



Day 9: Aeren Contest Analysis

Oleksandr Kulkov

Osijek, Croatia

February 23, 2025

Summary

- Author: Aeren (Codeforces: Halzion)
- Problems: A B C D E F G H I J
- Winner (onsite): Delft TU: Segfault go BRRRR

A. Saki and False Minoshiro

Statement

$\pi(s)$ is the length of the longest proper suffix of s , which is also its prefix.
Sum up $\pi(s)^2$ over $|s| = N$, with the alphabet size M .
Constraints: $N \leq 100$; $2 \leq M \leq 10^9$.

Topics: Bruteforce, combinatorics of strings.

p is a period of s if $s_i = s_{i+p}$ for all valid i .

Self-correlation $A(s)$ is defined as $A(s)_p = [p \text{ is a period of } s]$.

Theorem

The set of all possible self-correlations is the same for $M \geq 2$.

There is a set of complicated criteria for A to be a valid self-correlation.
They allow to find all 35 200 of them for $N \leq 100$.

It is then possible to count valid strings for each self-correlation.
See full text editorial for details (some time in the future).

B. Saki and Sewage System

Statement

You are given two graphs A and B with N nodes and M undirected edges. You need to pick M capacities to assign to edges in the given order. You have to make sure that the undirected flow in B is larger than in A . Constraints: $N \leq 20$; $M \leq 200$.

Topics: Brute force, graphs, flows and cuts.

Check if there is a flow path in B s.t. its edges are not a flow path in A .
Try all splits $A = S \sqcup T$ and look for a flow path in B in S and T .

C. Saki and Separation

Statement

You're given a snapshot of a grid with some cells marked A or B .

You can shift all A cells in the same direction.

Is it possible to separate the two sets of cells?

Constraints: Snapshot of size $N \times M$ for $N, M \leq 1\,000$.

Topics: FFT, DFS.

- Assume x changed by Δ_x and y by Δ_y .
- Check if there is $(x_A, y_A) \in A$ and $(x_B, y_B) \in B$ with such difference;
 - Use 2D convolution;
- Check if there is a valid diff path from $(0, 0)$ to (∞, ∞) via DFS.

D. Saki and Railway Construction

Statement

You are given a graph with the $(n + 1) \times (n + 1)$ adjacency matrix:

$$\begin{pmatrix} 0 & x-1 & 2(x-1) & 2(x-1) & \dots & 2(x-1) \\ x-1 & 0 & 1 & 0 & \dots & 0 \\ 2(x-1) & 1 & 0 & 1 & \dots & 0 \\ 2(x-1) & 0 & 1 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & 1 \\ 2(x-1) & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Let $f(x)$ be the number of its spanning trees.

Find the minimum $k > 0$ s.t. $f^k(x) \equiv x \pmod{m}$.

Constraints: $n \leq 10^{18}$; $m \leq 10^9$; m is prime.

Topics: Matrix tree theorem, Chebyshev polynomials, field extension.

Use matrix tree theorem:

$$f(x) = \begin{vmatrix} x & -1 & 0 & \dots & 0 \\ -1 & 2x & -1 & \dots & 0 \\ 0 & -1 & 2x & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & -1 \\ 0 & 0 & 0 & -1 & 2x \end{vmatrix} = T_n(x)$$

In other words, $f(x)$ is the n -th Chebyshev polynomial.

Use core properties of Chebyshev polynomials:

$$T_n(\cos \theta) = \cos n\theta \implies T_a(T_b(x)) = T_{ab}(x) \implies f^k(x) = T_{n^k}(x)$$

From $\cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$, we can also say

$$T_n\left(\frac{t + t^{-1}}{2}\right) = \frac{t^n + t^{-n}}{2}$$

For $T_n(x)$, each x has a pre-image t in $GF(p^2)$:

$$x = \frac{t + t^{-1}}{2} \iff t = x \pm \sqrt{x^2 - 1}$$

We can rewrite the equation $T_a(x) = x$ as follows:

$$t^a + t^{-a} = t + t^{-1} \iff t^{-a}(t^{a+1} - 1)(t^{a-1} - 1) = 0 \iff \begin{cases} t^{a+1} = 1 \\ t^{a-1} = 1 \end{cases}$$

$x^p = \frac{t^p + t^{-p}}{2} = x$ for any $x \in GF(p)$, so $a = p$ satisfies the above.

It means that $t^{p+1} = 1$ or $t^{p-1} = 1$ for all pre-images t .

Thus, period of t always divides $p - 1$ or $p + 1$.

Let's show that both $p - 1$ and $p + 1$ are achieved periods:

1. For $p - 1$, use $t = g$ for any primitive root g of $GF(p)$;
2. For $p + 1$, use $t = g^{p-1}$ for any primitive root g of $GF(p^2)$.

Note that in the latter case, for $x = \frac{t+t^{-1}}{2}$,

$$t^{p+1} = 1 \implies t^p + t^{-p} = t + t^{-1} \implies x^p = x,$$

but only $x \in GF(p)$ satisfy $x^p = x$ in $GF(p^2)$. Thus,

$$T_a(x) = x \iff \begin{cases} a \equiv \pm 1 \pmod{p+1}, \\ a \equiv \pm 1 \pmod{p-1} \end{cases}$$

This is true if and only if $a \in \{\pm 1, \pm p\} \pmod{\frac{p^2-1}{2}}$.

Since $f^k(x) = T_{n^k}(x)$, we need to find the smallest k s.t.

$$\begin{cases} n^k \equiv \pm 1 \pmod{p+1}, \\ n^k \equiv \pm 1 \pmod{p-1} \end{cases}$$

This is done by finding the order of n modulo $p-1$ and $p+1$ in $O(\sqrt{p})$.

E. Saki and Hope

Statement

Select 10^5 distinct rays in 3D space with integer directions so that there are at least $1.4 \cdot 10^6$ pairs of orthogonal rays.

Constraints: $|x_i|, |y_i|, |z_i| \leq 10^9$.

Topics: Ad hoc, constructive, heuristic.

1. Add rays $(x, y, 1)$ for $|x|, |y| \leq 110$;
2. Greedily connect their endpoints with $k = 10^5 - 220^2$ lines, each line covering as much points as possible;
3. For each line, add the normal ray to the plane containing the line and the origin point $(0, 0, 0)$.

Actual number of orthogonal pairs: 1 418 266.

Asymptotically, around $O(n^{4/3})$ pairs expected.

F. Saki and Summer Festival

Statement

You're given N distinct points (X_i, Y_i) on a plane.
Find the number of subsets that lie on the same circumference.
Constraints: $N \leq 300$; $X_i, Y_i \leq 30$.

Topics: Basic geometry, Combinatorics.

- Circumference is uniquely defined by any 3 points;
- Group all triples by the common circle;
- N points means $2^N - \frac{n^2}{2} - \frac{n}{2} - 1$ valid sets, in particular $\binom{N}{3}$ triples.

G. Saki and Cantus

Statement

Find the sum of the totient function $\varphi(a + bi)$ over $a^2 + b^2 \leq N$.
Constraints: $N \leq 10^{10}$.

Topics: Gaussian integers, number theory.

Let p be a Gaussian prime, then

$$\varphi(p^e) = \|p^e\| - \|p^{e-1}\| = (\|p\| - 1)\|p\|^{e-1}$$

I.e., total number of residues¹ is $\|p^e\|$, and $\|p^{e-1}\|$ are divisible by p .
This allows us to generally define

$$F(n) = \sum_{\|x\|=n} \varphi(x),$$

and the answer is $F(1) + \cdots + F(N)$.

¹Due to Pick's theorem

For $\|x\| = p$ (prime), ignoring units, we have three cases:

- $p = 4k + 3$ is a prime.
- $p = 4k + 1$ corresponds to two primes $a + bi$ and $a - bi$.
- $p = 2$ corresponds to the prime $1 + i$.

Thus, we also have three cases for $F(p^e)$.

We have 3 cases to determine the value of $\frac{1}{4}F(p^e)$:

$$p = 4k + 3$$

$$[e \text{ is even}] \varphi(p^{\frac{e}{2}}) = [e \text{ is even}] (p^2 - 1) p^{e-2}$$

$$p = 4k + 1$$

$$\sum_{t=0}^e \varphi((a + bi)^t (a - bi)^{e-t}) = 2(p-1)p^{e-1} + (e-1)(p-1)^2 p^{e-2}$$

$$p = 2$$

$$\varphi((1+i)^e) = 2^{e-1}$$

$F(n)$ is multiplicative, apply “standard” ways to find the sum in $O(N^{2/3})$:

- Min25’s sieve;
- Something something Dirichlet convolution?

H. Saki and Tree

Statement

Make a tree circuit out of $+$, $-$, $\times$, mod , rem , pow .

Input x is given on all leaves, output is the final value in the root.

Output must be 1 if $x \in \{561, 1105, 1729, 2465, 2821\}$, otherwise 0.

Constraints: $100 \leq x \leq 3000$; $n \leq 150$ (nodes in the tree).

Topics: Ad hoc, number theory.

The numbers are the first 5 Carmichael numbers:

$$a^{x-1} \equiv 1 \pmod{x}$$

- Fermat test to filter everything except primes and target numbers;
- Target numbers are multiples of 7 or 17;
- $[(2^{x-1} \bmod x) = 1 \wedge (23^{x-1} \bmod x) = 1 \wedge (x \bmod 7)(x \bmod 17) = 0]$.

Use $0^{(k-1)^2}$ to check if $k = 1$.

I. Saki and Encoding

Statement

You're given a tree. Do the following for $k = 0..N - 1$:

1. Assign label $(u + k) \bmod n$ to the node u ;
2. Find the sum of last two nodes in the Prüfer sequence algorithm².

Constraints: $N \leq 10^6$.

Topics: Ad hoc, trees.

²Repeatedly find smallest leaf and remove it

One of the remaining labels is $N - 1$.

The answer is $N - 1 + a$, where a is the first vertex on the path

$$(N - 1) \rightarrow a \rightarrow \cdots \rightarrow (N - 2)$$

J. Saki and Decryption

Statement

There are primes p and q s.t. $2p - 1$ and $2p^2 - 2p + 1$ are primes.
You are given $n = p(2p - 1)(2p^2 - 2p + 1)q^2$. Find p and q .
Constraints: $2^{100} < p, q < 2^{150}$.

Topics: Number theory, field theory.

Note that $4p(2p^2 - 2p + 1) = \frac{(2p-1)^4 - 1}{(2p-1) - 1}$.

- Consider random polynomial $f(x)$ over $\mathbb{Z}_n$ of degree 4;
 - It's likely irreducible over $\mathbb{Z}_{2p-1}$;
 - I.e., remainders modulo $f(x)$ form $GF((2p-1)^4)$;
- Consider a random remainder $a(x)$ modulo $f(x)$;
 - It's likely a generator of $GF((2p-1)^4)$;
 - It means it has period $(2p-1)^4 - 1$;
- Consider $a^{4N} \bmod f$;
 - It has period $(2p-1) - 1$;
 - It means it corresponds to an element of $GF(2p-1)$;
 - It means coeffs near x^1, x^2, x^3 are divisible by $2p-1$;
 - Find their gcd with n ;
- Try again if couldn't recover $2p-1$;
 - Success probability at least $\frac{1}{8}$.

Recover $2p-1$, and from that p , and from that q .

Possibly consider $q = p$ and $q = 2p-1$ separately.