CS 3430: S19: SciComp with Py
Lecture 21

Pell Equations

Vladimir Kulyukin
Department of Computer Science
Utah State University

Review

The Newton-Raphson Algorithm

Many applications in scientific computing involve solving equations.

There is a function $f(x)$ and we must find a value of x, say $x = r$, such that $f(r) = 0$. This value of x is called a **root** of the equation $f(x) = 0$ (another frequently used term is a **zero** of the equation $f(x) = 0$).

When $f(x)$ is a polynomial, sometimes it is possible to factor and find zeros, sometimes it is impossible or not feasible computationally.

There are several methods for finding an approximation value of a zero to any desired degree of accuracy. The Newton-Raphson algorithm is one such method.

Outline of the Algorithm

To solve $f(x) = 0$, start with an initial guess x_0. If $f(x)$ can be plotted, plot it and take the value of the initial guess from the plot.

If $f(x)$ doesn't look plottable, the only thing to use is your mathematical intuition (and trial and error).

Use the following recurrence to obtain the next approximation x_n from the previous approximation x_{n-1}:

$$x_n = x_{n-1} - \tfrac{f(x_{n-1})}{f'(x_{n-1})}.$$

The termination condition can be determined by the number of iterations or an error of approximation value (if the ground truth is known).

Pell Equations

Motivation

When are the integers x^2 and $2y^2$ are consecutive? We can make the question more general and ask, when are x^2 and ky^2 consecutive?

Who cares?!!! People who do cryptography care, because such numbers are not easy to come by and any numbers that are not easy to come by can be put to productive use to make encryption more bulletproof.

People who do scientific computing also care, because, as we'll see in this lecture, the answer to this question allows us to approximate square roots better.

When Are x^2 and $2y^2$ Consecutive?

Looks like $x = y = 1$ gives us a solution since 1^2 and $2 \cdot 1^2$ are consecutive.

If we play with small numbers or write a simple program to search for such consecutive integers in a given range, we quickly discover that $x = 3$ and $y = 2$ is another solution ($3^2 = 9$ and $2 \cdot 2^2 = 8$ are consecutive).

Another solution is $x = 7$ and $y = 5$, because $7^2 = 49$ and $2 \cdot 5^2 = 50$ are also consecutive.

We'll also find $x = 17$ and $y = 12$, because $17^2 = 289$ and $2 \cdot 12^2 = 288$.

When $x^2 - 2y^2 = \pm 1$?

We can observe that sometimes $x^2 - 2y^2 = 1$ (e.g., 9 - 8) and sometimes $x^2 - 2y^2 = -1$ (e.g., 49 - 50).

We can generalize our previous question and ask, when $x^2 - 2y^2 = \pm 1$?

Number theory tells us that it happens infinitely often. Let's see why.

When $x^2 - 2y^2 = \pm 1$?

Assume that integers x and y satisfy $x^2 - 2y^2 = \pm 1$ and consider the following two recurrences:

$$x' = x + 2y$$
$$y' = x + y$$

Now, $(x')^2 - 2(y')^2 = (x + 2y)^2 - 2(x + y)^2 = x^2 + 4xy + 4y^2 - 2x^2 - 4xy - 2y^2 = -x^2 + 2y^2 = -(x^2 - 2y^2)$.

Since $x^2 - 2y^2 = \pm 1$, $(x')^2 - 2(y')^2 = - \pm 1$.

Looking for x and y in $x^2 - 2y^2 \pm 1$

We can use the recurrences on the previous slide to compute the successive x and y pairs that satisfy $x^2 - 2y^2 \pm 1$. Let's call it `compute_xy`.

```
>>> for n in range(10):
        print(compute_xy(n))
(1, 1)
(3, 2)
(7, 5)
(17, 12)
(41, 29)
(99, 70)
(239, 169)
(577, 408)
(1393, 985)
(3363, 2378)
(8119, 5741)
```

Let's tabulate these results.

Looking for x and y in $x^2 - 2y^2 \pm 1$

Pair number	x	y
0	1	1
1	3	2
2	7	5
3	17	12
4	41	29
5	99	70
6	239	169
7	577	408
8	1393	985
9	3363	2378
10	8119	5741

Pell Equation: Definition

An equation of the form $x^2 - ky^2 = \pm 1$ is called a **Pell equation**.

Solving Pell Equations

We want to find x and y that satisfy $x^2 - ky^2 = 1$. Let's find a pair of positive integers a and b that satisfy $a^2 - kb^2 = 1$. These are initial guesses similar to x_0 in the Newton-Raphson algorithm.

Example: if $k = 2$, then $x^2 - 2y^2 = 1$ has a solution $x = a = 3$ and $y = b = 2$.

Once we have a and b, we know that $(a^2 - kb^2)^n = 1^n = 1$, where n is a positive integer.

Solving Pell Equations

For any $n = 1, 2, 3, 4, \ldots$, we have

$$x^2 - ky^2 = 1 \Rightarrow x^2 - ky^2 = (a^2 - kb^2)^n.$$

We can factor both $x^2 - ky^2$ and $a^2 - kb^2$ as the difference of two squares:

$$(x - \sqrt{k}y)(x + \sqrt{k}y) = (a - \sqrt{k}b)^n(a + \sqrt{k}b)^n,$$

which, in turn, gives us

$$\begin{aligned} x + \sqrt{k}y &= (a + \sqrt{k}b)^n \\ x - \sqrt{k}y &= (a - \sqrt{k}b)^n. \end{aligned}$$

Solving Pell Equations

We can solve for x and y by adding and subtracting the last two equations on the previous slide.

$$x_n = \frac{(a+\sqrt{k}b)^n+(a-\sqrt{k}b)^n}{2}$$
$$y_n = \frac{(a+\sqrt{k}b)^n-(a-\sqrt{k}b)^n}{2\sqrt{k}}$$

If we use the Binomial Theorem, we can show that, despite the presence of $\sqrt{k}$, these equations yield only positive integers.

Ancient Greeks' Awareness of Pell Equations

The ancient Greeks used the table on slide 11 to approximate $\sqrt{2}$. Let's suppose that we want to find $x^2 - 2y^2 = \pm 1$. Let's divide both sides by y^2:

$$\left(\frac{x}{y}\right)^2 - 2 = \frac{\pm 1}{y^2}.$$

As we go down the chart, we see that as $y \to \infty$, $\frac{\pm 1}{y^2} \to 0$. But, then $\left(\frac{x}{y}\right)^2 \to 2$ and $\left(\frac{x}{y}\right) \to \sqrt{2}$.

Generalizing Ancient Greeks' Approach

Let's suppose that we want to find $x^2 - ky^2 = \pm 1$. If we divide both sides by y^2:

$$\left(\frac{x}{y}\right)^2 - k = \frac{\pm 1}{y^2}.$$

As we compute larger and larger x and y pairs, we see that as $y \to \infty$, $\frac{\pm 1}{y^2} \to 0$. But, then $\left(\frac{x}{y}\right)^2 \to k$ and $\left(\frac{x}{y}\right) \to \sqrt{k}$.

Using Pell Equations to Approximate Square Roots

If we want to compute $\sqrt{k}$, we know that we can use these recurrences to compute x_n and y_n for a given value of n (e.g., 100):

$$\begin{aligned} x_n &= \tfrac{(a+\sqrt{k}b)^n+(a-\sqrt{k}b)^n}{2} \\ y_n &= \tfrac{(a+\sqrt{k}b)^n-(a-\sqrt{k}b)^n}{2\sqrt{k}} \end{aligned}$$

However, we quickly see that we have a circular argument: to compute $\sqrt{k}$, we need $\sqrt{k}$. Can be break out of this circle?

Newton-Raphson to the Rescue

We can use the Newton-Raphson algorithm to approximate $\sqrt{k}$ and use it in conjunction with these two Pell recurrences:

$$x_n = \frac{(a+\sqrt{k}b)^n+(a-\sqrt{k}b)^n}{2}$$
$$y_n = \frac{(a+\sqrt{k}b)^n-(a-\sqrt{k}b)^n}{2\sqrt{k}}$$

Let's experiment with this approach and compare it with `math.sqrt` and Newton-Raphson by itself.

Experiments

I've implemented two procedures `nra_sqrt(n)` and `pell_approx_sqrt(n, a, b)`, the first one implements Newton-Raphson to approximate $\sqrt{n}$ and the second one approximates $\sqrt{n}$ with the Pell recurrences and Newton-Raphson.

$\sqrt{k}$	`math.sqrt`	Newton-Raphson	Pell
$\sqrt{3}$	1.7320508075688772	1.73205080757	1.7320508075688774
$\sqrt{5}$	2.23606797749979	2.2360679775	2.23606797749979
$\sqrt{7}$	2.6457513110645907	2.64575131106	2.6457513110645907
$\sqrt{8}$	2.8284271247461903	2.82842712475	2.8284271247461903

Looks like combining Newton-Raphson with Pell give us a better approximation to the ground truth (if we're willing to take `math.sqrt` as the ground truth).

References

1. M. Lewinter, J. Meyer. *Elementary Number Theory with Programming*, Chapter 2. Wiley.
2. `www.python.org`.