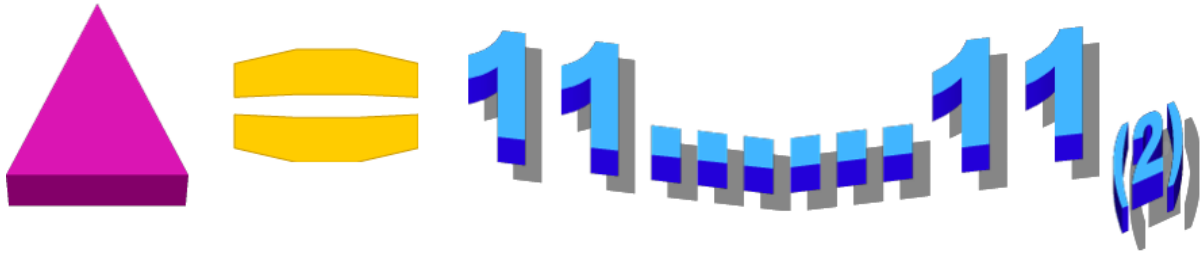
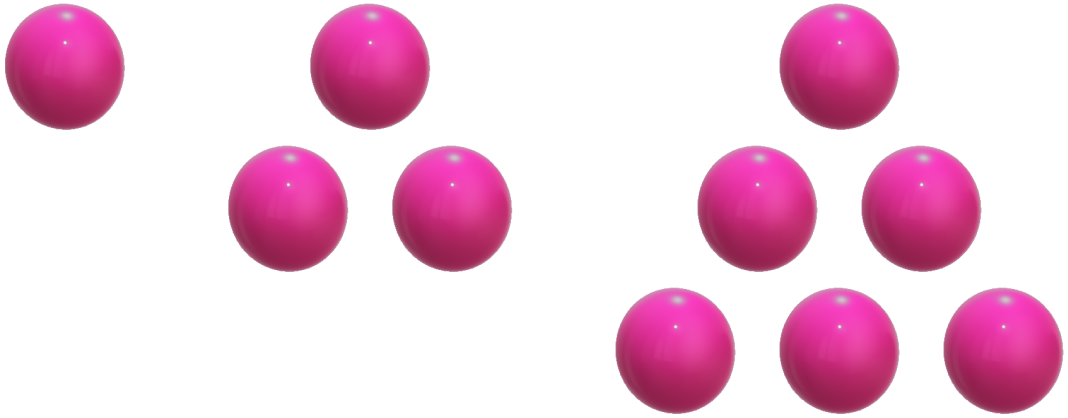


Tomohiro Yamada

Apr 1, 2018

三角数

$$
\begin{aligned}
(0 &= 0),\\
1 &= 1,\\
3 &= 1+2,\\
6 &= 1+2+3,\\
10 &= 1+2+3+4,\\
15 &= 2^4-1 = 1+2+3+4+5,\\
&\cdots\cdots
\end{aligned}
$$



1 3 6

メルセンヌ数

$$
\begin{aligned}
(0 &= 2^0 - 1),\\
1 &= 2^1 - 1 = 1,\\
3 &= 2^2 - 1 = 1 + 2,\\
7 &= 2^3 - 1 = 1 + 2 + 4,\\
15 &= 2^4 - 1 = 1 + 2 + 4 + 8,\\
31 &= 2^5 - 1 = 1 + 2 + 4 + 8 + 16,\\
&\cdots\cdots
\end{aligned}
$$

符号なし n ビット（2進数で n 桁）であらわされる最大の数

現在知られている最大の素数は $2^{77232917} - 1$

$$0 = 2^0 - 1,$$
$$1 = 2^1 - 1,$$
$$3 = 2^2 - 1 = 1 + 2,$$
$$15 = 2^4 - 1 = 1 + 2 + 3 + 4 + 5,$$
$$4095 = 2^{12} - 1 = 1 + 2 + 3 + \cdots + 90$$

は三角数かつメルセンヌ数！

ここでRamanujanが登場！

Ramanujanの問題464

$2^n - 7$ は n の値が $3, 4, 5, 7, 15$ であるときに平方数となる。他の値を見つけよ。

参考URL

http://www.imsc.res.in/~rao/ramanujan/collectedpapers/question/q464.htm

つまり

$$x^2 + 7 = 2^n \qquad (1)$$

となる整数 (x, n) を $(1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$
以外に見つけることが問題。

$$\frac{u(u+1)}{2} = 2^m - 1$$

は

$$\begin{aligned}(2u+1)^2 &= 4u(u+1)+1 \\ &= 8(2^m-1)+1 = 2^{m+3}-7\end{aligned}$$

と変形できるので、２つの問題は同値！

- 1948年 Nagellにより解決（ノルウェー語で出版）

- 1959年 Chowla, Lewis and Skolem 系統的な証明方法

- 1961年 Nagell 最初の証明の英語版を出版

出題したRamanujanと最初に解いたNagellにちなんで、(1) をRamanujan-Nagell方程式という。

参考（INTEGERSブログより）

http://integers.hatenablog.com/entry/Ramanujan-Nagell

さらに一般化

- 1960年 Apéry p が素数で $D > 0, (p, D) \neq (2, 7)$ ならば $x^2 + D = p^k$ の解の個数 ≤ 2

- 1980年 Beukers $D > 0$ で $x^2 + D = 2^n$ が2個の解をもつとき $D = 7, 23$ または $D = 2^k - 1, k > 3$ さらに $w = x^2 + D = 2^n, D \neq 0$ ならば $w < 2^{435} |D|^{10}$

- 1984年 Evertse $x^2 + D = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ の解の個数 $\leq 3 \times 7^{4k+6}$

- 2017-2018年 Yamada $x^2 + D = 2^s p_1^{e_1} p_2^{e_2} (s = 0, 2)$ の解の個数 ≤ 63

方程式を解くアルゴリズム

1996年 Christoph Hering が

$$ax^2 + bx + c = c_0 c_1^{y_1} \cdots c_r^{y_r}$$

の解をすべて決定する方法を考察（すべての場合に使えるわけではない）

$x^2 + 7 = 2^k$ の場合は単純な合同式により解けることを証明！

$n = 2m$ が偶数のとき

$$7 = 2^n - x^2 = (2^m)^2 - x^2 = (2^m + x)(2^m - x)$$

より

$$2^m - x \geq 1, 2^m + x \leq 7$$

よって $x \leq 3$ となり解は $(x, n) = (3, 4)$ しかない

$n = 2m + 1$ が奇数のとき

$n = 2m + 1$ が奇数のとき

$$-7 = x^2 - 2^n = x^2 - 2(2^m)^2$$

$y = 2^m$ とおくと (x, y) はPell方程式

$$x^2 - 2y^2 = -7 \qquad (2)$$

の解となる

このPell方程式は

$$(x + y\sqrt{2})(x - y\sqrt{2}) = -7 \qquad (3)$$

と同値

Pell方程式を解く

整数列 $(s_n), (t_n), (u_n), (v_n)(n \geq 0)$ を

$$(s_n + t_n\sqrt{2}) = (1 + 2\sqrt{2})(3 + 2\sqrt{2})^n,$$
$$(u_n + v_n\sqrt{2}) = (-1 + 2\sqrt{2})(3 + 2\sqrt{2})^n$$

により定める。

(2) の解は $(x, y) = (s_n, t_n)$ または $(x, y) = (u_n, v_n)$ によりあらわされる。

$$(\pm 1 + 2\sqrt{2})(\pm 1 - 2\sqrt{2}) = -7,$$
$$(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$$

よりこれらが解であることはすぐにわかる。

$$M = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$$

とおくと

$$\begin{pmatrix} s_n \\ t_n \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} u_n \\ v_n \end{pmatrix} = M^n \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

と行列によりあらわされる。

合同式を解く

$y = 2^m, m \geq 8$ とすると $y = t_n$ または $y = v_n$ よりも $t_n = 2^m$ または $v_n = 2^m$ よって

$$t_n \equiv 0 \pmod{2^8}$$

または

$$v_n \equiv 0 \pmod{2^8}$$

実際に 2^8 を法として t_n, v_n を求めると

$$t_n \equiv 0 \pmod{2^8} \Leftrightarrow n \equiv 61 \pmod{2^7},$$
$$v_n \equiv 0 \pmod{2^8} \Leftrightarrow n \equiv 67 \pmod{2^7}$$

一方、

$$M^{256} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{7681}$$

より

$$t_n \equiv t_{61} \equiv 2988 \pmod{7681},$$
$$t_n \equiv t_{189} \equiv 4693 \pmod{7681},$$
$$v_n \equiv v_{67} \equiv 4693 \pmod{7681},$$
$$v_n \equiv v_{195} \equiv 2988 \pmod{7681}$$

のいずれかが成り立つ。

つまり

$$2^m \equiv 2988, 4693 \pmod{7681}$$

のいずれかが成り立つ。しかし $2^{3840} \equiv 1$, $2988^{3840} \equiv 4693^{3840} \equiv -1 \pmod{7681}$ より

$$1 \equiv 2^{3840m} \equiv -1 \pmod{7681}$$

となって矛盾する！

平方剰余の言葉では、

$$\left(\frac{2}{7681}\right) = 1, \left(\frac{2988}{7681}\right) = \left(\frac{4693}{7681}\right) = -1$$

より

$$2^m \equiv 2988, 4693 \pmod{7681}$$

となる m は存在しない、ということもできる。

このほかにも

$$M^{256} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p}$$

となる小さな素数 p は $577, 1409, 11777$ があるが、
これらをこの議論で使うことはできない。

たとえば

$$t_{61} \equiv 128 \equiv 2^7 \pmod{577},$$
$$t_{61} \equiv 128 \equiv 2^7 \pmod{1409},$$
$$t_{61} \equiv -128 \equiv -2^7 \pmod{11777}$$

となるから $577, 1409$ は解が存在しないことの証明に使うことはできない。$2^{1472} \equiv -1 \pmod{11777}$ だから $2^{1479} \equiv -128 \pmod{11777}$ となるので 11777 もこの議論で使うことはできない。

References

R. Apéry, Sur une équation diophantinne, *C. R. Acad. Sci. Paris, Sér. A* **251** (1960), 1451–1452.

F. Beukers, On the generalize Ramanujan-Nagell equation I, *Acta Arith.* **38** (1980/81), 389–410.

J.-H. Evertse, On equations in S-units and the Thue-Mahler equation, *Inv. Math.* **75** (1984), 561–584.

Christoph Hering, On the Diophantine Equations $ax^2 + bx + c = c_0 c_1^{y_1} \cdots c_r^{y_r}$, *Appl. Algebra Engrg. Comm. Comput.* **7** (1996), 251–262.

T. Yamada, A generalization of the Ramanujan-Nagell equation, arXiv:1712.02199.

MANY THANKS
FOR YOUR ATTENTION

Tomohiro Yamada
Center for Japanese language and culture
Osaka University
562-8558
8-1-1, Aomatanihigashi, Minoo, Osaka
Japan
e-mail: tyamada1093@gmail.com