Fall 2023 CIS 3362 Homework #5: Number Theory
Check WebCourses for the due date

1) (5 pts) Without the aid of a computer program, determine the prime factorization of 2,427,559,200. Show your work. You may do division on a calculator.

2) (5 pts) What is φ(2,427,559,200)?

3) (5 pts) Use Fermat's Theorem to calculate the remainder when 12^{7250} is divided by 907?

4) (5 pts) Use Euler's Theorem to calculate the remainder when 77^{32641} is divided by 26010?

5) (10 pts) Show the steps of running the Miller-Rabin algorithm, testing n = 1729 for primality with the randomly chosen value of a = 2. Please use a calculator or computer program to calculate the modular exponents and just show the result of each squaring/mod operations

6) (10 pts) Trace through the Fermat Factoring algorithm to factor 45,241 as the product of two prime numbers. You may use a calculator or computer program to execute each calculation, but print out the result of each number being tested as a perfect square.

7) (10 pts) A primitive root, α, of a prime, p, is a value such that when you calculate the remainders of $\alpha, \alpha^2, \alpha^3, \alpha^4, \ldots, \alpha^{p-1}$, when divided by p, each number from the set {1, 2, 3, ..., p-1} shows up exactly once. Prove that a prime p has exactly φ(p-1) primitive roots. In writing your proof, you may assume that at least one primitive root of p exists. (Normally, this is the first part of the proof.) (Note: This question is difficult, so don't feel bad if you can't figure it out.) **(Note: The solution to this can probably be found on the internet, so I'll be looking for original explanations that show understanding but aren't identical to the book proofs…ie what a normal person would come up with after thinking about the problem on their own)**

8) (10 pts) In class, we made a chart, for p = 7, of the different lengths of cycles produced by exponentiating each of the possible non-zero mod values, mod 7. We found that two of the values (3, 5) have a cycle length of 6, two of the values (2, 4) have a cycle length of 3, 1 value (6) has a cycle length of 2, and 1 value (1) has a cycle length of 1. Based on this example, give a counting/logical argument proving the sum below, for prime numbers, p:

$$\sum_{d \in Divisor(p-1)} \phi\left(\frac{p-1}{d}\right) = p - 1$$

9) (40 pts) Write a program that will take in as input a prime number, p ($2 \le p < 10^9$) and will calculate the **sum of the cycle lengths for each possible base, 1 through p-1, inclusive for exponentiation mod p.** More formally, the input format for the program is as follows:

The first line contains a single integer, *n*, representing the number of input cases.
The input cases follow, one per line. Each of these lines has a single integer, p ($2 \le p < 10^9$), representing the input for the case. It is guaranteed that *p* will be prime.

The output for each test case (on a line by itself) should simply be a single integer equal to the value described above. **(Note: This answer can be quite a bit larger than 10^9, so please use a long long in C/C++ or long in Java to store the result.)**

You may write your program in C, C++, Java or Python.

<u>**Sample Input**</u>	<u>**Sample Output**</u>
`4`	`1`
`2`	`21`
`7`	`77`
`13`	`473`
`29`	

<u>**Note: Brute force, where you manually run all cycles will earn ½ credit (20 pts out of 40).**</u>

An efficient solution requires a calculation of phi in O($\sqrt{n}$) for calculating phi(n) and an overall run time of the summation code should be O($\tau(n)\sqrt{n}$), where $\tau(n)$ equals the number of divisors of n.