平成 29 年度　上越教育大学公開講座

はじめての整数論

日時：9 月 1 日 (金)，9 月 8 日 (金)，9 月 15 日 (金)，9 月 22 日 (金)，9 月 29 日 (金)
19:00〜21:00
場所：上越教育大学　人文棟 1 階 104 教室

目次

はじめに

素数が無限に多く存在することは，与えられた素数のリストの中には書かれていない素数があることを示すことによって証明される．それでは与えられた自然数が素数かどうかを効率よく判定するにはどうしたらよいだろうか．本講座では素数判定法を中心に整数の基本的な性質と様々な問題への応用について，具体的な計算を通して解説する．

この講座を準備するにあたり，ジョセフ・H. シルヴァーマンの著書 [6] と中村憲氏による解説 [5] を主に参考にした．

1　素数

自然数 a, b について，$a = bc$ となる自然数 c が存在するとき，b は a の**約数**，a は b の**倍数**という．

例えば，$15 = 3 \times 5$ より，3 は 15 の約数，15 は 3 の倍数．

$a > 1$ を自然数とする．$a = 1 \times a$ より，1 と a は a の約数である．

7 の約数は 1 と 7 だけである．11 の約数も 1 と 11 だけである．このように自然数 $p > 1$ について，p の約数が 1 と p だけのとき，p は**素数**であるという．素数を小さい方から順に挙げると，

$$2,\quad 3,\quad 5,\quad 7,\quad 11,\quad 13,\quad 17,\quad 19,\quad 23,\quad 29,\quad 31,\ \ldots.$$

このように素数は非常に不規則に現れる．この素数の列は無限に続く．この事実はどうのように証明できるのだろうか？

補題 1.1. $n > 1$ を自然数とする．a を 1 より大きい n の約数の中で最小のものとする．このとき a は素数である．

[証明]　もし a が素数でないとすれば $a = bc,\ 1 < b < a,\ 1 < c < a$ と表せる (b, c は整数)．$b > 1$ は a より小さな n の約数だから，a が 1 より大きい n の約数の中で最小のものであることに矛盾する．ゆえに a は素数でなければならない．　□

定理 1.2 (ユークリッド)**.** 素数は無数に存在する．

[証明]　素数が有限個しかないと仮定する．それらを $p_1 < p_2 < \cdots < p_k$ とする．

$$n = p_1 p_2 \cdots p_k + 1$$

とおく．a を 1 より大きい n の約数の中で最小のものとする．補題 1.1 より a は素数である．素数は $p_1, p_2, \cdots, p_n$ しかないから，$a = p_i$ となる $1 \leq i \leq k$ がある．a は n の約数だから n は a で割り切れる．しかし n を $a = p_i$ で割ると 1 余るから矛盾である．　□

上の定理は背理法を用いて証明したが，その証明は単に矛盾を導いただけでなく，もう少し生産的な意味も含んでいることを説明しよう．$2, 3, 5$ という素数のリストに対して

$$2 \times 3 \times 5 + 1 = 31$$

を作れば，31 の約数の中に $2, 3, 5$ 以外の素数があると主張している．この場合は 31 自身が素数である．同様に $2, 3, 7$ という素数のリストに対して

$$2 \times 3 \times 7 + 1 = 43$$

を作れば，43 の約数の中に $2, 3, 7$ 以外の素数がある．この場合は 43 自身が素数である．$2, 3, 5, 7, 11, 13$ という素数のリストに対して

$$2 \times 3 \times 7 \times 11 \times 13 + 1 = 30031$$

を作れば，30031 の約数の中に $2, 3, 5, 7, 11, 13$ 以外の素数がある．この場合は $30031 = 59 \times 509$ は素数ではないが，その約数の 59, 509 は素数である．

次に与えられた自然数 n が素数かどうかを判定することを考える．

$$n \text{ が素数でない} \Longrightarrow n = ab, \quad 1 < a, b < n \text{ とかける}$$

$1 < a \leq b < n$ としてよい．このとき

$$a^2 \leq ab = n, \qquad a \leq \sqrt{n}.$$

したがって，n が素数でなければ，n は約数 a, $1 < a \leq \sqrt{n}$ をもつ．a の 1 より大きな約数で一番小さいものを p とすれば，補題 1.1 より p は素数である．$p \leq a \leq \sqrt{n}$ だから

$$n \text{ が素数でない} \Longrightarrow n \text{ は } \sqrt{n} \text{ 以下のある素数 } p \text{ で割り切れる．}$$

対偶をとれば，次の最も素朴な素数判定法を得る．

定理 1.3 (試し割算法)**.** 自然数 n について，n は $\sqrt{n}$ 以下のどんな素数 p でも割り切れないならば，n は素数である．

例 1.4. 109 は素数か？ $100 = 10^2 < 109 < 11^2 = 121$ より，$10 < \sqrt{109} < 11$．したがって，素数 $2, 3, 5, 7$ で割り切れなければ素数である．明らかに，2,5 では割り切れない．

$$109 = 3 \times 36 + 1, \quad 109 = 7 \times 15 + 4.$$

よって 109 は素数.

例 1.5. 197 は素数か？ $14^2 = 196 < 197 < 15^2 = 225$ より，$14 < \sqrt{197} < 15$．素数 $2, 3, 5, 7, 11, 13$ で割り切れなければ素数である．明らかに，2,5 では割り切れない.

$$197 = 3 \times 65 + 2, \quad 197 = 7 \times 27 + 1,$$
$$197 = 11 \times 17 + 10, \quad 197 = 13 \times 15 + 2.$$

よって 197 は素数である.

演習問題 1. 119 は素数か？素数でなければ 1 より大きな 2 つの整数の積として表せ.

100 までの素数すべて求めてみる．$1 < n \leq 100$ のとき，$\sqrt{n} \leq 10$ である．よって，$2, 3, 5, 7$ で n が割り切れなければ n は素数である．そこでまず，2 以外の 2 の倍数に / をつける．5 以外の 5 の倍数に / をつける．3 以外の 3 の倍数に / をつける．7 以外の 7 の倍数に / をつける．これで / がつかずに残ったものが素数である．100 以下の素数は 25 個あることがわかる．このようにして素数の表を作ることを**エラトステネスの篩の方法**という.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

演習問題 2. $\sqrt{200} = 10\sqrt{2} = 14.142\ldots$ であることを用いて，200 以下のすべての素数を求めよ.

2　整数の基本的性質

0 も負の整数も含めたすべての整数の集合を $\mathbb{Z}$ で表す．$\mathbb{Z}$ の部分集合 I が次の 2 つの性質

(M_1) $a \in I$ かつ $b \in I$ ならば $a+b \in I$
(M_2) $a \in I$ ならば $-a \in I$

をもつとき，I は $\mathbb{Z}$ の**加群**であるという．例えば，$0, -2, -4$ なども含めた偶数全体の集合を I とすれば，I は加群である．同様に，3 の倍数全体の集合，4 の倍数全体の集合，5 の倍数全体の集合なども $\mathbb{Z}$ の加群である．一般に $n \geq 0$ を与えたとき n の倍数全体の集合を $n\mathbb{Z}$ で表す．

$$n\mathbb{Z} = \{nx \,|\, x \in \mathbb{Z}\}.$$

$n\mathbb{Z}$ は $\mathbb{Z}$ の加群である．$0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$ である．

$\mathbb{Z}$ の加群はこれら以外にもあるだろうか？

定理 2.1. *I を $\mathbb{Z}$ の加群とすれば，整数 $n \geq 0$ が存在して $I = n\mathbb{Z}$ である．*

[証明]　I を $\mathbb{Z}$ の加群とする．$I = \{0\}$ のときは $I = 0\mathbb{Z}$ である．そうでないとする．$a \in I$, $a \neq 0$ がとれる．このとき I は加群だから (M_2) より $-a \in I$ である．a と $-a$ のどちらかは正整数だから，I は正整数を含む．n を I に含まれる最小の正整数とする．$n \in I$ だから (M_1) より $2n = n + n \in I$, $3n = n + 2n \in I$ である．これを繰り返せば $kn \in I$ $(k = 1, 2, \dots)$ がわかる．(M_2) より $-n \in I$ である．(M_1) より $-2n = (-n) + (-n) \in I$, $-3n = (-n) + (-2n) \in I$ である．これを繰り返せば $-kn \in I$ $(k = 1, 2, \dots)$ がわかる．$n \in I$, $-n \in I$ だから $0 = n + (-n) \in I$ もわかる．結局 $n\mathbb{Z} \subset I$ となることがわかる．逆向きの包含関係を示すために，任意の $a \in I$ をとる．a を n で割ったときの商を q，余りを r とする．

$$a = nq + r, \quad 0 \leq r < n$$

である．$a \in I$, $n(-q) \in n\mathbb{Z} \subset I$ だから $r = a + n(-q) \in I$ である．もし $r \neq 0$ とすると r は I に含まれる正整数で n よりも小さい．これは n が I に含まれる最小の正整数であることに矛盾する．ゆえに $r = 0$ でなければならない．したがって $a = nq \in n\mathbb{Z}$ である．これがすべての $a \in I$ についていえるから $I \subset n\mathbb{Z}$ である．$n\mathbb{Z} \subset I$ は既にみたから $I = n\mathbb{Z}$ であることが示された．　□

定理 2.1 から素因数分解の一意性等の整数の重要な性質が導かれる．ここでは素数のもつ性質として以下の 2 つの命題を証明しておく．

命題 2.2. p を素数とし，a を p で割り切れない整数とする．このとき

$$ax + py = 1$$

を満たす整数 x, y が存在する．

[証明]　$\mathbb{Z}$ の部分集合 I を

$$I = \{ax + py \,|\, x, y \in \mathbb{Z}\}$$

によって定義する (I は a の整数倍と p の整数倍をたした形に表せる整数全体の集合)．I は $\mathbb{Z}$ の加群である．実際，$\alpha, \beta \in I$ とすれば $\alpha = ax_1 + py_1$, $\beta = ax_2 + py_2$, $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ とかける．このとき

$$\begin{aligned} \alpha + \beta &= (ax_1 + py_1) + (ax_2 + py_2) = a(x_1 + x_2) + p(y_1 + y_2) \in I, \\ -\alpha &= -(ax_1 + py_1) = a(-x_1) + p(-y_1) \in I. \end{aligned}$$

よって I は $\mathbb{Z}$ の加群である．定理 2.1 より $I = n\mathbb{Z}$ となる整数 $n \geq 0$ が存在する．$a = a \times 1 + p \times 0 \in I$, $p = a \times 0 + p \times 1 \in I$ だから $I = n\mathbb{Z}$ より，$a = nb$, $b \in \mathbb{Z}$, $p = nq$, $q \in \mathbb{Z}$ とかける．特に $n \neq 0$ である．よって $n \geq 1$ である．p は素数で n は p の正の約数だから，$n = 1$ または $n = p$ である．しかし $a = nb$ で a は p で割り切れないとしたから，$n = p$ ではない．ゆえに $n = 1$ である．したがって $I = \mathbb{Z}$ である．特に $1 \in \mathbb{Z} = I$ だから $1 = ax + py$, $x, y \in \mathbb{Z}$ と表せる．　□

命題 2.2 のような p, a が与えられたときに具体的に $ax + py = 1$ を満たす整数 x, y を求めるには**ユークリッドの互除法**を応用すればよい．これを具体例で説明する．

例 2.3. $2017x + 908y = 1$ を満たす整数 x, y を 1 組求める．2017 を 908 で割り算すると商が 2 で余りが 201 になる：

$$2017 = 908 \times 2 + 201.$$

次に 908 を上の割り算の余りの 201 で割り算すると商が 4 で余りが 104 になる：

$$908 = 201 \times 4 + 104.$$

さらに 201 を上の割り算の余りの 104 で割り算すると商が 1 で余りが 97 になる：

$$201 = 104 \times 1 + 97.$$

同様に 104 を 97 で割り算すると商が 1 で余りが 7 になる：

$$104 = 97 \times 1 + 7.$$

97 を 7 で割り算すると商が 13 で余りが 6 になる：

$$97 = 7 \times 13 + 6.$$

7 を 6 で割り算すると商が 1 で余りが 1 になる：

$$7 = 6 \times 1 + 1.$$

以上の割り算の結果を「余り =」の形に書き直して逆の順番でかけば

$$\begin{aligned} 1 &= 7 - 6 \times 1, \\ 6 &= 97 - 7 \times 13, \\ 7 &= 104 - 97 \times 1, \\ 97 &= 201 - 104 \times 1, \\ 104 &= 908 - 201 \times 4, \\ 201 &= 2017 - 908 \times 2. \end{aligned}$$

これから

$$\begin{aligned} 1 &= 7 - 6 \times 1 = 7 - (97 - 7 \times 13) \times 1 = 7 - 97 + 7 \times 13 \\ &= 7 \times (1 + 13) - 97 = 7 \times 14 - 97 = (104 - 97 \times 1) \times 14 - 97 \\ &= 104 \times 14 - 97 \times 14 - 97 = 104 \times 14 - 97 \times (14 + 1) \\ &= 104 \times 14 - 97 \times 15 = 104 \times 14 - (201 - 104 \times 1) \times 15 \\ &= 104 \times 14 - 201 \times 15 + 104 \times 15 = 104 \times (14 + 15) - 201 \times 15 \\ &= 104 \times 29 - 201 \times 15 = (908 - 201 \times 4) \times 29 - 201 \times 15 \\ &= 908 \times 29 - 201 \times 4 \times 29 - 201 \times 15 = 908 \times 29 - 201 \times (4 \times 29 + 15) \\ &= 908 \times 29 - 201 \times 131 = 908 \times 29 - (2017 - 908 \times 2) \times 131 \\ &= 908 \times (29 + 2 \times 131) - 2017 \times 131 = 908 \times 291 - 2017 \times 131. \end{aligned}$$

よって $x = -131$, $y = 291$ とおけば $2017x + 908y = 1$ を満たす $(264228 - 264227 = 1)$.

命題 2.4. p を素数とする．整数 a, b の積 ab が p で割り切れるならば，a または b は p で割り切れる．

[証明]　a が p で割り切れないとする．命題 2.2 より整数 x, y で $ax + py = 1$ となるものが存在する．また仮定より $ab = pc$ となる整数 c が存在する．このとき $1 = ax + py$

より

$$b = b \times 1 = b(ax + py) = abx + pby = pcx + pby = p(cx + by)$$

となり，b は p で割り切れる．　□

3　合同式とフェルマーの小定理

n を 1 より大きな整数とする．整数 a, b に対して $a - b$ が n で割り切れるとき，すなわち $a - b = nc$ となる整数 c が存在するとき

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

とかいて，a と b は n を**法として合同**であるという．例えば，$n = 9$ とする．25 を 9 で割ったときの商は 2 で余りは 7 だから

$$25 = 9 \times 2 + 7, \quad 25 - 7 = 9 \times 2.$$

よって

$$25 \equiv 7 \pmod{9}.$$

一般に a を n で割ったときの商を q，余りを r とすれば，$a = nq + r$, $0 \leq r < n$ である．$a - r = nq$ だから

$$a \equiv r \pmod{n}$$

である．

合同式は等式と似た性質をもつ．

命題 3.1. $a \equiv b \pmod{n}$ かつ $c \equiv d \pmod{n}$ ならば次の合同式が成り立つ．

$$\begin{aligned} a + c &\equiv b + d \pmod{n}, \\ a - c &\equiv b - d \pmod{n}, \\ ac &\equiv bd \pmod{n}. \end{aligned}$$

[証明]　$a - b = ns$, $c - d = nt$, s, t は整数とかける．このとき

$$\begin{aligned} (a + c) - (b + d) &= (a - b) + (c - d) = ns + nt = n(s + t), \\ (a - c) - (b - d) &= (a - b) - (c - d) = ns - nt = n(s - t) \end{aligned}$$

だから，$a+c \equiv b+d \pmod{n}$, $a-c \equiv b-d \pmod{n}$ である．積については $a = b+ns$, $c = d+nt$ とかけるから

$$ac = (b+ns)(d+nt) = bd + nbt + nds + n^2st,$$
$$ac - bd = nbt + nds + n^2st = n(bt + ds + nst).$$

よって $ac \equiv bd \pmod{n}$ である． □

注意 3.2. 割り算については合同式と等式では異なることに注意する．例えば a, b, c が整数で $a \neq 0$ のとき $ab = ac$ ならば $b = c$ が成り立つが，$ab \equiv ac \pmod{n}$ でも $b \equiv c \pmod{n}$ が成り立つと限らない．実際，

$$3 \times 5 \equiv 3 \times 1 \pmod{12}, \quad 5 \not\equiv 1 \pmod{12}.$$

$5 \equiv 1 \pmod{4}$ は成り立っている．

一般に正の整数 a と n に対して

$$I = \{ax + ny \,|\, x, y \in \mathbb{Z}\}$$

とおけば，I は $\mathbb{Z}$ の加群である．定理 2.1 より $I = d\mathbb{Z}$ となる整数 $d \geq 1$ がある．$n \in I$ だから $n = dn'$, $n' \in \mathbb{Z}$ とかける．このとき

$$ab \equiv ac \pmod{n} \Longrightarrow b \equiv c \pmod{n'}$$

が成り立つことを示す．$a \in I$ だから $a = da'$, $a' \in \mathbb{Z}$ とかける，また $d \in I$ だから $d = ax + ny$ となる $x, y \in \mathbb{Z}$ がある．$a = da'$, $n = dn'$ を代入して $d = da'x + dn'y$, $1 = a'x + n'y$ を得る．

$ab \equiv ac \pmod{n}$ より $ab - ac = nk$, $k \in \mathbb{Z}$ である．これに $a = da'$, $n = dn'$ を代入して

$$da'b - da'c = dn'k, \quad a'(b-c) = n'k.$$

したがって

$$b - c = (b-c) \times 1 = (b-c)(a'x + n'y) = a'(b-c)x + n'(b-c)y$$
$$= n'\big(kx + (b-c)y\big).$$

ゆえに $b \equiv c \pmod{n'}$ である．

合同式を応用して，9 の倍数，11 の倍数を簡単に判定することができる．

例 3.3. $n = 9$ とする．

$$\begin{aligned}
10 &\equiv 1 \pmod 9,\\
10^2 &\equiv 1^2 \equiv 1 \pmod 9,\\
427 &\equiv 4 \times 10^2 + 2 \times 10 + 7 \equiv 4 + 2 + 7 \equiv 13 \equiv 4 \pmod 9,\\
513 &\equiv 5 \times 10^2 + 1 \times 10 + 3 \equiv 5 + 1 + 3 \equiv 9 \equiv 0 \pmod 9.
\end{aligned}$$

例 3.4. $n = 11$ とする．

$$\begin{aligned}
10 &\equiv -1 \pmod{11},\\
10^2 &\equiv (-1)^2 \equiv 1 \pmod{11},\\
321 &\equiv 3 \times 10^2 + 2 \times 10 + 1 \equiv 3 + 2 \times (-1) + 1 \equiv 2 \pmod{11},\\
726 &\equiv 7 \times 10^2 + 2 \times 10 + 6 \equiv 7 + 2 \times (-1) + 6 \equiv 11 \equiv 0 \pmod{11}.
\end{aligned}$$

$p = 7$, $a = 3$ とすると

$$\begin{aligned}
3 \cdot 1 &\equiv 3 \pmod 7, \qquad 3 \cdot 4 \equiv 5 \pmod 7,\\
3 \cdot 2 &\equiv 6 \pmod 7, \qquad 3 \cdot 5 \equiv 1 \pmod 7,\\
3 \cdot 3 &\equiv 2 \pmod 7, \qquad 3 \cdot 6 \equiv 4 \pmod 7.\\
(3 \cdot 1)(3 \cdot 2)(3 \cdot 3)(3 \cdot 4)(3 \cdot 5)(3 \cdot 6) &\equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \pmod 7,\\
3^6 6! &\equiv 6! \pmod 7,\\
6!(3^6 - 1) &\equiv 0 \pmod 7.
\end{aligned}$$

よって，$6!(3^6 - 1)$ は 7 で割りきれる．$6!$ は素数 7 で割り切れないから，$3^6 - 1$ は 7 で割り切れる．これは次のように一般的に成り立つ．

定理 3.5 (フェルマーの小定理)**.** p を素数とし，a を p で割り切れない整数とすれば

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

が成り立つ．

[証明]　まず，$ax \equiv ay \pmod p$ ならば $x \equiv y \pmod p$ であることを示す．$ax \equiv ay \pmod p$ とすると，$a(x - y) \equiv 0 \pmod p$，すなわち $a(x - y)$ は素数 p で割り切れる．a は p で割り切れないとしたから，命題 2.4 より $x - y$ は p で割り切れる．よって $x \equiv y \pmod p$ である．この対偶をとると，$x \not\equiv y \pmod p$ ならば $ax \not\equiv ay \pmod p$ である．したがって，x が $1, 2, \ldots, p - 1$ を動くとき，ax の値は p を法として，0 でなく，また互

いに合同ではない．よって ax の値は p を法として，$1, 2, \ldots, p-1$ をすべて丁度 1 回ずつとる．したがって

$$\begin{aligned}
&(a\cdot 1)(a\cdot 2)\cdots(a\cdot(p-1)) \equiv 1\cdot 2\cdots(p-1) \pmod{p},\\
&a^{p-1}(p-1)! \equiv (p-1)! \pmod{p},\\
&(p-1)!(a^{p-1}-1) \equiv 0 \pmod{p}.
\end{aligned}$$

すなわち $(p-1)!(a^{p-1}-1)$ は素数 p で割り切れる．$(p-1)!$ は p で割り切れないから，命題 2.4 より $a^{p-1}-1$ は p で割り切れる． □

例 3.6. $p=7$ のとき，$2^6-1=63=7\times 9$, $5^6-1=15624=7\times 2232$.
$p=11$ のとき，$2^{10}-1=1023=11\times 93$, $3^{10}-1=59048=11\times 5368$.

応用として 2^{125} を 7 で割った余りを求めてみる．フェルマーの小定理より，$2^6\equiv 1 \pmod 7$ である．割り算によって，$125=6\times 20+5$ だから

$$2^{125}=2^{6\times 20+5}=2^{6\times 20}2^5=(2^6)^{20}2^5.$$

ここで $2^6\equiv 1 \pmod 7$, $(2^6)^{20}\equiv 1^{20}\equiv 1 \pmod 7$ だから

$$2^{125}=(2^6)^{20}2^5\equiv 1\times 2^5\equiv 32\equiv 4 \pmod 7.$$

フェルマーの小定理の証明において素数 p に対して $(p-1)!$ は p で割り切れないことを用いた．それでは $(p-1)!$ は p を法としていくつと合同になるのだろうか？

$p=11$ ならば，$9\times 5\equiv 1 \pmod{11}$, $8\times 7\equiv 1 \pmod{11}$, $6\times 2\equiv 1 \pmod{11}$, $4\times 3\equiv 1 \pmod{11}$ だから

$$\begin{aligned}
10! &= 10\times 9\times 8\times 7\times 6\times 5\times 4\times 3\times 2\times 1\\
&= 10\times(9\times 5)\times(8\times 7)\times(6\times 2)\times(4\times 3)\times 1\\
&\equiv (-1)\times 1\times 1\times 1\times 1\times 1\equiv -1 \pmod{11}.
\end{aligned}$$

これは次のように一般的に成り立つ．

定理 3.7 (ウィルソンの定理)**.** p を素数とすれば，$(p-1)!+1$ は p で割り切れる．

[証明]　命題 2.2 より，各 $a=1,2,\ldots,p-1$ に対して，$ax\equiv 1 \pmod p$ となる x, $1\le x\le p-1$ が存在する．

$$\begin{aligned}
a^2\equiv 1 \pmod p &\iff a^2-1=(a-1)(a+1) \text{ が } p \text{ で割り切れる}\\
&\iff a-1 \text{ または } a+1 \text{ が } p \text{ で割り切れる}\\
&\iff a=1 \text{ または } a=p-1. \qquad (1\le a\le p-1 \text{ より})
\end{aligned}$$

したがって $a = 1, p-1$ を除けば，$ax \equiv 1 \pmod{p}$ を満たす x は $x \not\equiv a \pmod{p}$ である．積

$$(p-1)! = 1 \times 2 \times \cdots \times (p-2) \times (p-1)$$

において，1 と $p-1$ 以外は，積の順序をかえて，かけて p を法として 1 と合同になるようなペアに組み合わせることができるから

$$(p-1)! \equiv 1 \times (p-1) \equiv -1 \pmod{p}.$$

□

例 3.8. $(5-1)! + 1 = 25 = 5 \times 5$, $(7-1)! + 1 = 721 = 7 \times 103$, $(11-1)! + 1 = 3628801 = 11 \times 329891$.

演習問題 3. 2^{1000} を 7 で割ったときの余りを求めよ．

4 RSA 暗号

$m > 1$ を自然数とする．0 以上 $m-1$ 以下の整数全体の集合を R_m で表す．さらに，1 以上 $m-1$ 以下の自然数で，m と互いに素なもの全体の集合を G_m とかく．G_m は R_m の部分集合である．R_m の元の個数は m である．G_m の元の個数

$$\varphi(m) = |G_m|$$

を**オイラーの関数**という．p が素数ならば，$\varphi(p) = p-1$ である．

R_m は次のように和と積を定義することによって環になる．$a, b \in R_m$ に対して

$$a + b = \text{整数としての和 } a+b \text{ を } m \text{ で割った余り},$$
$$ab = \text{整数としての } ab \text{ を } m \text{ で割った余り}.$$

G_m は R_m における積によって可換群になっている．

いま $m = pq$, p, q は相異なる素数とする．R_p の元 a と R_q の元 b を並べた組 (a, b) の全体の集合を $R_p \times R_q$ で表す．すなわち，

$$R_p \times R_q = \{(a, b) \,|\, a \in R_p,\ b \in R_q\}.$$

$R_p \times R_q$ における和と積を

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b)(c, d) = (ac, bd) \quad ((a, b), (c, d) \in R_p \times R_q)$$

によって定義する．さらに写像 $f : R_m \longrightarrow R_p \times R_q$ を

$$f(x) = (x \text{ を } p \text{ で割った余り}, x \text{ を } q \text{ で割った余り}) \qquad (x \in R_m)$$

によって定義する．このとき f は環 R_m から環 $R_p \times R_q$ への同型になる．すなわち f は 1 対 1 対応であり任意の $x, y \in R_m$ に対して

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y)$$

が成り立つ．

[証明]　$x, y \in R_m$, $x \geq y$ とする．$f(x) = f(y)$ とすると

$(x \text{ を } p \text{ で割った余り}, x \text{ を } q \text{ で割った余り}) = (y \text{ を } p \text{ で割った余り}, y \text{ を } q \text{ で割った余り})$

である．よって

$$x \equiv y \pmod{p}, \quad x \equiv y \pmod{q}$$

である．したがって $x - y$ は p で割り切れ，かつ q で割り切れる．したがって $x - y$ は $pq = m$ で割り切れる．$0 \leq x - y \leq m - 1$ だから $x - y = 0$, $x = y$ である．よって対応 $f : R_m \to R_p \times R_q$ によって，異なる 2 つの元 x, y は異なる元にうつされる．R_m も $R_p \times R_q$ もともに $m = pq$ 個の元からなる有限集合だから，対応 f によって 1 対 1 にうつりあう．f が足し算とかけ算を保つことは明らかである．　□

環の同型 f を G_m に制限すれば，可換群の同型 $G_m \cong G_p \times G_q$ が得られる．したがって特に

$$\varphi(m) = |G_m| = |G_p||G_q| = \varphi(p)\varphi(q) = (p-1)(q-1)$$

を得る．

例 4.1. $m = 15$, $p = 3$, $q = 5$ とする．$G_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$, $G_3 = \{1, 2\}$, $G_5 = \{1, 2, 3, 4\}$ である．$|G_{15}| = 8$, $|G_3| = 2$, $|G_5| = 4$ だから $|G_{15}| = |G_3||G_5|$ が成り立っている．可換群の同型 $G_{15} \cong G_3 \times G_5$ は具体的に次のような対応で与えられる：

$$\begin{aligned}
1 &\longmapsto (1,1)\\
2 &\longmapsto (2,2)\\
4 &\longmapsto (1,4)\\
7 &\longmapsto (1,2)\\
8 &\longmapsto (2,3)\\
11 &\longmapsto (2,1)\\
13 &\longmapsto (1,3)\\
14 &\longmapsto (2,4)
\end{aligned}$$

フェルマーの小定理によって任意の $a \in G_p$ に対して $a^{p-1} = 1$ である．同様に任意の $b \in G_q$ に対して $b^{q-1} = 1$ である．したがって g を $p-1$ と $q-1$ の最小公倍数とすれば，$g = (p-1)d = (q-1)d'$, d, d' は整数，とかけるから，任意の $(a, b) \in G_p \times G_q$ に対して

$$(a, b)^g = (a^g, b^g) = (a^{(p-1)d}, b^{(q-1)d'}) = (1, 1)$$

である．同様に

$$(a, b)^{(p-1)(q-1)} = (a^{(p-1)(q-1)}, b^{(p-1)(q-1)}) = (1, 1)$$

である．$x \in G_m$ とし，$f(x) = (a, b)$ とすれば

$$f(x^g) = f(x)^g = (a, b)^g = (1, 1) = f(1)$$

である．f は 1 対 1 だから $x^g = 1$ である．同様に $x^{(p-1)(q-1)} = 1$ である．

RSA 暗号では暗号を受け取る B さんが m と k の値を公開しておく．ここで k は $\varphi(m)$ と互いに素であるとする．A さんが B さんへ暗号データ $x \in G_m$ を送るとき，x ではなく G_m における x^k の値 y を送る．この値を受け取った B さんは，B さんしか知らない $\varphi(m)$ の値を用いて，ユークリッドの互除法によって，

$$k\ell = 1 + \varphi(m)n$$

となるような ℓ を求める．さらに，G_m において，y^ℓ を計算する．このとき

$$y^\ell = (x^k)^\ell = x^{k\ell} = x^{1+\varphi(m)n} = x(x^{\varphi(m)})^n = x1^n = x$$

である．これによって B さんは A さんが送ろうとした暗号を復号できたことになる．

これを具体例でみてみる．$m = 55$ とする．55 が 5×11 と素因数分解できることは暗号を受け取る側の B さんしか知らないとする (m がもっと大きな素数 p と q の積であることを B さんしか知らないとする)．$\varphi(55) = \varphi(5)\varphi(11) = 4 \times 10 = 40$ の値は B さんしか知らない (と思う)．この値 40 と互いに素な k として $k = 7$ をとる．B さんは公開鍵として $m = 55$ と $k = 7$ を公開する．A さんは B さんへ暗号データとして $x = 3$(G_{55} の元) を送りたいとする．A さんは公開鍵 $m = 55$ と $k = 7$ を使ってこのデータを暗号化する：$y = x^7 = 3^7$ を G_{55} で計算する．合同式の計算により

$$\begin{aligned}
&3^2 \equiv 9 \pmod{55},\\
&3^3 \equiv 27 \pmod{55},\\
&3^4 \equiv 9^2 \equiv 81 \equiv 26 \pmod{55},\\
&3^7 \equiv 3^3 \times 3^4 \equiv 27 \times 26 \equiv 702 \equiv 42 \pmod{55}.
\end{aligned}$$

A さんは暗号化されたデータとして $y = 42$ を B さんに送信する．これを受信した B さんは $\varphi(m) = 40$ の値を知っているからこれを用いて，ユークリッドの互除法によって，

$$7\ell = 1 + 40n$$

を満たす整数 ℓ と n を求める．

$$\begin{aligned} 40 &= 7 \times 5 + 5, \\ 7 &= 5 \times 1 + 2, \\ 5 &= 2 \times 2 + 1. \end{aligned}$$

$$\begin{aligned} 1 &= 5 - 2 \times 2 = 5 - (7 - 5 \times 1) \times 2 \\ &= 5 - 7 \times 2 + 5 \times \times 2 = 5 \times 3 - 7 \times 2 \\ &= (40 - 7 \times 5) \times 3 - 7 \times 2 = 40 \times 3 - 7 \times 5 \times 3 - 7 \times 2 \\ &= 40 \times 3 - 7 \times 17 = 40 \times (3 - 7) + 7 \times 40 - 7 \times 17 \\ &= 7 \times 23 - 40 \times 4. \end{aligned}$$

よって $\ell = 23$, $n = 4$ が求まる．B さんはこれを使って $y = 42$ の $\ell = 23$ 乗を G_{55} で計算する．$23 = 16 + 4 + 2 + 1$ に注意する．

$$\begin{aligned} 42^2 &\equiv (-13)^2 \equiv 169 \equiv 4 \pmod{55}, \\ 42^3 &\equiv 4 \times 42 \equiv 168 \equiv 3 \pmod{55}, \\ 42^4 &\equiv 4^2 \equiv 16 \pmod{55}, \\ 42^8 &\equiv (16)^2 \equiv 256 \equiv 36 \equiv -19 \pmod{55}, \\ 42^{16} &\equiv (-19)^2 \equiv 361 \equiv 31 \pmod{55}, \\ 42^{20} &\equiv 31 \times 16 \equiv 496 \equiv 1 \pmod{55}, \\ 42^{23} &\equiv 1 \times 42^3 \equiv 3 \pmod{55}. \end{aligned}$$

したがって B さんにだけは $y^{23} = 3$ が A さんの送りたかったデータであることがわかった．

p, q を十分大きな素数とすれば，m の値だけからは，実際に $m = pq$ と素因数分解することはできない．$\varphi(m)$ や g は，m が pq と素因数分解されることがわかってはじめて求められるものだから，暗号の安全性が保証される．

5　素数判定法

5.1　フェルマーテスト

フェルマーの小定理 (定理 3.5) により，n が素数で b が n で割り切れない整数ならば

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

が成り立つ．したがって

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

が成り立つ．これは b が n で割り切れるときでも明らかに成り立つ．よって

$$n \text{ が素数} \implies b^n \equiv b \pmod{n} \text{ (すべての } b \in \mathbb{Z}\text{)}.$$

対偶をとれば

$$\text{ある } b \in \mathbb{Z} \text{ に対して } b^n \not\equiv b \pmod{n} \implies n \text{ は素数ではない.}$$

このように $b^n \not\equiv b \pmod{n}$ となる b をみつけることによって n が素数でないことと判定できる．これを**フェルマーテスト**という．

例 5.1. $n = 119$ とする．3^{119} を法 119 で計算してみよう．そのためには 119 をまず 2 のべき乗の和として表す (2 進法で表すことと同じ).

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad 2^5 = 32, \quad 2^6 = 64, \quad 2^7 = 128$$

だから

$$119 = 2^6+55 = 2^6+2^5+23 = 2^6+2^5+2^4+7 = 2^6+2^5+2^4+2^2+3 = 2^6+2^5+2^4+2^2+2+1.$$

よって $119 = (1110111)_2$ である.

$$\begin{aligned}
3^1 &\equiv 3 \pmod{119},\\
3^2 &\equiv 9 \pmod{119},\\
3^4 &\equiv 9^2 \equiv 81 \pmod{119},\\
3^8 &\equiv 81^2 \equiv 6561 \equiv 16 \pmod{119},\\
3^{16} &\equiv 16^2 \equiv 256 \equiv 18 \pmod{119},\\
3^{32} &\equiv 18^2 \equiv 324 \equiv 86 \pmod{119},\\
3^{64} &\equiv 86^2 \equiv 7396 \equiv 18 \pmod{119}.
\end{aligned}$$

これから

$$\begin{aligned} 3^{119} &= 3^{64+32+16+4+2+1} = 3^{64} \times 3^{32} \times 3^{16} \times 3^4 \times 3^2 \times 3^1 \\ &\equiv 18 \times 86 \times 18 \times 81 \times 9 \times 3 \pmod{119} \\ &\equiv 1 \times 18 \times 81 \times 9 \times 3 \pmod{119} \\ &\equiv 30 \times 27 \pmod{119} \equiv 96 \pmod{119}. \end{aligned}$$

したがって $3^{119} \equiv 96 \not\equiv 3 \pmod{119}$ である．フェルマーテストにより 119 は素数ではない．

フェルマーテストよりも試し割り算法の方が効率がいいように見えるかもしれない．a^n を法 n で計算することは $\log n$ に比例する計算量である．一方，試し割り算法では $\sqrt{n}$ に比例する計算量である．よっていくつかの a についてのフェルマーテストで素数判定ができれば非常に大きな n に対してはその方が効率が各段によいことになる．

5.2 絶対擬素数

$b^n \not\equiv b \pmod{n}$ となる b がみつかれば n が素数でないことと判定できた．それではそのような b が存在しないとき，すなわちすべての $b \in \mathbb{Z}$ に対して $b^n \equiv b \pmod{n}$ が成り立てば n は素数であるといえるだろうか？残念ながらそれはいえないことを具体例で示す．

例 5.2. $n = 561 = 3 \times 11 \times 17$ とする．すべての整数 b に対して $b^{561} \equiv b \pmod{561}$ が成り立つことを示す．b を 561 で割ったときの余りを r とすれば，$0 \leq r \leq 560$ である．$b \equiv r \pmod{561}$ だから，561 通りの r について $r^{561} \equiv r \pmod{561}$ を計算で確かめればよい．しかしもっと簡単にこれを示すことができる．$b^{561} \equiv b \pmod{561}$ が成り立つことをいうためには

$$b^{561} \equiv b \pmod{3}, \quad b^{561} \equiv b \pmod{11}, \quad b^{561} \equiv b \pmod{17}$$

を示せばよい．実際，これらが成り立てば，$b^{561} - b$ は 3 でも 11 でも 17 でも割り切れるから，$3 \times 11 \times 17 = 561$ で割り切れて，$b^{561} \equiv b \pmod{561}$ がいえる．

b が 3 で割り切れるときは $b^{561} \equiv b \pmod{3}$ は明らか (両辺とも 0)．b が 3 で割り切れないときは，フェルマーの小定理により $b^2 \equiv 1 \pmod{3}$ であり，

$$b^{561} = b^{2\times 280+1} \equiv (b^2)^{280} b \equiv 1 \cdot b \equiv b \pmod{3}.$$

b が 11 で割り切れるときは $b^{561} \equiv b \pmod{11}$ は明らか (両辺とも 0)．b が 11 で割り切れないときは，フェルマーの小定理により $b^{10} \equiv 1 \pmod{11}$ であり，

$$b^{561} = b^{10\times 56+1} \equiv (b^{10})^{56} b \equiv 1 \cdot b \equiv b \pmod{11}.$$

b が 17 で割り切れるときは $b^{561} \equiv b \pmod{17}$ は明らか (両辺とも 0)．b が 17 で割り切れないときは，フェルマーの小定理により $b^{16} \equiv 1 \pmod{17}$ であり，

$$b^{561} = b^{16\times 35+1} \equiv (b^{16})^{35} b \equiv 1 \cdot b \equiv b \pmod{17}.$$

以上によってすべての $b \in \mathbb{Z}$ に対して $b^{561} \equiv b \pmod{561}$ が成り立つが，$n = 561$ は素数ではない．

561 のようにすべての $b \in \mathbb{Z}$ に対して $b^n \equiv b \pmod{n}$ が成り立つような合成数を**絶対擬素数**あるいは**カーマイケル数**という．10000 までの絶対擬素数は

$$561, \quad 1105, \quad 1729, \quad 2465, \quad 2821, \quad 6601, \quad 8911$$

の 7 個である．絶対擬素数が無数に存在することはカーマイケルが予想してから 80 年以上経った 1992 年に W.R. アルフォード，A. グランヴィル，C. ポマランスによって証明された．

5.3 拡張フェルマーテスト

自然数 $n > 1$ が素数かどうかを $\log n$ の多項式の計算量で判定することができるだろうかという問題は長い間未解決であったが，2002 年にインドの 3 人の研究者 M. Agrawal, N. Kayal, N. Saxena により解決された ([1])．ニューヨークタイムズによるその紹介記事の見出しは “2200 年来の数学の問題解決！” であった．以下，[5] に基づいて拡張フェルマーテストとよばれる彼らの方法を解説する．

X を変数とする整数係数の多項式全体を $\mathbb{Z}[X]$ で表す．$f(X) \in \mathbb{Z}[X]$ は

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n, \qquad a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{Z}$$

と表される．いま，$f(X), g(x), F(X) \in \mathbb{Z}[X]$ と自然数 $n > 1$ に対して，

$$f(X) - g(X) = n h_1(X) + F(X) h_2(X)$$

となる $h_1(X), h_2(X) \in \mathbb{Z}[X]$ が存在することを

$$f(X) \equiv g(X) \pmod{(n, F)}$$

と表す．この多項式の合同式も，命題 3.1 における整数の合同式と同様な性質をもつ．特に $F(X) = 0$ のときには，$f(X) \equiv g(X) \pmod{(n, F)}$ を単に $f(X) \equiv g(X) \pmod{n}$ とかく．このとき次の定理が成り立つ．

定理 5.3 (拡張フェルマー小定理)**.** b を n と互いに素 (b と n の最大公約数が 1) な整数とする．このとき n が素数であるためには

$$(X + b)^n \equiv X^n + b \pmod{n} \tag{5.1}$$

が成り立つことが必要十分である．

[証明]　n が素数であるとする．二項定理より

$$(X + b)^n = X^n + \sum_{k=1}^{n-1} \binom{n}{k} b^k X^{n-k} + b^n.$$

ここで $1 \leq k \leq n-1$ に対して

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad k!(n-k)!\binom{n}{k} = n!$$

だから，$k!(n-k)!\binom{n}{k} = n!$ は素数 n で割り切れる．命題 2.4 より，$k!(n-k)!$ または $\binom{n}{k}$ は n で割り切れる．しかし $k!(n-k)!$ は n より小さな自然数の積だから n では割り切れない．したがって二項係数 $\binom{n}{k}$ は n で割り切れる．フェルマーの小定理より $b^n \equiv b \pmod{n}$ である．よって

$$(X + b)^n \equiv X^n + b^n \equiv X^n + b \pmod{n}.$$

次に n が素数でないとする．n を割る素数 p をとり，$n = p^r n'$, n' は p で割れない自然数とかく．$n > p$ である．$k = p$ のときの二項係数 $\binom{n}{p}$ は

$$\binom{n}{p} = \frac{n!}{(n-p)!p!} = \frac{n(n-1)\cdots(n-p+1)}{p!} = p^{r-1} n' \frac{(n-1)\cdots(n-p+1)}{(p-1)!}$$

であり，この右辺の n' は p で割り切れず，かつ $p-1$ 個の整数 $n-j$ $(j = 1, \ldots, p-1)$ はいずれも p で割り切れない (n が p で割り切れるから) ので，$\binom{n}{p}$ は p^{r-1} で割り切れるが p^r では割り切れない．したがって $\binom{n}{p}$ は n で割り切れないから，合同式 (5.1) は成り立たない．　□

定理 5.3 は n が素数であるための必要十分条件を与えているが，その確認のためには左辺の多項式の n 個の係数を別々に計算しなければならず，計算量は n に比例する．

そこで各 b に加えて，別に自然数 r に対して，もし n が素数であれば

$$(X+b)^n \equiv X^n + b \pmod{(n, X^r-1)} \tag{5.2}$$

が成り立つことを利用する．これは n が素数であるための必要条件しか与えないが，これを満たさない r, b があれば n が素数でないと判定できる．しかも計算に必要な多項式の次数は r より小さく，また係数は n より小さいので，もし r が n より十分小さくとれれば高速に計算できる．どの程度の r と b に対して試せば n が素数となるための十分条件を与えるかが重要なポイントになる．

いま

$$\begin{aligned} A &= \{1\} \cup \{a^j \mid a, j \in \{2,3,4,\dots\}\}, \\ \boldsymbol{P}_x &= \{p \mid p \text{ は } x \text{ 以下の素数 }\} \quad (x>0), \\ N &= (n-1)(n^2-1)(n^3-1)\cdots(n^{4\lceil \lg^2 n\rceil -1}-1), \\ r &= N \text{ を割り切らない最小の素数} \end{aligned}$$

とおく．ここで $\lg n = \log_2 n$ は 2 を底とする n の対数，$\lg^2 n = (\lg n)^2$ であり，$\lceil x \rceil$ は $x>0$ の小数点以下を切り上げた値を表す．

アルゴリズム 5.4 (拡張フェルマーテスト XFT)．記号は上の通りとする．

入力 正整数 n.

出力 n が素数でないという判定，または n が素数であるという判定.

手順 (i) $n \in A$ ならば n は素数でないと判定して終了する．

(ii) $\boldsymbol{P}_r$ を含む素数表を計算する．

(iii) 以下を昇順に各素数 p に対して反復する．

（a）もし $n=p$ ならば n は素数であると判定して終了する．

（b）もし $n \equiv 0 \pmod{p}$ ならば n は素数でないと判定して終了する．

（c）もし $N \equiv 0 \pmod{p}$ ならば反復を継続する．そうでなければ $r=p$ として反復を終了する．

(iv) もしある $b \in S = \{1,2,\dots,r\}$ に対して (5.2) が不成立ならば，n は素数でないと判定して終了する．

(v) そうでなければ n は素数であると判定して終了する．

注意 5.5. もし n が偶数ならば，$p=2$ の場合に，$n=2$ のときは手順 (iiia) で，$n>2$ のときは手順 (iii-b) で終了する．手順 (iii-c) に実際に到達するのは奇数 $n>2$ のときで

あり，しかも $p \leq 4\lceil \lg^2 n \rceil$ の場合はフェルマーの小定理により $N \equiv 0 \pmod{p}$ だから反復が継続される．したがって手順 (iv) が実際に実行されるのは，$4\lceil \lg^2 n \rceil < r < n$, n は奇数のときに限る．

注意 5.6. 手順 (ii) で $\boldsymbol{P}_r$ を作成すれば十分であるが，実際には r の具体的上界があればそこまででよい．次の補題 5.9 にある評価に基づけば，素数表 $\boldsymbol{P}_{6.5\lceil \lg^2 n \rceil^{5/2}}$ を作成することになる．この計算は n の入力ごとに必要ではなく，大きい素数表を一度求めておいてそれを何度も再利用すればよい．

注意 5.7. 手順 (iii-c) では，実際に N を計算して p で割るのではなく，合同式 $n^j \equiv 1 \pmod{p}$ $(j = 1, 2, \ldots, 4\lceil \lg^2 n \rceil - 1)$ を順次確認する．

このアルゴリズムの計算量は多項式時間である ($\lg n$ の多項式) ことを次に示す．

テスト (i) の部分の計算量は $\lg n^{1+\varepsilon}$ (ε は任意の正の数) である．実際，$j = 2, \ldots, [\lg n]$ に対して $a = [n^{1/j}]$ が $a^j = n$ を満たすかどうか確かめればよい．

以降の計算量は r の大きさに依存するが，r の評価は後回しにしてとりあえず r と n の式でかく．n 以下の整数の加減乗除の計算量は

$$O(\lg n \lg\lg n \lg\lg\lg n) \tag{5.3}$$

エラトステネスのふるいによる素数表作成 (ii) の繰り返しの回数は

$$\sum_{p \leq r} \left[\frac{r}{p} \right] < r \sum_{p \leq r} \frac{1}{p} = O(r \log\log r)$$

である．改良されたエラトステネスのふるいによる素数表作成 (ii) の計算量は

$$O\left(\frac{r \log r}{\log\log r} \right)$$

となる ([2, Algorithm 3.2.2] を参照)．注意 5.7 によれば試し割り算 (iii)1 回は高々 $O(\lg^2 n)$ 回の法 q, $q \leq r$ の合同式の演算であり，その計算量は (5.3) より $O(\lg r \lg\lg r \lg\lg\lg r)$ だから，全体としての計算量は $O(\pi(r) \lg r \lg\lg r \lg\lg\lg r \lg^2 n)$ である．命題 A.14 より $\pi(r) = O(r/\log r)$ だからこれは

$$O(r \lg\lg r \lg\lg\lg r \lg^2 n)$$

である．最も主要な (iv) の部分については，各 $b \in S$ に対して (5.2) のテストに必要な計算量の評価は次の補題 5.8 で与えられるから，全体として $\#S = r$ 回のテストをする計算量は

$$O(r^2 \lg r \lg^2 n \lg\lg n \lg\lg\lg n) \tag{5.4}$$

で評価され，これがまた拡張フェルマーテスト XFT の計算量でもある．

補題 5.8. 1 回の (5.2) のテストに必要な計算量は

$$O(r \lg r \lg^2 n \lg\lg n \lg\lg\lg n)$$

である．

[証明]　べき乗の計算は反復平方法を用いれば高々 $O(\lg n)$ 回の多項式乗算で十分である．1 回の多項式乗算は高速フーリエ変換による算法を用いれば高々 $O(r \lg r)$ 回の法 n の合同式の演算で済む．1 回の法 n の演算の計算量は (5.3) である．よって補題の主張を得る．□

r の上界を与える．注意 5.5 により $4\lceil \lg^2 n \rceil < r < n$, $n \not\equiv 0 \pmod 2$ のとき，したがって $n \geq 263$ のときに考えればよい．

$$M = \operatorname{lcm}\left\{ n-1, n^2-1, n^3-1, \ldots, n^{4\lceil \lg^2 n \rceil - 1} - 1 \right\}$$

とおけば

$$r = \min\{ p \,|\, p \text{ は } M \text{ を割り切らない素数} \}$$

である．

補題 5.9. 上の仮定と記号の下で

$$r \leq \lceil \lg M \rceil < 6.5 \lceil \lg^2 n \rceil^{5/2}$$

である．

[証明]　補題 A.20 より $k \geq 31$ ならば $\prod_{p \leq k} p > 2^k$ である．そこで $k = \lceil \lg M \rceil$ とおけば，$n \geq 263$ のときは

$$k = \lceil \lg M \rceil \geq \lceil \lg(n^{4\lceil \lg^2 n \rceil - 1} - 1) \rceil \geq \lceil \lg(263^{4\lceil \lg^2 263 \rceil - 1} - 1) \rceil \geq 2083 > 31$$

だから，$\prod_{p \leq k} p > 2^k \geq M$ である．したがってある素数 $p \leq k$ で M を割り切らないものが存在する (そうでないとすると $\prod_{p \leq k} p \leq M$ となるから)．よって $r \leq p \leq k = \lceil \lg M \rceil$ である．また $\ell = \lceil \lg^2 n \rceil$, $m = 4\ell - 1$ とおく．

$$M = \operatorname{lcm}\left\{ n-1, n^2-1, n^3-1, \ldots, n^m - 1 \right\}.$$

各整数 $1 \leq s \leq \lfloor (m+2)/4 \rfloor = \ell$ に対して $4s - 2 = 2(2s-1)$ より

$$n^{4s-2} - 1 = (n^{2s-1} - 1)(n^{2s-1} + 1)$$

となるので，M の定義において $n^{2s-1}-1$ $(1 \le s \le \ell)$ は不要になる．同様に $1 \le s \le [(m+4)/8] = [\ell/2]$ に対して $8s-4 = 2(4s-2)$ より

$$n^{8s-4}-1 = (n^{4s-2}-1)(n^{4s-2}+1)$$

となるので，M の定義 (最小公倍数をとっている) において $n^{4s-2}-1$ $(1 \le s \le [\ell/2])$ は不要になる．したがって

$$\begin{aligned} M &< \prod_{s=1}^{\ell-1}(n^{4s}-1) \prod_{s=[\ell/2]+1}^{\ell}(n^{4s-2}-1) \prod_{s=\ell+1}^{2\ell}(n^{2s-1}-1) \\ &< \prod_{s=1}^{\ell-1} n^{4s} \prod_{s=[\ell/2]+1}^{\ell} n^{4s-2} \prod_{s=\ell+1}^{2\ell} n^{2s-1} \\ &= n^{4\sum_{s=1}^{\ell-1} s} n^{2\sum_{s=[\ell/2]+1}^{\ell}(2s-1)} n^{\sum_{s=\ell+1}^{2\ell}(2s-1)} \\ &= n^{2\ell^2-2\ell} n^{2\ell^2-2[\ell/2]^2} n^{4\ell^2-\ell^2} = n^{7\ell^2-2[\ell/2]^2-2\ell}. \end{aligned}$$

ここで $[\ell/2] > \ell/2-1$ だから

$$7\ell^2-2[\ell/2]^2-2\ell < 7\ell^2-2(\ell/2-1)^2-2\ell = \frac{13\ell^2}{2}-2.$$

したがって

$$\begin{aligned} \lg M &< (6.5\ell^2-2)\lg n, \\ \lceil \lg M \rceil &\le \lg M + 1 < (6.5\ell^2-2)\lg n + 1 \le 6.5\ell^2 \lg n \\ &= 6.5\lceil \lg^2 n \rceil^2 ((\lg n)^2)^{1/2} \le 6.5\lceil \lg^2 n \rceil^{5/2}. \end{aligned}$$

□

以上により (5.4) から

定理 5.10. 拡張フェルマーテスト XFT の計算量は

$$O(\lg^{12} n \lg^2 \lg n \lg\lg\lg n)$$

である．

拡張フェルマーテスト XFT が素数判定の正しいアルゴリズムであることを示す．次の定理がその根拠となる．

定理 5.11. いま整数 $n > 1$ に対して，正整数 r と有限集合 $S \subset \mathbb{Z}$ が以下の条件 (i)–(iv) を満たすとする．

(i) $\gcd(n, r) = 1$.

(ii) すべての正整数 q, $\varphi(r)/m \equiv 0 \pmod{q}$ に対して

$$\binom{\#S + \varphi(r) - 1}{\#S} \geq n^{2q[(\varphi(r)/q)^{1/2}]}.$$

ただし $\varphi(r) = \#(\mathbb{Z}/r\mathbb{Z})^\times$, $m = \#\langle n \bmod r \rangle$ である．

(iii) すべての $a, b \in S$, $a > b$ に対して $\gcd(a - b, n) = 1$.

(iv) すべての $b \in S$ に対して (5.2) が成立する．

このときある素数 p と正整数 w があり $n = p^w$，すなわち n は素数べきである．

この定理の証明は後回しにして，先に拡張フェルマーテスト XFT が正しいアルゴリズムであることを証明する．

定理 5.12. 拡張フェルマーテスト XFT は素数判定の正しいアルゴリズムである．

[証明]　まず，手順 (v) 以外の結論が正しいことは明らかである．手順 (v) が正しいことを示す．手順 (iii) では小さい素数 p から順に計算しているから，手順 (iii-c) で求めた r 以下の n の素因数はなく，定理 5.11 の条件 (i) は満たされる (もし $\gcd(n, r) > 1$ とすると素数 p で $p|n$, $p|r$ となるものがあるが，$p < r$ となることはないから $p = r$, $p|n$ となる．これはすでに (iii-a) か (iii-b) で終了している)．また，手順 (iv) で定めた S の相異なる 2 つの元の差は r より小さいから同様に定理 5.11 の条件 (iii) も満たされる．さらに，注意 5.5 から $r > 2$ であり，また $n \bmod r$ の位数 m は $4\lceil \lg^2 n \rceil - 1$ よりも大きいから

$$q \leq m^{-1}\varphi(r), \quad m \geq 4\lceil \lg^2 n \rceil \geq (2 \lg n)^2$$

である．したがって

$$\begin{aligned} n^{2q[(\varphi(r)/q)^{1/2}]} &\leq n^{2q^{1/2}\varphi(r)^{1/2}} \leq n^{2m^{-1/2}\varphi(r)} \leq n^{(\lg n)^{-1}\varphi(r)} \\ &= (e^{\log n})^{(\varphi(r) \log 2/\log n)} = e^{\varphi(r)\log 2} = 2^{\varphi(r)} = 2^{r-1} \end{aligned}$$

である．一方，r に関する帰納法により

$$\binom{\#S + \varphi(r) - 1}{\#S} = \binom{2r-2}{r} \geq 2^{r-1}$$

が示される．実際，$r = 3$ のときは $\binom{2\cdot 3-2}{3} = \binom{4}{3} = 4 = 2^{3-1}$ である．$r \geq 3$ として $\binom{2r-2}{r} \geq 2^{r-1}$ が成り立つとすれば

$$\binom{2r}{r+1} = \frac{(2r)(2r-1)(2r-2)!}{(r+1)(r-1)r!(r-2)!} = \frac{2r(2r-1)}{(r^2-1)}\binom{2r-2}{r} \geq \frac{2r(2r-1)}{r^2-1}2^{r-1}.$$

ここで $r \geq 3$ に対して

$$r(2r-1) - (r^2-1) = r^2 - r + 1 > 0$$

だから，$\binom{2r}{r+1} > 2^r$ となる．したがって

$$\binom{\#S + \varphi(r) - 1}{\#S} = \binom{2r-2}{r} \geq 2^{r-1} \geq n^{2q[(\varphi(r)/q)^{1/2}]}$$

となり，定理 5.11 の条件 (ii) も満たされる．したがって手順 (iv) を通過した n に関しては必然的に定理 5.11 の条件 (iv) も満たす．定理 5.11 によって n は素数べきとなる．手順 (i) により n は素数である． □

残されているのは定理 5.11 を証明することである．

[定理 5.11 の証明] $n \equiv 0 \pmod{p}$ となる素数 p を 1 つとる．I, J, K を次のように定める．

$$\begin{aligned}
I &= \left\{ p^i n^j \,\middle|\, i, j \in \{0\} \cup \mathbb{N} \right\} \subset \mathbb{N}, \\
J &= \left\{ \prod_{b \in S} (X+b)^{k_b} \bmod p \,\middle|\, k_b \in \{0\} \cup \mathbb{N} \ \ (b \in S) \right\} \subset \mathbb{Z}[X], \\
K &= \left\{ f(X^t) \,\middle|\, f \in J,\ t \in \mathbb{N},\ \gcd(t, r) = 1 \right\} \subset \mathbb{Z}[X].
\end{aligned}$$

拡張フェルマー小定理 (5.1) と条件 (iv) により，すべての $b \in S$ に対して

$$\begin{aligned}
(X+b)^p &\equiv X^p + b \pmod{p}, \\
(X+b)^n &\equiv X^n + b \pmod{(n, X^r - 1)}
\end{aligned}$$

が成り立つ．$n \equiv 0 \pmod{p}$ だから

$$(X+b)^n \equiv X^n + b \pmod{(p, X^r - 1)}$$

が成り立つ．帰納的に $i, j = 0, 1, 2, \ldots$ に対して次がが成り立つ．

$$\begin{aligned}
(X+b)^{p^i} &\equiv X^{p^i} + b \pmod{p}, \\
(X+b)^{n^j} &\equiv X^{n^j} + b \pmod{(p, X^r - 1)}.
\end{aligned}$$

前者については明らか．後者については $(X+b)^{n^j} \equiv X^{n^j} + b \pmod{(p, X^r - 1)}$ が成り立つとすれば，X に X^n を代入すれば

$$(X^n + b)^{n^j} \equiv X^{n^{j+1}} + b \pmod{(p, X^{nr} - 1)}$$

であり，$X^{nr}-1 \in (X^r-1)\mathbb{Z}[X]$ だから $(X^n+b)^{n^j} \equiv X^{n^{j+1}}+b \pmod{(p, X^r-1)}$ である．さらに $(X+b)^n \equiv X^n+b \pmod{(p, X^r-1)}$ だから

$$(X+b)^{n^{j+1}} \equiv (X^n+b)^{n^j} \equiv X^{n^{j+1}}+b \pmod{(p, X^r-1)}$$

となる．$(X+b)^{n^j} \equiv X^{n^j}+b \pmod{(p, X^r-1)}$ において X に X^{p^i} を代入すれば

$$(X^{p^i}+b)^{n^j} \equiv X^{p^i n^j}+b \pmod{(p, X^{p^i r}-1)},$$

したがって

$$(X^{p^i}+b)^{n^j} \equiv X^{p^i n^j}+b \pmod{(p, X^r-1)}$$

である．$(X+b)^{p^i} \equiv X^{p^i}+b \pmod{p}$ だからこの両辺を n^j 乗すれば

$$(X+b)^{p^i n^j} \equiv (X^{p^i}+b)^{n^j} \pmod{p},$$

したがって

$$(X+b)^{p^i n^j} \equiv (X^{p^i}+b)^{n^j} \equiv X^{p^i n^j}+b \pmod{(p, X^r-1)}$$

が成り立つ．$s \in I$, $f \in K$ とすれば $s = p^i n^j$, $i, j \in \{0\} \cup \mathbb{N}$，$f(X) = f_1(X^t)$, $f_1 \in J$, $t \in \mathbb{N}$, $\gcd(t, r) = 1$ とかける．$f_1(X) \equiv \prod_{b \in S}(X+b)^{k_b} \pmod{p}$, $k_b \in \{0\} \cup \mathbb{N}$ の形である．したがって

$$\begin{aligned} f(X^s) = f(X^{p^i n^j}) = f_1(X^{t p^i n^j}) &\equiv \prod_{b \in S}(X^{t p^i n^j}+b)^{k_b} \\ &\equiv \prod_{b \in S}(X^t+b)^{p^i n^j k_b} \equiv f(X)^s \pmod{(p, X^r-1)} \end{aligned}$$

が成り立つ．そこでモニック多項式 $h \in \mathbb{Z}[X]$ を $h \bmod p \in (\mathbb{Z}/p\mathbb{Z})[X]$ が 1 の原始 r 乗根の最小多項式であるようにとり固定する．$h \bmod p = 0$ の根で生成される有限体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ の拡大体の乗法群は位数 $p^{\deg h}-1$ の巡回群だから，$p^{\deg h} \equiv 1 \pmod{r}$ であり，$\deg h$ は $m_1 = \#\langle p \bmod r \rangle$ の倍数である．$\mathbb{F}_p$ の m_1 次拡大体の乗法群は位数 $p^{m_1}-1$ の巡回群であり，$r | (p^{m_1}-1)$ だから 1 の原始 r 乗根を含む．よって $\deg h$ は m_1 の約数である．ゆえに $\deg h = m_1 = \#\langle p \bmod r \rangle$ である．1 の原始 r 乗根は X^r-1 の根だから，$X^r-1 \bmod p$ は $h \bmod p$ で割り切れる．したがって

$$f(X^s) \equiv f(X)^s \pmod{(p, h)} \qquad (s \in I,\ f \in K) \tag{5.5}$$

となる．条件 (i) より乗法群 $(\mathbb{Z}/r\mathbb{Z})^\times$ の部分群

$$G = \langle p \bmod r, n \bmod r \rangle$$

を考える．自然な写像 $\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$ による I の像を $I \bmod r$ で表せば，$G = I \bmod r$ である．$q = ((\mathbb{Z}/r\mathbb{Z})^\times : G)$ とおく．$(\mathbb{Z}/r\mathbb{Z})^\times/G$ の完全代表系 $T \subset \mathbb{N}$ を 1 つとる．

$$(\mathbb{Z}/r\mathbb{Z})^\times/G = \{(t \bmod r)G \,|\, t \in T\}, \qquad |T| = q.$$

さらに (5.5) に注意して，$\mathbb{Z}[X]/(p,h)$ ($\mathbb{F}_p$ の $\deg h$ 次の拡大体) の部分集合で

$$\{0\} \cup \{X^t + b \bmod (p,h) \,|\, b \in S,\ t \in T\}$$

によって乗法的に生成されるものを H とする．$\#H$ を下から評価する．まず条件 (iii) より 1 次既約式 $X + b \bmod p$ $(b \in S)$ はすべて相異なる．したがって自然な写像 $\mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ の J への制限は単射である．次に

$$L = \{0\} \cup \{e \in J \,|\, \deg e < \varphi(r)\}$$

とおくとき，$f, g \in L$ については，もしすべての $t \in \mathbb{N}$, $\gcd(t,r) = 1$ に対して

$$f(X^t) \equiv g(X^t) \pmod{(p,h)}$$

ならば，$f, g \in L$ より $f - g \bmod p \in (\mathbb{Z}/p\mathbb{Z})[X]$ は次数が $\varphi(r)$ より小さい多項式であり，$\gcd(t,r) = 1$ だから $\varphi(r)$ 個の 1 の原始 r 乗根をすべて根にもつ．これは $f - g \bmod p$ が恒等的に 0 であることを意味する．以上をまとめると

$$\begin{aligned} f \neq g &\iff f \not\equiv g \pmod{p} \\ &\iff f(X^t) \not\equiv g(X^t) \pmod{(p,h)} \quad (\text{ある } t \in \mathbb{N},\ \gcd(t,r) = 1 \text{ について}) \end{aligned}$$

となる．(5.5) より $s \in I$, $f, g \in L \subset J \subset K$ に対して $f(X^{ts}) \equiv f(X^t)^s \pmod{(p,h)}$, $g(X^{ts}) \equiv g(X^t)^s \pmod{(p,h)}$ が成り立つから，t に対して，$t_1 \in T$ と $s \in I$ が存在して $t \equiv t_1 s \pmod{r}$ となるものをとれば，$f(X^t) \equiv f(X^{t_1 s}) \equiv f(X^{t_1})^s \pmod{(p,h)}$, $g(X^t) \equiv g(X^{t_1 s}) \equiv g(X^{t_1})^s \pmod{(p,h)}$ となる．これから

$$\begin{aligned} &f(X^t) \not\equiv g(X^t) \pmod{(p,h)} \quad (\text{ある } t \in \mathbb{N},\ \gcd(t,r) = 1 \text{ について}) \\ \iff &f(X^{t_1}) \not\equiv g(X^{t_1}) \pmod{(p,h)} \quad (\text{ある } t_1 \in T \text{ について}) \end{aligned}$$

となる．よって

$$f \neq g \iff f(X^t) \not\equiv g(X^t) \pmod{(p,h)} \quad (\text{ある } t \in T \text{ について})$$

が成り立つ．したがって $T = \{t_1, \ldots, t_q\}$ として集合 L から $H^q = \overbrace{H \times \cdots \times H}^{q}$ への写像

$$f \longmapsto (f(X^{t_1}) \bmod (p,h), \ldots, f(X^{t_q}) \bmod (p,h))$$

を考えれば，これは単射となる．ゆえに条件 (ii) より

$$(\#H)^q \geq \#L = 1 + \binom{\#S + \varphi(r) - 1}{\#S} > n^{2cq}, \quad c = [(\varphi(r)/q)^{1/2}],$$

すなわち $\#H > n^{2c}$ を得る．$c = [(\varphi(r)/q)^{1/2}]$ だから

$$(\varphi(r)/q)^{1/2} < c + 1, \quad \#G = \frac{\varphi(r)}{q} < (c+1)^2$$

である．したがって写像

$$\{0, 1, \ldots, c\}^2 \longrightarrow G, \quad (i, j) \longmapsto p^i n^j \bmod r$$

は単射ではない．よって c 以下の非負整数の異なる 2 つの組 (i, j) と (k, ℓ) で $p^i n^j \equiv p^k n^\ell \pmod{r}$ となるものが存在する．このとき $u = p^i n^j$, $v = p^k n^\ell$ とおけば，$p|n$ だから

$$1 + |u - v| \leq 1 + p^c n^c - 1 = p^c n^c \leq n^{2c} < \#H$$

となる．$u, v \in I$ だから $f \in H$ に対して (5.5) より $f(X^u) \equiv f(X)^u \pmod{(p, h)}$, $f(X^v) \equiv f(X)^v \pmod{(p, h)}$ が成り立つ．また $u \equiv v \pmod{r}$ だから $X^u \equiv X^v \pmod{(p, h)}$ である．よって

$$f(X)^u \equiv f(X^u) \equiv f(X^v) \equiv f(X)^v \pmod{(p, h)}$$

である．$H \subset (\mathbb{Z}[X]/(p, h))$ だから，これは変数 Y の多項式 $Y^u - Y^v$ が有限体 $\mathbb{Z}[X]/(p, h)$ において $\#H$ 個以上の相異なる根をもつことを示している．ここでもし $u \neq v$ とすると，$u > v$ としもよく，このとき多項式

$$Y^u - Y^v = Y^v(Y^{u-v} - 1)$$

の有限体 $\mathbb{Z}[X]/(p, h)$ における根の個数は高々 $1 + u - v = 1 + |u - v| + < \#H$ だから，これは矛盾である．ゆえに $u = v$ でなければならない．すなわち $p^i n^j = p^k n^\ell$ である．もし $j = \ell$ ならば $i = k$ となって $(i, j) \neq (k, \ell)$ に矛盾する．よって $j \neq \ell$ である．このとき $n^{j-\ell} = p^{k-i}$ となるから，n は素数 p のべきである． □

A　素数の個数の評価

正の実数 x に対して，

$$\pi(x) = (x \text{ 以下の素数の個数})$$

とする．例えば 10 以下の素数は $2,3,5,7$ だから $\pi(10) = 4$ であり，20 以下の素数は $2,3,5,7,11,13,17,19$ だから $\pi(20) = 8$ である．$\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10000) = 1229$ となる．x を大きくしていくとき $\pi(x)$ はどうなるだろうか？素数定理とよばれる次の定理はガウスによって予想され，1896 年にプーサンとアダマールによって独立に証明された．

定理 A.1 (素数定理)**.** $\log x$ を自然対数 (底 $e = 2.718281\ldots$ の対数) とすれば

$$\pi(x) \sim \frac{x}{\log(x)} \quad (x \to \infty)$$

が成り立つ．ここで $f(x) \sim g(x)$ $(x \to \infty)$ とは，$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ を意味する．

定理 A.1 の定理は簡単ではない．そこで初等的に素数の個数 $\pi(x)$ を評価してみる．以下は小山 [4] を参考にした．まず対数関数の大きさを評価する．

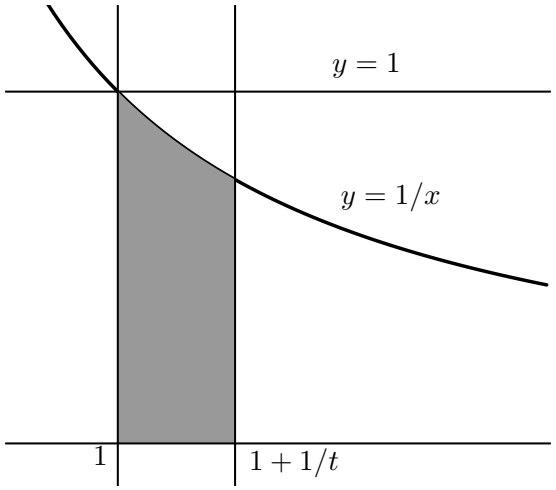

図 1　$y = 1/x$ のグラフで囲まれる図形の面積

補題 A.2. $t > 0$ に対して次の不等式が成り立つ．

$$\log\left(1 + \frac{1}{t}\right) = \int_1^{1+1/t} \frac{1}{x}\, dx < \frac{1}{t}.$$

[証明]　図 1 において $y = 1/x$ のグラフと $x = 1$, $x = 1 + 1/t$ で囲まれた図形の面積は縦の長さが 1 で横の長さが $1/t$ の長方形の面積よりも明らかに小さい．　□

自然数 n に対して 1 から n までの自然数の積を $n!$ で表す．$n!$ を n の**階乗**とよぶ．$n!$ を素因数分解してみよう．素数 p が $n!$ を割り切るならば $p \le n$ であり，逆に $p \le n$ なら

ば p は $n!$ を割り切る．p を $p \leq n$ なる素数とする．$n!$ が p^a で丁度割り切れるとする．そのような a を $a = e(p,n)$ とかく．$e(p,n)$ を求めるために，**ガウス記号**を定義する．

定義 A.3. 実数 x に対して x を越えない最大の整数を $[x]$ で表す．

$$[x] \leq x < [x] + 1.$$

補題 A.4. 任意の実数 x, y に対して $[x+y]$ は $[x]+[y]$ または $[x]+[y]+1$ である．

[証明]　$x = [x] + x_1$, $y = [y] + y_1$, $0 \leq x_1 < 1$, $0 \leq y_1 < 1$ とかける．このとき

$$[x] + [y] \leq [x] + [y] + x_1 + y_1 = x + y < [x] + [y] + 2$$

だから，$0 \leq x_1 + y_1 < 1$ ならば $[x+y] = [x] + [y]$ であり，$1 \leq x_1 + y_1 < 2$ ならば $[x+y] = [x] + [y] + 1$ である． □

補題 A.5. $n!$ の素因数分解を $n! = \prod_{p \leq n} p^{e(p,n)}$ とすれば，

$$e(p,n) = \sum_{r=1}^{\left[\frac{\log(n)}{\log(p)}\right]} \left[\frac{n}{p^r}\right] = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right].$$

[証明]

$$\begin{aligned} e(p,n) &= \sum_{\substack{r \geq 1 \\ p^r \leq n}} r\#\{1 \leq a \leq n \,|\, a \text{ は丁度 } p^r \text{ で割りきれる }\} \\ &= \sum_{r=1}^{\left[\frac{\log(n)}{\log(p)}\right]} r\left(\left[\frac{n}{p^r}\right] - \left[\frac{n}{p^{r+1}}\right]\right) = \sum_{r=1}^{\left[\frac{\log(n)}{\log(p)}\right]} r\left[\frac{n}{p^r}\right] - \sum_{r=1}^{\left[\frac{\log(n)}{\log(p)}\right]-1} r\left[\frac{n}{p^{r+1}}\right] \\ &= \sum_{r=1}^{\left[\frac{\log(n)}{\log(p)}\right]} r\left[\frac{n}{p^r}\right] - \sum_{r=1}^{\left[\frac{\log(n)}{\log(p)}\right]} (r-1)\left[\frac{n}{p^r}\right] = \sum_{r=1}^{\left[\frac{\log(n)}{\log(p)}\right]} \left[\frac{n}{p^r}\right]. \end{aligned}$$

□

次に整数 $1 \leq k \leq n$ に対して **2 項係数** $\binom{n}{k}$ を

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{(n-k)!k!}$$

によって定義する．また $\binom{n}{0} = 1$ とする．2 項係数は $1 \leq k \leq n$ について

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \tag{A.1}$$

を満たす．実際，

$$\binom{n}{k-1}+\binom{n}{k}=\frac{n!}{(k-1)!(n-k+1)!}+\frac{n!}{k!(n-k)!}=\frac{n!(k+n-k+1)}{k!(n-k+1)!}$$
$$=\frac{(n+1)!}{k!(n+1-k)!}=\binom{n+1}{k}.$$

(A.1) を用いれば次を示せる．

補題 A.6 (2 項定理)**.**

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

[証明]　$n=1$ のときは明らか．

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

が成り立つとすると (A.1) より

$$\begin{aligned}(a+b)^{n+1}&=(a+b)(a+b)^n=(a+b)\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k\\&=\sum_{k=0}^{n}\binom{n}{k}a^{n-k+1}b^k+\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1}\\&=\sum_{k=0}^{n}\binom{n}{k}a^{n-k+1}b^k+\sum_{k=1}^{n+1}a^{n-k+1}b^k\\&=a^{n+1}+\sum_{k=1}^{n}\left(\binom{n}{k-1}+\binom{n}{k}\right)a^{n-k+1}b^k+b^{n+1}\\&=a^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}a^{n-k+1}b^k+b^{n+1}=\sum_{k=0}^{n+1}\binom{n+1}{k}a^{n-k+1}b^k.\end{aligned}$$

よって $n+1$ のときも成り立つ．　□

系 A.7. $0\le k\le n$ に対して 2 項係数 $\binom{n}{k}$ は整数である．

$\pi(n)$ を下から評価する．そのために自然数 n に対して

$$b_n=\binom{2n}{n}=\frac{(2n)!}{(n!)^2}$$

とおく．まず b_n の大きさについて次が成り立つ．

補題 A.8. $n \geq 4$ に対して $b_n \geq \dfrac{2^{2n}}{n}$.

[証明]　帰納法による．$n = 4$ のとき，$b_4 = 70 > 64 = \dfrac{2^8}{4}$ である．$n \geq 4$ について補題の不等式が成り立つとする．このとき

$$b_{n+1} = \frac{(2n+2)!}{(n+1)!^2} = \frac{(2n+2)(2n+1)(2n)!}{(n+1)^2(n!)^2} = \frac{2(2n+1)}{(n+1)} b_n > \frac{4n}{(n+1)} b_n$$

だから帰納法の仮定によって

$$b_{n+1} = \frac{4n}{(n+1)} b_n > \frac{4n}{(n+1)} \cdot \frac{2^{2n}}{n} = \frac{2^{2(n+1)}}{n+1}.$$

したがって $n+1$ に対しても主張は正しい．帰納法によって 4 以上のすべての自然数 n に対して補題の不等式が成り立つ．　□

補題 A.9. 任意の $n \geq 1$ に対して $b_n \leq (2n)^{\pi(2n)}$.

[証明]　$b_n = (2n)!/(n!)^2$ だから補題 A.5 より

$$b_n = \prod_{p \leq 2n} p^{e(p,2n) - 2e(p,n)},$$

$$e(p,2n) - 2e(p,n) = \sum_{r=1}^{\left[\frac{\log(2n)}{\log(p)}\right]} \left[\frac{2n}{p^r}\right] - 2 \sum_{r=1}^{\left[\frac{\log(2n)}{\log(p)}\right]} \left[\frac{n}{p^r}\right] = \sum_{r=1}^{\left[\frac{\log(2n)}{\log(p)}\right]} \left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right] \right).$$

補題 A.4 より

$$\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \leq 1$$

だから

$$e(p,2n) - 2e(p,n) \leq \sum_{k=1}^{\left[\frac{\log(2n)}{\log(p)}\right]} 1 = \left[\frac{\log(2n)}{\log(p)}\right].$$

したがって

$$\begin{aligned} \log(b_n) &= \sum_{p \leq 2n} (e(p,2n) - 2e(p,n)) \log(p) \leq \sum_{p \leq 2n} \left[\frac{\log(2n)}{\log(p)}\right] \log(p) \\ &\leq \sum_{p \leq 2n} \frac{\log(2n)}{\log(p)} \cdot \log(p) = \sum_{p \leq 2n} \log(2n) = \pi(2n) \log(2n) \\ &= \log\left((2n)^{\pi(2n)} \right). \end{aligned}$$

ゆえに $b_n \leq (2n)^{\pi(2n)}$ である． □

$n \geq 4$ とする．補題 A.8 と補題 A.9 より

$$\frac{2^{2n}}{n} < b_n \leq (2n)^{\pi(2n)}.$$

したがって

$$\begin{aligned} 2n\log(2) - \log(n) &< \pi(2n)\log(2n), \\ \pi(2n) &> \log(2)\frac{2n}{\log(2n)} - \frac{\log(2n) - \log(2)}{\log(2n)} \\ &= \log(2)\frac{2n+1}{\log(2n)} - 1. \end{aligned} \tag{A.2}$$

$n \geq 4$ より $2n$ は素数でないから $\pi(2n) = \pi(2n-1)$ である．したがって

$$\begin{aligned} \pi(2n-1) = \pi(2n) &\geq \log(2)\frac{2n+1}{\log(2n)} - 1 \\ &= \log(2)\frac{2n}{\log(2n-1)} \cdot \frac{(2n+1)\log(2n-1)}{2n\log(2n)} - 1. \end{aligned}$$

ここで

$$\begin{aligned} (2n+1)\log(2n-1) - 2n\log(2n) &= \log(2n-1) - 2n(\log(2n) - \log(2n-1)) \\ &= \log(2n-1) - 2n\log\left(\frac{2n}{2n-1}\right) \\ &= \log(2n-1) - 2n\log\left(1 + \frac{1}{2n-1}\right). \end{aligned}$$

ここで補題 A.2 より $\log\left(1 + \frac{1}{2n-1}\right) < \frac{1}{2n-1}$ だから

$$\begin{aligned} (2n+1)\log(2n-1) - 2n\log(2n) &> \log(2n-1) - 2n \cdot \frac{1}{2n-1} \\ &= \log(2n-1) - \frac{8}{7} \geq \log(7) - \frac{8}{7} = 0.803\cdots > 0. \end{aligned}$$

よって $(2n+1)\log(2n-1) > 2n\log(2n)$, $\dfrac{(2n+1)\log(2n-1)}{2n\log(2n)} > 1$ である．したがって

$$\pi(2n-1) \geq \log(2)\frac{2n}{\log(2n-1)} - 1. \tag{A.3}$$

(A.2) と (A.3) より任意の $n \geq 7$ に対して

$$\pi(n) \geq \log(2)\frac{n+1}{\log(n)} - 1$$

が成り立つ．これは $n = 3, 4, 5, 6$ のときも成り立つ．$x \geq 3$ とすれば

$$\pi(x) = \pi([x]) \geq \log(2)\frac{[x]+1}{\log([x])} - 1 \geq \log(2)\frac{x}{\log(x)} - 1. \tag{A.4}$$

次に $\pi(n)$ を上から評価する．そのために

$$c_n = \binom{2n+1}{n} = \frac{(2n+1)!}{(n+1)!n!}$$

とおく．c_n の大きさについて次が成り立つ．

補題 A.10. $n \geq 1$ に対して $c_n < 2^{2n}$.

[証明]　補題 A.6 より

$$2^{2n+1} = (1+1)^{2n+1} = \sum_{k=0}^{2n+1}\binom{2n+1}{k} > \binom{2n+1}{n} + \binom{2n+1}{n+1} = 2\binom{2n+1}{n}.$$

よって $\binom{2n+1}{n} < 2^{2n+1}/2 = 2^{2n}$ である． □

補題 A.11. $n \geq 1$ に対して $c_n \geq \displaystyle\prod_{n+1<p\leq 2n+1} p$.

[証明]

$$c_n = \frac{(2n+1)!}{(n+1)!n!} = \frac{(2n+1)(2n)\cdots(n+2)(n+1)!}{(n+1)!n!} = \frac{(2n+1)(2n)\cdots(n+2)}{n!}$$

より，p が $n+1 < p \leq 2n+1$ を満たす素数ならば c_n は p で割り切れる．したがって c_n は $\prod_{n+1<p\leq 2n+1} p$ で割り切れる．よって $c_n \geq \prod_{n+1<p\leq 2n+1} p$. □

補題 A.10 と補題 A.11 から，任意の自然数 n に対して

$$\prod_{n+1<p\leq 2n+1} p \leq c_n < 2^{2n}$$

が成り立つ．したがって

$$\sum_{n+1<p\leq 2n+1} \log(p) < 2n\log(2).$$

ここで実数 $x \geq 1$ に対して

$$\theta(x) = \sum_{p\leq x}\log(p) \tag{A.5}$$

とおけば，任意の自然数 n に対して，

$$\theta(2n+1) - \theta(n+1) < 2n\log(2). \tag{A.6}$$

が成り立つ．

命題 A.12. $n \geq 1$ に対して

$$\theta(n) < 2n\log(2).$$

[証明]　$\theta(1) = 0 < 2\log(2)$, $\theta(2) = \log(2) < 4\log(2)$ だから，$n = 1, 2$ のときは命題の不等式は成り立つ．$m \geq 1$ として $n \leq 2m$ に対して，命題の不等式が成り立つとする．このとき (A.6) と帰納法の仮定から

$$\begin{aligned}\theta(2m+1) &< \theta(m+1) + 2m\log(2) < 2(m+1)\log(2) + 2m\log(2) \\ &= 2(2m+1)\log(2).\end{aligned}$$

よって $n = 2m+1$ のときも命題の不等式は成り立つ．さらに $n = 2m+2$ のときは，n は素数でないから

$$\theta(2m+2) = \theta(2m+1) < 2(2m+1)\log(2) < 2(2m+2)\log(2)$$

であり，$n = 2m+2$ のときも命題の不等式は成り立つ．帰納法によってすべての自然数 n に対して命題の不等式は成り立つ．□

系 A.13.

$$\theta(x) < 2x\log(2) \quad (x \geq 1).$$

[証明]　命題 A.12 より

$$\theta(x) = \theta([x]) < 2[x]\log(2) \leq 2x\log(2).$$

□

これを用いて $\pi(x)$ の上からの評価を導く．

$$\begin{aligned}\theta(x) &= \sum_{p \leq x} \log(p) = \sum_{p \leq x^{1/2}} \log(p) + \sum_{x^{1/2} < p \leq x} \log(p) \\ &\geq \sum_{x^{1/2} < p \leq x} \log(x^{1/2}) = \frac{1}{2}\log(x)\left(\pi(x) - \pi(x^{1/2})\right)\end{aligned}$$

したがって系 A.13 と自明な評価 $\pi(x^{1/2}) \leq x^{1/2}$ より

$$\pi(x)\log(x) \leq 2\theta(x) + \pi(x^{1/2})\log(x) < 4x\log(2) + x^{1/2}\log(x).$$

これから

$$\frac{\pi(x)\log(x)}{x} < 4\log(2) + \frac{\log(x)}{x^{1/2}} = 4\log(2) + 2\frac{\log(x^{1/2})}{x^{1/2}}.$$

関数 $\log(x)/x$ は $x = e$ で最大値 $1/e$ をとり $x \geq e$ では単調減少である．したがって $x \geq 2^{10} = 1024$ ならば，$x^{1/2} \geq 2^5 = 32$ だから

$$\frac{\pi(x)\log(x)}{x} < 4\log(2) + 2\frac{\log(2^5)}{2^5} = 4\log(2) + 5\frac{\log(2)}{2^4} = \frac{69}{16}\log(2) = 2.9891\cdots < 3.$$

一方，$3 \leq x < 1024$ に対して $n \leq x < n+1$, $n \in \mathbb{Z}$, $2 \leq n \leq 1023$ とかけて，$\pi(x) = \pi(n)$, $\log(x)/x \leq \log(n)/n$ だから

$$\frac{\pi(x)\log(x)}{x} \leq \frac{\pi(n)\log(n)}{n}$$

である．この右辺はすべての整数 $3 \leq n \leq 1023$ に対して 3 以下 (実際，1.2551 以下) であることがコンピュータにより確かめられる．よってすべての実数 $x \geq 3$ に対して

$$\pi(x) \leq \frac{3x}{\log(x)}$$

が成り立つ．$2 \leq x \leq 3$ のとき，

$$\frac{3x}{\log(x)} \geq \frac{6}{\log(3)} = 5.461\cdots > 2 = \pi(3) \geq \pi(x)$$

だからすべての $x \geq 2$ に対して

$$\pi(x) \leq \frac{3x}{\log(x)}$$

が成り立つ．これと (A.4) より次を得た．

命題 A.14. $x \geq 3$ に対して

$$\log(2)\frac{x}{\log(x)} - 1 \leq \pi(x) \leq 3\frac{x}{\log(x)}$$

が成り立つ．

系 A.15. $x \geq 3$ に対して

$$\theta(x) \geq \frac{\log(2)}{2}x - \frac{1}{2}\log(x) - 3x^{1/2}.$$

[証明]　(A.4) より

$$\begin{aligned}\theta(x) &= \sum_{p\le x}\log(p) \ge \sum_{x^{1/2}<p\le x}\log(p)\\ &\ge \sum_{x^{1/2}<p\le x}\log(x^{1/2}) = \frac{1}{2}\log(x)\sum_{x^{1/2}<p\le x}1\\ &= \frac{1}{2}\log(x)\big(\pi(x)-\pi(x^{1/2})\big).\end{aligned}$$

命題 A.14 より

$$\begin{aligned}\pi(x) &\ge \log(2)\frac{x}{\log(x)} - 1,\\ \pi(x^{1/2}) &\le 3\frac{x^{1/2}}{\log(x^{1/2})} = \frac{6x^{1/2}}{\log(x)}.\end{aligned}$$

したがって

$$\begin{aligned}\theta(x) &\ge \frac{1}{2}\log(x)\left(\log(2)\frac{x}{\log(x)} - 1\right) - \frac{1}{2}\log(x)\frac{6x^{1/2}}{\log(x)}\\ &= \frac{\log(2)}{2}x - \frac{1}{2}\log(x) - 3x^{1/2}.\end{aligned}$$

□

正整数 n に対して C_n を

$$C_n = \frac{(6n)!n!}{(3n)!(2n)!(2n)!}$$

によって定義する.

補題 A.16. C_n は整数である.

[証明]　p を $3n$ 以下の素数とする．補題 A.5 より C_n の分母を割る p のべき $e(p,3n)+2e(p,2n)$ と分子の p のべき $e(p,6n)+e(p,n)$ は

$$\begin{aligned}e(p,3n)+2e(p,2n) &= \sum_{k=1}^{\infty}\left[\frac{3n}{p^k}\right] + 2\sum_{k=1}^{\infty}\left[\frac{2n}{p^k}\right],\\ e(p,6n)+e(p,n) &= \sum_{k=1}^{\infty}\left[\frac{6n}{p^k}\right] + \sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]\end{aligned}$$

で与えられる．$n/p^k = a + x$, $a \in \mathbb{Z}$, $0 \le x < 1$ とかくとき

$$\left[\frac{3n}{p^k}\right] + 2\left[\frac{2n}{p^k}\right] = \begin{cases} 7a, & 0 \le x < \frac{1}{3}, \\ 7a+1, & \frac{1}{3} \le x < \frac{1}{2}, \\ 7a+3, & \frac{1}{2} \le x < \frac{2}{3}, \\ 7a+4, & \frac{2}{3} \le x < 1, \end{cases}$$

$$\left[\frac{6n}{p^k}\right] + \left[\frac{n}{p^k}\right] = \begin{cases} 7a, & 0 \le x < \frac{1}{6}, \\ 7a+1, & \frac{1}{6} \le x < \frac{1}{3}, \\ 7a+2, & \frac{1}{3} \le x < \frac{1}{2}, \\ 7a+3, & \frac{1}{2} \le x < \frac{2}{3}, \\ 7a+4, & \frac{2}{3} \le x < \frac{5}{6}, \\ 7a+5, & \frac{5}{6} \le x < 1 \end{cases}$$

となるから，いずれの場合も

$$\left[\frac{3n}{p^k}\right] + 2\left[\frac{2n}{p^k}\right] \le \left[\frac{6n}{p^k}\right] + \left[\frac{n}{p^k}\right] \le \left[\frac{3n}{p^k}\right] + 2\left[\frac{2n}{p^k}\right] + 1 \tag{A.7}$$

が成り立つ．したがって $e(p,3n) + 2e(p,2n) \le e(p,6n) + e(p,n)$ が成り立ち，C_n は整数である． □

補題 A.17. 素数 p が $p > (6n)^{1/k}$ を満たせば，p^k は C_n を割り切らない．

[証明] $p > (6n)^{1/k}$ ならば $6n/p^k < 1$ となるから補題 A.16 の証明で示した (A.7) により

$$\begin{aligned} &e(p,6n) + e(p,n) - e(p,3n) - 2e(p,2n) \\ &= \sum_{j=1}^{\infty} \left(\left[\frac{6n}{p^j}\right] + \left[\frac{n}{p^j}\right] - \left[\frac{3n}{p^j}\right] - 2\left[\frac{2n}{p^j}\right] \right) \\ &= \sum_{j=1}^{k-1} \left(\left[\frac{6n}{p^j}\right] + \left[\frac{n}{p^j}\right] - \left[\frac{3n}{p^j}\right] - 2\left[\frac{2n}{p^j}\right] \right) \le \sum_{j=1}^{k-1} 1 \le k-1. \end{aligned}$$

したがって C_n は p^k では割り切れない． □

補題 A.18.

$$\prod_{p \le 6n} p > \frac{C_n}{4^{(6n)^{1/2} + (6n)^{1/3} \lg(1.5n)}}.$$

[証明]　p を $3n < p \le 6n$ を満たす素数とすれば，p は C_n の分子を割るが分母は割らない．よって C_n は $P = \prod_{3n<p\le 6n} p$ で割り切れる．またそのような素数 p は $p^2 > (3n)^2 > 6n$，したがって $p > (6n)^{1/2}$ を満たすから補題 A.17 より C_n は p^2 では割れない．$C_n = PQ$ とかく．Q が素数 q のべき q^a でちょうど割り切れるとする．上に述べたことから $q \le 3n$ である．q^a が C_n を割るから補題 A.17 より $q \le (6n)^{1/a}$ である．よって $a \le \log(6n)/\log q$ である．したがって各 $a = 1, 2, \ldots$ に対して

$$S_a = \{q \,|\, q \text{ は素数で } Q \text{ が } q^a \text{ で割り切れる }\}$$

とおけば

$$S_{a+1} \subset S_a \subset \{p \,|\, p \text{ は素数，} p \le 3n,\, p \le (6n)^{1/a}\}$$

である．

$$\begin{aligned} Q = \prod_{q\le 3n} q^a &= \Big(\prod_{q\in S_1\setminus S_2} q\Big)\Big(\prod_{2\le a\le \log(6n)/\log 2}\ \prod_{q\in S_a\setminus S_{a+1}} q^a\Big) \\ &= \Big(\prod_{q\in S_1} q\Big)\Big(\prod_{2\le a\le \log(6n)/\log 2}\ \prod_{q\in S_a} q\Big) \\ &\le \Big(\prod_{p\le 3n} p\Big)\Big(\prod_{2\le a\le \log(6n)/\log 2}\ \prod_{p\le (6n)^{1/a}} p^a\Big). \end{aligned}$$

系 A.13 より $\theta(x) < (2\log 2)x$, $\prod_{p\le x} p < 4^x$ である．したがって

$$\begin{aligned} Q &< \Big(\prod_{p\le 3n} p\Big)\Big(\prod_{2\le a\le \log(6n)/\log 2} 4^{(6n)^{1/a}}\Big) \\ &= 4^{\sum_{2\le a\le \log(6n)/\log 2}(6n)^{1/a}} \prod_{p\le 3n} p. \end{aligned}$$

ここで

$$\begin{aligned} &\sum_{2\le a\le \log(6n)/\log 2} (6n)^{1/a} \\ &= (6n)^{1/2} + \sum_{3\le a\le \log(6n)/\log 2} (6n)^{1/a} \\ &\le (6n)^{1/2} + (6n)^{1/3}\,(\log(6n)/\log 2 - 2) \\ &= (6n)^{1/2} + (6n)^{1/3}\,(\lg(6n) - \lg 4) = (6n)^{1/2} + (6n)^{1/3}\lg(3n/2). \end{aligned}$$

したがって

$$C_n = PQ < 4^{(6n)^{1/2}+(6n)^{1/3}\lg(3n/2)} P \prod_{p\le 3n} p$$
$$= 4^{(6n)^{1/2}+(6n)^{1/3}\lg(3n/2)} \prod_{p\le 6n} p,$$
$$\prod_{p\le 6n} p > \frac{C_n}{4^{(6n)^{1/2}+(6n)^{1/3}\lg(3n/2)}}.$$

□

補題 A.19. すべての自然数 n に対して

$$C_n > \frac{108^n}{4\sqrt{n}}.$$

[証明]　$n = 1$ のとき，$C_1 = 6!/3!(2!)^2 = 30 > 108/4$ より主張は正しい．$n \ge 1$ として $C_n > \frac{108^n}{4\sqrt{n}}$ が成り立つとする．このとき

$$C_{n+1} = \frac{(6n+6)!(n+1)!}{(3n+3)!(2n+2)!(2n+2)!}$$
$$= \frac{(6n+6)(6n+5)(6n+4)(6n+3)(6n+2)(6n+1)(n+1)}{(3n+3)(3n+2)(3n+1)(2n+2)^2(2n+1)^2} \frac{(6n)!n!}{(3n)!(2n)!(2n)!}$$
$$= \frac{6(6n+5)(6n+1)}{(n+1)(2n+1)} C_n > \frac{6(6n+5)(6n+1)}{(n+1)(2n+1)} \frac{108^n}{4\sqrt{n}}$$

ここで

$$\frac{(6n+5)(6n+1)}{(n+1)(2n+1)} > 18\frac{\sqrt{n}}{\sqrt{n+1}}$$

がつねに成り立つことを示せば $C_{n+1} > 108^{n+1}/4\sqrt{n+1}$ がいえる．これは

$$(6n+5)^2(6n+1)^2 - 18^2 n(n+1)(2n+1)^2 = 36n^2 + 36n + 25 > 0$$

より明らかに成り立つ．　□

補題 A.20. $x \ge 31$ に対して

$$\prod_{p\le x} p > 2^x.$$

[証明]　まず，$x \ge 2^{12}$ に対して $\prod_{p\le x} p > 2^x$ が成り立つことを示す．$n = [x/6]$ とお

く．$n \geq 682$ である．$6n \leq x < 6n+6$ だから補題 A.18 と補題 A.19 より

$$\prod_{p \leq x} p \geq \prod_{p \leq 6n} p > \frac{C_n}{4^{(6n)^{1/2}+(6n)^{1/3}\lg(1.5n)}} > \frac{108^n}{4\sqrt{n}4^{(6n)^{1/2}+(6n)^{1/3}\lg(1.5n)}}$$
$$= \frac{108^n}{\sqrt{n}4^{3n+4+(6n)^{1/2}+(6n)^{1/3}\lg(1.5n)}} 4^{3n+3}.$$

$108^n > \sqrt{n}4^{3n+4+(6n)^{1/2}+(6n)^{1/3}\lg(1.5n)}$ を示す．

$$\frac{\log 108}{\log 4} > \frac{\log n}{2n \log 4} + \frac{1}{n}(3n + 4 + (6n)^{1/2} + (6n)^{1/3}\lg(1.5n))$$

を示せばよい．

$$f(t) = \frac{\log t}{2t \log 4} + \frac{1}{t}(3t + 4 + (6t)^{1/2} + (6t)^{1/3}\lg(1.5t))$$

とおく．

$$f(t) = \frac{\log t}{2t \log 4} + 3 + \frac{4}{t} + \frac{6^{1/2}}{t^{1/2}} + \frac{6^{1/3}(\log 3/2) + (3/2)\log t^{2/3})}{(\log 2)t^{2/3}}$$

とかけば，この右辺は $t \geq e^{3/2}$ において単調減少関数である．よって $n \geq 682$ ならば

$$f(n) \leq f(682) = 3.33760\cdots < 3.37744\cdots = \frac{\log 108}{\log 4}.$$

したがって

$$\prod_{p \leq x} p > 4^{3n+3} = 2^{6n+6} > 2^x.$$

$31 \leq x \leq 2^{12} = 4096$ に対してコンピュータにより

$$\frac{\theta(x)}{x} = \frac{\theta([x])}{x} > \frac{\theta([x])}{[x]+1} \geq 0.70336 > \log 2$$

を確かめられる．したがってすべての $x \geq 31$ に対して，$\theta(x) > x \log 2$, $\prod_{p \leq x} p > 2^x$ である． □

命題 A.21. (i) すべての $x \geq 5$ に対して

$$\pi(x) > \frac{(\log 2)x}{\log x}$$

が成り立つ．

(ii) すべての $x > 1$ に対して

$$\pi(x) < \frac{2x}{\log x}$$

が成り立つ.

[証明] (i) 補題 A.20 より $x \geq 31$ に対して $\prod_{p \leq x} p > 2^x$ が成り立つから対数をとって

$$\theta(x) = \sum_{p \leq x} \log p = \log \left(\prod_{p \leq x} p \right) > \log 2^x = x \log 2.$$

また自明な評価により

$$\theta(x) = \sum_{p \leq x} \log p < \sum_{p \leq x} \log x = (\log x) \sum_{p \leq x} 1 = \pi(x) \log x.$$

よって $x \geq 31$ に対して

$$\pi(x) \log x > \theta(x) > x \log 2, \quad \pi(x) > \frac{(\log 2)x}{\log x}.$$

$5 \leq x \leq 31$ に対して，$x/\log x$ は単調減少だからコンピュータにより

$$\frac{\pi(x) \log x}{x} = \frac{\pi([x]) \log x}{x} > \frac{\pi([x]) \log([x]+1)}{[x]+1} \geq 0.83396 \cdots > \log 2.$$

したがってすべての $x \geq 5$ に対して $\pi(x) > (\log 2)x/\log x$ が成り立つ.

(ii) まず $\pi(x)$ は $\theta(x)$ を用いて次のような積分として表せる.

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t \log^2 t}\, dt. \tag{A.8}$$

$0 < x < 2$ ならば $0 = 0$ としてこれは成り立つ．$x \geq 2$ とする．x 以下の素数の個数を

$n = \pi(x)$ とおき，x 以下の素数を $2 = p_1 < \cdots < p_n$ とかく．

$$\begin{aligned}
\int_2^x \frac{\theta(t)}{t\log^2 t}\,dt &= \sum_{k=1}^{n-1}\int_{p_k}^{p_{k+1}} \frac{\theta(t)}{t\log^2 t}\,dt + \int_{p_n}^{x}\frac{\theta(t)}{t\log^2 t}\,dt \\
&= \sum_{k=1}^{n-1}\theta(p_k)\int_{p_k}^{p_{k+1}} \frac{1}{t\log^2 t}\,dt + \theta(p_n)\int_{p_n}^{x}\frac{1}{t\log^2 t}\,dt \\
&= \sum_{k=1}^{n-1}\theta(p_k)\left[-\frac{1}{\log t}\right]_{p_k}^{p_{k+1}} + \theta(p_n)\left[-\frac{1}{\log t}\right]_{p_n}^{x} \\
&= \sum_{k=1}^{n-1}\theta(p_k)\left(\frac{1}{\log p_k} - \frac{1}{\log p_{k+1}}\right) + \theta(p_n)\left(\frac{1}{\log p_n} - \frac{1}{\log x}\right) \\
&= \sum_{k=1}^{n-1}\frac{\theta(p_k)}{\log p_k} - \sum_{k=1}^{n-1}\frac{\theta(p_k)}{\log p_{k+1}} + \frac{\theta(p_n)}{\log p_n} - \frac{\theta(p_n)}{\log x}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{k=1}^{n}\frac{\theta(p_k)}{\log p_k} - \sum_{k=2}^{n}\frac{\theta(p_{k-1})}{\log p_k} - \frac{\theta(p_n)}{\log x} \\
&= \sum_{k=2}^{n}\frac{\theta(p_k)-\theta(p_{k-1})}{\log p_k} + \frac{\theta(p_1)}{\log p_1} - \frac{\theta(p_n)}{\log x} \\
&= \sum_{k=2}^{n} 1 + \frac{\log(p_1)}{\log p_1} - \frac{\theta(p_n)}{\log x} = n - 1 + 1 - \frac{\theta(x)}{\log x} \\
&= \pi(x) - \frac{\theta(x)}{\log x}.
\end{aligned}$$

系 A.13 より $\theta(x) < (2\log 2)x$ $(x \geq 1)$ だから (A.8) にこの評価を用いれば

$$\begin{aligned}
\pi(x) &= \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t\log^2 t}\,dt < \frac{(2\log 2)x}{\log x} + \int_2^x \frac{(2\log 2)t}{t\log^2 t}\,dt \\
&= \frac{(2\log 2)x}{\log x} + \int_2^x \frac{(2\log 2)}{\log^2 t}\,dt \\
&= \frac{(2\log 2)x}{\log x} + (2\log 2)\int_2^x \left(\frac{1}{\log t} - \frac{d}{dt}\left(\frac{t}{\log t}\right)\right)dt \\
&= \frac{(2\log 2)x}{\log x} + (2\log 2)\int_2^x \frac{1}{\log t}\,dt - (2\log 2)\left[\frac{t}{\log t}\right]_2^x \\
&= 4 + (2\log 2)\int_2^x \frac{1}{\log t}\,dt.
\end{aligned}$$

ここで

$$f(x) = \frac{2x}{\log x} - 4 - (2\log 2)\int_2^x \frac{1}{\log t}\,dt$$

とおく．

$$f'(x) = \frac{2}{\log x} - \frac{2}{\log^2 x} - \frac{(2\log 2)}{\log x} = 2\frac{(1-\log 2)\log x - 1}{\log^2 x}.$$

したがって，$\alpha = e^{1/(1-\log 2)} = 26.02067\cdots$ において $f(x)$ は最小値 $f(\alpha)$ をとり，$x > \alpha$ で単調増加である．コンピュータにより $f(128) > 0$ がわかるから，$x \geq 128$ において $f(x) > 0$ である．よって $x \geq 128$ において

$$\pi(x) < 4 + (2\log 2)\int_2^x \frac{1}{\log t}\,dt < \frac{2x}{\log x}$$

が成り立つ．$3 \leq x \leq 128$ に対して，$\log x/x$ は単調減少だからコンピュータにより

$$\frac{\pi(x)\log x}{x} = \frac{\pi([x])\log x}{x} \leq \frac{\pi([x])\log[x]}{[x]} \leq 1.255\cdots < 2$$

が確かめられる．$1 < x < 3$ のとき

$$\frac{\pi(x)\log x}{x} \leq \frac{\log x}{x} \leq \frac{1}{e} = 0.3678\cdots < 2.$$

以上によりすべての $x > 1$ に対して

$$\pi(x) < \frac{2x}{\log x}$$

が成り立つことが示された． □

参考文献

[1] M. Agrawal, N. Kayal and N. Saxena, Primes is in P, Ann. of Math. **160**(2) (2004), 781–793.

[2] R. Crandall and C. Pomerance, Prime Numbers: A Computational Perspective 2nd Ed., Springer, 2005.

[3] 木田　雅成，素数判定の決定的多項式時間アルゴリズム，RIMS Kokyuroku **1324** (2003), 22–32.

[4] 小山　信也，素数とゼータ関数，共立出版，2015.

[5] 中村　憲，素数判定 PRIMES が決定性多項式時間 P である事の証明について，数学 **56**(1) (2004), 73–87.

[6] ジョセフ・H. シルヴァーマン，はじめての数論 原著第 3 版—発見と証明の大航海-ピタゴラスの定理から楕円曲線まで，ピアソンエデュケーション，2007.