Calculus and Analysis
Discrete Mathematics
Foundations of Mathematics
Geometry
History and Terminology
Number Theory
Probability and Statistics
Recreational Mathematics
Topology

Alphabetical Index
Interactive Entries
Random Entry
New in *MathWorld*

MathWorld Classroom

About *MathWorld*
Contribute to *MathWorld*
Send a Message to the Team

MathWorld Book

Wolfram Web Resources »

13,681 entries
Last updated: Fri Feb 8 2019

Created, developed, and nurtured by Eric Weisstein at Wolfram Research

Diophantine Equation

EXPLORE THIS TOPIC IN The *MathWorld* Classroom

A Diophantine equation is an equation in which only integer solutions are allowed.

Hilbert's 10th problem asked if an algorithm existed for determining whether an arbitrary Diophantine equation has a solution. Such an algorithm does exist for the solution of first-order Diophantine equations. However, the impossibility of obtaining a general solution was proven by Yuri Matiyasevich in 1970 (Matiyasevich 1970, Davis 1973, Davis and Hersh 1973, Davis 1982, Matiyasevich 1993) by showing that the relation $n = F_{2m}$ (where F_{2m} is the $(2m)$th Fibonacci number) is Diophantine. More specifically, Matiyasevich showed that there is a polynomial P in n, m, and a number of other variables $x, y, z, \ldots$ having the property that $n = F_{2m}$ iff there exist integers $x, y, z, \ldots$ such that $P(n, m, x, y, z, \ldots) = 0$.

Matiyasevich's result filled a crucial gap in previous work by Martin Davis, Hilary Putnam, and Julia Robinson. Subsequent work by Matiyasevich and Robinson proved that even for equations in thirteen variables, no algorithm can exist to determine whether there is a solution. Matiyasevich then improved this result to equations in only nine variables (Jones and Matiyasevich 1982).

Ogilvy and Anderson (1988) give a number of Diophantine equations with known and unknown solutions.

A linear Diophantine equation (in two variables) is an equation of the general form

$$a x + b y = c, \tag{1}$$

where solutions are sought with a, b, and c integers. Such equations can be solved completely, and the first known solution was constructed by Brahmagupta. Consider the equation

$$a x + b y = 1, \tag{2}$$

Now use a variation of the Euclidean algorithm, letting $a = r_1$ and $b = r_2$

$$r_1 = q_1 r_2 + r_3 \tag{3}$$
$$r_2 = q_2 r_3 + r_4 \tag{4}$$
$$r_{n-3} = q_{n-3} r_{n-2} + r_{n-1} \tag{5}$$
$$r_{n-2} = q_{n-2} r_{n-1} + 1, \tag{6}$$

Starting from the bottom gives

$$1 = r_{n-2} - q_{n-2} r_{n-1} \tag{7}$$
$$r_{n-1} = r_{n-3} - q_{n-3} r_{n-2}, \tag{8}$$

so

$$1 = r_{n-2} - q_{n-2}(r_{n-3} - q_{n-3} r_{n-2}) \tag{9}$$
$$= -q_{n-2} r_{n-3} + (1 + q_{n-2} q_{n-3}) r_{n-2}. \tag{10}$$

Continue this procedure all the way back to the top.

Take as an example the equation

$$1027 x + 712 y = 1 \tag{11}$$

and apply the algorithm above to obtain

$$\begin{array}{lll} 1027 = 712 \cdot 1 + 315 & \| & 1 = -165 \cdot 1027 + 238 \cdot 712 \uparrow \\ 712 = 315 \cdot 2 + 82 & \| & 1 = 73 \cdot 712 - 165 \cdot 315 \| \\ 315 = 82 \cdot 3 + 69 & \| & 1 = -19 \cdot 315 + 73 \cdot 82 \| \\ 82 = 69 \cdot 1 + 13 & \| & 1 = 16 \cdot 82 - 19 \cdot 69 \| \\ 69 = 13 \cdot 5 + 4 & \| & 1 = -3 \cdot 69 + 16 \cdot 13 \| \\ 13 = 4 \cdot 3 + 1 \downarrow & \| & 1 = 1 \cdot 13 - 3 \cdot 4 \| \\ & & 1 = 0 \cdot 4 + 1 \cdot 1 \| \end{array} \tag{12}$$

The solution is therefore $x = -165$, $y = 238$.

The above procedure can be simplified by noting that the two leftmost columns are offset by one entry and alternate signs, as they must since

$$1 = -A_{i+1} r_i + A_i r_{i+1} \tag{13}$$
$$r_{i+1} = r_{i-1} - r_i q_{i-1} \tag{14}$$
$$1 = A_i r_{i-1} - (A_i q_{i-1} + A_{i+1}), \tag{15}$$

so the coefficients of r_{i-1} and r_{i+1} are the same and

$$A_{i-1} = -(A_i q_{i-1} + A_{i+1}). \tag{16}$$

Repeating the above example using this information therefore gives

$$\begin{array}{lll} 1027 = 712 \cdot 1 + 315 & \| & (-) \quad 165 \cdot 1 + 73 = 238 \uparrow \\ 712 = 315 \cdot 2 + 82 & \| & (+) \quad 73 \cdot 2 + 19 = 165 \| \\ 315 = 82 \cdot 3 + 69 & \| & (-) \quad 19 \cdot 3 + 16 = 73 \| \\ 82 = 69 \cdot 1 + 13 & \| & (+) \quad 16 \cdot 1 + 3 = 19 \| \\ 69 = 13 \cdot 5 + 4 & \| & (-) \quad 3 \cdot 5 + 1 = 16 \| \\ 13 = 4 \cdot 3 + 1 \downarrow & \| & (+) \quad 1 \cdot 3 + 0 = 3 \| \\ & & (-) \quad 0 \cdot 1 + 1 = 1 \| \end{array} \tag{17}$$

and we recover the above solution.

Call the solutions to

$$a x + b y = 1 \tag{18}$$

x_0 and y_0. If the signs in front of $a x$ or $b y$ are negative, then solve the above equation and take the signs of the solutions from the following table:

equation	x	y

$ax+by=1$	x_0	y_0
$ax-by=1$	x_0	$-y_0$
$-ax+by=1$	$-x_0$	y_0
$-ax-by=1$	$-x_0$	$-y_0$

In fact, the solution to the equation

$$ax-by=1 \tag{19}$$

is equivalent to finding the continued fraction for a/b, with a and b relatively prime (Olds 1963). If there are n terms in the fraction, take the $(n-1)$th convergent p_{n-1}/q_{n-1}. But

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^n, \tag{20}$$

so one solution is $x_0 = (-1)^n q_{n-1}$, $y_0 = (-1)^n p_{n-1}$, with a general solution

$$x = x_0 + kb \tag{21}$$
$$y = y_0 + ka \tag{22}$$

with k an arbitrary integer. The solution in terms of smallest positive integers is given by choosing an appropriate k.

Now consider the general first-order equation of the form

$$ax+by=c. \tag{23}$$

The greatest common divisor $d \equiv \mathrm{GCD}(a, b)$ can be divided through yielding

$$a'x+b'y=c', \tag{24}$$

where $a' \equiv a/d$, $b' \equiv b/d$, and $c' \equiv c/d$. If $d \nmid c$, then c' is not an integer and the equation cannot have a solution in integers. A necessary and sufficient condition for the general first-order equation to have solutions in integers is therefore that $d \mid c$. If this is the case, then solve

$$a'x+b'y=1 \tag{25}$$

and multiply the solutions by c', since

$$a'(c'x)+b'(c'y)=c'. \tag{26}$$

D. Wilson has compiled a list of the smallest nth powers of positive integers that are the sums of the nth powers of *distinct* smaller positive integers. The first few are 3, 5, 6, 15, 12, 25, 40, ...(OEIS A030052):

$$3^1 = 1^1 + 2^1 \tag{27}$$
$$5^2 = 3^2 + 4^2 \tag{28}$$
$$6^3 = 3^3 + 4^3 + 5^3 \tag{29}$$
$$15^4 = 4^4 + 6^4 + 8^4 + 9^4 + 14^4 \tag{30}$$
$$12^5 = 4^5 + 5^5 + 6^5 + 7^5 + 9^5 + 11^5 \tag{31}$$
$$25^6 = 1^6 + 2^6 + 3^6 + 5^6 + 6^6 + 7^6 + 8^6 + 9^6 + 10^6 + 12^6 + 13^6 + 15^6 + 16^6 + 17^6 + 18^6 + 23^6 \tag{32}$$
$$40^7 = 1^7 + 3^7 + 5^7 + 9^7 + 12^7 + 14^7 + 16^7 + 17^7 + 18^7 + 20^7 + 21^7 + 22^7 + 25^7 + 28^7 + 39^7 \tag{33}$$
$$84^8 = \begin{array}{l} 1^8 + 2^8 + 3^8 + 5^8 + 7^8 + 9^8 + 10^8 + 11^8 + 12^8 + 13^8 + 14^8 + 15^8 + \\ 16^8 + 17^8 + 18^8 + 19^8 + 21^8 + 23^8 + 24^8 + 25^8 + 26^8 + 27^8 + 29^8 + \\ 32^8 + 33^8 + 35^8 + 37^8 + 38^8 + 39^8 + 41^8 + 42^8 + 43^8 + 45^8 + 46^8 + 47^8 + \\ 48^8 + 49^8 + 51^8 + 52^8 + 53^8 + 57^8 + 58^8 + 59^8 + 61^8 + 63^8 + 69^8 + 73^8 \end{array} \tag{34}$$
$$47^9 = \begin{array}{l} 1^9 + 2^9 + 4^9 + 7^9 + 11^9 + 14^9 + 15^9 + 18^9 + \\ 26^9 + 27^9 + 30^9 + 31^9 + 32^9 + 33^9 + 36^9 + 38^9 + 39^9 + 43^9 \end{array} \tag{35}$$
$$63^{10} = \begin{array}{l} 1^{10} + 2^{10} + 4^{10} + 5^{10} + 6^{10} + 8^{10} + 12^{10} + 15^{10} + 16^{10} + 17^{10} + 20^{10} + 21^{10} + \\ 25^{10} + 26^{10} + 27^{10} + 28^{10} + 30^{10} + 36^{10} + 37^{10} + 38^{10} + 40^{10} + 51^{10} + 62^{10}. \end{array} \tag{36}$$

SEE ALSO:

abc Conjecture, Archimedes' Cattle Problem, Bachet Equation, Brahmagupta's Problem, Cannonball Problem, Catalan's Problem, Diophantine, Diophantine Equation--2nd Powers Diophantine Equation--3rd Powers, Diophantine Equation--4th Powers, Diophantine Equation--5th Powers Diophantine Equation--6th Powers, Diophantine Equation--7th Powers, Diophantine Equation--8th Powers, Diophantine Equation--9th Powers, Diophantine Equation--10th Powers, Diophantine Equation--*n*th Powers, Diophantus Property, Euler Brick, Euler Quartic Conjecture, Fermat's Last Theorem, Fermat Elliptic Curve Theorem, Genus Theorem, Hurwitz Equation, Markov Number, Monkey and Coconut Problem, Multigrade Equation, *p*-adic Number, Pell Equation, Pythagorean Quadruple, Pythagorean Triple, Rational Distance Problem, Thue Equation

REFERENCES:

Alpern, D. "Sums of Powers." http://www.alpertron.com.ar/SUMPOWER.HTM.

Bashmakova, I. G. *Diophantus and Diophantine Equations.* Washington, DC: Math. Assoc. Amer., 1997.

Beiler, A. H. *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains.* New York: Dover, 1966.

Carmichael, R. D. *The Theory of Numbers, and Diophantine Analysis.* New York: Dover, 1959.

Courant, R. and Robbins, H. "Continued Fractions. Diophantine Equations." §2.4 in Supplement to Ch. 1 in *What Is Mathematics?: An Elementary Approach to Ideas and Methods, 2nd ed.* Oxford, England: Oxford University Press, pp. 49-51, 1996.

Davis, M. "Hilbert's Tenth Problem is Unsolvable." *Amer. Math. Monthly* **80**, 233-269, 1973.

Davis, M. and Hersh, R. "Hilbert's 10th Problem." *Sci. Amer.* **229**, 84-91, Nov. 1973.

Davis, M. "Hilbert's Tenth Problem is Unsolvable." Appendix 2 in *Computability and Unsolvability.* New York: Dover, 1999-235, 1982.

Dickson, L. E. "Linear Diophantine Equations and Congruences." Ch. 2 in *History of the Theory of Numbers, Vol. 2: Diophantine Analysis.* New York: Dover, pp. 41-99, 2005.

dmoz. "Equal Sums of Like Powers." http://dmoz.org/Science/Math/Number_Theory/Diophantine_Equations/Equal_Sums_of_Like_Powers/.

Dörrie, H. "The Fermat-Gauss Impossibility Theorem." §21 in *100 Great Problems of Elementary Mathematics: Their History and Solutions.* New York: Dover, pp. 96-104, 1965.

Ekl, R. L. "New Results in Equal Sums of Like Powers." *Math. Comput.* **67**, 1309-1315, 1998.

Guy, R. K. "Diophantine Equations." Ch. D in *Unsolved Problems in Number Theory, 2nd ed.* New York: Springer-Verlag, pp. 139-198, 1994.

Hardy, G. H. and Wright, E. M. *An Introduction to the Theory of Numbers, 5th ed.* Oxford, England: Clarendon Press, 1979.

Hunter, J. A. H. and Madachy, J. S. "Diophantos and All That." Ch. 6 in *Mathematical Diversions.* New York: Dover, pp. 52-64, 1975.

Ireland, K. and Rosen, M. "Diophantine Equations." Ch. 17 in *A Classical Introduction to Modern Number Theory, 2nd ed.* New York: Springer-Verlag, pp. 269-296, 1990.

Jones, J. P. and Matiyasevich, Yu. V. "Exponential Diophantine Representation of Recursively Enumerable Sets." *Proceedings of the Herbrand Symposium, Marseilles, 1981.* Amsterdam, Netherlands: North-Holland, pp. 159-177, 1982.

Lang, S. *Introduction to Diophantine Approximations, 2nd ed.* New York: Springer-Verlag, 1995.

Matiyasevich, Yu. V. "Solution of the Tenth Problem of Hilbert." *Mat. Lapok* **21**, 83-87, 1970.

Matiyasevich, Yu. V. *Hilbert's Tenth Problem.* Cambridge, MA: MIT Press, 1993. http://www.informatik.uni-stuttgart.de/ifi/ti/personen/Matiyasevich/H10Pbook/.

Meyrignac, J.-C. "Computing Minimal Equal Sums of Like Powers." http://euler.free.fr/.

Mordell, L. J. *Diophantine Equations.* New York: Academic Press, 1969.

Nagell, T. "Diophantine Equations of First Degree." §10 in *Introduction to Number Theory.* New York: Wiley, pp. 29-32, 1951.

Ogilvy, C. S. and Anderson, J. T. "Diophantine Equations." Ch. 6 in *Excursions in Number Theory.* New York: Dover, pp. 65-83, 1988.

Olds, C. D. Ch. 2 in *Continued Fractions.* New York: Random House, 1963.

Sloane, N. J. A. Sequence A030052 in "The On-Line Encyclopedia of Integer Sequences."

Weisstein, E. W. "Books about Diophantine Equations." http://www.ericweisstein.com/encyclopedias/books/DiophantineEquations.html.

Referenced on Wolfram|Alpha: Diophantine Equation

CITE THIS AS:

Weisstein, Eric W. "Diophantine Equation." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/DiophantineEquation.html

Diophantine equation, equation involving only sums, products, and powers in which all the constants are integers and the only solutions of interest are integers. For example, 3x + 7y = 1 or x2 – y2 = z3, where x, y, and z are integers. Diophantine equations fall into three classes: those with no solutions, those with only finitely many solutions, and those with infinitely many solutions. Solving a linear Diophantine equation means that you need to find solutions for the variables x and y that are integers only. Finding integral solutions is more difficult than a standard solution... How to Solve a Linear Diophantine Equation. Co-authored by wikiHow Staff |17 References. This article was co-authored by our trained team of editors and researchers who validated it for accuracy and comprehensiveness.