Project Euler: Problem 258

> **Problem.** Define a sequence g_k by
>
> $$g_{k+2000} = g_k + g_{k+1},$$
>
> and $g_k = 1$ for $0 \leq k \leq 1999$.
>
> Find $g_K \bmod 20092010$, where $K := 10^{18}$.

Solution. We may model the linear recurrence with the following 2000×2000 matrix:

$$T = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Effectively, if we have some input vector

$$\mathbf{v} = \begin{bmatrix} g_k \\ g_{k+1} \\ \vdots \\ g_{k+1999} \end{bmatrix},$$

applying our matrix T transitions to the next state. In other words,

$$T\mathbf{v} = \begin{bmatrix} g_{k+1} \\ g_{k+2} \\ \vdots \\ g_{k+2000} \end{bmatrix}.$$

Thus, we can rephrase our problem as finding the value of the state vector given by

$$T^K \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \pmod{20092010},$$

where the modulus implies element-wise modular arithmetic.

An initial reaction to this formulation may be either fast matrix exponentiation or diagonalization, however the first fails because even with the time complexity of $O(n^3 \log_2 K)$, it is still slow, and the second fails due to floating point errors. What we can do, however, is simplify things just a bit.

Interestingly enough, we can show that taking powers of this matrix forms a group, and in particular, a cyclic group isomorphic to the integers modulo 20092010. Indeed, since $\det T = -1$, this holds.

Equipped with this, we can use some useful tools from number theory. In particular, one may observe that

$$T^K \equiv T^{K \bmod \lambda(20092010)} \pmod{20092010},$$

where $\lambda(n)$ represents the Carmichael function. Using this, we drastically decrease the exponent, as $\lambda(20092010) = 2006004$. In particular, this tells us that

$$g_K \equiv g_{K \bmod 2006004} \equiv g_{939940} \pmod{20092010}.$$

This works out well, as now we can simply calculate the value from the linear recurrence in suitable time (specifically $O(\lambda(M))$, where M is the modulus).

This seems to be incorrect and the underlying reason why perchance has to do with like the using number theory for matrices part. Empirically it seems that for an $n \times n$ matrix that has a non-zero determinant in $\mathbb{Z}_p$, where p is prime is

$$\operatorname{ord}(T) = p^{2^{n-2}},$$

which makes no sense :sob: but also since this grows way too fast the entire approach isn't going to be useful at all noooooo.