What's a fast algorithm to find the remainder of the division of a huge Fibonacci number by some big integer?

Michal Forišek, Ph. D. in theoretical Computer Science
Updated Apr 25, 2014

Each recurrence similar to Fibonacci numbers can be expressed in terms of matrix multiplication as follows:
In order to compute the next Fibonacci number F_{n+2}, we need two previous ones: (F_n, F_{n+1}). The transformation that changes (F_n, F_{n+1}) to (F_{n+1}, F_{n+2}) is linear, and therefore we can find a matrix that performs it:

$$\forall a, b : (a, b) \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = (b, a+b).$$

Let's call the above matrix A. Obviously, for any n we have:

$$(F_n, F_{n+1}) \cdot A = (\ F_{n+1},\ F_n + F_{n+1}\ )$$

which is precisely (F_{n+1}, F_{n+2}).

We can use A multiple times. For example:

$$\left(\left((F_0, F_1) \cdot A\right) \cdot A\right) \cdot A = (F_3, F_4)$$

$(F_0, F_1) \cdot A^3 = (F_3, F_4)$

And, in general:

$(0, 1) \cdot A^n = (F_n, F_{n+1})$

The above equation is valid in integers, therefore it is valid modulo any m.

Computing modulo m, we can use Exponentiation by squaring to compute A^n using $O(\log n)$ operations on numbers smaller than m^2.

In terms of a practical implementation: as long as m fits into a 32-bit integer variable, all intermediate values will fit into 64-bit variables, and you can use the above formula to compute $F_n \mod m$ even for $n = 10^{1000}$.

(Or use a language with arbitarary precision integers if you need larger values of m. For example, $n = m = 10^{1000}$ is still perfectly feasible.)

Sample implementation: http://ideone.com/fP8krp

About the Author

teacher, scientist, competitive programmer

Works at Comenius University in Bratislava

Studied at Comenius University in Bratislava

Lives in Bratislava

7.4m answer views
50.1k this month

Top Writer
2018, 2017, 2016, and 2015

Published Writer
Slate

More Answers from Michal Forišek

If you were hired to test a program, how would you try to crash it?
121.6k Views

Are new data structures still being invented in computer science? Are they getting increasingly complex or can we still expect to find useful data structures, like a priority queue?
41.9k Views

If Tourist, Petr and ACrush were to form a group, could any group defeat them?
15.3k Views

Layman's Terms: What is a Bloom filter?
10.9k Views

What are the advantages of using BFS over DFS or using DFS over BFS? What are the applications and downsides of each?
40.2k Views

Upvote 37 Downvote