約数の和に関する考察

高校 1 年 2 組 39 番　西本将樹

1　はじめに

本日は文化祭にお越しいただきありがとうございます。

さて、この記事でどんな事を扱っているかとい事を少し説明しておきましょう。この記事では、自然数 a が与えられた時、約数の和が a の冪となるような自然数について、特に、n の素因数の形や、n としてありうるものの個数などについて考察します。本来別の内容を書こうと思っていたのですが、ちょうどこの問題の $a = 2$ の場合について考える機会があり、やっぱりこういう記事には自分で考察した内容について書きたいという思いからこういう内容を書く事になりました。内容については恐らく間違った内容を書いていないと思います。誤りを見つけた人は是非知らせてください。また、常体と敬体の混同などといった文法的な問題は見逃してください。高校生だけでなく中学生や小学生も、「どんなことやってんねやろ」と是非一通り目を通してみて下さい。

少し言葉の意味について説明しておきます。

約数　自然数 n に対してそれを割り切る自然数を n の約数といいます。

$a \mid b$　a が b の約数である事を $a \mid b$ で表し、そうでない事を $a \nmid b$ で表します。

素数　自然数 p が約数であるとは、p が $1, p$ 以外の約数を持たない事をいいます。

素因数　自然数 n の約数のうち素数であるものを n の素因数といいます。

冪　a の冪 (べき) とは、$a^n (n \geq 1)$ の形をした自然数の事をいいます。

代数的数　α がある整数係数多項式 $a_x^n + a_2 x^{n-1} + \cdots + a_1 x + a_0$ の根になる時、α を代数的数といいます。

$a \equiv b \pmod{p}$　$a - b$ が p で割り切れる時このように表記します。

(a, b)　a と b の共通の約数のうち最大のもの (最大公約数) をこのように表します。

和記号 $\sum$　例えば $\displaystyle\sum_{k=1}^{n} a_k$ は $a_1 + a_2 + \cdots + a_n$ を意味します。$k = 1$ から始めて n まで動かした時の a_k の値の和をとるという意味です。

積記号 $\prod$　例えば $\displaystyle\prod_{k=1}^{n} a_k$ は $a_1 \times a_2 \times \cdots \times a_n$ を意味します。$\sum$ と対にすると分かりやすいでしょう。

2　素因数分解と約数の和

2.1　素因数分解

次の定理は整数論の基本定理と言われている定理である。

定理 2.1 (整数論の基本定理) 全ての自然数は素数の積に一意的に表す事ができる。
$(\text{例} : 30 = 2 \times 3 \times 5, 2002 = 2 \times 7 \times 11 \times 13, 123456789 = 3^2 \times 3607 \times 3803)$

この定理は当たり前のように思えますが、実は大変重要な定理なのです。数学では整数と同じように素数とか割り切れるとかいう概念を定義出来る集合を扱う事がありますが、その時に素因数分解の一意性が成り立つのと成り立たないのとでは様子が大きく異なるのです。定理 2.1 より、任意の自然数は相異なる素数 $p_1, p_2, \cdots$ を用いて

$$n = p_1^{e_1} p_2^{e_2} \cdots$$

と表す事が出来る。

2.2　約数の和

n の約数の和を $S(n)$ で表すことする。n の素因数分解を

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

とする。a を n の約数とする時、a の素因数分解は

$$a = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m} (0 \leq d_i \leq e_i) \tag{1}$$

の形をしており、また (1) の形の数はみな n の約数である。

$$S = (1 + p_1 + \cdots + p_1^{e_1})(1 + p_2 + \cdots + p_2^{e_2}) \cdots (1 + p_m + \cdots + p_m^{e_m}) \tag{2}$$

を展開した各項は (1) の形をしており、(1) の形の数はみなその項に一度ずつ現れるから、$S = S(n)$ である。等比数列の和の公式

$$1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}$$

を利用して (2) 式を整理すると、

$$S = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_m^{e_m+1} - 1}{p_m - 1}$$

となる。素数 p と整数 k に対して、$f(p, k) = \dfrac{p^k - 1}{p - 1}$ と表す事にすると、次の定理を得る。

定理 2.2 $S(n) = \displaystyle\prod_{i=1}^{m} f(p_i, e_i + 1)$ が成り立つ。

3　準備

これからいくつかの問題について考察するが、この章ではその準備として、少し一般的な議論をしておこう。

定理 3.1 n が素数 p でちょうど e 回割り切れるとする。r を $e+1$ の約数とする。この時 $f(p,r)$ は $S(n)$ の約数である。

定理 2.1 より、$\dfrac{p^{e+1}-1}{p-1}$ は $S(n)$ の約数。p^r-1 は $p^{e+1}-1$ の約数であるから、$f(p,r)$ は、$f(p,e+1)=\dfrac{p^{e+1}-1}{p-1}$ の約数なので、これらを併せて定理 3.1 を得る。

定理 3.2 $x^a \equiv 1 \pmod p, x^b \equiv 1 \pmod p$ が成り立つとすると、$x^{(a,b)} \equiv 1 \pmod p$ が成り立つ。

ある自然数 m,n が存在して、$(a,b)=ma-nb$ となる事に注意する。

$$x^{(a,b)} \times x^{nb} \equiv x^{ma} \pmod p \text{ より、} x^{(a,b)} \times (x^b)^n \equiv (x^a)^m \pmod p$$

$$x^{(a,b)} \times 1 \equiv 1 \pmod p \quad \therefore x^{(a,b)} \equiv 1 \pmod p$$

よって示された。

定理 3.3 (フェルマーの小定理) p を素数とする時任意の自然数 a に対して $a^p \equiv a \pmod p$ が成り立つ。特に $a \not\equiv 0 \pmod p$ なら $a^{p-1} \equiv 1 \pmod p$ が成り立つ。

この定理には色々な証明がありますが、ここでは帰納法を使って示しておきます。
$a=1$ で成り立つのは明らか。
$a=k$ で成り立つと仮定する。

$$(k+1)^p = \sum_{i=1}^{p} {}_pC_i k^i \text{で、}{}_pC_i \text{は } 1 \le i \le p-1 \text{ に対して } p \text{ の倍数になるから}$$

$$(k+1)^p \equiv k^p + 1 \equiv k+1 \pmod p \text{ よって } a=k+1 \text{ でも成り立つ}$$

よって数学的帰納法により任意の a に対して成立する。
また、定理の後半部分はこれから直接分かる。

定理 3.4 $a-1$ と $\dfrac{a^r-1}{a-1}$ の最大公約数は r の約数である。

多項式 $\dfrac{x^r-1}{x-1} = x^{r-1}+x^{r-2}+\cdots+x+1$ を $x-1$ で割った余りが r だからである。

定理 3.5 p を奇素数とし、$a \equiv 1 \pmod{p}$ とする。$p \Big| \dfrac{a^q-1}{a-1}$ なら $p=q$ であり、その時 $\dfrac{a^q-1}{a-1} \equiv p \pmod{p^2}$ である。

定理の前半部分は定理 3.4 の直接の結果である。後半部分を証明しよう。$a=cp+1$ とする。

$$\frac{a^p-1}{a-1} \equiv \sum_{i=0}^{p-1}(cp+1)^i \equiv \sum_{i=0}^{p-1}\sum_{j=0}^{i} {}_iC_j (cp)^j$$

$$\equiv \sum_{i=0}^{p-1}({}_iC_0 + {}_iC_1 cp) \equiv \sum_{i=0}^{p-1}(1+icp) \equiv p + cp \times \frac{p(p+1)}{2}$$

$$\equiv p + p^2 \times \frac{c(p+1)}{2} \equiv p \pmod{p^2}$$

よって成り立つ。

定理 3.6 p,q,r を素数とする。$f(p,r^2)$ は q の冪とは成り得ない。

$f(p,r)$ は $f(p,r^2)$ の約数なので、この時 $f(p,r)$ も q の冪でなければならない。

$r=2$ **の時** $f(p,r^2)=(p+1)(p^2+1)$ でありこれが q の冪であるから $p+1$ も p^2+1 も q の冪であるが、これらの最大公約数は高々2 なので、$q=2$ である。
この時 $p^2+1 \geq 2^2+1=5$ であるから、$p^2+1 \equiv 0 \pmod{4}$ であるが、これは不可能である。

$r \neq 2$ **の時** $f(p,r)$ が q の冪であることより、$p^r \equiv 1 \pmod{q}$。$a=p^r$ として定理 3.4 を適用すれば、$f(p,r^2)$ は q で高々1 回しか割り切れない事が分かる。
よって、$f(p,r^2)=q$ でなければならないが、$q=f(p,r^2)>f(p,r) \geq q$ だからこれは不可能である。

4 $S(n)=2^m$

この章では $S(n)$ が 2 の冪になる自然数 n がどのような数かについて調べてみる。
まず、$f(p,r)$ が 2 の冪となるような素数 p,r について考察する。
$p \neq 2$ である事は明らかである。
よって、$p-1$ は偶数。$f(p,r)$ は偶数であるから、定理 3.5 により、$r=2$ である。
この時 $f(p,r)=p+1$ が 2 の冪であるから、p は 2^k-1 型の素数である。

n を割り切る素数 p をとり、n が p でちょうど e 回割れるとする。
$e+1$ の適当な素因数を r とする。この時定理 3.1 より、$f(p,r)$ は 2 の冪であるので、$r=2$ で p は 2^k-1 型の素数である。
よって $e+1$ は 2 の冪である。定理 3.6 より、$e+1$ は 4 で割り切れないから $e+1=2$ で、$e=1$
以上より、n は相異なる 2^k-1 型の素数の積である。

定理 4.1 $S(n)$ が 2 の冪なら、n は相異なる 2^k-1 型の素数の積である。

ところで、2^k-1 型の素数は、**メルセンヌ (Mersenne) 素数**と呼ばれている。2^k-1 が素数なら k が素数である事は容易に示せるが、k が素数でも 2^k-1 は素数とは限りません。例えば $2^{11}-1=2047=23\times 89$ です。メルセンヌ素数がどのくらい多くあるか (例えば有限個か無限個か) は知られていません。メルセンヌ素数は小さい方から順に、
$3,7,31,127,8191,131071,524287,2147483647,\cdots$ となっています。
現在知られている最大のメルセンヌ素数は 39 番目のメルセンヌ素数で、$2^{13466917}$ という、4053946 桁の数である。この素数は昨年 11 月に発見された物で、(恐らく）現在知られている最大の素数でもあります。405 万桁というのはなかなか想像出来ませんが、我々が大きいと感じる (であろう)1 兆でさえ、たった 13 桁の数であり、405 万桁とはその数十万倍もの長さであり、想像出来ないくらい大きな数である事が分かるでしょう。
この事実より、約数の和が 2 の冪であるような自然数が少なくとも $2^{39}-1$ 個ある事が分かります。

5 $S(n)=3^m$

同じ事を、3 の冪の場合を調べてみよう。実は $S(n)$ が 3 の冪となるような n は 2 しか無い。準備に手間をかけた甲斐あって、簡単にできる。

まず $f(p,q)$ が 3 の冪となる素数 p,q を考察する。
$p\neq 3$ は明らかである。今 $q\neq 2$ としよう。
$p^q-1\equiv(p-1)f(p,q)\equiv 0 \pmod 3$ より、$p^q\equiv 1 \pmod 3$
フェルマーの小定理より、$p^2\equiv 1 \pmod 3$
よって、定理 3.2 により、$p\equiv p^{(2,q)}\equiv 1 \pmod 3$
$3\left|\dfrac{p^q-1}{p-1}\right.$ かつ $p\equiv 1 \pmod 3$ だから、定理 3.5 より、$q=3$ であり、
$f(p,q)\equiv 3 \pmod 9$ となる。$f(p,q)$ は 3 の冪だから $f(p,q)=3$ 一方 $f(p,3)\geq f(2,3)=7>3$ だから、これは不可能。
つまり、$q=2$ である。定理 3.6 より、$f(p,2^2)$ は 3 の冪でない。
よって、n を割り切る適当な素数を p とし、

n が p でちょうど e 回割り切れるとすれば、
$e+1$ は 2 以外の素因数を持たず 2^2 で割り切れないから $e+1=2$
$f(p,2)=p+1$ が 3 の冪だから p は偶数なので、$p=2$
よって $n=2$ である。

定理 5.1 自然数 n の約数の和が 3 の冪であるならば、$n=2$ である。

さて、上の証明を少し変形すれば、次の定理を得る。

定理 5.2 q を 5 以上の 2^k+1 型の素数とする。$S(n)$ が q の冪となるような n は存在しない。

先ほどと同じ手順をたどればよい。$q=2^k+1$ とする。
$f(p,r)$ が q の冪となるような素数 p,r を考察する。
$p\neq q$ は明らか。今 $q\neq 2$ と仮定する。
$p^r-1\equiv(p-1)f(p,r)\equiv 0 \pmod q$ より、$p^r\equiv 1 \pmod q$
フェルマーの小定理より、$p^{2^k}\equiv 1 \pmod q$ よって定理 3.2 により、$p\equiv 1 \pmod q$
$q\left|\dfrac{p^r-1}{p-1}\right.$ かつ $p\equiv 1 \pmod q$ だから、定理 3.5 より、$r=q$ であり、
$f(p,q)\equiv q \pmod{q^2}$ となる。$f(p,r)$ は q の冪だから $f(p,r)=q$
一方 $f(p,r)\geq f(2,q)>q$ だから、これは不可能。
つまり、$q=2$ である。定理 3.6 より、$f(p,2^2)$ は q の冪でない。
よって、n を割り切る適当な素数を p とし、n が p でちょうど e 回割り切れるとすれば、$e+1$ は 2 以外の素因数を持たず 2^2 で割り切れないから $e+1=2$ である。
$f(p,2)=p+1$ が q の冪。この時 p は 4 以上の偶数なので素数ではありえない。よってこのような n は存在しない。

2^k+1 型の素数という物を考えたが、これは実は **フェルマー (Fermat) 素数** と呼ばれている。この時ある整数 n があって $k=2^n$ となることが簡単に示せる。
$k=2^n\times l(l$:奇数) とすると 2^k+1 は 2^{2^n} で割り切れるのである。$F_n=2^{2^n}+1$ としよう。昔フェルマーは F_n は全ての非負整数に対して素数であると予想した。しかしこれは間違いであることがオイラー (Euler) によって示された。
$F_0=3, F_1=5, F_2=17, F_3=257, F_4=65537257$ は素数であるが、
$F_5=4294967297=641\times 6700417$ となるのである。
実際 $n\geq 5$ で、F_n が素数となる n は未だ見つかっていない。
F_n が無限個の n に対して素数となるか。
F_n が無限個の n に対して合成数となるか。
などはいずれも難しい未解決問題である。

フェルマー素数には面白い性質がある。例えば、正 p 角形 (p:素数) が定規とコンパスで作図出来る為の必要十分条件は p がフェルマー素数であることが知られているが、ここでは深くは立ち入らない事にする。

6 $S(n) = q^m$

さて、奇素数 q が与えられた時に約数の和が q の冪となるような自然数 n について考察する。ここでは、解が高々有限個しかないことを証明する。この証明はなかなか苦労した。

さて、定理 3.1 や定理 3.6 から、$S(n)$ が q の冪になる n が有限個である事と $f(p,r)$ が q の冪となる素数 p,r の組が有限個である事は有限個である事は同値である。

$f(p,r)$ が q の冪であるとする。$p \neq q$ は明らか。
今 $r \nmid q-1$ を仮定する。$p^r \equiv 1 \pmod{q}$ である。
フェルマーの小定理より、$p^{q-1} \equiv 1 \pmod{q}$
定理 3.2 より、$p \equiv 1 \pmod{q}$
よって $f(p,r) = \dfrac{p^r-1}{p-1}$ が q の冪となるが、
定理 3.5 より、$r = q$ であり、$f(p,r) = q$ とならなければならないが、
$f(p,r) \geq f(2,r) > r$ だからこれは不可能。よって $r \mid q$
よって r として考えられる物は有限個である。また $r = 2$ はありえない。

今 $f(p,r)$ が q の冪となる素数 p,r の組が無限個あると仮定する。この時ある r があって、$f(p,r)$ が q の冪となる p が無限個存在する。$n = r-1 \geq 2$ とする。$f(p,r) = q^m$ となる組 p,r をとり、m の $\pmod{n}$ での値によって、p,r の組を n 個に分けると、ある $0 \leq l \leq n-1$ があって、$f(p,r) = q^m, m \equiv l \pmod{n}$ なる p,r の組は無限個であることが分かる。$p^n < f(p,r) < (p+1)^n$ であるから $l = 0$ である事はありえない。$C_1 = q^l$ とする。この時

$$1 + p + p^2 + \cdots + p^n = C_1 x^n (\text{ただし } x \text{ は } q \text{ の冪})$$

が無限個の解 p,x を持つ事になる。これが不可能である事を示せばよい。$y = np+1$ とすると、

$$n^n + n^n p + \cdots + n^n p^n = C_1 n^n x^n \text{であるから、}$$

$$n^n + n^{n-1}(y-1) + \cdots + (y-1)^n = C_2 x^n (C_2 = C_1 n^n)$$

左辺を展開すると、ある整数 $a_0, a_1, \cdots, a_n - 1$ があって、

$$a_0 + a_1 y + \cdots + a_{n-2} y^{n-2} + a_{n-1} y^{n-1} + y^n = C_2 x^n$$

$a_{n-1}=0$ である事はすぐに分かる。よって

$$a_0+a_1+\cdots+a_{n-2}y^{n-2}=C_2x^n-y^n$$

$C_3=max(|a_0|,|a_1|,\cdots,|a_{n-2}|)$ とすると、
| 左辺 | $<C_3(y+1)^{n-2}<2^{n-2}C_3y^{n-2}$
$C_4=\dfrac{2^{n-2}C_3}{C_2}$ とする。$t=\dfrac{x}{y}$ とする。この時

$$t^n-\frac{1}{C_2}<\frac{C_4}{y^2}$$

C_2 は自然数の n 乗ではないから、$t^n-\dfrac{1}{C_2}=0$ は有理数解を持たず、また、
$\dfrac{d}{dt}\left(t^n-\dfrac{1}{C_2}\right)=t^{n-1}$ だから、$t^n-\dfrac{1}{C_2}=0$ は重解を持たない。
$t^n-\dfrac{1}{C_2}=0$ の解を $\alpha_1,\alpha_2,\cdots,\alpha_n$ とする。この時

$$t^n-\frac{1}{C_2}=(t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n)<\frac{C_4}{y^2}$$

$t=\dfrac{x}{y}$ だから、

$$\left(\frac{x}{y}-\alpha_1\right)\left(\frac{x}{y}-\alpha_2\right)\cdots\left(\frac{x}{y}-\alpha_n\right)<\frac{C_4}{y^2}$$

これが無限個の解 $(x_1,y_1)(x_2,y_2)\cdots(x_k,y_k)\cdots$ を持つとする。
ただし $|y_1|<|y_2|<|y_3|<\cdots$
$k\to\infty$ の時 $|y_k|\to\infty$ だから、

$$\left(\frac{x_k}{y_k}-\alpha_1\right)\left(\frac{x_k}{y_k}-\alpha_2\right)\cdots\left(\frac{x_k}{y_k}-\alpha_n\right)\to 0$$

うまく無限列 x_k,y_k を取り直せばある i が存在して、$\left|\dfrac{x_k}{y_k}-\alpha_i\right|\to 0$ である。
$\alpha_1,\alpha_2,\cdots,\alpha_n$ の番号を適当に付け直す事により、$i=1$ としてよい。
$d=min\left|\alpha_{i_1}-\alpha_{i_2}\right|(i_1\neq i_2)$ とする。この時十分大きな N を取れば、$k>N$ なら

$$\left|\frac{x_k}{y_k}-\alpha_1\right|<d/2$$

この時 d の取り方より、

$$\left|\frac{x_k}{y_k}-\alpha_i\right|>d/2(i\neq 1)$$

よって、

$$\left|\frac{x_k}{y_k}-\alpha_1\right|<\frac{C_4}{y^2}\times\left(\frac{2}{d}\right)^{n-1}$$

$C_5 = C_4 \times \left(\frac{2}{d}\right)^{n-1}$ とすると、$\left|\frac{x_k}{y_k} - \alpha_1\right| < \frac{C_5}{y_k^2}$
ここで次の定理を用いる。

定理 6.1 (リドゥ(Ridout) の定理) $\alpha \neq 0$ を代数的数とする。
$P_1, \cdots, P_s, Q_1, \cdots, Q_t$ を相異なる素数 , $d > 0, 0 \leq \lambda \leq, 0 \leq \rho \leq 1$ とする。p, q を次の形の整数とする。

$$p = p^* P_1^{\sigma_1} \cdots P_s^{\sigma_s}, q = q^* Q_1^{\tau_1} \cdots Q_t^{\tau_t}$$

ただし $\sigma_1, \cdots, \sigma_s, \tau_1, \cdots, \tau_t$ は非負整数で、p^*, q^* は

$$0 < |p^*| \leq dp^{\lambda}, 0 < |q^*| \leq dq^{\rho}$$

を満たす。この時 $\kappa > \lambda + \rho$ ならば、不等式

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\kappa}}$$

を満たす p, q は有限個しかない。

次のように言い換える事も出来る。$\alpha, \kappa, \lambda, \rho, d, P_1, \cdots, P_s, Q_1, \cdots, Q_t$ のみに依存する正定数 c が存在し、不等式

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{\kappa}}$$

が上の形の全ての p, q に対して成り立つ。

この定理の証明は非常に難しく (私が解説して欲しいです。)、ここで紹介する事は出来ない。$\lambda = \rho = 1$ の場合は、1955 年に証明された次の定理である。

定理 6.2 (ロス (Roth) の定理) α を $n(\geq 2)$ 次代数的数、$\kappa > 2$ とすると、不等式

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\kappa}}$$

を満たす p, q は有限個しかない。

α_1 はその決め方から代数的数であり、y_k は q の冪だから、
$d = 1, x_k^* = x_k, Y = q, y_k^* = 1, \lambda = 1, \rho = 0, \kappa = 1.5$ とすると、これらはリドゥの定理の条件を全て満たすので、ある正定数 C_6 が存在して、

$$\left|\frac{x_k}{y_k} - \alpha_1\right| > \frac{C_6}{y_k^{1.5}}$$

一方 $\left|\frac{x_k}{y_k}-\alpha_1\right|<\frac{C_5}{y_k^2}$ であったから、

$$\frac{C_6}{y_k^{1.5}}<\left|\frac{x_k}{y_k}-\alpha_1\right|<\frac{C_5}{y_k^2}$$

よって $y_k^{0.5}<\frac{C_5}{C_6}$ である。$C=\frac{C_5^2}{C_6^2}$ とすると、

$$y_k<C$$

が成り立つ。C は (x や y に依存しない) 定数である。一方 $y_k\to\infty$ だからこれは矛盾である。
よって $f(p,r)$ が q の冪となるような p,r の組は高々有限個であるので、約数の和が q の冪となる自然数も高々有限個であることが示された。

定理 6.3 q を奇素数とするとき、約数の和が q の冪となるような自然数は高々有限個しか存在しない。

非常に長かったが、いつのまにか示すべき事が得られた。リドゥの定理とは凄い物だと感服させられたが、この問題にこれほどの定理が必要なのかどうかは疑問である。初等的な証明を得た人は是非教えてください！

7 $S(n)=a^m(a:\text{奇数})$

前章では奇素数 q に対して $S(n)$ が q の冪となる n について考察した。それを振り返ってみると、リドゥの定理の条件の強さから、もう少し頑張れば q の部分を任意の奇数 a に拡張出来そうな気がしてくる。この時 $f(p,r)$ は $q_1,\cdots,q_m$ 以外の素因数を持ちません。さて、証明に入りましょう。

$S(n)$ が a の冪となる n の冪となる n が無限に多く存在したと仮定する。この時 $f(p,r)$ が $q_1,\cdots,q_m$ 以外の素因数を約数に持たないような $f(p,r)$ が無限に多く存在することになる。
$S(n)>n$ だから、$S(n)$ が素数 $q_1,\cdots,q_m$ の 2 乗で割り切れない物は有限個であるから、ある i があって、$f(p,r)$ が q_i^2 で割り切れ $q_1,\cdots,q_m$ 以外の素因数を持たないような p,r の組は無限に多くある。特に $q_1,\cdots,q_m$ の添え字を適当に付け直せば、$i=1$ としてもよい。以後 q_1 をただ単に q と書くことがある。
$f(p,r)$ が $\star$ を満たすとは、$f(p,r)$ が q^2 で割り切れ、$q_1,\cdots,q_m$ 以外の素因数を持たないことを言うものとする。

$\star$ を満たす p,r が無限個あるとして矛盾を示そう。

$\star$ を満たす p, r を考察の対象とする。r を素数とする。
$f(p, r^e)$ で $\star$ を満たす e が無限個あったと仮定する。

$$f_e = \frac{p^{r^{e+1}} - 1}{p^{r^e} - 1}$$

とする。この時各 e に対して f_e は、$q_1, \cdots, q_m$ 以外の素因数を持たない。$e_1 < e_2$ に対して

$$(f_{e_1}, f_{e_2}) = \left(\frac{p^{r^{e_1+1}-1} - 1}{p^{r^{e_1}} - 1}, \frac{p^{r^{e_2+1}} - 1}{p^{r^{e_2}} - 1} \right) \leq \left(p^{r^{e_2}} - 1, \frac{p^{r^{e_2+1}} - 1}{p^{r^{e_2}} - 1} \right)$$

定理 3.4 より $(f_{e_1}, f_{e_2}) \leq r$ であり、さらに定理 3.5 より、f_e は高々1 回しか r で割り切れない。
$f_e > r$ だから f_e は r 以外の約数を持つ。そのひとつを x_e とすると、$x_e = x_{e'}$ なら先程の議論から $e = e'$ である。
よって、x_e は無限個の値を持つ事になるが、f_e は、$q_1, \cdots, q_m$ 以外の素因数を持たないので、これは矛盾である。よって、各 p, r に対して $f(p, r^e)$ が $\star$ を満たすような e は高々有限個である。

次に $\star$ を満たす r が高々有限個である事を示そう。この場合は r が $q-1$ の約数である事が分かる。r が $q-1$ の約数で無いとして矛盾を示せばよい。
$\frac{p^r - 1}{p - 1} \equiv 0 \pmod{q}$ だから $p^r \equiv 1 \pmod{q}$
フェルマーの小定理より、$p^{q-1} \equiv 1 \pmod{q}$
よって定理 3.2 より、$p \equiv 1 \pmod{q}$
よって定理 3.5 より、$\frac{p^r - 1}{p - 1} \equiv 0 \pmod{q^2}$ となる事はありえない。よってこれは不可能なので、r は $q-1$ の約数である。また、$r \neq 2$ である事は明らかである。

r としてありうる値は有限個である事が示された。よって $f(p, r)$ が $\star$ を満たすような p, r の組が無限個存在するとすれば、ある r があって、$f(p, r)$ が $\star$ を満たすような p が無限に多く存在する。

$n = r - 1$ とする。r に対する無限個の $\star$ を満たす p に対して $f(p, r) = q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m}$ として、$e_1, \cdots, e_m$ の $\pmod{n}$ の値の組み合わせは m^n 通りであるから、
ある $l_1, \cdots, l_m (0 \leq l_1, \cdots, l_m \leq n)$ が存在して、無限に多くの p に対して

$$f(p, r) = q_1^{e_1} q_2^{e_2} \cdots q_m^{e_m} (e_i \equiv l_i \pmod{n})$$

となる。$p^n < f(p, r) < (p+1)^n$ であるから右辺はいかなる整数の n 乗でも無いので、$a = q_1^{l_1} \cdots q_m^{l_m}$ とすると a はいかなる自然数の n 乗でも無い。右辺は ay^n とかける (ただし y は $q_1, \cdots, q_m$ 以外の素因数を持たない。よって

$$1 + p + \cdots + p^n = ay^n (\text{ただし } y \text{ は } q_1, \cdots, q_m \text{以外の約数を持たない})$$

となる。先ほどの章と全く同じ議論が適用することで、出来る。
つまり無理数の代数的数 α と正定数 C が存在して、$\left|\frac{x}{y}-\alpha\right|<\frac{C}{y^2}$ を満たす整数 x,y が無限個存在する。ここで x,y にリドゥの定理を適用すればいいのである。これから前章と同様にして矛盾が示せるのである。

定理 7.1 a を任意の奇数とする。約数の和が a の冪となるような自然数は高々有限個しか存在しない。

これでこの章は終わりである。

8 $S(n)=10^m$

さて、一般の奇数 a に対して約数の和が a の冪となる自然数が有限個である事が示された。この章では偶数の例として自然数 n の約数の和が 10 の冪となるような n について考察してみよう。

$f(p,r)$ が $2,5$ 以外の素因数を持たないような素数 p,r について考察する。
$f(p,r)$ が 2 の冪となる時 $r=2$ となる事は定理 4.1 で述べた通りである。また、$f(p,r)$ が 5 の冪となるような素数 p,r が存在しない事は定理 5.2 で述べた通りである。
$f(p,r)$ が 2 でも 5 でも割り切れ他の素数では割り切れないような素数 p,r について考察する。$p\neq 2$ である事は明らか。よって $p\equiv 1 \pmod 2$ なので定理 3.4 より、$r=2$ である。
よって $p+1$ は $2,5$ 以外の素因数を持たない。よって n の適当な素因数を p とし、n が p でちょうど e 回割り切れるとすれば p は $2,5$ 以外の素因数を $e+1$ は 2 の冪である。今 $e+1>2$ であるとすると、$e+1$ は 4 で割り切れるから、定理 3.1 より、$f(p,4)$ は $2,5$ 以外の素因数を持たない。
よって $\frac{p^4-1}{p^2-1}$ は $2,5$ 以外の素因数を持たない。定理 5.2, 4.1 より、これが $2,5$ の一方だけで割り切れる事は不可能。よって $\frac{p^4-1}{p^2-1}$ は 10 の倍数である。一方定理 3.4 より、

$$\left(\frac{p^4-1}{p^2-1},\frac{p^2-1}{p-1}\right)\leq\left(\frac{p^4-1}{p^2-1},p^2-1\right)\leq 2$$

である。よって、$f(p,2)$ は 5 で割り切れないから 2 の冪なので、p はメルセンヌ素数である。
$p=2^k-1$ とする。$\frac{p^4-1}{p^2-1}$ は 2 で 1 回しか割り切れないので、ある l があって、$\frac{p^4-1}{p^2-1}=2\times 5^l$ となる。$p^2+1=2^{2k}-2^{k+1}+2$ であり、$\frac{p^4-1}{p^2-1}=p^2+1$ であるから、$5^l=2^{2k-1}-2^k+1=2^k(2^{k-1}-1)$ よって 5^l-1 は 2 で k 回割り切れる。5^l-1 が 2 でちょうど何回割れるかについて考察する。$l=2^e l'(l'$:奇数) とする。定理 3.4 か

ら $\frac{5^l-1}{5^{2^e}-1}$ は偶数であるから、5^l-1 が 2 で割り切れる回数は $5^{2^e}-1$ が 2 で割り切れる回数に等しい。この回数を a_e とする。
$a_1=2$ は明らか。また定理 3.4 より、$\frac{5^{2^{e+1}}-1}{5^{2^e}-1}$ は 2 で一度だけ割り切れる。よって、$a_{e+1}=a_e+1$ である。よって $a_e=e+1$ が成り立つ。
5^l-1 は 2 で k 回割り切れるのであったから、$a_l=l+1\geq k$ なので、$l\geq k-1$ である。よって、

$$2^k(2^{k-1}-1)=5^l\geq 5^{k-1}$$

$$\frac{4^k}{2}=2^{2k-1}>2^k(2^{k-1}-1)\geq 5^{k-1}\quad\therefore 2>(\frac{5}{4})^{k-1}$$

よって $k=2,3,4$ であるが、$k=4$ の時は $2^k-1=15$ は素数ではない。よって、$k=2,3$ であり、$p=3,7$ である。この時 $f(p,2^e)$ が $2,5$ 以外の素因数を持たないような e は 1 または 2 である事は容易に確認出来る。よって次の定理を得る。

定理 8.1 約数の和が 10 の冪となる自然数 n の適当な素因数を p とする。
p はメルセンヌ素数か 2^i5^j-1 型の素数であり、$p\neq 3,7$ であれば、n は p で 1 回しか割れない。$p=3,7$ であれば、n は p でちょうど 1 回または 3 回割り切れる。

約数の和が 10 の冪となるような自然数をいくつか求めてみよう。$S(p^{r-1})$ の値を計算すると $S(3)=4,S(3^3)=40,S(7)=8,S(7^3)=400,S(19)=20,$
$S(79)=80,S(1249)=1250,S(499)=500$ などを組み合わせて積が 10 の冪になるようにすると、
$n=7\times 1249,3\times 19\times 1249,343\times 19\times 1249$ などが得られる。
　このような自然数 n が有限個か無限個か決定する問題は非常に難しいだろう。2^k-1 型の素数でさえどのくらいあるのか分かっていないのだから、2^i5^j-1 型の素数などはより難しい問題であろうと思われる。

9　$S(n)=a^m(a:$偶数$)$

　さて、同様に 10 を一般の偶数 a に変えてみるとどのような事が言えるだろう。実は次の事がいえる。

定理 9.1 n を、$S(n)$ が a の冪となるような自然数とする。このような n を割り切る素数の平方としてありうる物は高々有限個しか存在しない。

$a=10$ である場合は、n を割り切る素数の平方としてありうる物は、$3^2,7^2$ であった。

さて、このような素数が無限に多く存在したとする。

$$a = 2^e q_1^{e_1} \cdots q_m^{e_m}$$

とする。$f(p,r)$ が $q_1, \cdots, q_m$ 以外の素因数を持たないような p, r の組は有限個 (定理 7.1) であったから、この時 $f(p,r)$ が偶数で $2, q_1, \cdots, q_m$ 以外の素因数を持たないような物が無限に多くある事になる。よって $r = q^e$(q:素数) であって、$f(p,r)$ が偶数で $2, q_1, \cdots, q_m$ 以外の素因数を持たないような物が無限に多くある事になる。この時 $p \neq 2$ は明らかである。今 q が奇数であるとすると、定理 3.4 より、$\dfrac{p^r - 1}{p - 1}$ は偶数ではない。よって、$q = 2$

よって、$f(p,4)$ が $2, q_1, \cdots, q_m$ 以外の素因数を持たないような p が高々有限個である事を示せばよい。このような p が無限個あるとすれば、今までやってきたように、リドゥの定理から矛盾を示せる事は前の証明を模倣すれば容易に分かるだろう。そうして定理 9.1 が得られる。

10　あとがき

最後までお付き合い下さってありがとうございます。記事の出来としては、結構良い結果が得られて満足しています。説明が分かりにくい所が (特に最後の方はページ数の都合からある程度省略したので) あるかもしれません。その時はご遠慮なく尋ねて下さい。若しくは

nisimotomasaki@funifuni.net までメール下さい。お待ちしております。

さて、今回はパソコンで記事を打ったのですが、数式などが綺麗に出来ていると思いません?実はこの記事を打つのに TEX というソフトを使いました。これは特に数式を打つ時に分数や指数、積分、和記号などがかなり綺麗に出るので非常に便利です。私も使ったのは今年になってからなのですが、別に難しくもありません。

TEX については**日本語 TEX 情報**

http://www.matsusaka-u.ac.jp/ okumura/texfaq/

などを御覧下さい。

また、今回の記事を書くにあたって、

無理数と超越数 (塩川宇賢　著)

などが大変役に立ちました。リドゥの定理の証明なども載っています。興味のある方は是非御覧下さい。

また、今回の記事を編集してくれた中 3 の矢野君にも感謝です。