Continued Fractions in disguise

Short Undergraduate Mathematics Seminar - 54
Gaurish Korpal*
gaurish4math.wordpress.com

October 16, 2015

Abstract

Continued Fractions have fascinated many mathematicians due to their mystical properties. Today I will discuss one of my personal experiences with continued fractions (without giving its exact mathematical definition). I will illustrate two methods (without proof) for solving equations in two variables in integers. Ability to do basic arithmetic is required.

1 $ax + by = c$, where $a, b, c \in \mathbb{Z}$; $a, b \neq 0$

Theorem 1.1. *Let $a, b, c \in \mathbb{Z}$; $a, b \neq 0$. Consider the linear equation $ax + by = c$. If $d = \gcd(a, b)$ then this linear equation is solvable in integers if and only if $d \mid c$.*

Sketch of Proof. The basic idea behind proof is to apply Euclid's Division Algorithm in bottom-up fashion

Now I will compare two forms of Euclid's Division Algorithm (for proof see pp. 34 of [Si]). Let's consider following example (pp. 47-48 of [K]):

Example 1.1. *Solve $127x - 52y + 1 = 0$ for integers.*

Solution. Firstly we will calculate $\gcd(127, 52)$

$$127 = 52 \times 2 + 23$$

$$52 = 23 \times 2 + 6$$

$$23 = 6 \times 3 + 5$$

$$6 = 5 \times 1 + 1$$

$$5 = 1 \times 5 + 0$$

Since $\gcd(127, 52) = 1$ this equation is solvable.

Method 1: **Last Partial Quotient Omission & Subtraction**[1]
First step is to create an improper fraction by dividing bigger coefficient by smaller coefficient (magnitude only)
Thus in this example we get: $\frac{127}{52}$
Now separate out the integral part of this fraction:

$$\frac{127}{52} = 2 + \frac{23}{52}$$

Then re-write the fractional part in terms of terminating continued fraction as:

$$\frac{127}{52} = 2 + \frac{23}{52} = 2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5}}}}$$

*2nd year Int. MSc. student, National Institute of Science Education and Research, Jatni
[1]I first time came across this method in [G]

Now we will omit the last partial quotient and simplify the continued fraction so formed:

$$2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1}}} = \frac{22}{9}$$

Now we will subtract this new fraction from our original improper fraction:

$$\frac{127}{52} - \frac{22}{9} = \frac{-1}{52 \times 9}$$

Cross multiply denominators to get:

$$127 \times 9 - 52 \times 22 + 1 = 0$$

Compare it with original equation and get $x = 9$ and $y = 22$ as a particular solution.

Method 2: **Remainder Substitution & Isolation**
The first step is to rewrite the equation first step of division algorithm as:

$$23 = a - 2b, \qquad \text{where we let } a = 127 \quad \& \quad b = 52$$

Next we substitute this value into second equation and also replace 52 by b:

$$b = (a - 2b) \times 2 + 6$$

Now rearrange the terms and isolate the reminder:

$$6 = 5b - 2a$$

Now substitute 6 and 23 in terms of a and b in next equation of division algorithm:

$$a - 2b = (5b - 2a) \times 3 + 5$$

Again rearrange terms and isolate remainder:

$$5 = 7a - 17b$$

Now substitute 5 and 6 in next equation of division algorithm:

$$5b - 2a = (7a - 17b) \times 1 + 1$$

Now rearrange the terms to get:

$$9a - 22b + 1 = 0$$

Comparing with given equation we get: $x = 9$ and $y = 22$ as a particular solution.

Remark: Note that both the methods described above lead to same solutions, which provides a verification to my assertion that at base level both methods are equivalent. It may be noted that these methods provide the least solution of the equation, namely that for which $x < |b|$ and $y < |a|$.

2 $x^2 - Dy^2 = 1$, where $D \in \mathbb{Z}^+$

Theorem 2.1. *Given an equation:*

$$x^2 - Dy^2 = 1$$

where $D \in \mathbb{Z}^+$ and $\sqrt{D}$ is irrational[2]*. This equation possesses a non-trivial solution (x_1, y_1) in positive integers.*

[2] The equation is of no interest when D is a perfect square, since the difference of two perfect squares can never be 1, except in the case $1^2 - 0^2$

Remark: (x_1, y_1) is called the least solution or minimal solution of equation if for $x = x_1$ and $y = y_1$ the binomial $x + y\sqrt{D}$, assumes the least possible value among all the possible values which it will take when all the possible positive integral solutions of the equation are substituted for x and y.

Challenge: Prove this theorem using Diophantine Approximation! (for hints and alternate proof using continued fractions see pp. 50-58 of [K])

Now let's again consider an example to illustrate the steps involved in finding particular solution.

Example 2.1. *Find an integer solution for:* $x^2 - 67y^2 = 1$

Solution. For proof of both of these methods and their equivalence see [Su].

Method 1: **Lagrange's Method**[3]

We can write $\sqrt{D}$ in continued fraction form as:

$$\sqrt{D} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots \atop q_1 + \cfrac{1}{2q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots}}}}}$$

where $q_0 = \lfloor\sqrt{D}\rfloor$.

Because any continued fraction for $\sqrt{N}$ is necessarily of the form:

$$q_0, \underbrace{\overline{q_1, q_2, \ldots, q_2, q_1, 2q_0}}_{n \quad terms}$$

where the period begins immediately after the first term q_0 , and it consists of a symmetrical part $q_1, q_2, \ldots, q_2, q_1$, followed by the number $2q_0$ (for proof see pp. 92 of [D]).

Then the least solution to this equation turns out to be:

$$(x_1, y_1) = \begin{cases} (P_{n-1}, Q_{n-1}) & \text{if } n \quad \text{is even} \\ (P_{2n-1}, Q_{2n-1}) & \text{if } n \quad \text{is odd} \end{cases}$$

where $\frac{P_k}{Q_k} = \delta_k$ is k^{th} convergent of the continued fraction[4] and $\delta_0 = q_0$.

Google says that sqrt(67) = 8.18535277187, so let's start writing our continued fraction:

$$\sqrt{67} = 8 + 0.18535277187 = 8 + \frac{1}{5.3951175907} = 8 + \frac{1}{5 + 0.3951175907}$$

[3]Such equation was first solved in Europe by Brouncker in 1657-58 in response to a challenge by Fermat, using continued fractions. But a method for the general problem was first completely described rigorously by Lagrange in 1766

[4]The expression obtained by omitting all terms of its continued fraction (of say α) starting with some particular term is called *convergent.* The first convergent δ_1 is equal to first partial quotient (q_0). Also convergents satisfy following inequality: $\delta_1 < \delta_3 < \ldots < \delta_{2k-1} < \alpha$ and $\delta_2 > \delta_4 > \ldots > \delta_{2k} > \alpha$. Also we can write k^{th} convergent as: $\delta_k = \frac{P_k}{Q_k}$, $(1 \le k \le n)$ Then we write a recursive formula:

$$\begin{cases} P_k = P_{k-1}q_k + P_{k-2} \\ Q_k = Q_{k-1}q_k + Q_{k-2} \end{cases}$$

Also for consecutive convergents:

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \quad (k > 1)$$

proceed so on 'or' use SAGE math code `continued_fraction(sqrt(67))` to get:

$$\sqrt{67} = 8 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{16 + \cfrac{1}{\ddots}}}}}}}}}}} = [8; 5, 2, 1, 1, 7, 1, 1, 2, 5, 16, 5, 2, \ldots]$$

Hence here, $n = 10$, thus least solution is, (P_9, Q_9).

$$\delta_9 = [8; 5, 2, 1, 1, 7, 1, 1, 2, 5, 16] = 8 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{16}}}}}}}}}}$$

Evaluate manually or use SAGE math code `a = continued_fraction(sqrt(67)); a.convergent(9)` to get:

$$\delta_9 = \frac{48842}{5967} = \frac{P_9}{Q_9}$$

So, $x = 48842$ and $y = 5967$ is a particular solution.

Method 2: **Chakravala Method**[5]

We can prove [6]that the Chakravala does give *all* the solutions using the continued fractions method developed by Lagrange. Moreover, Chakravala algorithm can easily be implemented on a computer.

We will write $(u, v; n)$ to mean $u^2 - Nv^2 = n$. Start with $p_0 = \lfloor\sqrt{N}\rfloor$, here,

$$p_0 = \lfloor\sqrt{67}\rfloor = 8$$

Now, take $q_0 = 1$ and $m_0 = p_0^2 - N$ (note $m_0 < 0$), here,

$$m_0 = 8^2 - 67 = -3$$

Then, we have $\boxed{(p_0, q_0; m_0) = (8, 1; -3)}$

[5]This method is due to Jayadeva, Bhaskara and Narayana from the 11th and 12th centuries. The amazing thing is that this method produces *all* solutions!

[6]As defined below, we need to show that each $m_i \in (-2\sqrt{N}, 2\sqrt{N})$. The m_i's will repeat in cycles - hence called chakravala. However, it is not obvious as yet that some $m_k = 1$ but we can prove this using continued fractions.

Now, choose $x_1 \equiv -p_0 \mod |m_0|$ and $x_1 < \sqrt{N} < x_1 + |m_0|$, here,

$$x_1 \equiv -8 \pmod 3 \qquad \Rightarrow \boxed{x_1 = 7}$$

Suppose (p,q) is a solution of $x^2 - Ny^2 = m$ and (r,s) is a solution of $x^2 - Ny^2 = n$. Then[7],

$$(p,q) * (r,s) := (pr + Nqs, ps + qr) \qquad \text{is a solution of} \quad x^2 - Ny^2 = mn$$

Now note that since $q_0 = 1$,

$$(p_0, q_0) * (x_1, 1) = (p_0x_1 + N, p_0 + x_1) \qquad \text{is the solution of} \quad \big(p_0x_1 + N, p_0 + x_1; m_0(x_1^2 - N)\big)$$

where the numbers $(p_0x_1 + N)$, $(p_0 + x_1)$, $(x_1^2 - N)$ are all multiples of m_0. Also, $|x_1^2 - N|$ is as small as possible. Here:

$$(123, 15; 54) \qquad \text{is another equation-solution generated for } N = 67$$

Indeed,

$$p_0 + x_1 \equiv 0 \pmod{m_0} \qquad \text{and} \qquad p_0x_1 + N \equiv -p_0^2 + N = -m_0 \equiv 0 \pmod{m_0}$$

Moreover, we also have

$$x_1^2 - N \equiv p_0^2 - N = m_0 \equiv 0 \pmod{m_0}$$

We have then, $(p_1, q_1; m_1)$ such that:

$$\begin{cases} p_1 = \dfrac{p_0x_1 + N}{|m_0|} \\ q_1 = \dfrac{p_0 + x_1}{|m_0|} \\ m_1 = \dfrac{x_1^2 - N}{m_0} \end{cases}$$

Also $m_1 > 0$ as $x_1^2 - N < 0$ and $m_0 < 0$.
Here, we have, $\boxed{(p_1, q_1; m_1) = (41, 5; 6)}$

Knowing p_i, q_i, m_i, x_i we shall describe (in that order) $x_{i+1}, m_{i+1}, p_{i+1}, q_{i+1}$ such that $(p_{i+1}, q_{i+1}; m_{i+1})$ holds and stop when (and if!) we reach $m_k = 1$.[Su]

Thus in general, we have following recursive definition:

$$\begin{cases} p_i = \dfrac{p_{i-1}x_i + Nq_{i-1}}{|m_{i-1}|} \\ q_i = \dfrac{p_{i-1} + x_iq_{i-1}}{|m_{i-1}|} \\ m_i = \dfrac{x_i^2 - N}{m_{i-1}} \end{cases}$$

where, $x_{i+1} \equiv -x_i \mod |m_i|$ with $x_{i+1} < \sqrt{N} < x_{i+1} + |m_i|$ and $x_0 = p_0$.
The key point to note is that the choice of the congruence defining x_{i+1} ensures that we get integer values for p_{i+1}, q_{i+1} and m_{i+1} (extend the argument used in obtaining $(p_1, q_1; m_1)$ from $(p_0, q_0; m_0)$) Here, $x_2 \equiv -7 \pmod 6$ and $x_2 < \sqrt{67} < x_2 + 6$, thus $\boxed{x_2 = 5}$ and substitute all values to get $\boxed{(p_2, q_2; m_2) = (90, 11; -7)}$

Continuing in same way we get:

$\boxed{x_3 = 2}$ and $\boxed{(p_3, q_3; m_3) = (131, 16; 9)}$
$\boxed{x_4 = 7}$ and $\boxed{(p_4, q_4; m_4) = (221, 27; -2)}$
$\boxed{x_5 = 7}$ and $\boxed{(p_5, q_5; m_5) = (1678, 205; 9)}$
$\boxed{x_6 = 2}$ and $\boxed{(p_6, q_6; m_6) = (1899, 232; -7)}$
$\boxed{x_7 = 5}$ and $\boxed{(p_7, q_7; m_7) = (3577, 437; 6)}$
$\boxed{x_8 = 7}$ and $\boxed{(p_8, q_8; m_8) = (9053, 1106; -3)}$
$\boxed{x_9 = 8}$ and $\boxed{(p_9, q_9; m_9) = (48842, 5967; 1)}$

[7] This 'composition law' or 'samasabhavana' was discovered by Brahmagupta.

Exercise 2.1. *Find an integer solution for* $x^2 - 61y^2 = 1$

Hint. *Observe that:*

$$\sqrt{61} = [7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, 2, 1, 3, ...] \qquad \Rightarrow (x_1, y_1) = (P_{21}, Q_{21})$$

Remark: The method of finding solutions by using continued fractions can even be extended to equations of form: $ax^2 - by^2 = c$, see [M]. Also we can reduce lot's of calculation steps by using "Brahmagupta's Shortcuts", see pp. 3 of [Su].

References

[D] H. Davenport : *The Higher Arithmetic*, Eighth Edition, Cambridge University Press, ISBN 978-0-511-45555-1 eBook(EBL) (2008)

[G] A. O. Gelfond : *Solving Equations in Integers*, English translation, Little Mathematics Library, Mir Publishers Moscow (1981)

[K] Gaurish Korpal, *Diophantine Equations*, Summer Internship Project Report, http://upgrade.bprim.org/articles-notes/2015/Diophantine-Equations-Gaurish-Korpal (2015)

[M] R. A. Mollin, K. Cheng & B. Goddard : *The diophantine equation* $Ax^2 - By^2 = C$ *solved via continued fraction*, Acta Math. Univ. Comenianae, Vol. LXXI (2), pp. 121-138 (2002)

[Si] Joseph H. Silverman, *A Friendly Introduction to Number Theory*, Fourth Edition, Pearson Education, Inc., ISBN: 978-0-321-81619-1 (2012)

[Su] B. Sury, *Chakravala - a modern Indian method*, Lecture Notes, http://www.isibang.ac.in/~sury/chakravala.pdf (2010)