The Second International Conference "Problems of Cybernetics and Informatics"
September 10-12, 2008, Baku, Azerbaijan. The plenary paper
www.pci2008.science.az/5/01.pdf

DIOPHANTINE ANALYSIS

Djangir Babayev

Cox Associates, Denver, CO, USA
4834 Macintosh Place, Boulder CO, USA, 80301
djangirbabayev@aol.com

Diophantus was a Greek Mathematician sometimes known as"the father of algebra", who lived in 3rd century of AD (200-284). He is best known for his *Arithmetica*. Diophantus studied solving equations or systems of equations with numbers of equations less than number of variables for finding integer solutions and was first to try to develop algebraic notations. His works had enormous influence on the development of Number Theory. Modern Diophantine Analysis embraces mathematics of solving equations and problems in integer numbers.

While its roots reach back to the third century, diophantine analysis continues to be an extremely active and powerful area of number theory. Many diophantine problems have simple formulations, but they can be extremely difficult to attack, and many open problems and conjectures remain.

Division algorithm.

If $a>b>0$, integers, then
$a=bq+r$, where q and r are integers and $b>r\geq 0$.

Let $gcd(a,b)$ be the greatest common divisor of integers a and b.

Theorem 1. $gcd(a,b) = gcd(b,r)$

P R O O F.

Suppose $gcd(a,b) =d$. Then $a=sd$ and $b=td$. $r=a-bq=sd-bqd=(s-bq)d$. This implies $gcd(b,r)=d$ and completes the proof. ▓

Euclids algorithm for determining $gcd(a,b)$ works based on

$gcd(a,b) = gcd(b,r)$, and $b=r q_2+r_2$, $r > r_2 \geq 0$ by repeatedly applying the division algorithm to the last two remainders.

Consider the most simple Diophantine equation, **linear equation** with two variables

(1) $ax+by=c$.

In the case of $c= gcd(a,b)$ (or $c=k\, gcd(a,b)$, with $k>1$ a positive integer) equation (1) has infinitely many solutions of the form

$x=\frac{b}{\gcd(a,b)}k+x_0$, $y=-\frac{a}{\gcd(a,b)}k+y_0$, where

(x_0, y_0) is a partial solution.

If c is not divided by $gcd(a,b)$, then equation (1) has no integer solutions.

Equation (1) can be solved by Extension of the Euclidean algorithm for determining $gcd(a,b)$.

In the case of $c= gcd(a,b)$ (1) is called Etienne Bezuot's (1730-1783) identity.

It can be generalized to the case of arbitrary number of variables

(2) $a_1x_1 + a_2x_2 + ... + a_nx_n = c$ with the same properties.

An indian mathematician Brahmagupta (598-668) developed an elementary, but comprehensive method of parameters for solving (1).

Example 1. (Brahmagupta's approach)

Consider equation

(3) $37x-107y =25$.

Solve for a variable with the smallest absolute value coefficient

$$x=\frac{107y+25}{37}=\frac{111y-4y+37-12}{37}$$

$x=3y+1-\frac{12+4y}{37}$.

x and $3y+1$ are integers, so $z=\frac{12+4y}{37}$ must be integer. Solve this last equation for

$y=\frac{37z-12}{4}= -3+9z+\frac{z}{4}$.

y and -3+9z are integers, so $t=\frac{z}{4}$ must be integer.

Now we have a general solution to (3) which includes an integer parameter t

$z=4t$,

$y=9z-3+t = 37t-3$,

$x=3y+1-z=111t-9+1-4t=107t-8$,

where t is an arbitrary integer, $t=\pm 1, \pm 2, \ldots$.

Pyphagorean Triples

Three integers *a, b, c* are *Pyphagorean Triples* if the sum of squares of two of them is equal to the square of the third $a^2+ b^2=c^2$. Pyphagoras of Samos lived in 569-475 BC. Theorem known as Pyphagoras Theorem was known to Babylonians for about 1000 years earlier, but Pyphagoras was first to prove it. Pyphagorean triples were studied By Babylonians and collection of Triples carved on clay plates were excavated in the territory of modern Irak by English researchers and now are stored in Louvre Museum in Paris. Pyphagoras is credited for analytical formulae for Pyphgorean numbers

$a=m$,

$b=\frac{1}{2}(m^2-1)$,

$c=\frac{1}{2}(m^2+1)$,

$m^2+\{\frac{1}{2}(m^2-1)\}^2=\{\frac{1}{2}(m^2+1)\}^2$, where m is an odd number.

For an arbitrary integer m the following is true

$a=2m$,

$b=(m^2-1)$

$c=(m^2+1)$,

$4m^2+(m^2-1)^2=(m^2+1)^2$.

This second Triple are twice larger than the previous.

In general, if *a, b, c* are Pyphagorean numbers, then *ka, kb and kc* are Pyphagorean too.

Chinese Remainders problem

An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

$x=2q_2+1$;

$x=3q_3+1$;

$x=4q_4+1$;
$x=5q_5+1$;
$x=6q_6+1$;
$x=7q_7$;

Problems of this kind are all examples of what universally became known as the *Chinese Remainder Theorem*. In mathematical parlance the problems can be stated as finding n, given its remainders of division by several numbers $m_1, m_2, ..., m_k$:

$n = n_1 \pmod{m_1}$
$n = n_2 \pmod{m_2}$
...
$n = n_k \pmod{m_k}$

Nonlinear equations.

Pell's equation is a Diophantine equation of the form $x^2 - ny^2 = \pm 1$, where *n* is a nonsquare integer and *x* and *y* are integers. Trivially, *x* = 1 and *y* = 0 always solve this equation. Lagrange proved that for any natural number *n* that is not a perfect square there are *x* and *y* > 0, that satisfy Pell's equation. Moreover, infinitely many such solutions of this equation exist. These solutions yield good rational approximations of the form *x*/*y* to the square root of *n*. This equation was first studied extensively in India, starting with Brahmagupta, who developed the *chakravala* method to solve Pell's equation and other quadratic indeterminate equations in his *Brahma Sphuta Siddhanta* in 628, about a thousand years before Pell's time. His *Brahma Sphuta Siddhanta* was translated into Arabic in 773 and was subsequently translated into Latin in 1126. Bhaskara II in the 12th century and Narayana in the 14th century both found general solutions to Pell's equation and other quadratic indeterminate equations. Solutions to specific examples of the Pell equation, such as the Pell numbers arising from the equation with *n* = 2, had been known for much longer, since the time of Pythagoras in Greece and to a similar date in India.

Pell numbers arise historically and most notably in the rational approximation to the square root of 2. If two integers *x* and *y* form a solution to the Pell equation

$$x^2 - 2y^2 = \pm 1,$$

then their ratio provides a close approximation to $\sqrt{2}$. The sequence of approximations of this form is

$$\frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \ldots, \frac{P_{n-1} + P_n}{P_n},$$

where the denominator of each fraction is a Pell number (starting with *n*=2) and the numerator is the sum of a Pell number and its predecessor in the sequence of Pell numbers. Pell numbers are defined as

$P_0=0$, $P_1=1$, and for $n>1$, $P_n=2P_{n-1}+P_{n-2}$, consequently

0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, …

That is, the approximations to $\sqrt{2}$ have the form $\frac{P_{n-1}+P_n}{P_n}$. The approximation of this type was known to Indian mathematicians in the third or fourth century B.C. The Greek mathematicians of the fifth century B.C. also knew of this sequence of approximations; These approximations can be derived from the continued fraction expansion of $\sqrt{2}$.

Erdosh-Straus conjecture

The Erdős–Straus conjecture states that, for every positive integer $n \geq 2$, there exists a solution to equation

$$\frac{4}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z},$$

with *x*, *y*, and *z* all positive integers. In other words The **Erdős–Straus conjecture** states that for all integers $n \geq 2$, the rational number $4/n$ can be expressed as the sum of three unit fractions.

For instance, for $n = 1801$, there exists a solution $\frac{4}{1801}=\frac{1}{451}+\frac{1}{295364}+\frac{1}{3249004}$.
Paul Erdos and Ernst G. Straus formulated the conjecture in 1948.

Various authors have used computers to perform brute-force searches for counterexamples to the conjecture. These searches can be greatly sped up by considering only prime numbers that are not covered by known congruence relations. Searches of this type by Allan Swett confirmed that the conjecture is true for all n up to 10^{14}

If we multiply both sides of the Erdosh equation by $nxyz$ we find an equivalent form $4xyz=n(xy+xz+yz)$ for the problem as a Diophantine equation. The restriction that *x*, *y*, and *z* be positive is essential to the difficulty of the problem.

The great Theorem of Ferma, and Hilbert's tenth problem are related to Diophantine Analysis.