Diophantus, ca. 240[1]

1 Introduction

So little is known of **Diophantus**, that the dates of his life are given in the two century range 150 AD - 350 AD, likely ∼250 AD. He is believed to have lived to be about 84 years. According to tradition his age is determined from the "conundrum", dating from the fifth-sixth century:

> *God granted him to be a boy for the sixth part of his life, and adding a twelfth part to this, He clothed his cheeks with down; He lit him the light of wedlock after a seventh part, and five years after his marriage He granted him a son. Alas! late-born wretched child; after attaining the measure of half his father's life, chill Fate took him. After consoling his grief by this science of numbers for four years he ended his life.*

2 Works

Diophantus was prolific. He wrote

Arithmetica (13 Books – only 6 are now Extant)

On Polygonal Numbers of which only fragments now exist

Porisms (may have originally been part of Arithmetica, as in the latter they are referenced as though they are there

In ancient and even in more recent times, commentaries would frequently be written on notable books. Indeed, one measure of the book's value to the professional community is the number of commentaries written on it. For *Arithmetica* commentaries were written by

[1]

- Hypatia, daughter of Theon of Alexandria, who commented only on the first 6 books.
- Psellus 11^{th} century,
- Georgius Pachymeres (1240-1310)
- M. Plamides (1260-1310)
- several Arab mathematicians

Translations of *Arithmetica*:

- Regionontanus – 1463 first to call attention to Diophantus.
- Rafael Bombelli – 1570 translated a manuscript found in the Vatican. It was not published but was included in his own book *Algebra* (1572).
- Wilhelm Holzman (aka Xylander) – produced an excellent Latin translation in 1575.
- Bachet – 1621, published the present standard edition. The second edition was carelessly produced, but does contain the epoch-making notes of Fermat – the editor was S. Fermat.
- Simon Stevin $\sim$ 1585, French version of Books I–IV based on Xylander.
- $\left.\begin{array}{l}\text{Otto Schultz – 1822}\\ \text{G. Wertheria } \sim 1890\end{array}\right\}$ German versions based on Bachet.

3 *Arithmetica*

Before considering several of the types of results found in *Arithmetica* it is worth taking a few moments to consider a little background about algebra and the types of problems Diophantus solves. In the first case, because geometrical reasoning is not particularly penalized by rhetoric and was the dominant mathematical form of the day, algebra was compelled to follow suit. However, the problems solved by Diophantus are every bit as *tricky* today as they were two millenia ago.

To be specific, we may ask what was the form of algebra in these very early days? There are roughly three classifications of algebra centered on the form of presentation.

1. Rhetorical algebra $\sim$ complete prose.
2. Syncopated Algebra $\sim$ use of some abbreviations and symbols – Diophantus and latter to early 17^{th} century
3. Symbolic Algebra $\sim$ complete symbolic notation – no prose.

The last form did not appear until relatively recent times. Symbolism was not in anything near wide usage until the early seventeenth century. Pure symbolism in mathematical expression is unquestionably a contributing factor that has resulted in the explosion of mathematics dating from that time, which if anything is expanding today at an ever increasing pace[2]. Diophantus wrote with limited symbols, but it must be surmised that after a length of time he must have developed a deep intuition and problem familiarity that permitted him to use many abbreviations (semi-symbolism) that never appeared in the published works.

First of all the problems of *Arithmetica* are algebraic. Diophantus was not the first to consider such problems nor was he the originator of his principle technique, that of *false position*. Indeed, the Egyptians used the method of false position to solve relatively simple algebraic equations. Recall the solution of the problem $x + \frac{1}{7}x = 19$ was solved first by assuming that $x = 7$ and then correcting the *false* solution by multiplication $7 \times \frac{19}{8}$. Other, similar, problems were solved by this method as well. We have also seen the Babylonian mathematicians solve simple linear systems using a *false* assumption.

In Heron's *Metrica* several indeterminate problems are posed. Indeterminate problems are of a type where there may be several solutions and the student is asked to find one or all of them. In most of these problems the student is asked to find an integer or rational solutions. Here is an example of one such problem.

[2] Equally, one might argue that modern computers and computer algebra systems, with their immense numeric and symbolic computational power may contribute to another explosive wave of mathematical development, one that has only just begun. To be sure, the powerful mathematics is being done today without any technology whatever and will continue throughout next millennium. However, the opportunities that modern technology afford may inspire new directions of research impossible without them, just as symbols permitted four centuries ago.

Example. Find two rectangles for which the perimeter of the first is three times that of the second and the area of the second is three times that of the first. Mathematically, we are asked to find integers $a,\ ,b,\ c,$ and d for which

$$\begin{aligned} a+b &= 3cd \\ c+d &= 3ab \end{aligned}$$

Example. Find a triangle having rational sides with area 5. Alternatively, find a right triangle with rational sides such that the sum of its area and perimeter is a given value.

Problems of these types can be prodigiously challenging to solve, even with modern symbolism. Moreover, the use of a purely rhetorical system can only make them more difficult. A good number of mathematicians, high on our lists of the truly great, are remembered partly if not exclusively due to their genius at solving indeterminate problems and proving theorems about them.

3.1 Symbolism of Diophantus

$\star$ The beginning of symbolism: The unknown (x – to us)

$$x = \begin{cases} \zeta \quad S \quad \zeta' & \text{invarious editions} \\ y \qquad {}'S^{\circ} \quad \alpha\rho & \end{cases}$$

$$\begin{aligned} x^2 &:= \Delta^{\Upsilon} \\ x^3 &:= K^{\Upsilon} \\ x^4 &:= \Delta^{\Upsilon}\Delta \\ x^5 &:= \Delta K^{\Upsilon} \\ x^6 &:= K^{\Upsilon}K \\ \zeta^{x} &:= 1/x \\ \Delta^{\Upsilon^{x}} &:= 1/x^2 \end{aligned}$$

There is no symbol for $+$. Essentially, the plus operation was the default. No symbol between variables implies the plus operation. We also have

$$\mathrlap{\Lambda}\,\uparrow \ := \ \text{minus} \qquad \overset{\circ}{M} := \text{units}$$

An example:

$$K^{\Upsilon}\alpha\,\Delta^{\Upsilon}i\gamma\,\zeta\varepsilon\;\overset{\circ}{M}\,\beta = x^3+13x^3+5x+2$$

More examples:

$$K^{\Upsilon}\alpha\,\zeta\eta\,\pitchfork\Delta^{\Upsilon}\varepsilon\;\overset{\circ}{M}\,\alpha = x^3-5x^2+8x-1$$

$$\Delta^{\Upsilon}i\varepsilon\,\pitchfork\overset{\circ}{M}\,\lambda\theta = 15x^2-39$$

Note that in the first example above Diophantus collects the negative terms so that what was written corresponds literally to $x^3 + 8x - (5x^2 + 1)$. Diophantus introduced sufficient symbolism to become well aware of the laws of exponents, which is relatively simple to perceive from modern notation.

3.2 The methods and ground rules of Diophantus

The types of solutions.

- No solutions are accepted other than positive rational numbers.
- Excluded are negative numbers and surds[3], and imaginary numbers. For examples, Diophantus would describe $4 = 4x + 20$ as absurd because the solution $x = -4$. Neither would the solution of $x^2+1 = 0$ be permitted, as the roots are imaginary.

The types of equations:

- (A) Determinate equations – single variable.
- (B) Indeterminate equations – two or more unknowns. Here there is a weakness in notation.

[3] A number that is can be obtained from rational numbers by a finite number of additions, multiplications, divisions, *and* root extractions is called a surd. An irrational number of the form $\sqrt[n]{a}$ in which a is rational is called a pure surd of index n. For $n = 2$ the surd is quadratic. Surds that are not pure are called mixed. Geometrically, surds are all *constructable numbers* on the basis of a compass and straight edge.

3.3 Some examples

General form for intermediate equations of the second degree:

$$\begin{array}{cl} Ax^2+Bx+C=y^2 & \text{– single equation} \\ \begin{array}{l} x+y=m \\ x^2+y^2=n \end{array} & \text{– two variables} \end{array}$$

---

(1) The single equation: $Ax^2+Bx+C=y^2$

Case (i) $\begin{array}{ll} A=C=0 & Bx=y^2 \\ A=0 & Bx+C=y^2 \end{array}\Bigg\}$ Soln. Take $y^2=m^2$ and solve

Case (ii) $C=0$ $Ax^2+Bx=y^2$ Soln. Take $y=\frac{m}{n}x$

Case (iii) $B=0$ $Ax^2+C=y^2$

$$\begin{array}{lll} (\alpha) & A=a^2: & a^2x^2+c=(ax\pm m)^2\to x=\pm\frac{C-m^2}{2ma} \\ (\beta) & C=c^2: & Ax+c^2=(mx\pm c)^2\to x=\pm\frac{2mc}{A-m^2} \end{array}$$

Case (iv) $Ax^2+Bx+C=y^2$

(2) Double equations:

$$\begin{aligned} mx^2+\alpha x+a &= u^2 \\ nx^2+\beta x+b &= w^2 \end{aligned}$$

- Simplest case:

$$\begin{aligned} \alpha x+a=u^2 \\ \beta x+b=w^2 \end{aligned}$$

To add the same number to two given numbers so as to make each a square.

Diophantus gives two complex solutions, the second assuming $a=b=n^2$.

⋆ Other examples from Book II:

$$x^2 + y = u^2, \quad y^2 + x = v^2$$

(Assume $y = 2mx + m^2$, and one equation is satisfied.)

$$\begin{gathered} x^2 - y = u^2, \quad y^2 - x = v^2 \\ x^2 + (x+y) = u^2, \quad y^2 + (x+y) = v^2 \\ (x+y)^2 + x = u^2, \quad (x+y)^2 + y = v^2 \\ y^2 - z = u^2, \quad z^2 - x = v^2, \quad x^2 - y = w^2 \end{gathered}$$

Solve.

$$\begin{aligned} x + a &= u^2 \\ x + b &= v^2 \end{aligned}$$

Solution.

$$a - b = u^2 - v^2 = (u-v)(u+v)$$

Select

$$\begin{aligned} u - v &= a - b \\ u + v &= 1. \end{aligned}$$

Solve for u, v. Hope x comes out to be plus. Else factor differently.

Example. Solve

$$\begin{aligned} x + 3 &= u^2 \\ x + 2 &= v^2 \\ 1 = u^2 - v^2 &= (u-v)(u+v) = \tfrac{1}{4} \times 4. \end{aligned}$$

Take

$$\begin{array}{c} u - v = 1/4 \\ u + v = 4 \\ \hline \end{array}$$

$$\begin{gathered} 2u = 17/4 \to u = 17/8 \\ 2v = 15/4 \to v = 15/8 \\ \to x = 97/64. \end{gathered}$$

Note: The factorization $\frac{1}{2} \times 2$ above yields a negative x.

$\star$ From Book III come the quadratic systems.

$$(x+y+z)^2 - x^2 = u^2, \quad (x+y+z)^2 - y^2 = v^2,$$
$$(x+y+z)^2 - z^2 = w^2$$

and

$$x+y+z = t^2, \quad y+z-x = u^2,$$
$$z+x-y = v^2, \quad x+y-z = w^2$$

and

$$yz + x^2 = u^2, \quad zx + y^2 = v^2,$$
$$xy + z^2 = w^2$$

$\star$ From Book IV come the examples.

$$x^2 + y^2 + z^2 = (x^2 - y^2) + (y^2 - z^2) + (x^2 - z^2)$$
$$x^2 + y^2 + z^2 + w^2 - (x+y+z+w) = a$$

and the quadratic type system

$$x^2 + y = u^2 \quad x + y = u$$
$$x^2 + y = u \quad x + y = u^2$$

$\star$ From Book IV we also have the cubic type systems

$$x^2 y = u, \quad xy = u^3$$

and

$$x^3 + y^2 = u^3, \quad z^2 + y^2 = v^2$$
$$x^3 + y^3 = x + y$$

Example. Solve $x^3 + y = (x+y)^3$.

Solution. (Method of False Position.) Assume $x = 2y$. Thus

$$\begin{aligned} 8y^3 + y = (3y)^3 &= 27y^3 \\ y &= 19y^3 \\ 19y^2 &= 1 \end{aligned}$$

But 19 is not a square!! Retracing steps, note that $19 = 3^3 - 2^3$, and 3 comes from the assumption $x = 2y$. Hence, we need to find two consecutive numbers such that the difference of their cubes is a square. That is, we will take $x = zy$, where z is chosen so that $(z+1)^3 - z^3$ is a perfect square. Thus,

$$\begin{aligned} (z+1)^3 - z^3 = 3z^2 + 3z + 1 \equiv & \quad (1-2z)^2 \\ & 1 + 4z^2 - 4z \end{aligned}$$

Or

$$\begin{gathered} z^2 - 7z = 0 \\ z(z-7) = 0. \end{gathered}$$

So

$$z = 7.$$

Take $x = 7y$. It follows that $343y^3 + y = (8y)^3$, or $169y^2 = 1$. Hence $y = 1/13$ and $x = 7/13$.

3.4 Other Problems

The Method of Limits It is desired to find a power x^n between two given numbers a and b.

> To solve this problem Diophantus multiplies a and b by powers 2^n, 3^n, ... until some n^{th} power, c^n lies between ap^n and bp^n. Then he sets $x = c/p$ as it is easily seen that $x^n = c^n/p^n$ lies between a and b.

More Method of Limits. Divide a number into a sum of squares each one of which satisfies some property.

Example 1. Divide 13 into the sum of two squares, each of which is greater than 6.

Example 2. Divide 10 into the sum of three squares, each of which is greater than 3.

The work of Diophantus has attracted mathematicians for the last two millenia. No diminution of effort has occurred. Indeed, solving polynomial equations for integer solutions is now a major area of mathematics usually included within analytic number theory, with countless applications. It includes some of the deepest and most difficult mathematics being done today. For example, the so-called “Fermat’s last theorem” is among the many Diophantine equations whose solutions were extraordinarily difficult to decide.

4 Modern Diophantine Equations.

Definitions. A polynomial **Diophantine equation** is an equation of the form

$$(1) \qquad P(x_1, x_2, \ldots, x_m) = 0$$

where $m \in Z^+$ and $P \in Z[x_1, x_2, \ldots, x_m]$, i.e. P is a polynomial with integer coefficients. The x_i, $i = 1, \ldots, m$ are assumed to be integers. If $P(a_1, a_2, \ldots, a_m) = 0$ for $a_i \in Z$, $i = 1, \ldots, m$, we say that $(a_1 \ldots a_m)$ is a **solution** of (1).

Examples.

$$y^3 = x^2 + 999 \qquad \text{Solution: } (1,10)$$

$$x_1^2 + x_2^2 + x_3^2 = 7 \qquad \textbf{no} \text{ solutions}$$

There are two types of questions normally asked: **descriptive** and **quantitative**. Consider the Diophantine equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$$

The descriptive question asks for a solution in integers for a given and fixed n. The quantitative question asks for the number of solutions.

Here’s a typical theorem in the theory of Diophantine Equations.

Theorem. If a, b, c, d and e are not zero and not all of the same sign, there exist integral solutions, not all zero, of

$$ax^2 + by^2 + cz^2 + du^2 + ev^2 = 0.$$

However, the same theorem for

$$ax^2 + by^2 + cz^2 + du^2 = 0$$

must have additional conditions. (Namely, two of a, b, c, d must not be even and

$$\frac{1}{4}abcd = 5(\text{mod } 8)$$

.

Theorem. If k is any integer, then

$$k^2 = 0 \text{ or } 1(\text{mod4}).$$

Corollary. For any two integers u and v,

$$u^2 + v^2 = 0,\ 1,\ \text{or } 2(\text{mod4}).$$

Therefore, no integer congruent to 3(mod 4) can be written as the sum of two squares.

Theorem. (Lagrange) Every positive integer can be written as the sum of four squares. (Zero is admissible as one of the squares.)

Theorem. If a, b, c have no common factor > 1, all integral solutions of $ax + by + cz = 0$ are given by

$$x = bk - cn \qquad y = cs - ak \qquad z = an - bs,$$

where s, n, and k are integers.

A famous example. Consider the polynomial

$$P(x, y, z) = x^n + y^n - z^n.$$

If $n = 2$, solutions of $P(x, y, z) = 0$ are Pythagorean triples for which it can be shown that, if primitive, it must have the form

$$x = m^2 - n^2 \quad y = 2mn, \qquad z = m^2 + n^2.$$

If $n \geq 3$ Fermat conjectured and in 1995 Andrew Wiles proved that there can be no integer solutions.

Recall the polynomial:

$$P(x_1, x_2, \ldots, x_n) = 0.$$

A. Hilbert (10^{th} problem). "Is there an algorithm for determining whether or not a given Diophantine equation (polynomial) has a solution?" (1902)

Answer. No. J. Robinson (1952) Mitijasević (1970).

B. If we *know* there is a solution, then we can find it by applying all m-tuples and testing them.

C. To find algorithms for restricted classes of Diophantine equations

yes,	$n = 1$	Greeks	$n = 3$	A. Baker
for	$n = 2$	Gauss		

D. Is there an upper bound on the number of solutions? Or are there an infinite number?

Compare: $x^2 + y^2 = z^2$ and $x^3 + y^3 = z^3$

Note. *The value of finding only some solutions of a fixed Diophantine equation is usually rather small.*

Diophantine approximation The approximation of irrationals by rationals is one problems characteristic to the field of Diophantine approximation. For example, as is well known any irrational α is approximable by infinitely many rationals $\frac{h}{k}$. Thus

$$|\alpha - \frac{h}{k}| < \epsilon$$

has infinitely many solutions for every ϵ. But how small can this be in terms of the rational approximants? Can we have

$$|\alpha - \frac{h}{k}| < \frac{1}{k}\epsilon$$

which means that $|k\alpha - h| < \epsilon$. Can we have

$$|\alpha - \frac{h}{k}| < \frac{1}{k^2}\epsilon$$

which means that $|k\alpha - h| < \frac{1}{k}\epsilon$. The answer is contained in the following theorem.

Theorem. For any irrational α there exist infinitely many rationals $\frac{h}{k}$ such that

$$|\alpha - \frac{h}{k}| < \frac{1}{\sqrt{5}k}\epsilon.$$

No number greater than $\sqrt{5}$ can replace the $\sqrt{5}$ above.

For algebraic numbers, there are more general versions of this theorem pertaining to the zeros of polynomial with integer coefficients.

Another type of result is this:

Theorem. For any irrational α the numbers α, 2α, 3α, $\ldots$ are uniformly distributed modulo 1.

Recall that a sequence α_1, α_2, α_3, $\ldots$ is **uniformly distributed** over an interval I if for every subinterval J, the number of elements of the sequence α_1, α_2, $\ldots$, α_n that are in J, denoted by $n(J)$, satisfies

$$\lim_{n\to\infty} \frac{n(J)}{n} = \frac{|J|}{|I|}$$

where $|J|$ is the length of J.