Integer Factorization

Chinese Remainder Theorem

Modular Exponentiation

Reading: Modular Exponentiation
10 min

Reading: Fast Modular Exponentiation
7 min

Quiz: Fast Modular Exponentiation: Code
2 questions

Reading: Fermat's Little Theorem
10 min

Reading: Euler's Theorem
10 min

Quiz: Modular Exponentiation
4 questions

Fermat's Little Theorem

Last Digits of Powers

Looking at the powers of 2, we see a sequence of fast growing numbers:

$$1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, \dots$$

But let us concentrate on the sequence of last digits, or, in other words, consider a sequence of $2^n \mod 10$:

$$1, 2, 4, 8, 6, 2, 4, 8, 6, 2, 4, 8, \dots$$

Stop and think! It seems that the group $2, 4, 8, 6$ repeats in a loop. Will this behavior continue indefinitely?

The key observation: the last digit of 2^{n+1} is determined by the last digit of 2^n. (Recall the school multiplication algorithm, or note that $a \equiv b \pmod{10}$ implies $2a \equiv 2b \pmod{10}$.) So as soon as some digit appears the second time (and this is unavoidable because we have only 10 digits), a cyclic repetitions starts.

We can look in the same way on the last digits of 3^n:

$$1, 3, 9, 7, 1, 3, 9, 7, \dots$$

For 4^n we have

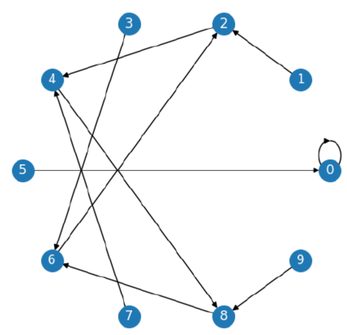
$$4, 6, 4, 6, 4, 6, \dots$$

for 5^n the sequence is even simpler:

$$1, 5, 5, 5, \dots .$$

To understand better the behavior of the last digits of 2^n, we draw a graph that shows how the last digit changes when multiplied by 2. The vertices of this graph are digits $0, 1, 2, \dots, 9$, and for each digit i, we draw an arrow from i to the last digit of $2i$. Here is the program and the picture it draws.

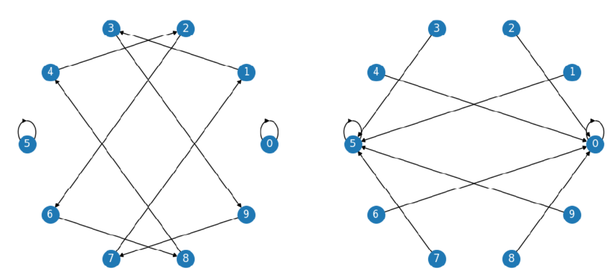
```
import networkx as nx
import matplotlib.pyplot as plt
from math import cos, sin, pi

n, factor, rad = 10, 3, 10

graph = nx.DiGraph()
graph.add_edges_from([(i, i * factor % n) for i in range(n)])

positions = [(rad * cos(i * 2 * pi / n), (rad * sin(i * 2 * pi / n)))
             for i in range(n)]

nx.draw(graph, pos=positions, with_labels=True,
        font_color='white', node_size=400, font_size=12)

plt.gca().set_aspect('equal')
plt.savefig('fermat.png')
```



Stop and think! Do you see the sequence of last digits, $1, 2, 4, 8, 6, 2, 4, 8, 6, \dots$ in this picture?

It is easy: we start at 1 and follow the arrows (each of them shows what happens with the last digit when we multiply 2^k by 2 and get 2^{k+1}).

The same pictures can be drawn for multiplication by other numbers. Here are pictures for factors 3 and 5:

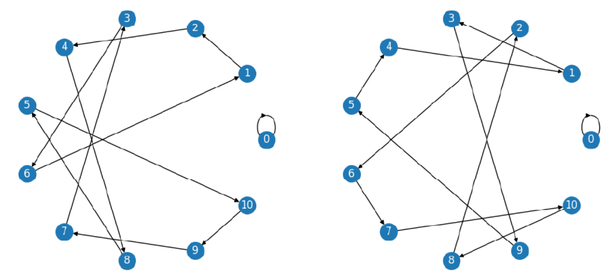


Problem

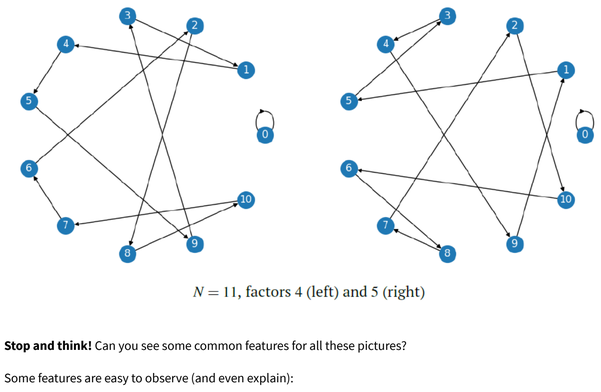
Trace the last digits of 3^n and 5^n on these pictures.

Prime Moduli and Fermat's Little Theorem

Comparing these pictures, we see that the behavior is quite complicated. One of the reasons is that the base of our number system, 10, is not a prime number. Let us draw the same graphs for some prime numbers, e.g., 11. In other words, we show how the remainder modulo 11 changes when we multiply the number by some factor:



$N = 11$, factors 2 (left) and 3 (right)



$N = 11$, factors 4 (left) and 5 (right)

Stop and think! Can you see some common features for all these pictures?

Some features are easy to observe (and even explain):

- An arrow from the zero node goes to the same node. This is true for all N for a simple reason: if x is divisible by N, then any multiple of x is divisible by N.
- Every node has exactly one outgoing arrow, by construction.
- For $N = 11$ (but not for $N = 10$) every node has only one incoming edge: it is not possible that arrows from different nodes u and v arrive at the same node w. What does it mean in terms of modular arithmetic? Nodes u and v are different, so $u \not\equiv v \pmod{N}$. To draw arrows, we multiply u and v by the same factor f (chosen for the picture) and get into nodes $fu \mod N$ and $fv \mod N$. Can these nodes be the same? This means that $fu \equiv fv \pmod{N}$, so the product $f(u - v) = fu - fv$ is divisible by N. At the same time $u - v$ is not divisible by N (since u and v are different nodes), factor f is not divisible by N (otherwise all arrows go to node 0, we do not consider this case), and $N = 11$ is prime. This is a contradiction (the product of two numbers is divisible by prime number p, but both factors are not).

The last observation has consequences: the edges (arrows) are grouped into cycles: starting from every node and going along the edges we return to the starting point. (Indeed, we have to return to the vertex that is already visited, and the starting point is the only option, otherwise two edges arrive at the same node.)

For $f = 2$ and $f = 5$ there is only one cycle that includes all non-zero nodes (there are ten of them); for $f = 3$ and $f = 4$ there are two cycles, each contains five nodes.

The pictures for $f = 3$ and $f = 4$ look almost identical: one should take a close look to notice that arrows are reversed. And this is easy to understand: if we multiply remainder x modulo 11 by 3, and then by 4, we arrive at $12x$, and $12x \equiv x \pmod{11}$.

Still, our observation does not say anything about the length of the cycles. One can try remaining factors $f = 6, 7, 8, 9, 10$; we do not show the pictures to save the space, but at the last moment (for $f = 10$) we get a different picture: