数学の研究を始めよう (15a) 2014/august
フェルマー素数の積と恐怖のシナリオ

飯高 茂

平成 26 年 5 月 2 日

1　オイラー陪関数

自然数 $a > 1$ に対して $1 < b < a$ を満たし, a と互いに素な自然数 b の個数を $\varphi(a)$ と書き, オイラー関数という. たとえば $a = 6$ のとき $b = 1, 5$ なので $\varphi(6) = 2$.

自然数 a の相異なる素因子の数を $s(a)$ と書き, $s = s(a)$ とおく. $\varphi(a)/2^s$ を $\widetilde{\varphi}(a)$ と書く. すなわち $\widetilde{\varphi}(a) = \frac{\varphi(a)}{2^s}$ となるが $\widetilde{\varphi}(a)$ を**オイラー陪関数** と呼ぶ.

$\widetilde{\varphi}(6) = \frac{1}{2}$ のようにオイラー陪関数の値は半整数 (2 倍すれば整数になる数のこと) になることもあるが乗法性をもっているので扱いやすい.

2　スーパーアカデミア

2014 年の 3 月, 都内にある私立の高校でスーパーアカデミアという催しが開かれた. その目的は高校生が科学や数学の研究を行ってきた結果を一般に広く発表し公開することである. 数学関連は 3 本あり, 全員がポスター発表と 20 分の口頭発表を行った. そのうちの 1 つがオイラー陪関数についてであった. 私としては自分の定義した関数が取り上げられたので大変うれしい.

さて, 私は 2013 年 3 月に大学を定年退職したが縁あって, この高校で高校生の数学研究の助言をすることになった. 月曜には, 昼ごろ高校に出かけ講師室に入り自分にあてがわれた机で持参した弁当を食べる. それから, パソコンで数学の論文を書いて時間をつぶす. たまには, 先生から数学の質問がある. 生徒からの質問もある.5 時を過ぎると専任の数学の先生がきて「時間が終わったので数学の研究を始めましょう」と言う. そこで教室に行くと 3 人の生徒が数学研究に入っている.

初めに高校生の話を聞いたところオイラー関数について研究したいという. そこで,「素数の 2 倍, 3 倍さらには一般に m 倍をオイラー関数で研究を行うのはどうか」と提案した.

提案しただけで放任するわけにはいかないのでいろいろ考えてみた. 意外にも研究は順調に発展し, 雑誌「現代数学」の連載記事「数学の研究を始めよう」の原稿になっていった. またできた原稿を高校生に読んでもらった.

高校生が読んでいて難しそうな顔をする箇所は論文の書き方が不十分な箇所であった. 始めの頃彼らは国語の文章のように読み上げて「こう書いてあります」などと言う. 「計算を自分でもきちんとして, 正しいかどうか確かめて下さい.」と要望する. そのうち高校生も数学の論文の読み方が分かってくる. 7 時には下校する決まりなのだが高校生は止めないし帰ろうとしない. 「おなかが空きましたね. 帰りましょうか」というのが私の常套句になって来た.

受験の勉強に関係のない数学をこんなにも熱心に高校生が取り組むのである. 私は深く感動した.

新たにオイラー陪関数というのを考え「これについて研究した人は未だ他にいない. 少しでも何かできれば新しい研究になる」と言って励ました.

たとえば , $a = 2p(p$: 奇素数), とすると乗法性によって $2\widetilde{\varphi}(a) = 2\widetilde{\varphi}(2p) = \widetilde{\varphi}(p) = \frac{p-1}{2} = \frac{a-2}{4}$ と変形できるから $a-2 = 8\widetilde{\varphi}(a)$ となる. そこで $a - 8\widetilde{\varphi}(a) = 2$ を満たす自然数 a はどんな数になるか, などの問いかけをする.

3 $a - 2 = 8\widetilde{\varphi}(a)$ の研究

パソコンを使って 200 までの a について $a - 8\widetilde{\varphi}(a)$ の順に並べ替えた表を作った. ただしページを過大にとらないように適当に省いた.

この結果から法則を見つけ, 一般法則が推測できたら証明を考えることにしよう.

表 1: $a - 4\widetilde{\varphi}(a)$ および $a - 8\widetilde{\varphi}(a) < 0$

a	素因子分解	$\widetilde{\varphi}(a)$	$a - 4\widetilde{\varphi}(a)$	$a - 8\widetilde{\varphi}(a)$
64	$[2^6]$	16	0	-64
25	$[5^2]$	10	-15	-55
19	[19]	9	-17	-53
91	[7, 13]	18	19	-53
95	[5, 19]	18	23	-49
17	[17]	8	-15	-47
27	$[3^3]$	9	-9	-45
77	[7, 11]	15	17	-43
85	[5, 17]	16	21	-43
13	[13]	6	-11	-35
32	$[2^5]$	8	0	-32
65	[5, 13]	12	17	-31
11	[11]	5	-9	-29
93	[3, 31]	15	33	-27
55	[5, 11]	10	15	-25
87	[3, 29]	14	31	-25
99	$[3^2, 11]$	15	39	-21
69	[3, 23]	11	25	-19
7	[7]	3	-5	-17
16	$[2^4]$	4	0	-16
9	$[3^2]$	3	-3	-15
57	[3, 19]	9	21	-15
35	[5, 7]	6	11	-13
51	[3, 17]	8	19	-13
5	[5]	2	-3	-11
39	[3, 13]	6	15	-9
63	$[3^2, 7]$	9	27	-9
8	$[2^3]$	2	0	-8
33	[3, 11]	5	13	-7
3	[3]	1	-1	-5
75	$[3, 5^2]$	10	35	-5
4	$[2^2]$	1	0	-4
21	[3, 7]	3	9	-3
45	$[3^2, 5]$	6	21	-3
2	[2]	0.5	0	-2
15	[3, 5]	2	7	-1

表 2: $a-4\widetilde{\varphi}(a)$ および $a-8\widetilde{\varphi}(a)>0$

a	素因子分解	$\widetilde{\varphi}(a)$	$a-4\widetilde{\varphi}(a)$	$a-8\widetilde{\varphi}(a)$
6	$[2,3]$	0.5	4	2
10	$[2,5]$	1	6	2
14	$[2,7]$	1.5	8	2
22	$[2,11]$	2.5	12	2
26	$[2,13]$	3	14	2
34	$[2,17]$	4	18	2
38	$[2,19]$	4.5	20	2
46	$[2,23]$	5.5	24	2
58	$[2,29]$	7	30	2
62	$[2,31]$	7.5	32	2
74	$[2,37]$	9	38	2
82	$[2,41]$	10	42	2
86	$[2,43]$	10.5	44	2
94	$[2,47]$	11.5	48	2
12	$[2^2,3]$	1	8	4
20	$[2^2,5]$	2	12	4
28	$[2^2,7]$	3	16	4
44	$[2^2,11]$	5	24	4
52	$[2^2,13]$	6	28	4
68	$[2^2,17]$	8	36	4
76	$[2^2,19]$	9	40	4
92	$[2^2,23]$	11	48	4
18	$[2,3^2]$	1.5	12	6
24	$[2^3,3]$	2	16	8
40	$[2^3,5]$	4	24	8
56	$[2^3,7]$	6	32	8
88	$[2^3,11]$	10	48	8
50	$[2,5^2]$	5	30	10
36	$[2^2,3^2]$	3	24	12
98	$[2,7^2]$	10.5	56	14
48	$[2^4,3]$	4	32	16
80	$[2^4,5]$	8	48	16
54	$[2,3^3]$	4.5	36	18
100	$[2^2,5^2]$	10	60	20
30	$[2,3,5]$	1	26	22
72	$[2^3,3^2]$	6	48	24
42	$[2,3,7]$	1.5	36	30

表の観察結果からは $x\neq 1,3,5,7,9$ が成立しそうである.

4　$a-8\widetilde{\varphi}(a)$ の平行移動

この表をみると $a=16$ のとき $\widetilde{\varphi}(a)=-16$ に気づく.

次に $a=8$ に注目すると $\widetilde{\varphi}(a)=-8$ となる. その結果 $a=2^e$ が同様の性質を持つことが推察される. しかも, これ以外は皆負の奇数である.

この観察結果を証明するために $s(a)=1, s(a)=2, s(a)\geq 3$ に分けて調べよう.

4.1　$s(a)=1$ ならば

$s(a)=1$ ならば $a=p^e$ と素数 p の累乗で書けることに着目する.

$2\widetilde{\varphi}(a)=p^{e-1}\overline{p}, (\overline{p}=p-1)$ なので

$$a-8\widetilde{\varphi}(a)=p^e-4p^{e-1}\overline{p}=4p^{e-1}-3p^e=p^{e-1}(4-3p).$$

$p=2$ のときは $a=2^e, a-8\widetilde{\varphi}(a)=-2^e=-a.$

したがって $a=2^e$ のみ並べると

表 3: $a-4\widetilde{\varphi}(a)$ および $a-8\widetilde{\varphi}(a)$

a	素因子分解	$\widetilde{\varphi}(a)$	$a-4\widetilde{\varphi}(a)$	$a-8\widetilde{\varphi}(a)$
64	$[2^6]$	16	0	-64
32	$[2^5]$	8	0	-32
16	$[2^4]$	4	0	-16
8	$[2^3]$	2	0	-8
4	$[2^2]$	1	0	-4
2	[2]	0.5	0	-2

となっていて気持ちがいい. $p>2$ のときは $p^{e-1}(4-3p)$ は負の奇数になる.

ここで $p=3$ のときが最大値で値は $4-3p=-5.$

これにより $s(a)=1$ ならば $a=2^e$ 以外は $a-8\widetilde{\varphi}(a)$ が -5 より小さい負の奇数になることが示された.

意外に簡単に証明できた. これは幸先が良い.

4.2 $s(a)=2$ ならば

表によれば $a-8\widetilde{\varphi}(a)<0$ の場合でも $s(a)=1$ とは限らない.

$s(a)=2$ ならば $a=p^eq^f$ と相異なる素数 $p<q$ のそれぞれの累乗で書けるから $4\widetilde{\varphi}(a)=\varphi(a)=p^{e-1}q^{f-1}\overline{pq}$ によって

$$a-8\widetilde{\varphi}(a)=p^{e-1}q^{f-1}(pq-2\overline{p}\cdot\overline{q})=p^{e-1}q^{f-1}(2-(p-2)(q-2)).$$

$p=2,q\geq 3$ のとき $a-8\widetilde{\varphi}(a)=2^eq^{f-1}$. これは正の偶数である。

とくに $q=3$ のとき $a-8\widetilde{\varphi}(a)=2^eq3^{f-1}$ となる.

$p\geq 3$ のとき $2-(p-2)(q-2)<0$ なのでこの場合は $a-8\widetilde{\varphi}(a)=p^{e-1}q^{f-1}(2-(p-2)(q-2))<0$ でしかも負の奇数.

4.3 $a-8\widetilde{\varphi}(a)=-1$ とする

$a-8\widetilde{\varphi}(a)=-1$ とすると $p^{e-1}q^{f-1}((p-2)(q-2)-2)=1$ になるので $e=f=1,(p-2)(q-2)-2=1$. これより $(p-2)(q-2)=3$. よって $p-2=1,q-2=3$. したがって $p=3,q=5,a=15$.

先月号では $a-4\widetilde{\varphi}(a)=-1$ のとき $a=3$ になることが示された.

4.4 $s(a) \geq 3$ なら

$s = s(a) \geq 3$ ならば $\widetilde{\varphi}(a) = \frac{\varphi(a)}{2^s} \leq \frac{a-2}{8}$ によって $a - 8\widetilde{\varphi}(a) \geq 2$.

したがって $a - 8\widetilde{\varphi}(a) \leq 1$ なら $s = 1$ または $s = 2$ である. とくに $a - 8\widetilde{\varphi}(a) = -1$ のときは $s = 2$ になり, この場合 $a = 15 = 3 \times 5$ になる.

一般に相異なる素数 $p, q, r (p < q < r)$ について $a = p^e q^f r^g$ と書かれるとき

$$a - 8\widetilde{\varphi}(a) = a - p^e q^f r^g = p^{e-1} q^{f-1} r^{g-1} (pqr - \overline{p} \cdot \overline{q} \cdot \overline{r})$$

となる. これに注意して関数 $f(x, y, z) = xy + xz + yz - x - y - z + 1 (1 < x < y < z)$ を導入すると

$$a - 8\widetilde{\varphi}(a) = p^{e-1} q^{f-1} r^{g-1} f(p, q, r)$$

となる. $f(x, y, z) = x(y + z - 1) + yz - y - z + 1$ とかけば分かるように x について単調増大. そこで $f(p, q, r) \geq f(2, 3, 5) = 30 - 8 = 22$ なので

$s = 3$ ならば

$$a - 8\widetilde{\varphi}(a) \geq f(2, 3, 5) = 22.$$

さて $s = s(a) \geq 3$ のとき $8\widetilde{\varphi}(a) < a$ が成立し,

$$x = a - 4\widetilde{\varphi}(a) > 4\widetilde{\varphi}(a)$$

を満たす.

さらに $a - 8\widetilde{\varphi}(a)$ の最小値は 22 であり, $x \neq 1, 3, 5, 7, 9$ を証明するには $s(a) = 2$ を仮定してもよいことがわかった.

$s(a) = 2$ のときは $a - 8\widetilde{\varphi}(a)$ が正の数ならこれは偶数になることが示されていた.

5　フェルマー素数の積

$2^{e+1}-1$ として書ける素数をメルセンヌ素数といい, 偶数の完全数の素因子として登場する. たとえば $2^3-1=7$ は第 2 の完全数 $28=4\times 7$ の素因子である.

一方 $2^{e+1}+1$ として書ける素数としては 3 , 5 , 17 , 257 , 65537 が見出されており, フェルマー素数と呼ばれている. その小さい方からの積, すなわち

$$3, 3\times 5, 3\times 5\times 17, 3\times 5\times 17, 3\times 5\times 17\times 255, 3\times 5\times 17\times 257\times 65537$$

をフェルマー素数積という. フェルマー素数積を a で示すと $a-2\varphi(a)=-1$ を満たす.

逆に $a-2\varphi(a)=-1$ を満たす自然数 a はフェルマー素数積となることを証明したいのだが私には歯が立たない. 難問らしい.

発想を転換してオイラー関数の代わりにオイラー陪関数を使って予想を立てよう. うまく予想を定式化すると証明できる可能性がある.

$s=s(a)$ とおくとき $\varphi(a)=2^s\widetilde{\varphi}(a)$ を満たすので条件式 $a-2\varphi(a)=-1$ は $a-2^{s+1}\widetilde{\varphi}(a)=-1$ となる.

この形では不十分であり, 次の形に一般化する. 自然数 e に対して $a-2^{e+1}\widetilde{\varphi}(a)=-1$ を満たす自然数 a を考える方が良い.

6　恐怖のシナリオ

自然数 e があり $a-2^{e+1}\widetilde{\varphi}(a)=-1$ を満たすなら a はフェルマー素数積となるであろう. これを予想とする. また e を予想の指数という.

これを解くにはどうしたらよいか. 解決に向かう指針ができてきたのでそれをシナリオと呼んだ. しかしシナリオの通りに推論を実行すると, その苦労は並大抵ではないことが事前に想像できた. そこで私は密かにこれを恐怖のシナリオと呼び恐れ戦いた.

スーパーアカデミアでの配布資料でも高校生はこの予想を提示した. このまま高校生に解くのをまかせるべきだろうか. しかしここまで公開された以上, 恐怖のシナリオに沿って自分が演じるしかない. このようにして私は追い込まれ, ついに決行した. 読者はともに恐怖劇に参加してほしい.

6.1　$e=1$ の場合

$a-4\widetilde{\varphi}(a)=-1$ を満たす自然数 a は 3 になることはすでに示されていた.

一般に $a-2^{e+1}\widetilde{\varphi}(a)=-1$ に素数解 $a=p$ があるとする. すると $-1=a-2^{e+1}\widetilde{\varphi}(a)=p-2^e(p-1)\leq 2-p$ を満たす. ゆえに $p\leq 3$. これより $p=3$.

6.2　$e=2$ の場合

$a-8\widetilde{\varphi}(a)=-1$ を満たす自然数 a は $15=3\times 5$ になることもすでに示されている.

7 補題

補題 1 $a-2^{e+1}\widetilde{\varphi}(a)=-1$ に解があれば $e\geq s=s(a)$.

Proof.
$s>e$ と仮定する. $\varepsilon=s-e-1\geq 0$ とおけば $s=e+1+\varepsilon$.

$$1\leq a-\varphi(a)=a-2^{s}\widetilde{\varphi}(a)=a-2^{\varepsilon}2^{e+1}\widetilde{\varphi}(a) \tag{1}$$

になりこれに $2^{e+1}\widetilde{\varphi}(a)=a+1$ を代入すると

$$a-2^{\varepsilon}2^{e+1}\widetilde{\varphi}(a)=a-2^{\varepsilon}(a+1)<0.$$

これは式 (1) に反する.

補題 2 $a-2^{e+1}\widetilde{\varphi}(a)=-1$ に解があれば a に平方因子はなく, 奇数になる.

Proof.
a に奇数の平方因子がないことは明らかなので a は偶数と仮定して矛盾を導く.
実際,a は偶数とすると $a=2k$ とかける. ここで k は 2 より大きい奇数.

$$-1=a-2^{e+1}\widetilde{\varphi}(a)=2k-2^{e}\widetilde{\varphi}(k)=2k-2^{e-s(k)}\varphi(k).$$

ゆえに

$$-1=2k-2^{e-s(k)}\varphi(k).$$

しかし $s(a)=1+s(k), e\geq s(a)=1+s(k)$ より $e-s(k)>0$ になり上の式の右辺は偶数となり左辺 $=-1$ に矛盾.

8 $s(a)=2$ の場合

$e\geq 2=s$ は成り立つ. $a=pq$ と素数 $p,q(;p<q)$ の積で表すとき

$$-1=a-2^{e+1}\widetilde{\varphi}(a)=pq-2^{e-1}\overline{pq}=pq-2^{e-1}p\overline{q}+2^{e-1}\overline{q}.$$

$p\geq 3$ に注意し $-1=pq-2^{e-1}p\overline{q}+2^{e-1}\overline{q}$ を次のように書き換える.

$$\begin{aligned}2^{e-1}\overline{q}+1&=p(2^{e-1}\overline{q}-q)\\&\geq 3(2^{e-1}\overline{q}-q)\\&\geq 3\times 2^{e-1}\overline{q}-3q.\end{aligned}$$

よって,

$$3q+1\geq 2^{e}\overline{q}\geq 4q-4.$$

$5\geq q$ なので $q=5,p=3$. ゆえに $a=15$.

9　$e = 3$ の場合

$a - 16\widetilde{\varphi}(a) = -1$ を満たす自然数 a は何か.

$s(a) = 3$ とする.
奇素数 $p, q, r (p < q < r)$ を用いて $a = pqr$ と書ける.
$\overline{p} = p-1, \overline{q} = q-1, \overline{r} = r-1$ とおけば (以下では $\overline{s} = s-1, \overline{t} = t-1$ も使われる.) $16\widetilde{\varphi}(a) = 2\overline{pqr}$ になって

$$pqr - 2\overline{pqr} = -1.$$

1). $p = 3$ とする.

$$-1 = pqr - 2\overline{pqr} = 3qr - 4\overline{qr} = -(q-4)(r-4) - 12$$

によって $(q-4)(r-4) = 13$. これより $q-4 = 1, r-4 = 13$. したがって $p = 3, q = 5, r = 17$. ゆえに $a = 3 \times 5 \times 17$ は解.

2) $p \geq 5$ とする.

$$0 = pqr - 2\overline{pqr} + 1 = pqr - 2p\overline{qr} + 2\overline{qr} + 1$$

によって $p \geq 5$ より

$$1 + 2\overline{qr} = p(2\overline{qr} - qr) \geq 5(2\overline{qr} - qr) = 10\overline{qr} - 5qr.$$

これを変形して

$$1 + 5qr \geq 8(q-1)\overline{r}.$$

$q \geq 7$ により

$$8\overline{r} + 1 \geq q(8\overline{r} - 5r) = q(3\overline{r} - 5) \geq 21\overline{r} - 35.$$

よって

$$36 \geq 13\overline{r} \geq 13 \times 10 = 130.$$

これで矛盾した.

$3 > s(a)$ のときは 補題 1 により $3 = e \geq s(a)$ なので $s(a) = 2$. このとき $a = 15$ は既に示されている.

10　$e = 4$ の場合

$a - 32\widetilde{\varphi}(a) = -1$ を満たす自然数 a は何か.

10.1 $s(a) = 4$

$s(a) = 4$ とする.
奇素数 $p, q, r, s (p < q < r < s)$ を用いて $a = pqrs$ と書ける. $32\widetilde{\varphi}(a) = 2\overline{pqrs}$ になって

$$pqrs - 2\overline{pqrs} = -1.$$

$A = pqrs, B = \overline{pqrs}$ とおけば $A - 2B = -1$ なので $C = qrs, D = \overline{qrs}$ とすると
$A = pC, B = \overline{p}D = pD - D$ により $2D + 1 = p(2D - C)$.

1). $p \geq 5$ とする.

$$2D + 1 = p(2D - C) \geq 10D - 5C$$

により

$$5C + 1 \geq 8D.$$

$E = rs, F = \overline{rs}$ とおくと $C = qE, D = (q - 1)F$.

$$5qE + 1 \geq 8qF - 8F$$

により, $q \geq 7$ を思い出すと

$$8F + 1 \geq q(8F - 5E) \geq 7(8F - 5E) = 56F - 35E.$$

よって

$$35rs + 1 = 35E + 1 \geq 48F = 48(r - 1)\overline{s}.$$

したがって $r \geq 11$ を思い出すと

$$1 + 48\overline{s} \geq r(48\overline{s} - 35s) = r(48\overline{s} - 35\overline{s} - 35) \geq 11(13\overline{s} - 35).$$

よって $143 - 48 = 95$ に注意して $s \geq 13$ から

$$386 = 1 + 11 \times 35 \geq 95(s - 1) \geq 95 \times 12 = 1140.$$

これは矛盾.

2). $p = 3, q = 5$ とする. 計算によって

$$15rs - 16\overline{rs} = -1.$$

式変形すると

$$(r - 16)(s - 16) = 16^2 - 15 = 241.$$

241 は素数なので $r - 16 = 1, s - 16 = 241$. ここで $r = 17, s = 257$ はともに素数. よって $a = 3 \times 5 \times 17 \times 257$ は解.

3). $p = 3, q = 7$ とする.

$p=3$ によって $3C-4D=-1$. $q=7$ を用いると

$$21rs-24\overline{rs}=-1$$

となるので 左辺は 3 で割れて矛盾.

4). $p=3, q\geq 11$ とする.
$E=rs, F=\overline{rs}$ とおくと

$$3qE-4qF+4F=-1.$$

によって

$$4F+1=q(4F-3E)\geq 11(4F-3E)=44F-33E.$$

$$33rs+1=33E+1\geq 40F=40(r-1)\overline{s}.$$

$r\geq 13$ を使うと

$$40\overline{s}+1\geq r(40\overline{s}-33s)=r(7\overline{s}-33)\geq 13(7\overline{s}-33).$$

よって

$$430=1+13\times 33\geq (13\times 7-40)\overline{s}\geq (13\times 7-40)\times 16=3216.$$

矛盾した.

10.2 $s(a)=3$

$s(a)=3$ のとき $a-4\varphi(a)=-1$ になるので $a=pqr, p<q<r$ とおけば

$$pqr-4\overline{pqr}=-1.$$

$4\overline{pqr}=4p\overline{qr}-4\overline{qr}$ に注意すると $p\geq 3$ だから

$$1+4\overline{qr}=p(4\overline{qr}-qr)\geq 3(4\overline{qr}-qr)=12\overline{qr}-3qr.$$

$q\geq 5, r\geq 7$ を用いて

$$1+3qr\geq 8\overline{qr}=8q\overline{r}-8\overline{r}.$$

よって

$$1+8\overline{r}\geq q(8\overline{r}-3r)=q(8\overline{r}-3r)=q(5\overline{r}-8)\geq 25\overline{r}-40.$$

かくて

$$1+40\geq 17\overline{r}\geq 17\times 6=102.$$

矛盾.

11 $e=5$ の場合

$a-64\widetilde{\varphi}(a)=-1$ を満たす自然数 a を求める.

11.1 $s(a)=5$ の場合

$s(a)=5$ とする.

奇素数 $p,q,r,s,t(p<q<r<s<t)$ を用いて $a=pqrst$ とすると $\varphi(a)=\overline{pqrs}\overline{t}$. $A=qrst, B=\overline{qrs}\overline{t}$ とおけば条件式は

$$pA-2\overline{p}B=-1.$$

1). $p\geq 5$ を仮定する.

$$2B+1=p(2B-A)\geq 10B-5A.$$

したがって

$$5A+1\geq 8B.$$

$C=rst, D=\overline{rs}\overline{t}$ とおくと $A=qC, B=(q-1)D.$ これを代入すると

$$5qC+1\geq 8(q-1)D=8qD-8D.$$

よって

$$8D+1\geq q(8D-5C).$$

$q\geq 7$ によれば

$$8D+1\geq q(8D-5C)\geq 56D-35C.$$

よって

$$35C+1\geq 56D-8D=48D.$$

$E=st, F=\overline{s}\overline{t}$ とおくと $C=rE, D=\overline{r}F.$ これを代入し $r\geq 11$ により

$$35rE+1\geq 48\overline{r}F=48rF-48F.$$

よって

$$48F+1\geq r(48F-35E)\geq 11(48F-35E)=48\times 11F-385E.$$

$385E+1\geq 480F$ によって

$$385st+1\geq 480(s-1)\overline{t}.$$

これより $s\geq 13$ を用いて

$$\begin{aligned}1+480\overline{t}&\geq s(480\overline{t}-385\overline{t}-385)\\&\geq s(95\overline{t}-385)\\&\geq 13(95\overline{t}-385).\end{aligned}$$

これから, $t\geq 17$ によって

$$5006=1+13\times 385\geq(13\times 95-480)\overline{t}=755\overline{t}\geq 755\times 16=12080.$$

これは矛盾.

2). $p=3$ を仮定する.
$pA-2(p-1)B=-1$ によって

$$3A-4B=-1.$$

$A=qC, B=(q-1)D$ を代入すると

$$3qC-4(q-1)D=-1.$$

4). $q=5$ と仮定する.
$15C-16D=-1$ が成り立つので

$$15rE-16(r-1)F=-1.$$

$r>5$ なので $r=7$ とすると $r-1=6$ なので左辺が 3 で割れて矛盾.
$r=11$ とすると $r-1=10$ なので左辺が 5 で割れて矛盾.

5). $r=17$ の場合.
計算によって

$$15\times 17st-16^2\bar{s}\bar{t}=-1.$$

$15\times 17=16^2-1$ より

$$\begin{aligned}15\times 17st-16^2\bar{s}\bar{t}&=16^2(st-\bar{s}\bar{t})-st\\&=16^2(s+t-1)-st\\&=-(s-16^2)(t-16^2)+16^4-16^2.\end{aligned}$$

よって

$$(s-16^2)(t-16^2)=16^4-16^2+1=65281.$$

65281 は素数なので $s-16^2=1, t-16^2=65281$ をえる. ここで $s=257, t=65537$ はともに素数. (この計算は美しい)
6). $r=19$ とする. $r-1=18$ なので左辺が 3 で割れて矛盾.
$r=31$ とする. $r-1=30$ なので左辺が 5 で割れて矛盾
$r=37$ とする. $r-1=36$ なので左辺が 3 で割れて矛盾

7).$r=23,29,r\geq 41,$ の場合を以下考える.

$$16F+1=r(16F-15E).$$

これより計算して

$$1+16\overline{rs}=t(rs-16(r+s)+16).$$

$0<rs-16(r+s)+16=(r-16)(s-16)+16-16^2$ によれば

$$16^2-16<(r-16)(s-16).$$

したがって $\frac{16^2-16}{r-16}+16<s$ が成り立つ.

$1+16\overline{rs}=t(rs-16(r+s)+16)$ を満たす素数 $r,s,t(23\leq r<s<t)$ は存在しないことが次のような計算で確認される.(詳細は略す)

表 4: $r=23$ のとき

分子/分母 $=t$	s
18305/19=963.421052631579	53
20417/61=334.7049180327869	59
21121/75=281.61333333333334	61
23233/117=198.57264957264957	67
24641/145=169.93793103448274	71
25345/159=159.40251572327045	73
27457/201=136.60199004975124	79
28865/229=126.04803493449782	83
30977/271=114.30627306273063	89
33793/327=103.34250764525994	97

表 5: $r=29$ のとき

分子/分母 $=t$	s
16129/33=488.75757575757575	37
17921/85=210.83529411764707	41
18817/111=169.52252252252254	43
20609/163=126.43558282208589	47
23297/241=96.66804979253112	53
25985/319=81.4576802507837	59
26881/345=77.91594202898551	61

このような計算で確認するところに恐怖のシナリオと呼ばれる所以があるのであろう.

8). $p=3,q\geq 7$ と仮定する

$q=7$ のとき左辺は 3 で割れるので矛盾. よって $q\geq 11$ が成り立つ.

変形して

$$4D+1=q(4D-3C)\geq 11(4D-3C)=44D-33C.$$

$$33C+1\geq 40D.$$

これより

$$33C+1=33rE+1\geq 40D=40(r-1)F.$$

$r\geq 13$ によって

$$40F+1\geq r(40F-33E)\geq 13(40F-33E)=520F-429E.$$

移項して

$$429E + 1 = 429st + 1 \geq 480F = 480s\bar{t} - 480\bar{t}.$$

よって $t \geq 17$ より

$$480\bar{t} + 1 \geq s(480\bar{t} - 429\bar{t} - 429 \geq 17(51\bar{t} - 429).$$

これより $7294 = 1 + 17 \times 429 \geq \bar{t}(17 \times 51 - 480) \geq 19(17 \times 51 - 480) = 6966$. これは矛盾ではないがわずかの差しかなくこの場合 $t = 19, s = 17, r = 13, q = 11, p = 3$ である.

実際,

$$A = 3 \times 11 \times 13 \times 17 \times 19 = 138567, B = 2 \times 10 \times 12 \times 16 \times 18 = 69210, A - 2 * B = 147 \neq -1.$$

これは題意に適さない.

$t \geq 23$ のとき

$$7294 = 1 + 17 \times 429 \geq \bar{t}(17 \times 51 - 480) \geq 23(17 \times 51 - 480) = 8901.$$

したがってここにも解はない.

11.2 $s(a)=4$ の場合

奇素数 $p,q,r,s(p<q<r<s)$ を用いて $a=pqrs$ とすると $32\widetilde{\varphi}(a)=4\overline{pqrs}$ になる.
$A=qrs, B=\overline{qrs}$ とおくと
$pA-4(p-1)B=-1$ を満たすので $p\geq 3$ によって

$$4B+1=p(4B-A)\geq 3(4B-A)=12B-3A.$$

よって

$$3A+1\geq 8B.$$

$E=rs, F=\overline{rs}$ とおけば $A=qE, B=\overline{q}F=qF-F$ となり

$$3qE+1\geq 8qF-8F.$$

よって

$$8F+1\geq q(8F-3E)\geq 40F-15E.$$

これより $15E+1\geq 32F$ となり

$$15rs+1\geq 32(r-1)\overline{s}=32r\overline{s}-32\overline{s}.$$

$$1+32\overline{s}\geq 32r\overline{s}-15rs=r(17\overline{s}-15)\geq 7(17\overline{s}-15). \tag{2}$$

$s\geq 11$ を使うと

$$106=1+7\times 15\geq (7\times 17-32)\overline{s}\geq 87\times 10=870.$$

矛盾.

11.3 $s(a)=3$ の場合

奇素数 $p,q,r(p<q<r)$ を用いて $a=pqr$ とすると $32\widetilde{\varphi}(a)=4\overline{pqrs}$ になる.
$A=qr, B=\overline{qr}$ とすれば

$$1+8B=p(8B-A)\geq 3(8B-A)=24B-3A.$$

よって

$$1+3qr\geq 16B=16(q-1)\overline{r}.$$

ゆえに

$$1+16\overline{r}\geq q(16\overline{r}-3r)\geq 5(13\overline{r}-3)=65\overline{r}-15.$$

$$16=1+15\geq 49\overline{r}\geq 49\times 6>49.$$

矛盾

$e=6$ のときは解がないはずであるが, それを示すためには真の意味で恐怖のシナリオを実行する羽目になるであろう.