \{(n/p)^i p^j \mid i, j \in \mathbb{Z}_{\ge 0}\}$ および $P = \{\prod_{a=0}^{\ell} (X + a)^{e_a} \mid e_0, \ldots, e_\ell \in \mathbb{Z}_{\ge 0}\}$ と定義します。また、$G = \{m \bmod r_0 \mid m \in I\}$ と定義します。n と p はともに r_0 と互いに素なので、G は $(\mathbb{Z}/r_0\mathbb{Z})^\times$ の部分集合です。この G は定義よりモノイドでもあります。さらに、オイラーの定理より $g \in G$ について r_0 を法として $g^{\varphi(r_0)} = 1$ なので、g は G において可逆です。よって G は $(\mathbb{Z}/r_0\mathbb{Z})^\times$ の部分群です。さらに $n = (n/p) \cdot p \in I$ であり、前述の通り $\mathrm{ord}(n) > (\log_2 n)^2$ なので、$|G| > (\log_2 n)^2$ が成り立ちます。

整数 $d \ge 1$ について、**円分多項式** $\Phi_d(X)$ を漸化式

$$\Phi_1(X) = X - 1\,,\ \Phi_d(X) = \frac{X^d - 1}{\prod_{d' \mid d,\, d' \ne d} \Phi_{d'}(X)}$$

によって定義します。この $\Phi_d(X)$ は実際に多項式であり、その係数はすべて整数であることが知られています。以降の議論では、この多項式 $\Phi_d(X)$ を有限体 $\mathbb{F}_p$ 上の多項式と考えたときに成り立つ以下の性質を用います（これには少々の代数学の知識を必要とします）。

命題 4.2. 体 $\mathbb{F}_p$ 上の多項式として、円分多項式 $\Phi_{r_0}(X)$ を割り切る $\mathrm{ord}(p)$ 次の既約多項式 $h(X)$ が存在する。この $h(X)$ について $F = \mathbb{F}_p[X]/(h(X))$ と定めると、F は $\mathbb{F}_p$ の有限な拡大体であり、正整数 m_1, m_2 が $m_1 \not\equiv_{r_0} m_2$ を満たすならば F の元として $X^{m_1} \ne X^{m_2}$ が成り立つ。

証明. $\mathbb{F}_p$ の $\mathrm{ord}(p)$ 次拡大体の一つを K とおく。系 2.2 により $K^\times$ は巡回群である。x をその生成元とする。$|K^\times| = p^{\mathrm{ord}(p)} - 1$ であり、$\mathrm{ord}(p)$ の定義より $p^{\mathrm{ord}(p)} \equiv_{r_0} 1$ なので、r_0 は $|K^\times|$ の約数である。$y = x^{|K^\times|/r_0}$ とすると、y は r_0 乗して初めて 1 となる。つまり y は 1 の原始 r_0 乗根である。

$y^{r_0} = 1$ であるから y は多項式 $X^{r_0} - 1$ の根である。一方で、$d \mid r_0$ かつ $1 \leq d < r_0$ のとき、$\Phi_d(X)$ は $X^d - 1$ を割り切り、また y は 1 の原始 r_0 乗根であるから $y^d \neq 1$ であり、したがって y は $\Phi_d(X)$ の根ではない。このことから y は $\Phi_{r_0}(X)$ の根である。

y の $\mathbb{F}_p$ 上の最小多項式を $h(X)$ とおくと、$h(X)$ は既約多項式である。前述の通り y は $\Phi_{r_0}(X)$ の根であるから、$h(X)$ は $\Phi_{r_0}(X)$ を割り切る。また、y は $\mathbb{F}_p$ の $\mathrm{ord}(p)$ 次拡大体の元なので、$h(X)$ の次数は $\mathrm{ord}(p)$ 次以下である。一方で、もし $h(X)$ が $\mathrm{ord}(p)$ 次未満、たとえば d 次であるとすると、y は $\mathbb{F}_p$ のある d 次拡大体の元となる。その乗法群は $p^d - 1$ 個の元からなり、一方でその中で y が生成する部分群は r_0 個の元からなるので、ラグランジュの定理より $r_0 \mid p^d - 1$ すなわち $p^d \equiv_{r_0} 1$ となる。しかし、これは $d < \mathrm{ord}(p)$ という仮定と矛盾する。よって $h(X)$ は $\mathrm{ord}(p)$ 次多項式である。このことから $K = \mathbb{F}_p(y)$ が成り立つ。

体 $F = \mathbb{F}_p[X]/(h(X))$ について、対応 $X \mapsto y$ は F から K への $\mathbb{F}_p$ 上の同型写像を定める。特に、y と同様に $X \in F$ も 1 の原始 r_0 乗根である。したがって、正整数 m_1, m_2 が $m_1 \not\equiv_{r_0} m_2$ を満たすならば F において $X^{m_1} \neq X^{m_2}$ となる。よって主張が成り立つ。 □

多項式 $h(X)$ と有限体 F を命題 4.2 の通りに定めます。また、P の元を F の元とみなしてできる F の部分集合を $\mathcal{G}$ と定めます。ここで、$\mathrm{ord}(p) > 1$ となるように p を選んでいますので、$X, X+1, \ldots, X+\ell$ は F の元として 0 でなく、$\mathcal{G}$ は $F^\times$ の部分モノイドとなります。さらに、F が有限体であることから、このモノイド $\mathcal{G}$ は群となります。ここで下記が成り立ちます。

補題 4.3. $|\mathcal{G}| \geq \binom{|G|+\ell}{|G|-1}$ が成り立つ。

証明. まず、$f(X), g(X) \in P$ が $|G|$ 次未満でかつ $f(X) \not\equiv_p g(X)$ であるとき、F においても $f(X) \neq g(X)$ であることを示す。F において $f(X) = g(X)$ であると仮定して矛盾を導く。各 $m \in I$ について、F において $f(X)^m = g(X)^m$ である。一方、m は $p, n/p$ たちの積の形で表わせて、$f(X)$ と $g(X)$ はどちらも多項式 $X, X+1, \ldots, X+\ell$ たちの積の形で表わせるため、補題 4.2 と補題 4.1 より m は

$f(X)$ と $g(X)$ の両方に関して introspective である。したがって $f(X)^m \equiv_{X^{r_0}-1,p} f(X^m)$ かつ $g(X)^m \equiv_{X^{r_0}-1,p} g(X^m)$ である。さらに、命題 4.2 より $h(X)$ は $\mathbb{F}_p$ 上で $\Phi_{r_0}(X)$ を、したがって $X^{r_0}-1$ を割り切るので、$f(X)^m \equiv_{h(X),p} f(X^m)$ かつ $g(X)^m \equiv_{h(X),p} g(X^m)$ となり、したがって F において $f(X)^m = f(X^m)$ かつ $g(X)^m = g(X^m)$ となる。よって F において $f(X^m) = g(X^m)$ となる。すると、$Q(Y) = f(Y) - g(Y) \bmod p$ とおくとき、各 $m \in I$ について X^m は体 F における多項式 $Q(Y)$ の根となる。そして、命題 4.2 より、$m \bmod r_0$ の値が異なれば X^m は F において異なる元となるので、G の元 m ごとに X^m は F 上の多項式 $Q(Y)$ の異なる根となる。以上の議論から、多項式 $Q(Y)$ は少なくとも $|G|$ 個の異なる根を持つことになるが、一方で $f(Y)$ と $g(Y)$ が $|G|$ 次未満であり $f(Y) \neq_p g(Y)$ であることから、$Q(Y)$ も $|G|$ 次未満である。これは矛盾であるから、F において $f(X) \neq g(X)$ である。

$\ell = \lfloor \sqrt{\varphi(r_0)} \log_2 n \rfloor < \sqrt{r_0} \log_2 n$ であり、また $r_0 > \mathrm{ord}(n) > (\log_2 n)^2$ であるから $\sqrt{r_0} > \log_2 n$ である。よって $\ell < r_0$ であり、また前に示した通り $r_0 < p$ であるから、$\ell < p$ となり、したがって $X, X+1, \ldots, X+\ell$ たちは $\mathbb{F}_p$ 上ですべて異なる多項式である。このことから、$1, X, X+1, \ldots, X+\ell$ から重複を許して $|G|-1$ 個選んで掛け合わせたもの（これは全部で $\binom{(|G|-1)+(\ell+2-1)}{\ell+2-1} = \binom{|G|+\ell}{\ell+1} = \binom{|G|+\ell}{|G|-1}$ 個ある）たちは、すべて $\mathbb{F}_p$ 上で異なる $|G|$ 次未満の多項式となる。これと前段落の結果より $|\mathcal{G}| \geq \binom{|G|+\ell}{|G|-1}$ となる。よって主張が成り立つ。 □

補題 4.4. *n が p のべき乗の形でないならば、$|\mathcal{G}| \leq n^{\sqrt{|G|}}$ が成り立つ。*

証明. n が p のべき乗の形でないという前提より、$i, j \leq \lfloor \sqrt{|G|} \rfloor$ の各々について $(n/p)^i p^j$ たちはすべて異なる I の要素である。これらは $(\lfloor \sqrt{|G|} \rfloor + 1)^2 > (\sqrt{|G|})^2 = |G|$ 個あるので、抽き出し論法により、どれか二つは G の要素とみたときに一致する、すなわち r_0 を法として等しくなる。その I の二つの要素を $m_1 > m_2$ とおく。すると $m_1 \equiv_{r_0} m_2$ であるから $X^{m_1} \equiv_{X^{r_0}-1} X^{m_2}$ が成り立つ。

ここで $f(X) \in P$ とすると、補題 4.2 と補題 4.1 より $m_1, m_2 \in I$ はともに $f(X)$ に関して introspective であるから、

$$f(X)^{m_1} \equiv_{X^{r_0}-1,p} f(X^{m_1}) \equiv_{X^{r_0}-1,p} f(X^{m_2}) \equiv_{X^{r_0}-1,p} f(X)^{m_2}$$

が成り立ち、したがって（$h(X)$ が $X^{r_0}-1$ を割り切るため）体 F において $f(X)^{m_1} = f(X)^{m_2}$ が成り立つ。つまり、$f(X)$ を $\mathcal{G}$ の要素とみたものは F 上の多項式 $Y^{m_1} - Y^{m_2}$ の根である。このことから、$Y^{m_1} - Y^{m_2}$ は $\mathcal{G}$ のすべての要

素を根として持つ。この多項式の次数は $m_1 \leq (n/p)^{\lfloor\sqrt{|G|}\rfloor} p^{\lfloor\sqrt{|G|}\rfloor} = n^{\lfloor\sqrt{|G|}\rfloor}$ なので、$|\mathcal{G}| \leq n^{\lfloor\sqrt{|G|}\rfloor}$ が成り立つ。よって主張が成り立つ。 □

さて、n が p のべき乗の形でないと仮定して矛盾を導きます。上の補題たちより

$$n^{\lfloor\sqrt{|G|}\rfloor} \geq |\mathcal{G}| \geq \binom{|G|+\ell}{|G|-1}$$

が成り立ちます。また、前に示したように $|G| > (\log_2 n)^2$ なので $|G| > \sqrt{|G|}\log_2 n$、したがって $|G| - 1 \geq \lfloor\sqrt{|G|}\log_2 n\rfloor$ です。さらに、$|G| \leq |(\mathbb{Z}/r_0\mathbb{Z})^\times| = \varphi(r_0)$ より $\ell = \lfloor\sqrt{\varphi(r_0)}\log_2 n\rfloor \geq \lfloor\sqrt{|G|}\log_2 n\rfloor$ であり、また $|G| > (\log_2 n)^2$ より $\lfloor\sqrt{|G|}\log_2 n\rfloor > \lfloor(\log_2 n)^2\rfloor \geq 1$ です。これらより、

$$\begin{aligned}
\binom{|G|+\ell}{|G|-1} &\geq \binom{\ell+1+\lfloor\sqrt{|G|}\log_2 n\rfloor}{\lfloor\sqrt{|G|}\log_2 n\rfloor} \\
&\geq \binom{2\lfloor\sqrt{|G|}\log_2 n\rfloor+1}{\lfloor\sqrt{|G|}\log_2 n\rfloor} \\
&= \frac{2\lfloor\sqrt{|G|}\log_2 n\rfloor+1}{\lfloor\sqrt{|G|}\log_2 n\rfloor} \cdots \frac{\lfloor\sqrt{|G|}\log_2 n\rfloor+3}{2} \cdot (\lfloor\sqrt{|G|}\log_2 n\rfloor+2) \\
&> 2\cdots 2\cdot 4 = 2^{\lfloor\sqrt{|G|}\log_2 n\rfloor-1}\cdot 4 = 2^{\lfloor\sqrt{|G|}\log_2 n\rfloor+1} \\
&> 2^{\sqrt{|G|}\log_2 n} = n^{\sqrt{|G|}}
\end{aligned}$$

となります。以上を合わせると、

$$n^{\lfloor\sqrt{|G|}\rfloor} \geq |\mathcal{G}| \geq \binom{|G|+\ell}{|G|-1} > n^{\sqrt{|G|}}$$

となりますが、これは矛盾です。よって n は p のべき乗の形であるということになりますが、一方でステップ 1 でアルゴリズムが終了していないことから、このべき乗の指数は 2 以上ではありえないことがわかります。したがって $n = p$ となり、n が素数であることが示されました。以上の議論により、アルゴリズムがステップ 4 までで終了しなかったときに、ステップ 5 で「n は素数」と判定されるのは正しい判定結果であることがわかりました。よって、このアルゴリズムはすべての場合に正しい判定結果を返すことが示されました。

5 素数や素因数分解の応用

素因数分解など素数の性質が応用される代表的な分野の一つに暗号分野があります。その中でも特に、公開鍵暗号化と呼ばれる技術に素数が用いられる例が多くあります。公開鍵暗号化方式の定式化には細部が微妙に異なるいくつかの流儀がありますが、例えば以下のように定式化されます。

定義 5.1 (公開鍵暗号化方式). 以下に挙げるような三つのアルゴリズムの組のことを **公開鍵暗号化方式** と呼ぶ。

- **鍵生成アルゴリズム** $\mathsf{Gen}(1^\lambda)$ は、**セキュリティパラメータ** と呼ばれる正整数値のパラメータ λ を入力とし、**公開鍵** pk と **秘密鍵** sk の組を出力する確率的アルゴリズムである。ここで入力 λ は、「1 を λ 個並べた文字列」1^λ の形で与えられるものとする。また、公開鍵 pk は **平文空間** $\mathcal{M}$ と **暗号文空間** $\mathcal{C}$ と呼ばれる二つの（有限）集合の情報およびセキュリティパラメータの情報を含むものとし、秘密鍵 sk は公開鍵 pk の情報も含むものとする（が、以降の記述ではこれらの情報は割愛されることが多い）。

- **暗号化アルゴリズム** $\mathsf{Enc}(m, \mathsf{pk})$ は、**平文** $m \in \mathcal{M}$ と公開鍵 pk を入力とし、**暗号文** $c \in \mathcal{C}$ を出力する確率的アルゴリズムである。この出力された暗号文 c のことを $[[m]]$ と書き表すこともある。

- **復号アルゴリズム** $\mathsf{Dec}(c, \mathsf{sk})$ は、暗号文 $c \in \mathcal{C}$ と秘密鍵 sk を入力とし、平文 $m \in \mathcal{M}$ もしくは「復号失敗」を表す特別な記号 $\perp$ のいずれかを出力する非確率的アルゴリズムである。

そして、公開鍵暗号化方式の **正当性** を以下の条件と定義する：$(\mathsf{pk}, \mathsf{sk})$ を $\mathsf{Gen}(1^\lambda)$ の出力、$m \in \mathcal{M}$ を平文とすると、$\mathsf{Dec}(\mathsf{Enc}(m, \mathsf{pk}), \mathsf{sk}) = m$ が常に成り立つ。

以下では原則として、公開鍵暗号化方式のうち、上述の正当性を有するものだけを取り扱います。

歴史上最初に提案された公開鍵暗号化方式とされている RSA 暗号[7] は以下のような構造を持ちます。

[7] R. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, vol.21, no.2, pp.120–126 (1978)

- 鍵生成アルゴリズムは、λ ビットの二進数表示を持つ素数（以降では単に「λ ビットの」素数、などという）二つ $p \neq q$ をランダムに選び、その積 $N = pq$ を計算する。また、$\varphi(N)$ を法として可逆な整数 e を選び、$\varphi(N)$ を法とするその逆元 d を計算する。そして、(N, e) を公開鍵、d を秘密鍵とする。平文空間は $\mathcal{M} = (\mathbb{Z}/N\mathbb{Z})^\times$、暗号文空間は $\mathcal{C} = \mathcal{M}$ である。

- 暗号化アルゴリズムは、平文 $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ に対して、暗号文 $c = m^e \in (\mathbb{Z}/N\mathbb{Z})^\times$ を計算する。

- 復号アルゴリズムは、暗号文 $c \in (\mathbb{Z}/N\mathbb{Z})^\times$ に対して、平文 $m = c^d \in (\mathbb{Z}/N\mathbb{Z})^\times$ を計算する。

RSA 暗号の正当性は以下のように確かめられます。まず、d の選び方から $ed \equiv_{\varphi(N)} 1$ が成り立ちます。すると、オイラーの定理により、平文 $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ について $m^{ed-1} \equiv_N 1$ したがって $m^{ed} \equiv_N m$ が成り立ちます。平文 m の暗号文は $c = m^e$ なので、上の関係式は $c^d \equiv_N m$ となり、これは m の暗号文の復号結果が m と一致することを意味しています。

一方、RSA 暗号の安全性について考えます。公開鍵暗号化方式については、少なくとも、「暗号文 $c = [[m]]$ と公開鍵 pk が与えられた状態で、もとの平文 m を見つけることが充分に難しい」という条件が満たされる必要があります。特に、暗号文と公開鍵から秘密鍵を簡単に計算できてしまうと、盗聴者（攻撃者）はそうして得た秘密鍵を用いて自分自身で暗号文を復号することによりもとの平文を知ることができますので、暗号文と公開鍵から秘密鍵を計算することが充分に難しい必要があります。この原則を RSA 暗号に適用してみましょう。RSA 暗号の公開鍵には合成数 N が含まれていますが、もしこの N を素因数分解して素数 p と q を得ることができたとすると、$\varphi(N) = (p-1)(q-1)$ の値も計算でき、公開鍵に含まれる e と先ほど計算した $\varphi(N)$ にユークリッドの互除法を用いることで、$\varphi(N)$ を法とする e の逆数として定義されていた秘密鍵 d を簡単に計算できてしまいます。したがって、RSA 暗号においては、素因数分解を実際に計算するのが充分に難しくなるぐらい巨大な合成数 N を公開鍵（の一部）として用いる必要があります。ここで、どのくらい大きな合成数であれば素因数分解が現実的に困難であるかを知るためには、どれくらい効率的な素因数分解の方法が存在するかを調べる必要があります。こうした理由から、素因数分解の効率的なアルゴリズムに関する研究が、暗号分野における一つの研究

テーマとして確立しています。

なお、上記の内容はあくまで「RSA 暗号が安全であるためには素因数分解が困難でなければならない」ということを言っているだけであり、「素因数分解が困難であれば RSA 暗号は安全である」（すなわち、RSA 暗号の安全性と素因数分解の困難性が「等価」である）とは言っていないことを注意しておきます。実際、RSA 暗号の暗号化アルゴリズムは確率的でないため、もし実際のシステム上で扱われる平文の候補が限られる場合、攻撃者は自分が手に入れた暗号文 c と、平文の候補 m' を自分で暗号化した結果 c' とを一つ一つ照合することで、どの m' が c に対応する平文であるかを見抜くことができてしまいます。このような事態を防ぐために、実用的な公開鍵暗号化方式の暗号化アルゴリズムは確率的である必要があります。実は、現在世の中で実用化されている公開鍵暗号化方式のうち「RSA 暗号」と呼ばれているものは、上述した初期版の RSA 暗号に変更を加えてこうした欠点を解消した改良版であり、良く知られた上記の構成とは異なります。しかし、こうした改良版 RSA 暗号についてもやはり、その安全性と素因数分解の困難性が完全に等価であるかどうかは（ほぼ等価であろうと予想する暗号学者が多いと思いますが、厳密な意味では）未だ不明です。

確率的な暗号化アルゴリズムを持つ公開鍵暗号化方式として初めて提案されたのが Goldwasser–Micali 暗号 [8] と呼ばれる方式です。その構成は以下のようになります。

- 鍵生成アルゴリズムは、λ ビットの素数 $p \neq q$ をランダムに選び、その積 $N = pq$ を計算する。また、N を法として可逆な整数 x で、$\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$ を満たすものを選ぶ。そして、(N, x) を公開鍵、(p, q) を秘密鍵とする。平文空間は $\mathcal{M} = \mathbb{F}_2$、暗号文空間は $\mathcal{C} = (\mathbb{Z}/N\mathbb{Z})^\times$ である。

- 暗号化アルゴリズムは、平文 $m \in \mathbb{F}_2$ に対して、m を自然に整数 0 または 1 とみなした上で、$(\mathbb{Z}/N\mathbb{Z})^\times$ のランダムな元 y を選び、暗号文 $c = y^2 x^m \in (\mathbb{Z}/N\mathbb{Z})^\times$ を計算する。

- 復号アルゴリズムは、暗号文 $c \in (\mathbb{Z}/N\mathbb{Z})^\times$ に対して、平文 m を、$\left(\frac{c}{p}\right) = 1$

[8] S. Goldwasser, S. Micali. Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information. In: Proceedings of STOC 1982, pp.365–377 (1982)

ならば $m = 0$、$\left(\frac{c}{p}\right) = -1$ ならば $m = 1$ と計算する。

Goldwasser–Micali 暗号の正当性は、x と y を上の構成の通りとするとき、命題 2.5 より

$$\left(\frac{c}{p}\right) = \left(\frac{y}{p}\right)^2 \left(\frac{x}{p}\right)^m = (-1)^m = \begin{cases} 1 & (m = 0 \text{ のとき}) \\ -1 & (m = 1 \text{ のとき}) \end{cases}$$

となることにより確かめられます。一方、安全性については、今度は暗号化アルゴリズムが確率的であるため、RSA 暗号の場合に考えたような「攻撃者が自分で平文の候補を暗号化して結果を照合する」という単純な攻撃は通用しません。また、詳細は割愛しますが、この方式が「暗号文と公開鍵を入手しても、対応する平文について何の情報も得られない」という意味合いの安全性（英語では “semantic security”、日本語では「強秘匿性」などと呼ばれます）を持つことと、$\left(\frac{a}{N}\right) = 1$ を満たす a についてそれが N を法とする平方剰余であるかどうか判定することの困難性が等価であることが知られています。なお、後者の問題が実際に困難であるためには、N の素因数分解が困難である必要がありますが、それだけで充分であるかどうかは知られていません。

Goldwasser–Micali 暗号は、上述した正当性と安全性に加えて、「加法準同型性」と呼ばれる特殊な性質を備えています。これはどのような性質かというと、平文 m, m' の（同じ公開鍵による）暗号文 c, c' がそれぞれ与えられた状況で、暗号文どうしを $(\mathbb{Z}/N\mathbb{Z})^\times$ の元として掛け算すると、その結果 cc' が平文 $m + m'$ に対する暗号文になる、というものです。つまり、暗号化された平文たちについて、暗号文の状態のままでそれらの和を計算できるということです。実際にこの性質が成り立つことは、$c = y^2 x^m$ および $c' = y'^2 x^{m'}$ としたとき、

$$cc' = (yy')^2 x^{m+m'}$$

であることからわかります（$m = m' = 1$ のときは、上の式の右辺は $(yy'x)^2 x^0$ と書き直せることに注意してください）。

Goldwasser–Micali 暗号は加法準同型性という便利な性質を持っているのですが、平文として 0 または 1 の 1 ビット入力しか扱えないという問題点があります。この点について、もっと大きなサイズの平文も扱える加法準同型暗号（加法準同型性を持つ公開鍵暗号化方式のこと）の代表例の一つとして、Paillier 暗

号[9] が知られています。その構成は以下のようになります。

- 鍵生成アルゴリズムは、λ ビットの素数 $p \neq q$ をランダムに選び、その積 $N = pq$ を計算する。また、$p-1$ と $q-1$ の最小公倍数を μ とする。そして、N を公開鍵、μ を秘密鍵とする。平文空間は $\mathcal{M} = \mathbb{Z}/N\mathbb{Z}$、暗号文空間は $\mathcal{C} = (\mathbb{Z}/N^2\mathbb{Z})^\times$ である。

- 暗号化アルゴリズムは、平文 $m \in \mathbb{Z}/N\mathbb{Z}$ に対して、m を自然に 0 から $N-1$ までの整数とみなした上で、N を法として可逆な 1 から $N-1$ までの整数 r をランダムに選び、暗号文 $c = (1+N)^m r^N \in (\mathbb{Z}/N^2\mathbb{Z})^\times$ を計算する。

- 復号アルゴリズムは、暗号文 $c \in (\mathbb{Z}/N^2\mathbb{Z})^\times$ に対して、まず $c^\mu \in (\mathbb{Z}/N^2\mathbb{Z})^\times$ を計算する。ここで、c が正しく作られた暗号文であれば、c^μ を 0 から N^2-1 までの整数と自然にみなしたときに、$c^\mu - 1$ は N の倍数となる（後述）。そこで、$c^\mu - 1$ を N で割った商（は 0 から $N-1$ までの整数なので、これを $\mathbb{Z}/N\mathbb{Z}$ の元とみなしたもの）を計算し、それに $\mathbb{Z}/N\mathbb{Z}$ における μ の逆元を掛けたものを出力とする。

Paillier 暗号の正当性を確認するには、中国式剰余定理により

$$(\mathbb{Z}/N^2\mathbb{Z})^\times \simeq (\mathbb{Z}/p^2\mathbb{Z})^\times \times (\mathbb{Z}/q^2\mathbb{Z})^\times$$

であることを利用します。オイラーの定理と $\varphi(p^2) = p(p-1)$ より、$(\mathbb{Z}/p^2\mathbb{Z})^\times$ の元はどれも $p(p-1)$ 乗すると単位元となります。同様に、$\varphi(q^2) = q(q-1)$ より、$(\mathbb{Z}/q^2\mathbb{Z})^\times$ の元はどれも $q(q-1)$ 乗すると単位元となります。これらの性質と、μ が $p-1$ と $q-1$ の公倍数であることより、$(\mathbb{Z}/N^2\mathbb{Z})^\times$ の元はどれも $pq\mu = N\mu$ 乗すると単位元となります。すると、暗号文 $c = (1+N)^m r^N$ について、$r^{N\mu} \equiv_{N^2} 1$ となるので、$c^\mu \equiv_{N^2} (1+N)^{m\mu}$ となります。この右辺について、二項定理より

$$(1+N)^{m\mu} = 1 + (m\mu)N + \frac{(m\mu)(m\mu-1)}{2}N^2 + \cdots + N^{m\mu} \equiv_{N^2} 1 + (m\mu)N$$

が成り立つため、$c^\mu \equiv_{N^2} 1 + (m\mu)N$ となり、$c^\mu - 1$ は確かに N の倍数となります。そして、$c^\mu - 1$ を N で割った値は $m\mu \in \mathbb{Z}/N\mathbb{Z}$ となるため、それに μ の逆元を掛けることで確かにもとの平文 $m \in \mathbb{Z}/N\mathbb{Z}$ が得られます。

[9] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: Proceedings of EUROCRYPT 1999, pp.223–238 (1999)

さらに、前述の通り Paillier 暗号は加法準同型性を備えています。実際、暗号文 $c = (1+N)^m r^N$ と $c' = (1+N)^{m'} r'^N$ について、暗号文どうしを掛け合わせると

$$cc' = (1+N)^{m+m'}(rr')^N$$

となり、これは確かに平文の和 $m + m'$ に対する暗号文となっています。

なお、Paillier 暗号の安全性についても、詳細は割愛しますが、その強秘匿性が、ある種の計算問題の困難性と等価であることが知られています。そして、後者の計算問題が困難であるためには、N の素因数分解が困難である必要がありますが、それだけで充分であるかどうかは知られていません。

6 素因数分解アルゴリズム（1）

前節で紹介したように、ある種の暗号技術が安全であるためには、そこで用いられている合成数を素因数分解する計算が現実的に不可能なほど困難である必要があります。このような理由から、整数の素因数分解をどのくらい効率的に行えるかを調べることが重要です。

まず、ある種の特殊な整数に関してその素因数分解を効率的に行う方法の一つである、Pollard の $p-1$ 法[10] を紹介します。N をこれから素因数分解したい整数とします。説明の簡略化のために、N は素数のべき乗の形ではないものとします。Pollard の $p-1$ 法（の最も基本的な形）は以下のように構成されます。

1. 1 から $N-1$ までの整数 a をランダムに選び、$\gcd(a,N)$ を計算する。もし $\gcd(a,N)>1$ であれば、$\gcd(a,N)$ は N の非自明な約数（つまり、1 でも N 自身でもない約数）となるので、$\gcd(a,N)$ を出力して終了する。

2. 整数 M をある基準に従って選び（後述）、$\gcd(a^M-1,N)$ を計算する。もし $1<\gcd(a^M-1,N)<N$ であれば、$\gcd(a^M-1,N)$ は N の非自明な約数となるので、$\gcd(a^M-1,N)$ を出力して終了する。それ以外の場合には「失敗」として終了する（あるいは、a や M を変更して手順をやり直す）。

Pollard の $p-1$ 法は、すべての入力 N についてその約数を効率的に見つけられるわけではありません。どのような N についてこの方法が成功するかを考える際に以下の補題が役立ちます。

補題 6.1. 上記の手順について、p を N の素因数の一つとする。もし M が $p-1$ の倍数であれば $p \mid \gcd(a^M-1,N)$ が成り立つ。

証明. フェルマーの小定理より $a^{p-1} \equiv_p 1$ であり、前提より M は $p-1$ の倍数なので、$a^M \equiv_p 1$ が成り立つ。よって a^M-1 は p の倍数であり、また前提より N も p の倍数であるから、$p \mid \gcd(a^M-1,N)$ が確かに成り立つ。 □

さて、上の手順において、N のある素因数 p について $p-1$ が M の約数となっていれば、補題 6.1 により少なくとも $\gcd(a^M-1,N)>1$ であることが保証されます。このとき、もし N の素因数 q のすべてについて $q-1$ が M の約数と

[10] J. M. Pollard. Theorems on Factorization and Primality Testing. Proc. Cambridge Phil. Soc., vol.76, pp.521–528 (1974)

なってしまうと困るのですが、幸いなことに（M をあまりにも大きく設定しすぎない限りは）このような状況が起きる可能性は充分に小さいと期待できます。すると、ランダムに選んだ a について、充分に高い確率で $\gcd(a^M - 1, N) < N$ も成り立ち、上の手順で N の非自明な約数が得られることになります。

あとは、N のある素因数 p について $p-1$ が M の約数となっているような M を選べばよいのですが、N の素因数が何であるかは前もってわかっていないため、百発百中で適切な M を選ぶことはできません。そこで、色々な入力 N について、$p-1$ が M の約数となる可能性がなるべく高くなるように M を選ぶことを考えます。そのためには、M としてなるべくたくさんの素数の積を用いるのがよさそうです。その方が M の約数の可能性が多くなるからです。そして、M の大きさをおおよそ一定に揃える場合、個々の素数をなるべく小さくした方が、M に含められる素因数の個数を増やすことができます。例えば、ある数 B を決めて、M を B 以下の素数すべての積やそのべき乗の形にしたり、$M = B!$ としたりすることが考えられます。このような M について、$p-1$ が M の約数となるとき、$p-1$ は比較的小さな素数のみを素因数に持つことになります。このように、素因数がどれも比較的小さい（「小さい」の厳密な定義は脇において）整数のことを “smooth” な整数と呼ぶことがあります。つまり、Pollard の $p-1$ 方法は、$p-1$ が smooth であるような N の素因数 p が存在するときに N の約数を高い確率で効率的に見つけることができます。したがって逆に、前節で紹介したような暗号技術において合成数を用いる際には、その素因数 p について $p-1$ が smooth な数にならないよう鍵の選び方に注意する必要があります。

例 6.1. $M = 10! = 3628800$ とします。まず、$N = 1331909$ とし、$a = 2$ について Pollard の $p-1$ 法の手順を試してみます。N を法とする $a^M = 2^M$ の計算にはバイナリ法を用います。今、$M = (11011101011111100000000)_2$ なので、バイ

ナリ法による $2^M \bmod N$ の計算は、

$2 \overset{2\text{乗}}{\mapsto} 4 \overset{2\text{倍}}{\mapsto} 8 \overset{2\text{乗}}{\mapsto} 64 \overset{2\text{乗}}{\mapsto} 4096 \overset{2\text{倍}}{\mapsto} 8192 \overset{2\text{乗}}{\mapsto} 67108864 \equiv_{1331909} 513414 \overset{2\text{倍}}{\mapsto} 1026828$
$\overset{2\text{乗}}{\mapsto} 1054375741584 \equiv_{1331909} 615641 \overset{2\text{倍}}{\mapsto} 1231282$
$\overset{2\text{乗}}{\mapsto} 1516055363524 \equiv_{1331909} 620911 \overset{2\text{乗}}{\mapsto} 385530469921 \equiv_{1331909} 86508 \overset{2\text{倍}}{\mapsto} 173016$
$\overset{2\text{乗}}{\mapsto} 29934536256 \equiv_{1331909} 1213390 \overset{2\text{乗}}{\mapsto} 1472315292100 \equiv_{1331909} 441047 \overset{2\text{倍}}{\mapsto} 882094$
$\overset{2\text{乗}}{\mapsto} 778089824836 \equiv_{1331909} 574217 \overset{2\text{倍}}{\mapsto} 1148434$
$\overset{2\text{乗}}{\mapsto} 1318900652356 \equiv_{1331909} 407559 \overset{2\text{倍}}{\mapsto} 815118$
$\overset{2\text{乗}}{\mapsto} 664417353924 \equiv_{1331909} 1208819 \overset{2\text{倍}}{\mapsto} 2417638 \equiv_{1331909} 1085729$
$\overset{2\text{乗}}{\mapsto} 1178807461441 \equiv_{1331909} 69082 \overset{2\text{倍}}{\mapsto} 138164 \overset{2\text{乗}}{\mapsto} 19089290896 \equiv_{1331909} 371108$
$\overset{2\text{乗}}{\mapsto} 137721147664 \equiv_{1331909} 425155 \overset{2\text{乗}}{\mapsto} 180756774025 \equiv_{1331909} 739817$
$\overset{2\text{乗}}{\mapsto} 547329193489 \equiv_{1331909} 1168574 \overset{2\text{乗}}{\mapsto} 1365565193476 \equiv_{1331909} 184955$
$\overset{2\text{乗}}{\mapsto} 34208352025 \equiv_{1331909} 933178 \overset{2\text{乗}}{\mapsto} 870821179684 \equiv_{1331909} 428758$
$\overset{2\text{乗}}{\mapsto} 183833422564 \equiv_{1331909} 678566$

となり、$a^M \equiv_N 678566$ したがって $a^M - 1 \equiv_N 678565$ となります。そして、ユークリッドの互除法により $\gcd(a^M - 1, N)$ を求めると、その過程は

$$(1331909, 678565) \mapsto (678565, 653344) \mapsto (653344, 25221) \mapsto (25221, 22819)$$
$$\mapsto (22819, 2402) \mapsto (2402, 1201) \mapsto (1201, 0)$$

となり、$\gcd(a^M - 1, N) = 1201$ が $N = 1331909$ の約数として得られます。実際、$N = 1109 \times 1201$ です。（ここまでの計算を手計算で行うのは無謀でしょうが、関数電卓を用いて少し頑張れば計算できる規模です。）Pollard の $p - 1$ 法がこの場合に成功したのは、$p = 1201$ とすると $p - 1 = 1200 \mid M = 10!$ であるためです。

次に、$N = 1356841$ として、上と同じ M と a についてこの手順を試してみま

す。バイナリ法による $2^M \bmod N$ の計算は、

$$2 \overset{2\text{乗}}{\mapsto} 4 \overset{2\text{倍}}{\mapsto} 8 \overset{2\text{乗}}{\mapsto} 64 \overset{2\text{乗}}{\mapsto} 4096 \overset{2\text{倍}}{\mapsto} 8192 \overset{2\text{乗}}{\mapsto} 67108864 \equiv_{1356841} 623655 \overset{2\text{倍}}{\mapsto} 1247310$$
$$\overset{2\text{乗}}{\mapsto} 1555782236100 \equiv_{1356841} 1208680 \overset{2\text{倍}}{\mapsto} 2417360 \equiv_{1356841} 1060519$$
$$\overset{2\text{乗}}{\mapsto} 1124700549361 \equiv_{1356841} 119210 \overset{2\text{乗}}{\mapsto} 14211024100 \equiv_{1356841} 828307$$
$$\overset{2\text{倍}}{\mapsto} 1656614 \equiv_{1356841} 299773 \overset{2\text{乗}}{\mapsto} 89863851529 \equiv_{1356841} 272099$$
$$\overset{2\text{乗}}{\mapsto} 74037865801 \equiv_{1356841} 479795 \overset{2\text{倍}}{\mapsto} 959590 \overset{2\text{乗}}{\mapsto} 920812968100 \equiv_{1356841} 964496$$
$$\overset{2\text{倍}}{\mapsto} 1928992 \equiv_{1356841} 572151 \overset{2\text{乗}}{\mapsto} 327356766801 \equiv_{1356841} 1236618$$
$$\overset{2\text{倍}}{\mapsto} 2473236 \equiv_{1356841} 1116395 \overset{2\text{乗}}{\mapsto} 1246337796025 \equiv_{1356841} 640747 \overset{2\text{倍}}{\mapsto} 1281494$$
$$\overset{2\text{乗}}{\mapsto} 1642226872036 \equiv_{1356841} 147665 \overset{2\text{倍}}{\mapsto} 295330 \overset{2\text{乗}}{\mapsto} 87219808900 \equiv_{1356841} 712579$$
$$\overset{2\text{乗}}{\mapsto} 507768831241 \equiv_{1356841} 937493 \overset{2\text{乗}}{\mapsto} 878893125049 \equiv_{1356841} 724140$$
$$\overset{2\text{乗}}{\mapsto} 524378739600 \equiv_{1356841} 398330 \overset{2\text{乗}}{\mapsto} 158666788900 \equiv_{1356841} 516042$$
$$\overset{2\text{乗}}{\mapsto} 266299345764 \equiv_{1356841} 303740 \overset{2\text{乗}}{\mapsto} 92257987600 \equiv_{1356841} 940646$$
$$\overset{2\text{乗}}{\mapsto} 884814897316 \equiv_{1356841} 1242283$$

となり、$a^M \equiv_N 1242283$ したがって $a^M - 1 \equiv_N 1242282$ となります。そして、ユークリッドの互除法により $\gcd(a^M - 1, N)$ を求めると、その過程は

$$(1356841, 1242282) \mapsto (1242282, 114559) \mapsto (114559, 96692) \mapsto (96692, 17867)$$
$$\mapsto (17867, 7357) \mapsto (7357, 3153) \mapsto (3153, 1051) \mapsto (1051, 0)$$

となり、$\gcd(a^M - 1, N) = 1051$ が $N = 1356841$ の約数として得られます。実際、$N = 1051 * 1291$ です。Pollard の $p-1$ 法がこの場合に成功したのは、$p = 1051$ とすると $p - 1 = 1050 \mid M = 10!$ であるためです。このように、同じ M（と a）を用いて複数の合成数 N を素因数分解し得るのが Pollard の $p-1$ 法の利点です。

7　素因数分解アルゴリズム（２）

前節で紹介した素因数分解アルゴリズムである Pollard の $p-1$ 法は、$p-1$ が smooth になるような素因数 p を持つ合成数 N に有効ですが、そのような素因数を持たないような一般の合成数には効果が薄いという欠点があります。Pollard の $p-1$ 法の基本的なアイデアを踏襲しつつこの欠点を解消した素因数分解アルゴリズムとして、楕円曲線法 [11] と呼ばれるアルゴリズムが知られています。この節ではこの楕円曲線法を紹介します。

楕円曲線法は、その名称の通り、楕円曲線という特殊な数学的対象を利用するアルゴリズムです。そこで、まずは楕円曲線について説明します。以下では、K を体とし、K の標数は 2 でも 3 でもないと仮定します（「標数」の定義は割愛しますが、この仮定は、K において $1+1\neq 0$ かつ $1+1+1\neq 0$ であるという意味です）。

定義 7.1 (楕円曲線)**.** $A, B\in K$ を、条件 $-16(4A^3+27B^2)\neq 0$ を満たす元とする。このとき、方程式

$$E\colon y^2=x^3+Ax+B$$

によって定まる図形を（体 K 上の）**楕円曲線** と呼ぶ。

例 7.1. $K=\mathbb{F}_{11}$ とし、$A=3$、$B=2$ とします。このとき体 K において $-16(4A^3+27B^2)=-16\cdot 7\neq 0$ なので、方程式 $E\colon y^2=x^3+3x+2$ は K 上の一つの楕円曲線を定めます。

ある体の上の楕円曲線 E が与えられたとき、その曲線上の特別な点たちに着目します。

定義 7.2 (楕円曲線の有理点)**.** $E\colon y^2=x^3+Ax+B$ を体 K 上の楕円曲線とする。このとき、方程式 E の解となる K の元の組 (a,b)、および **無限遠点** と呼ばれる特別な元 O のことを、楕円曲線 E の K 上の **有理点**（あるいは K-有理点）と呼ぶ。そして、E の K 上の有理点すべてからなる集合を $E(K)$ と書き、E の（K 上の）**有理点群** あるいは Mordell–Weil 群（モーデル・ヴェイユ群）と呼ぶ。すなわち、

$$E(K)=\{(a,b)\in K^2 \mid b^2=a^3+Aa+B\}\cup\{O\}$$

[11] H. W. Lenstra Jr. Factoring Integers with Elliptic Curves. Annals of Mathematics, vol.126, no.3, pp.649–673 (1987)

である。

例 7.2. 例 7.1 と同じ楕円曲線 E について、各 $a \in K = \mathbb{F}_{11}$ ごとに E の定義式の右辺を（体 K の中で）計算すると、表 1 の 2 段目のようになります。その各々について、b^2 がその値と一致する $b \in K$ は表の 3 段目のようになります。したがって、$E(K)$ はこれら 12 個の (a, b) と無限遠点 O を合わせた 13 個の有理点からなります。

表 1: 例 7.1 の楕円曲線の有理点 (a, b)

a	0	1	2	3	4	5	6	7	8	9	10
a^3+3a+2	2	6	5	5	1	10	5	3	10	10	9
b	—	—	$4, 7$	$4, 7$	$1, 10$	—	$4, 7$	$5, 6$	—	—	$3, 8$

集合 $E(K)$ が有理点「群」と呼ばれている理由は、この集合の元たちの間にある方法で「足し算」を定義できて、$E(K)$ が（可換な）群の構造を持つからです。その定義は以下の通りです。

定義 7.3 (楕円曲線上の加法)**.** E を体 K 上の楕円曲線とする。P と Q を E の K-有理点とする。このとき、$P + Q \in E(K)$ を以下のように定める。

- $P = O$ のときは $P + Q = Q$ と定める。
- $Q = O$ のときは $P + Q = P$ と定める。
- $P, Q \neq O$、$P = (a, b)$、$Q = (a, -b)$ という形のときは、$P + Q = O$ と定める。
- $P, Q \neq O$、$P = (a_1, b_1)$、$Q = (a_2, b_2)$、$a_1 \neq a_2$ という形のときは、$\lambda = \dfrac{b_2 - b_1}{a_2 - a_1}$ とおき、$P + Q = (a_3, b_3)$ を
$$a_3 = \lambda^2 - a_1 - a_2\,,\ b_3 = -\lambda(a_3 - a_1) - b_1$$
で定める。
- $P, Q \neq O$、$P = Q = (a, b)$、$b \neq 0$ という形のときは、$\mu = \dfrac{3a^2 + A}{2b}$ とおき、$P + Q = (a', b')$ を
$$a' = \mu^2 - 2a\,,\ b' = -\mu(a' - a) - b$$
で定める。

幾何学的な観点では、無限遠点以外の有理点 P, Q について、$P \neq Q$ のときには P と Q を通る直線、$P = Q$ のときには点 P における楕円曲線 E の接線を考えて、その直線と E との交点のうち P と Q 以外の点を取り、その点を x 軸に関して対称な点へと移して得られる点が $P + Q$ となります。ただし、y 軸と平行な直線と楕円曲線 E は無限遠点で交わると解釈し、また無限遠点を x 軸に関して対称な点へと移した結果もまた無限遠点になると解釈しています。この解釈によれば、$P + Q$ もまた楕円曲線 E の有理点であり、可換性 $P + Q = Q + P$ が成り立ちます（これらの性質を定義より直接確かめることもできます)。また、定義より $O + P = O$ かつ $P + O = O$ なので、無限遠点 O はこの演算 $+$ に関する単位元として振る舞います。さらに、この演算 $+$ については以下の性質が成り立ちます。

定理 7.1. 上で定義した楕円曲線 E の有理点群 $E(K)$ 上の演算 $+$ は結合法則 $(P + Q) + R = P + (Q + R)$ を満たす。したがって $E(K)$ は O を単位元とする可換群をなす。

定理 7.1 は、加法 $+$ の定義に基づいた直接計算で証明することができますが、あまりにも計算が煩雑になるためここでは証明を割愛します。上のように定義した演算 $+$ が結合法則を満たすという事実はとても不思議なことと感じられるでしょうが、実は複素解析学の知見を用いると、$E(K)$ がこのような形の演算によって群をなすことをより自然な形で説明付けることが可能です。詳細は割愛しますが、例えば光成滋生著『クラウドを支えるこれからの暗号技術』（秀和システム）の 17 章などにその解説があります。

例 7.3. 例 7.1 の楕円曲線 $E\colon y^2 = x^3 + 3x + 2$（$K = \mathbb{F}_{11}$）の K-有理点は例 7.2 で計算した通りです。例えば、有理点 $P = (2, 4)$、$Q = (3, 4)$、$R = (4, 1)$ について演算結果を計算してみます。

$(P + Q) + R$ について、まず、K において $\dfrac{4-4}{3-2} = 0$ なので、$P + Q = (6, 7)$ です。次に、K において $\dfrac{1-7}{4-6} = 3$ なので、$(P + Q) + R = (10, 3)$ です。

一方、$P + (Q + R)$ について、まず、K において $\dfrac{1-4}{4-3} = 8$ なので、$Q + R = (2, 4) = P$ です。次に、K において $\dfrac{3 \cdot 2^2 + 3}{2 \cdot 4} = 6$ なので、$P + (Q + R) = (10, 3)$ です。以上より、これらの点について確かに $(P + Q) + R = P + (Q + R)$ が成り立っています。

楕円曲線法では、こうした楕円曲線の有理点群の構造を利用して整数の素因数分解を行います。説明の簡略化のために、合成数 N は二つの異なる素数 p と q の積 $N = pq$ であるとし、$p > 3$ かつ $q > 3$ であるとします。この N を素因数分解するために、整数係数の方程式 $E\colon y^2 = x^3 + Ax + B$ と整数の組 $P = (a, b)$ で、$\gcd(-16(4A^3 + 27B^2), N) = 1$ かつ $b^2 \equiv_N a^3 + Aa + B$ を満たすものが与えられているとします。（実際の手順では、まず (a, b) を選び、続いて条件を満たす E を選ぶ、という順序で進められます。）このとき、E の係数を p および q を法として考えることで、$\mathbb{F}_p$ 上および $\mathbb{F}_q$ 上の楕円曲線が得られます。これらを E_p と E_q で表すことにします。また、P の成分を同様に p および q を法として考えたものを P_p および P_q で表すと、$P_p \in E_p(\mathbb{F}_p)$ および $P_q \in E_q(\mathbb{F}_q)$ が成り立ちます。

ここで、環 $\mathbb{Z}/N\mathbb{Z}$ は体ではありませんが、P を「$\mathbb{Z}/N\mathbb{Z}$ 上の楕円曲線 E の有理点」とみなして、定義式の通りに加法を繰り返し計算することでスカラー倍 $M \cdot P$（M は正の整数）を計算してみます。この計算の過程では、$\mathbb{Z}/N\mathbb{Z}$ の 0 でない元（例えば c と書きます）についてその逆元を計算する必要がありますが、もしこの c が N と互いに素であればユークリッドの互除法で逆元が求まります。一方、c が N と互いに素でない場合には、やはりユークリッドの互除法により $\gcd(c, N)$ が求まり、それが N の非自明な約数となるので N の素因数分解が得られます。いずれにせよ現在の目標を達成する上で問題にはなりません。

さて、$M \cdot P$ を計算する過程で得られる点のいずれかが、p を法として考えたときに無限遠点になると仮定します。さらに q を法として考えたときにはこうした状況が生じないものと仮定します。ここで、p を法としたときに無限遠点が得られる計算の直前の 2 点を $Q = (a_1, b_1)$ および $R = (a_2, b_2)$ とおきます。これは $Q_p + R_p = O$ を意味します。すると、a_1 と a_2 は p を法として等しいことになり、$Q + R$ の計算過程で分母に現れる数 $a_2 - a_1$ は N と互いに素ではなくなります。前述の通り、この場合には N の素因数分解が得られます。この考察から、E、P および M を、$M \cdot P$ を計算する過程で得られる点のいずれかが、p を法として考えたときに無限遠点になるように選べればよいことになります。特に、群 $E_p(\mathbb{F}_p)$ の位数 $|E_p(\mathbb{F}_p)|$ が M の約数であれば、ラグランジュの定理により $(M \cdot P)_p = O$ が成り立つため、所望の条件が満たされます。

一つの p に対して、楕円曲線 E の選び方を変えると、群 $E_p(\mathbb{F}_p)$ の位数は（範囲はある程度限られますが）様々に変化します。そこで、前節で紹介した Pollard の $p-1$ 法の場合と同様に、M として小さな素数の積を選び、楕円曲線 E をラ

ンダムに選ぶことで、$E_p(\mathbb{F}_p)$ の位数が smooth な数になり M の約数となる確率がなるべく高くなるよう期待します。この方法は、（合成数 N の桁数に関する）多項式オーダーの回数で成功するまでには至らないものの、例えば総当たりで N の素因数を探すのに比べればはるかに少ない回数の試行で N の素因数分解に成功する確率が充分に高いと試算されています。

例 7.4. $N = 77$ とし、$E\colon y^2 = x^3 + 3x + 2$、$P = (2, 4)$ とすると、P は E の $\mathbb{Z}/N\mathbb{Z}$ 上での有理点です。（この大きさの N なら総当たりで素因数分解する方が速いですが、）この状況で $M = 13$ として楕円曲線法の手順を試してみます。（N は 11 の倍数であり、例 7.2 で示したように $E_{11}(\mathbb{F}_{11})$ の位数は 13 なのでこれで上手くいくことが期待されます。）$M = (1101)_2$ なので、バイナリ法により $\mathbb{Z}/77\mathbb{Z}$ 上での P のスカラー倍の計算を以下のように進めていきます。

$$P + P = 2P = (32, 36)\,,\ 2P + P = 3P = (26, 32)\,,$$
$$3P + 3P = 6P = (40, 17)\,,\ 6P + 6P = 12P = (68, 18)$$

そして、$12P + P = 13P$ を求める際の λ の計算において、

$$\lambda = \frac{4 - 18}{2 - 68} = \frac{-14}{-66} = \frac{7}{33}$$

となりますが、分母について $\gcd(33, N) = 11$ ですので、$N = 77$ の素因数 11 が確かに得られました。

8 素因数分解アルゴリズム（３）

前節で紹介した楕円曲線法も、素朴な素因数分解の方法と比べると格段に効率的な方法ですが、さらに効率の良い素因数分解アルゴリズムとして、数体ふるい法と呼ばれる方法が知られています。この節ではこの数体ふるい法について紹介します。

数体ふるい法の最初のアイデアは Pollard が 1988 年に公表したとされていますが、論文としては Pollard を含む 4 名による 1990 年の共著論文[12] が最初のものであるようです。このときに提案されたアルゴリズムは、今日では特殊数体ふるい法と呼ばれている、入力となる整数の種類に制約のある版でしたが、それにもかかわらず特殊数体ふるい法は多くの重要な整数（例えば 9 番目のフェルマー数 $F_9 = 2^{2^9} + 1$、十進数で 155 桁の数）の素因数分解を実現するなどの成果を上げました。現在では、数体ふるい法のアイデアは一般の種類の整数に適用可能な形に整備され（一般数体ふるい法と呼ばれています）、本稿の執筆時点で知られている中で最も効率的な素因数分解アルゴリズムであるとされています。（ただし、一般数体ふるい法をもってしても素因数分解を入力の桁数に関する多項式時間で行うことはできていない点を注意しておきます。）

一般数体ふるい法を説明するのはかなり大変ですので、ここでは特殊数体ふるい法（のうち限定的な状況）の説明のみに留めておきます。[13] 以下の記述は、雪江明彦著『整数論１』（日本評論社）の 8.12 節を参考にしています。

以下、$N > 0$ を素因数分解したい合成数とします。数体ふるい法の基本方針は、整数 x, y で、条件

$$x^2 \equiv_N y^2 \text{ かつ } x \not\equiv_N \pm y$$

を見つけ出すことです。このとき、前者の条件より $x^2 - y^2 = (x-y)(x+y)$ は N の倍数であり、一方後者の条件より $x-y$ も $x+y$ も N の倍数ではないので、$\gcd(x \pm y, N)$ が N の非自明な約数を与えることがわかります。

整数係数の多項式 $f(x)$ を、有理数体 $\mathbb{Q}$ 上で既約な（つまり、より次数の低い有理数係数の多項式の積として表せない）ものとし、複素数 α を $f(\alpha) = 0$ となるものとします。また、整数 m を $f(m) \equiv_N 0$ となるように選びます。この m はなるべく絶対値が小さくなるように選んだ方が後々計算が楽になります。

[12] A. K. Lenstra, H. W. Lenstra Jr., M. S. Manasse, J. M. Pollard. The Number Field Sieve. In: Proceedings of STOC 1990, pp.564–572 (1990)

[13] 一般数体ふるい法についての文献は例えば `https://openaccess.leidenuniv.nl/handle/1887/2149` で公開されています。

複素数体 $\mathbb{C}$ の部分体（つまり、部分集合であって、$\mathbb{C}$ と同じ演算によって体をなすもの）で $\mathbb{Q}$ と α を含むようなもののうち最小の部分体が存在するので、それを $\mathbb{Q}(\alpha)$ で表します。この $\mathbb{Q}(\alpha)$ の具体的な表示を与えるために、いくつかの定義や性質を述べておきます。

定義 8.1 (最大公約式)**.** K を体とし、$F(x)$ と $G(x)$ を K 係数多項式とする。$F(x)$ と $G(x)$ の **最大公約式** $\gcd(F(x), G(x))$ を以下で定める。

- $F = 0$ かつ $G = 0$ のときは $\gcd(F, G) = 0$ とする。
- $F \neq 0$ または $G \neq 0$ のときは、F と G をともに割り切る K 係数多項式のうち、次数が最大で、かつ最高次の係数が 1 であるものを $\gcd(F, G)$ とする。

命題 8.1. K を体とし、$F(x)$ と $G(x)$ を K 係数多項式とすると、$A(x)F(x) + B(x)G(x) = \gcd(F, G)$ を満たす K 係数多項式 $A(x)$ と $B(x)$ が存在する。

証明. 証明の流れは整数に対するユークリッドの互除法とほぼ同様なので概略のみ説明する。$F = 0$ または $G = 0$ の場合は明白なので、$F \neq 0$ かつ $G \neq 0$ の場合を考える。必要であれば順番を交換して、F の次数 $\deg F$ が G の次数 $\deg G$ 以上であるとする。このとき、多項式の割り算を行って、$F = GQ + R$、R は 0 であるか $\deg R < \deg G$ を満たす、となる多項式 Q と R を計算できる。R が 0 でなければ次数が G の次数よりも小さくなっているので、次に G の R による割り算を考えて、という具合に順次繰り返していくと、いずれは余り R が 0 となる場合に到達する。このとき F は G で割り切れるため、$\deg(F, G)$ は G にある定数 c を掛けて最高次の係数を 1 に揃えたものであり、$\deg(F, G) = 0 \cdot F + c \cdot G$ という所望の形に表せる。あとは今までの手順を逆に辿ることで、元々の F と G に対しても条件を満たす A と B が得られる。 □

系 8.1. K を体とし、$F(x)$ を（0 でない）K 係数の既約多項式とする。K 係数多項式 $G(x)$ が $F(x)$ で割り切れなければ、$H(x)G(x) - 1$ が $F(x)$ で割り切れるような K 係数多項式 $H(x)$ が存在する。この $H(x)$ を、$F(x)$ を法とする $G(x)$ の逆元と呼ぶ。

証明. $F(x)$ は既約多項式なので、$\gcd(F(x), G(x))$ は 1 であるかまたは $F(x)$ の定数倍である。前提より $G(x)$ は $F(x)$ で割り切れないので後者の可能性はなく、

$\gcd(F(x), G(x)) = 1$ である。よって命題 8.1 により、ある K 係数多項式 $H(x)$ と $A(x)$ を用いて $AF + HG = 1$ と表せる。このとき確かに $HG - 1 = -AF$ は F で割り切れる。 □

命題 8.2. α と $f(x)$ を上記のようなものとし、$f(x)$ の次数を d とする。このとき

$$\mathbb{Q}(\alpha) = \{a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 \mid a_0, a_1, \ldots, a_{d-1} \in \mathbb{Q}\}$$

が成り立つ。

証明. 主張の式の右辺の集合を K と書く。$\mathbb{Q}$ と α を含む $\mathbb{C}$ の部分体はどれも K の元をすべて含むので、あとは K が実際に体になっていることを示せばよい。K の元は、ある 0 または有理数係数の $d-1$ 次以下の多項式 $g(x)$ を用いて $g(\alpha)$ という形に表せることを注意しておく。すると、K の元どうしの和が K の元となることは明らかであり、K の元どうしの積についても、多項式の積 $g(x)h(x)$ を $f(x)$ で割った余りを $r(x)$ とすると（$f(\alpha) = 0$ なので）$g(\alpha)h(\alpha) = r(\alpha)$ であることから積もまた K の元となる。つまり K は環である。あとは K の 0 以外の元 $g(\alpha)$ がどれも可逆であることを示せばよい。今、$g(\alpha) \neq 0$ であることから $g(x)$ は $f(x)$ で割り切れない。よって系 8.1 により、$f(x)$ を法とする $g(x)$ の逆元 $h(x)$ が存在する。このとき $h(x)g(x) - 1$ は $f(x)$ で割り切れるので $h(\alpha)g(\alpha) - 1 = 0$ したがって $h(\alpha)g(\alpha) = 1$ であり、$h(\alpha) \in K$ が $g(\alpha)$ の逆元となる。以上より K は体であり、$\mathbb{Q}(\alpha) = K$ が成り立つ。 □

命題 8.2 と同様に、$\mathbb{C}$ の部分環で $\mathbb{Z}$ と α を含むもののうち最小のものを $\mathbb{Z}[\alpha]$ と書くと、

$$\mathbb{Z}[\alpha] = \{a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 \mid a_0, a_1, \ldots, a_{d-1} \in \mathbb{Z}\}$$

が成り立ちます（ここで d は $f(x)$ の次数です）。すると、環準同型写像 $\varphi\colon \mathbb{Z}[\alpha] \to \mathbb{Z}/N\mathbb{Z}$ が

$$\varphi(a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0) = a_{d-1}m^{d-1} + \cdots + a_1m + a_0 \bmod N$$

によって定まります（$f(m) \equiv_N 0$ であることに注意してください）。

定義 8.2 (一意分解整域)**.** R を単位元を持つ可換環とする。

1. R の 0 でない元 r_1, r_2 について常に $r_1 r_2 \neq 0$ が成り立つとき、R を **整域** と呼ぶ。

2. $a, b \in R$ とする。$ac = b$ を満たす $c \in R$ が存在するとき、b は a で割り切れるといい、$a \mid b$ で表す。

3. R を整域とし、$p \in R \setminus R^\times$ とする。R の元 a, b が $p \mid ab$ を満たすとき常に $p \mid a$ または $p \mid b$ が成り立つならば、p を R の **素元** と呼ぶ。

4. R を整域とする。R の 0 でないどの元 r も、ある可逆元 $c \in R^\times$ と有限個（0 個の場合も含む）の素元 $p_1, \ldots, p_k \in R$ を用いて $r = cp_1 \cdots p_k$ という形で表せるとき、R を **一意分解整域** と呼ぶ。また、表示 $r = cp_1 \cdots p_k$ を r の **素元分解** と呼ぶ。

以降では、説明の簡略化のために、以下の条件を仮定します：

1. 体 $\mathbb{Q}(\alpha)$ の「整数環」と呼ばれる部分集合（定義は割愛する）が $\mathbb{Z}[\alpha]$ に一致する。

2. 環 $\mathbb{Z}[\alpha]$ は一意分解整域である。

すると、$\mathbb{Z}[\alpha]$ の元 x に $\mathbb{Z}/N\mathbb{Z}$ における $\varphi(x)$ の積への分解を対応付ける方法として、以下の二通りの方法が考えられます。

- x を写像 φ によって $\mathbb{Z}/N\mathbb{Z}$ へと写し、それを整数とみて素因数分解する。
- x を $\mathbb{Z}[\alpha]$ の中で素元分解しておき、それらを写像 φ によって $\mathbb{Z}/N\mathbb{Z}$ へと写す。

これら二通りの方法で得られた $\varphi(x)$ の分解は一般に異なるものとなります。この「ずれ」をうまく利用して所望の条件を満たす整数 x, y を見つけるのが（特殊）数体ふるい法の基本的アイデアです。

例 8.1. $N = 2117$ とします。まず、既約多項式 $f(x)$ を $f(x) = x^2 + 1$ と選び、$m = 46$ とすると、$f(m) = N$ なので確かに $f(m) \equiv_N 0$ が成り立ちます。また、$\alpha = \sqrt{-1} \in \mathbb{C}$ は $f(\alpha) = 0$ を満たしています。この α について、環 $\mathbb{Z}[\alpha] = \mathbb{Z}[\sqrt{-1}]$ は上記二つの仮定を満たすことが知られています。

$a+b\alpha$（$a,b\in\mathbb{Z}$）という形の $\mathbb{Z}[\alpha]$ の元について、$\varphi(a+b\alpha)=a+bm \bmod N$ が成り立ちます。例えば、

$$\beta_1=-1+\alpha\,,\ \beta_2=-1+2\alpha\,,\ \beta_3=2+3\alpha\,,\ \beta_4=-2+\alpha\,,\ \beta_5=3+\alpha\,,$$
$$\beta_6=3+4\alpha\,,\ \beta_7=5+\alpha\,,\ \beta_8=-7+\alpha\,,\ \beta_9=-11+2\alpha$$

と選び、$\mathbb{Z}[\alpha]$ の素元として

$$\pi_1=1+\alpha\,,\ \pi_2=1+2\alpha\,,\ \pi_3=2+\alpha\,,\ \pi_4=2+3\alpha$$

を取ると、$\alpha^2=-1$ に注意して

$$\begin{aligned}
\beta_1&=\alpha\cdot\pi_1\\
\beta_2&=\alpha\cdot\pi_3\\
\beta_3&=\pi_4\\
\beta_4&=\alpha\cdot\pi_2\\
\beta_5&=\alpha^3\cdot\pi_1\cdot\pi_2\\
\beta_6&={\pi_3}^2\\
\beta_7&=\alpha^3\cdot\pi_1\cdot\pi_4\\
\beta_8&=\pi_1\cdot{\pi_2}^2\\
\beta_9&=\alpha\cdot{\pi_3}^3
\end{aligned}$$

という分解が得られます。これらを辺ごとに掛け合わせることで、（$\alpha^4=1$ を用いて）

$$\beta_1\cdots\beta_9=\alpha^{10}{\pi_1}^4{\pi_2}^4{\pi_3}^6{\pi_4}^2=\left(\alpha{\pi_1}^2{\pi_2}^2{\pi_3}^3\pi_4\right)^2$$

したがって $\mathbb{Z}/N\mathbb{Z}$ において

$$\varphi(\beta_1\cdots\beta_9)=\left(\varphi(\alpha)\varphi(\pi_1)^2\varphi(\pi_2)^2\varphi(\pi_3)^3\varphi(\pi_4)\right)^2$$

という関係式が得られます。一方で、

$$\varphi(\beta_1) = 45 = 3^2 \cdot 5$$
$$\varphi(\beta_2) = 91 = 7 \cdot 13$$
$$\varphi(\beta_3) = 140 = 2^2 \cdot 5 \cdot 7$$
$$\varphi(\beta_4) = 44 = 2^2 \cdot 11$$
$$\varphi(\beta_5) = 49 = 7^2$$
$$\varphi(\beta_6) = 187 = 11 \cdot 17$$
$$\varphi(\beta_7) = 51 = 3 \cdot 17$$
$$\varphi(\beta_8) = 39 = 3 \cdot 13$$
$$\varphi(\beta_9) = 81 = 3^4$$

ですので、辺ごとに掛け合わせることで

$$\begin{aligned}\varphi(\beta_1 \cdots \beta_9) &= \varphi(\beta_1) \cdots \varphi(\beta_9) \\ &= 2^4 \cdot 3^8 \cdot 5^2 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17^2 = (2^2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17)^2\end{aligned}$$

という関係式が得られます。以上をあわせると、

$$(2^2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17)^2 \equiv_N \left(\varphi(\alpha)\varphi(\pi_1)^2\varphi(\pi_2)^2\varphi(\pi_3)^3\varphi(\pi_4)\right)^2$$

となります。

$$x = 2^2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17\,,$$
$$y = \varphi(\alpha)\varphi(\pi_1)^2\varphi(\pi_2)^2\varphi(\pi_3)^3\varphi(\pi_4)$$

とおくと、

$$x = 192972780\,,\ y = 46 \cdot 47^2 \cdot 93^2 \cdot 48^3 \cdot 140 = 13607275958599680$$

であり、$x^2 \equiv_N y^2$ および $x \not\equiv_N \pm y$ が成り立ちます。すると、

$$\gcd(x + y, N) = \gcd(13607276151572460, 2117) = 29$$

により、N の非自明な約数として 29 が得られます。実際 $N = 29 \cdot 73$ です。

上の例のように、$\beta_1\beta_2\cdots$ が $\mathbb{Z}[\alpha]$ において平方数となり、さらに $\varphi(\beta_1)\varphi(\beta_2)\cdots$ が整数としてみたときに平方数となるように $\beta_1, \beta_2, \cdots \in \mathbb{Z}[\alpha]$ を選ぶには、$\varphi(\beta_i)$ たちがなるべく小さな素数の積で表され、かつ β_i たちが $\mathbb{Z}[\alpha]$ の「なるべく小さな」素元の積で表せるようにすることが好都合です。実際の計算においては、$a + b\alpha$ という形の元がこれら二つの条件をともに満たすような a や b の値を探索する過程と、そうした条件を満たす元たちを掛け合わせて平方数の形にする掛け合わせ方を探索する過程に労力を割くことになり、この過程をどれだけ効率化できるかが数体ふるい法の実装における重要な課題となります。