Name: Date:

Chapter 14 Project

Catching the Big One!

What we've seen in this chapter is that large prime numbers play a crucial role in our society today: everything from e-commerce to the military security of our nation. What we haven't explored is how you go about finding one of these *very* large prime numbers. Even though there are infinitely many of them, it's rather like pulling the proverbial needle out of the haystack when looking for one. Luckily, in 1914, English schoolmaster H.C. Pocklington developed a test for prime numbers.

Here's a formal version of his theorem.

> Let p be an odd prime, and q be an even integer with $1 < q < p$.
>
> Furthermore, let $N = pq + 1$.
>
> If there exists an integer x that is relatively prime with N so that
>
> $$x^{(N-1)} \equiv 1 \pmod{N} \text{ and } \gcd\left(x^q - 1, N\right) = 1,$$
>
> then N is prime.

This theorem might seem a bit much at first glance, but it basically provides another way to show that a number is prime. Without this theorem the only way to establish that a number N is prime is to exhaustively try all of its possible divisors (like we saw with the Sieve of Eratosthenes) and make sure that none of them work. When the number is large, that can take a *very* long time. With the right x, however, Pocklington's theorem says that you can establish that N is prime by two direct calculations, both of which can be plugged into a calculator such as Wolfram|Alpha.

There is still an amount of calculation to be done, but at least it's better than completely guessing when looking for a large prime number. First, to show you how this theorem works, let's walk through the theorem with a small prime number.

To begin, we need an odd prime number p and an even integer q that is less than p. We'll use the small prime $p = 31$ and let $q = 10$.

We can then calculate the value of our possible prime N.

$$\begin{aligned} N &= pq + 1 \\ &= (31)(10) + 1 \\ &= 311 \end{aligned}$$

To determine whether $N = 311$ is a prime number, we need an x that satisfies the theorem. We can use any value that works, so let's try $x = 2$. First, x must be relatively prime with N. This means that the only positive integer that divides both of them is 1. Since 2 doesn't have any other divisors besides itself and 1, and N is not even, they are indeed relatively prime.

Now we must show that the following two things are true.

$$x^{(N-1)} \equiv 1 \pmod{N} \text{ and } \gcd\left(x^q - 1, N\right) = 1$$

1. Using Wolfram|Alpha, we can show that $x^{(N-1)} \equiv 1 \pmod{N}$ is true.

$$\begin{aligned} 2^{(311-1)} &= 2^{310} \\ &\equiv 1 \bmod (311) \end{aligned}$$

2. Again, we can use Wolfram|Alpha to check that $\gcd\left(x^q - 1, N\right) = 1$ is true. Let's check that this is the case.

$$\begin{aligned} \gcd\left(2^{10} - 1, 311\right) &= \gcd(1023, 311) \\ &= 1 \end{aligned}$$

   To perform these calculations using Wolfram|Alpha, go to www.wolframalpha.com, and type in "gcd((2^10-1), 311)" and then click the = button to obtain the answer.

   Now we can be certain that 311 is a prime number by just those two calculations, rather than trying the smaller primes (2, 3, 5, 7, 11, 13, and 17) to make sure that none of them are divisors of our N.

1. It's your turn to try. We'll again start with a small prime. Let $p = 31$, but this time let $q = 8$. Determine if N is a prime number.

2. This time let's use a bigger p. Let $p = 251$. Choose a q and determine whether the resulting N is a prime number. List how many different q values you tried before finding a prime number. Show your work below, even for the attempted values of q that do not produce a prime number.

Numbers tried for q: _____

3. Now, see if you can find another prime number that has at least five digits, using values of p and q of your choosing. List the different combinations of p and q you try until you find a large enough prime. Once you find a prime, fill in the appropriate blanks below.

N = _____

p = _____

q = _____

x = _____

List all of the p and q combinations that you attempted.

4. How many combinations of p and q did you try before finding a large enough prime?

Notice that for each N you checked, you needed to perform two calculations using the software application Wolfram|Alpha. Although it might have taken you many combinations of p and q to find a prime, this is still far less work than exhaustively checking all the prime factors less than $\sqrt{N}$, which is what the Sieve of Eratosthenes would have us do.

Class Competition Time

You will compete against your classmates to see who can generate the largest prime in a given amount of time. Your instructor will provide the time guidelines for the competition.