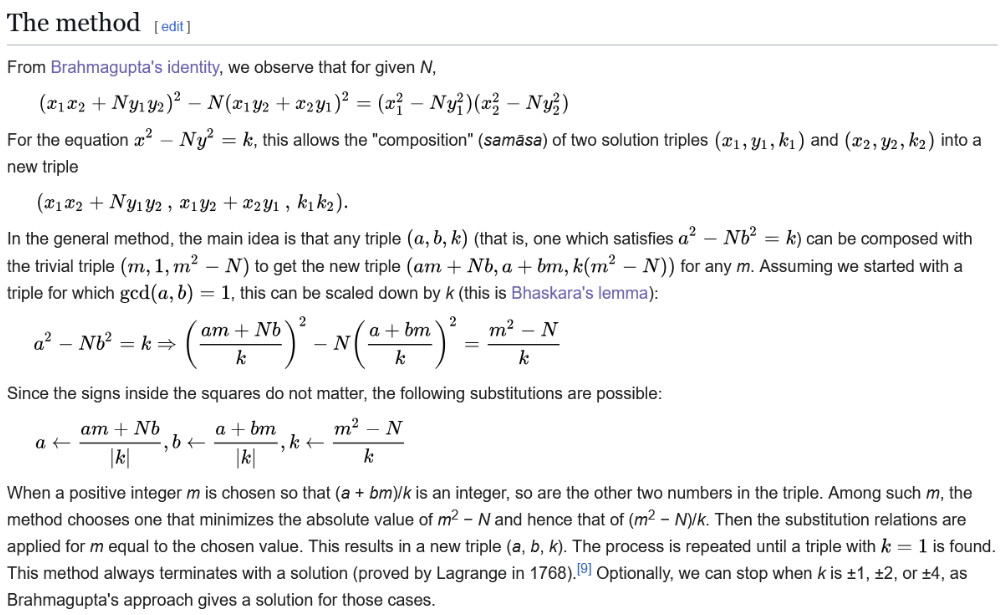
DiophantineEquations.c Learnings

- Diophantine Equations
    - Pell's Equations
        - Solve using Continued Fractions or Chakravala Method
        - https://en.wikipedia.org/wiki/Pell%27s_equation
        - https://en.wikipedia.org/wiki/Brahmagupta%27s_identity
        - https://en.wikipedia.org/wiki/Bhaskara%27s_lemma
        - https://en.wikipedia.org/wiki/Chakravala_method#The_method



The method [edit]

From Brahmagupta's identity, we observe that for given *N*,

$$(x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2 = (x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2)$$

For the equation $x^2 - Ny^2 = k$, this allows the "composition" (*samāsa*) of two solution triples (x_1, y_1, k_1) and (x_2, y_2, k_2) into a new triple

$$(x_1x_2 + Ny_1y_2\ ,\ x_1y_2 + x_2y_1\ ,\ k_1k_2).$$

In the general method, the main idea is that any triple (a, b, k) (that is, one which satisfies $a^2 - Nb^2 = k$) can be composed with the trivial triple $(m, 1, m^2 - N)$ to get the new triple $(am + Nb, a + bm, k(m^2 - N))$ for any *m*. Assuming we started with a triple for which $\gcd(a, b) = 1$, this can be scaled down by *k* (this is Bhaskara's lemma):

$$a^2 - Nb^2 = k \Rightarrow \left(\frac{am + Nb}{k}\right)^2 - N\left(\frac{a + bm}{k}\right)^2 = \frac{m^2 - N}{k}$$

Since the signs inside the squares do not matter, the following substitutions are possible:

$$a \leftarrow \frac{am + Nb}{|k|}, b \leftarrow \frac{a + bm}{|k|}, k \leftarrow \frac{m^2 - N}{k}$$

When a positive integer *m* is chosen so that (*a* + *bm*)/*k* is an integer, so are the other two numbers in the triple. Among such *m*, the method chooses one that minimizes the absolute value of $m^2 - N$ and hence that of $(m^2 - N)/k$. Then the substitution relations are applied for *m* equal to the chosen value. This results in a new triple (*a*, *b*, *k*). The process is repeated until a triple with $k = 1$ is found. This method always terminates with a solution (proved by Lagrange in 1768).[9] Optionally, we can stop when *k* is ±1, ±2, or ±4, as Brahmagupta's approach gives a solution for those cases.

- I used the Chakravala Method to compute solution to Pell's (quadratic) Equations for the largest minimal a for N <= 1000. I believe it is faster than the continued fractions method.
    - Euler challenges Broeker to solve, thinks Pell invented these equations

- GMP (GNU Multi Precision Library)
    - Large Numbers
    - Installation
    - Linux
        - Ubuntu
        - Commands
        - WSL

Installing GMP:

We’ll be using **a Precompiled GMP Library** that’s already available on your system or through your GCC installation.

- Faster set up, will be system compatible since precompiled.
- Building GMP from source
    - More customizable and allows for hardware + CPU optimization
    - Tried to install from source originally, caused some error with the libgmp.so file.

GMP is a Linux-first library. You need to run GMP on a Unix-like environment to install and use it. Use the WSL (Windows Subsystem of Linux) to install and access GMP. Let’s use a Ubuntu distribution to run GMP.

1. Install WSL; wsl –install. This will install Ubuntu as your default WSL configuration.
   - Run the following command in PowerShell as Admin

   a. Restart your computer if you want or if a next step fails.

Double "--"

2. Run wsl --list –verbose to see the WSL distributions on your pc wsl -l -v
3. Change the default (the one on top and *) to Ubuntu: wsl --set-default Ubuntu
4. Enter WSL in the shell

   a. This starts the default user session
5. You’re going to need GCC to compile in your distro.
6. Run sudo apt update; sudo apt install build-essential libgmp-dev;

   a. sudo apt update ⟶ Updates package lists.

   b. sudo apt install build-essential ⟶ Installs gcc, make, etc.

   c. sudo apt install libgmp-dev ⟶ Installs the precompiled GMP library
7. GMP is now ready to use.
8. Verification (in wsl):

   a. Run pkg-config --modversion gmp

   b. ls /usr/include/gmp.h

   c. ls /usr/lib/x86_64-linux-gnu/libgmp.*
9. Test (in wsl):

   a. Create a C program in your Ubuntu Distro

i. nano test_gmp.c

b. Paste this in: CTRL+X, then Y, then Enter to save.

```
#include <stdio.h>
#include <gmp.h>
int main() {
mpz_t a, b, result;
mpz_inits(a, b, result, NULL);
mpz_set_str(a, "12345678901234567890", 10);
mpz_set_str(b, "98765432109876543210", 10);
mpz_add(result, a, b);
gmp_printf("Result: %Zd\n", result);
mpz_clears(a, b, result, NULL);
return 0;
}
```

c. Run gcc -o test_gmp test_gmp.c -lgmp and then ./test_gmp.c. Assert Result: 111111111011111111100

i. If so, YOU DID IT, GMP has been installed!

Removing GMP:

CAN NOT RETURN GMP TYPES FROM FUNCTIONS AS C/C++ DOES NOT SUPPORT RETURN POINTERS/ARRAY FROM FUNCTIONS. PASS BY REF.!

```
sudo apt remove --purge libgmp-dev
sudo apt autoremove
```

In Linux Distributions, a user an environment with the specific packages that that user has sudo apt install'ed. Each user has a directory in the /home directory for personal files, config file, environment settings.

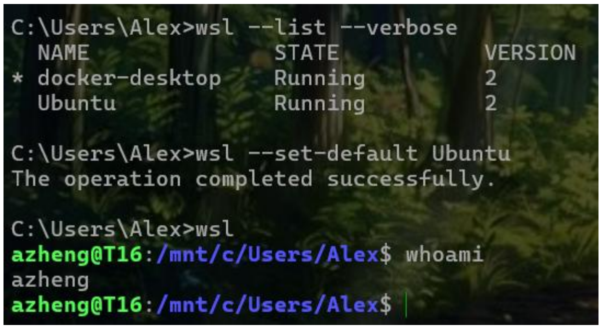
A root user, the superuser, has full administrative access to the Linux Distribution.

- This poses a security risk due to the root's power and possible mistakes
    - ○ Installing/updating software and system settings, managing users.

A regular user only has access to personal files and directories. They can not modify system-wide settings (installing/updating packages) without permission, SU.

- This offers security and personalization.

Note: When you log in as a user in WSL and other terminals, the system loads the regular user's environment configuration. This environment often has customizations like a bold prompt, colored text, and other visual enhancements. This is typically managed by the .bashrc or .zshrc configuration files for your shell.



```
C:\Users\Alex>wsl --list --verbose
  NAME              STATE           VERSION
* docker-desktop    Running         2
  Ubuntu            Running         2

C:\Users\Alex>wsl --set-default Ubuntu
The operation completed successfully.

C:\Users\Alex>wsl
azheng@T16:/mnt/c/Users/Alex$ whoami
azheng
azheng@T16:/mnt/c/Users/Alex$
```

In a Linux distribution, there exists a "mnt" MOUNT directory. This directory is directory that which storage can be integrated into the Linux distribution. The Linux distribution effectively mounts on top of it, like an ant hill mount and the directory becomes a part of the Linux Distribution. Or think of the directory attached to the Linux Distribution through this (saddle) mount.

WSL:

a **compatibility layer** that allows you to run Linux distributions on Windows without the need for a virtual machine or dual-boot setup. WSL is like a **bridge** between the Windows operating system (OS) and the Linux environment, allowing you to run Linux tools and applications alongside Windows applications.

□ **WSL 1**: The original version of WSL, which translated Linux system calls into Windows system calls. It didn’t use a Linux kernel but instead emulated one.

□ **WSL 2**: A major upgrade, which actually runs a real Linux kernel in a lightweight virtual machine (VM) on top of Windows. This improves performance and compatibility significantly, allowing you to run Docker, Kubernetes, and other containerized applications natively within Linux while still interacting with them from within Windows.

Ubuntu:

Ubuntu is a popular Linux distribution (or "distro") that you can install and run within WSL. A Linux distribution is a Linux environment/layer on top of the Windows OS, that one accesses it through WSL. Ubuntu is a Linux OS; but w.r.t. WSL it is a containerized + virtualized OS embedded in windows.

- Access your Windows files through the /mnt/c/ directory in WSL (which corresponds to your C: drive in Windows).

Linux: A kernel : the core part of the operating system that manages the system’s hardware resources. The liaison from the software applications to the hardware.

- Memory, process, and device management

Linux Distribution: A complete operating system built around the Linux Kernel, which includes the package managers, packages, user interface, and libraries to use the computer. Hence, many different Linux distros built around the Linux kernel, open source.

- Ubuntu
- Debian
- Fedora

- CentOS
- Arch Linux

Windows: an Operating System: A software that manages computer hardware and provides services for computer programs. It is a (Linux) Distribution [above]. Allows users and applications to interact with the hardware. Coordinates the software with the hardware resources for efficient, secure, and smooth completion of programs.

- HW:
    - CPU, memory, I/O. CPU and memory assigned by OS by concurrent programs.
- SW programs.
- UI between user and hardware; shell.
- Security
- File system, directories.
    -

Docker: Runs applications in containers, which are isolated environments (not OSes) that simulate an OS for specific software.

A story I want to tell you is how I got my first co-op in Summer 2024. In the beginning, I was so lost in finding a coop, my resume was very random and I just wanted to get any job. I was in no position to want anything; anything would've been appreciated. For 3 months I couldn't find a coop. I did 4 or so interviews at low-skilled jobs which exposed me to my terrible interviewing skills and the distress of getting unranked. The day of my first exam, in April, with only 2 weeks left of the term left, and still no job, I had an interview for what was my dream company. A challenging role which would really allow me to grow. The morning of, I did the interview, and I felt pretty good. I practiced a lot and studied for this interview, moreso than my exam. The hard part is, and something that has always shown up to me, especially at Waterloo, is that there's always a sad trade off for everything. I either could do well on the interview or on the exam. The thing is, is that an interview really tires me out, so after that interview, I started studying for my exam, and felt worried for my exam performance. Time passed, let's fast forward; and the exam ended, I felt really good. It was at this moment, I felt dread. I had a hunch that I could only get one, the job or the exam, not both. My success in the exam implied the detriment of my coop. Long story short, I didn't get the job. Luckily that day I got the news of the unranked, I didn't have any exams in the next 2 days. Since I could not do any work or study after that, I was in tears in the library. The truth is, I've actually been in tears every coop search (2). Then the term ended, and now it got real. I spent day after day applying to jobs online. I was starting to lose hope after a month, starting to become numb actually. Interviews felt meaningless. Then, one day I got an interview. And the next I got the job somehow. And I thank God for this. Thank you!