WhiteHat 2020 Quals: Prog 01 writeup

braindead, perfect blue CTF team

January 9, 2020

1 Introduction

We are greeted by this cryptic problem statement:

```
PROGRAMING - WHITEHAT GRANDPRIX 06:

--> COUNT THE NUMBER OF POSSIBLE TRIANGLES <--

HOW MANY TRIANGLES ARE CREATED BY N (1..N) NUMBER. N < 10^6

Example:  N = 5
OUTPUT : 3

(2,3,4),(3,4,5),(2,4,5)
................/\...................|\...................
.............../  \..................| \..................
............../    \.................|  \.................
............./      \................|   \................
............/        \...............|    \...............
.........../          \..............|     \..............
........../____________\.............|______\.............

n = 8
Answer:
```

After some trial and error we guess[1] that they want the number of tuples $a, b, c \in [0; N]$ that satisfy $a < b < c, a + b < c$, i.e. the triangle with sides of lenght a, b, c is non-degenerate.

2 Solution

Trying all tuples and evaluating the inequalities would take $O(N^3)$ time, which is too slow for $N < 10^6$. Instead we will derive a polynomial formula for the answer, and evaluate it in $O(log^2 N)$

[1] Guessing is major part of most challenges on this CTF.

time.

Let $A(n)$ be the number of triangular tuples in $[0; N]$.

Notice that all tuples for $N = n - 1$ are also valid for $N = n$, and all tuples that are only valid for $N \geq n$ have $c = n$. In other words, $A(n) = A(n-1) + f(n)$ where $f(n)$ is the number of tuples with $c = n$.

Fix a, then b must satisfy $n - a > b > a \Leftrightarrow n - 2a > b > 0$, i.e. there are $n - 2a - 1$ valid choices for b. To ensure at least one valid value for b, we add the following condition to a:

$$n - 2a - 1 > 0 \Leftrightarrow \frac{n-1}{2} > a \Leftrightarrow \left\lfloor \frac{n}{2} \right\rfloor > a$$

Now we can express $f(n)$ as

$$\begin{aligned} f(n) &= \sum_{a=1}^{\lfloor \frac{n}{2} \rfloor - 1} (n - 2a - 1) \\ &= (\left\lfloor \frac{n}{2} \right\rfloor - 1)(n-1) - 2 \sum_{a=1}^{\lfloor \frac{n}{2} \rfloor - 1} a \\ &= (\left\lfloor \frac{n}{2} \right\rfloor - 1)(n-1) - 2 \cdot \frac{\lfloor \frac{n}{2} \rfloor (\lfloor \frac{n}{2} \rfloor - 1)}{2} \\ &= (\left\lfloor \frac{n}{2} \right\rfloor - 1)(n-1) - \left\lfloor \frac{n}{2} \right\rfloor (\left\lfloor \frac{n}{2} \right\rfloor - 1) \end{aligned} \tag{1}$$

Let $r = \frac{n}{2} - \lfloor \frac{n}{2} \rfloor$, then:

$$\begin{aligned} f(n) &= (\left\lfloor \frac{n}{2} \right\rfloor - 1)(n-1) - \left\lfloor \frac{n}{2} \right\rfloor (\left\lfloor \frac{n}{2} \right\rfloor - 1) \\ &= (\frac{n}{2} + r - 1)(n-1) - (\frac{n}{2} + r)(\frac{n}{2} + r - 1) \\ &= \frac{n^2}{4} - n + 1 + r^2 \end{aligned} \tag{2}$$

Now that we have $f(n)$ in simple form, we will derive $A(n)$ using generating functions.

We will use notation $\mathrm{G}(g(n); x) = \sum_{i \geq 0} g(i+1) x^i$. Note how $g(n)$ is evaluated starting at 1, not 0.

First we find a generating function for $f(n)$:

$$\mathrm{G}(1; x) = \frac{1}{1-x} \tag{3}$$

$$\mathrm{G}(n; x) = \frac{1}{(1-x)^2} \tag{4}$$

$$\mathrm{G}(n^2; x) = \frac{1+x}{(1-x)^3} \tag{5}$$

$$\mathrm{G}(r^2; x) = \frac{1}{4 - 4x^2} \tag{6}$$

$$\begin{aligned}\mathrm{G}(f(n);x) &= \frac{1+x}{4(1-x)^3} - \frac{1}{(1-x)^2} + \frac{1}{1-x} - \frac{1}{4-4x^2} \\ &= \frac{-x^3}{x^4-2x^3+2x-1}\end{aligned} \tag{7}$$

Now $A(n)$ is simply a prefix sum of $f(n)$:

$$\begin{aligned}\mathrm{G}(A(n);x) &= \frac{\mathrm{G}(f(n);x)}{1-x} \\ &= \frac{x^3}{x^5-3x^4+2x^3+2x^2-3x+1} \\ &= \frac{x^3}{(x+1)(x-1)^4}\end{aligned} \tag{8}$$

Now it's obvious that $A(n)$ is just a 3rd degree polynomial plus a constant times the least significant bit of n:

$$A(n) = z_0 + z_1 n + z_2 n^2 + z_3 n^3 + z_4(-1)^n \tag{9}$$

After manually calculating first few values of $A(n)$ we can find z coefficients by solving a small linear system:

$$\begin{pmatrix}1 & 3 & 9 & 27 & -1 \\ 1 & 4 & 16 & 64 & 1 \\ 1 & 5 & 25 & 125 & -1 \\ 1 & 6 & 36 & 216 & 1 \\ 1 & 7 & 49 & 343 & -1\end{pmatrix}\begin{pmatrix}z_0 \\ z_1 \\ z_2 \\ z_3 \\ z_4\end{pmatrix} = \begin{pmatrix}1 \\ 3 \\ 7 \\ 13 \\ 22\end{pmatrix} \tag{10}$$

This yields $A(n+1) = \frac{1}{12}n^3 - \frac{1}{8}n^2 - \frac{1}{12}n + \frac{1}{16} - \frac{1}{16}(-1)^n$, always an integer. Since $|\frac{1}{16}(-1)^n| \le \frac{1}{16}$ we can simplify:

$$\begin{aligned}A(n+1) &= \frac{1}{12}n^3 - \frac{1}{8}n^2 - \frac{1}{12}n + \frac{1}{16} - \frac{1}{16}(-1)^n \\ &= \left\lfloor \frac{1}{12}n^3 - \frac{1}{8}n^2 - \frac{1}{12}n + \frac{1}{16} - \frac{1}{16}(-1)^n \right\rfloor \\ &= \left\lfloor \frac{1}{12}n^3 - \frac{1}{8}n^2 - \frac{1}{12}n + \frac{1}{16} - \frac{1}{16}(-1)^n + \frac{1}{16} \right\rfloor \\ &= \left\lfloor \frac{1}{12}n^3 - \frac{1}{8}n^2 - \frac{1}{12}n + \frac{1}{8} \right\rfloor \\ &= \left\lfloor \frac{(x+1)(x-1)(x-\frac{3}{2})}{12} \right\rfloor \\ &= \left\lfloor \frac{(x+1)(x-1)(2x-3)}{24} \right\rfloor \\ A(n) &= \left\lfloor \frac{x(x-2)(2x-5)}{24} \right\rfloor\end{aligned} \tag{11}$$

3 Full script

```
from braindead import *; log.enable(); Args().parse()

r = io.connect(('15.164.75.32', 1999))
while True:
        n = int(r.rla('n = ').decode())
        x = n*(n-2)*(2*n-5)//24
        r.sla(': ', str(x))
```