Run this once

Use this cell to install all of the necessary packages. You should only need to run it once.

[1]:
```
using Pkg

# each of these may take a second, if one of them fails, feel free to comment out the ones above it.

Pkg.add("Graphs")
Pkg.add("TikzGraphs")
Pkg.add("MetaGraphs")
Pkg.add("TravelingSalesmanExact")
Pkg.add("GLPK")
# Pkg.add("Plots")
```

Run this first ¶

To make sure all the tests work, please run the following code block. This one also might take a second, especially the first time.

Readonly, ID: bfce2e

In [2]:
```
using Test

using Primes
```

Readonly, ID: 402077

Problem 3: Primitive roots

3

Readonly, ID: ade146

Read Wikipedia about Artin's conjecture on primitive roots before working on this problem.

3

Readonly, ID: 37a6ec

3a) Compute an approximation to Artin's constant

4

$$\prod_p \left(1 - \frac{1}{p(p-1)}\right)$$

by taking the product all primes $p < n$.

Answer that will be automatically graded below, ID: 48fcff

In [ ]:
```
function approx_artin_const(n)
    YOUR ANSWER HERE
end
```

4

Test your code from above here (1 point), ID: 99b257

In [ ]:
```
# use n = 10^4 as a public test
approx_artin_const(10^4) ≈ 0.3739594844671063
```

42

Readonly, ID: b9fa2f

3b) Using the `is_primitive_root` function given below, compute the fraction of primes $p < K$ for which n is a primitive root mod p.

43

Food for thought: evaluate at n=2 and n=3 and K=10^4. How well are these approximated by Artin's constant?

Readonly, ID: 1a8790

In [ ]:
```
function is_primitive_root(n, p)
    (n < p) || (return false)
    ϕ = totient(p)
    factors = Set(factor(Vector, ϕ))
    for q in factors
        if powermod(n, Int(ϕ / q), p) == 1
            return false
        end
    end
    return true
end
```

44

Answer that will be automatically graded below, ID: 3ccd2d

In [ ]:
```
function fraction_is_primitive_root(n,K)
    YOUR ANSWER HERE
```

45

Answer that will be automatically graded below, ID: 3ccd2d

In [ ]:
```
function fraction_is_primitive_root(n,K)
    YOUR ANSWER HERE
end
```

Test your code from above here (1 point), ID: 8750c9

In [ ]:
```
# make these public tests
@test fraction_is_primitive_root(2,10^4) ≈ 0.3824247355573637
@test fraction_is_primitive_root(3,10^4) ≈ 0.387306753458096
```

Readonly, ID: 1127b2

3c) Now compute the fraction of primes $p < 10^4$ for which 5 is a primitive root. In this case, one must multiply Artin's constant by a rational number to get the correct prediction; what should this constant be? (You may optionally take the computation out further to get better numerical evidence.)

Enter your number in the form of a Julia rational number, like "41/301"

Enter your answer here, ID: a3d229

In [ ]:
```
answer_3c = ""   # enter your answer inside the string quotes
```

Answer that will be automatically graded below, ID: c3e697

In [ ]:
```
# scratch work here
YOUR ANSWER HERE
```

Problem 4: Quadratic Residues

A *quadratic residue* mod N is a residue class which can be written as a square mod N, i.e. a is a quadratic residue mod N if there exists x with $x^2 \equiv a \mod N$.

Readonly, ID: aafec6

4a)

Write a function `quad2(n)` which takes as input a positive integer n and returns

- True if 2 is a quadratic residue mod n
- False otherwise

In [ ]:
```
function quad2(n)
    ### BEGIN SOLUTION
    any(2 % n .== x^2 % n for x in 0:n-1)
    ### BEGIN SOLUTION
end
```


In [ ]:
```
@test quad2(7)
@test !quad2(11)
@test quad2(62)
```

Readonly, ID: b89524

4b) Write a function that takes an integer `N` and computes the ratio

$$\frac{\#\{p : p \text{ prime }, p < N, 2 \text{ is a quadratic residue mod } p\}}{\#\{p : p \text{ prime }, p < N\}}$$

Answer that will be automatically graded below, ID: 125613

In [ ]:
```
function prime_residue_2_ratio(N)
    YOUR ANSWER HERE
end
```

Test your code from above here (1 point), ID: aae157

In [ ]:
```
@test prime_residue_2_ratio(10) == 0.5
@test prime_residue_2_ratio(10000) ≈ 0.49145646867371845
@test prime_residue_2_ratio(7) == 1/3
```

Readonly, ID: b28986

Readonly, ID: b28986

4c) Write a function that takes an integer `N` and computes the ratio

$$\frac{\#\{p : p \text{ prime }, p < N, p \equiv 1 \mod 8 \text{ or } p \equiv 7 \mod 8, \text{ and 2 is a quadratic residue mod } p\}}{\#\{p : p \text{ prime }, p < N, p \equiv 1 \mod 8 \text{ or } p \equiv 7 \mod 8\}}$$

Answer that will be automatically graded below, ID: 58e120

In [ ]:
```
function prime_residue_1_and_7_ratio(N)
    YOUR ANSWER HERE
end
```

Test your code from above here (1 point), ID: 89b8e4

In [ ]:
```
@test prime_residue_1_and_7_ratio(10) == 1.0
@test prime_residue_1_and_7_ratio(10000) == 1.0
```

Readonly, ID: 97d9fe

4d) Write a function that takes an integer `N` and computes the ratio

$$\frac{\#\{p : p \text{ prime }, p < N, p \equiv 3 \mod 8 \text{ or } p \equiv 5 \mod 8, \text{ and 2 is a quadratic residue mod } p\}}{\#\{p : p \text{ prime }, p < N, p \equiv 3 \mod 8 \text{ or } p \equiv 5 \mod 8\}}$$

Answer that will be automatically graded below, ID: a8add5

Answer that will be automatically graded below, ID: a8add5

In [ ]:
```
function prime_residue_3_and_5_ratio(N)
    YOUR ANSWER HERE
end
```

Test your code from above here (1 point), ID: ea6a93

In [ ]:
```
@test prime_residue_3_and_5_ratio(10) == 0.0
@test prime_residue_3_and_5_ratio(10000) == 0.0
```

Readonly, ID: cb9654

What you are seeing is a combination of *Quadratic Reciprocity* and the *Cebotarev Density Theorem* (there are no other possibilities for what p could be mod 8, except for the prime $p = 2$, which is just an exception).

Readonly, ID: 846f83

Problem 5: Selfridge's Conjecture

Let N be an odd number. A conjecture of John Selfridge: https://en.wikipedia.org/wiki/John_Selfridge states that if

- $N \equiv 2 \mod 5$ or $N \equiv 4 \mod 5$
- $2^{N-1} \equiv 1 \mod N$
- $f_N \equiv 0 \mod N$

then N is prime. Here f_N is the Nth Fibonacci number; recall that in this class we are using the indexing

$$f_0 = f_1 = 1, \quad f_N = f_{N-1} + f_{N-2} \quad N \geq 2$$

but that this may differ from indexing used in other sources.

There are no known counterexamples to this claim. Selfridge and two of his collaborators, Carl Pomerance and Samuel Wagstaff, have offered $620 to anyone able to produce a counterexample.

5a)

Write a function `selfridge` which takes as input a positive integer N and returns a tuple (a, b, c) with

- a given by the residue of $N \mod 5$
- b given by the residue of $2^{N-1} \mod N$
- c given by the residue of $f_N \mod N$.

Hint: you might want to define your own fibonacci function that always works mod N. That will be faster than using a standard fibonacci function and then modding by N.

Answer that will be automatically graded below, ID: 300d58

In [ ]:
```
function selfridge(N)
    YOUR ANSWER HERE
end
```

Test your code from above here (1 point), ID: c4a6e9

In [ ]:
```
@test selfridge(1) == (1, 1, 0)
@test selfridge(5) == (0, 1, 3)
@test selfridge(323) == (3, 157, 0)
```

Readonly, ID: 53f616

5b)

A number N for which $f_N \equiv 0 \mod N$ but with N *not prime* is called a *Fibonacci pseudoprime*. Write a function that takes an integere `N` and returns the number of Fibonacci pseudoprimes which are less than or equal to N.

Answer that will be automatically graded below, ID: 9c0cef

In [ ]:
```
function num_fib_pseudoprimes(N)
    YOUR ANSWER HERE
end
```

Test your code from above here (1 point), ID: 47488f

In [ ]:
```
@test num_fib_pseudoprimes(1) == 1
@test num_fib_pseudoprimes(500) == 3
```

Readonly, ID: df6522

5c)

Are there any counterexamples to Selfridge's conjecture with $N \leq 100000$? Please answer `Y` or `N`.

Note: you may want to comment out any code that computes the answer before submitting, so the autograder won't time out.

Readonly, ID: df6522

5c)

Are there any counterexamples to Selfridge's conjecture with $N \leq 100000$? Please answer `Y` or `N`.

Note: you may want to comment out any code that computes the answer before submitting, so the autograder won't time out.

Enter your answer here, ID: 5894fa

In [ ]:
```
answer_5 = ""   # enter your answer inside the string quotes
```

Answer that will be automatically graded below, ID: 35d491

In [ ]:
```
# scratch work here
YOUR ANSWER HERE
```

Test your code from above here (1 point), ID: 7fa926

In [ ]:

In [ ]: