Problem Statement

The prime factors of 13195 are 5, 7, 13 and 29.

What is the largest prime factor of the number 600,851,475,143?

Solution

At the heart of this problem is the reason RSA encryption works, it is hard to determine the prime factors of large numbers (512 bits, so around 10^154). However, for numbers less than 10^{12}, a computer can quickly test for prime factors. Since I am expecting the number to be divisible by 2 or more primes, I use a recursive algorithm that attempts to divide the number of interest n by all odd numbers (and 2) up to $n/2$. This algorithm is called recursively on each of these factors until it is determined that either n is prime or the factors themselves are prime.

As an example, consider $n = 1105 = 5(13)(17)$. Thus, we start by testing to see if 1105 is divisible, 2, 3, 5, 7, ..., 552. Since it is first divisible by $p_1 = 5$, we check if 5 is prime (it is), so it is added to the list of factors. Then, the algorithm checks if $n_1 = 221$ is prime. To do that, we check numbers below 110, which yields 13 and 17. Note, since the algorithm found $1105 = 5(221)$, it does not need to check anymore. Also, it will return the prime factors from smallest to largest.

From this algorithm:

$$n = 600,851,475,143 = 71(839)(1471)(6857)$$

So the prime factors are 71, 839, 1471, 6857.

Factorization Rules

Here are some common divisibility tests for numbers up to 10:

- If the last digit is divisible by 2 (so 0, 2, 4, 6, or 8), then the number is divisible by 2. The rule comes from the fact that 10 is divisible by 2. Thus any number larger than 10 is also divisible by 2 if it's last digit is.

- If the sum of the digits is divisible by 3, then the number is divisible by 3.

- If the last two digits are divisible by 4, then the number is divisible by 4. Thus any number larger than 100 is also divisible by 4 if it's last two digits are.

- If the last digit is either a 0 or 5, then the number is divisible by 5. Similar to 2, in that any number larger than 10 is divisible by 5 if it's last digit is.

- If the sum of the digits is divisible by 3 and the number is even, then the number is divisible by 6. This just combines the rules for 2 and 3.

- If the last 3 digits are divisible by 8, then the number is divisible by 8. The rule comes from the fact that 1000 is divisible by 8. Note, in my opinion, it is easier to check if a number is divisible by 2 three times than to check if a number as large as 999 is divisible by 8.
- If the sum of the digits are divisible by 9, then the number is divisible by 9.
- If the last digit is zero, then the number is divisible by 10.

I don't know of a good rule for 7.

Since the rule for 6 is simply a consequence of the rules for 3 and 2, the two rules of interest are the rules for 3 and 9. Consider then what the digits in base 10 actually mean. By definition:

$$n = \sum_{i=0}^{k} d_i 10^i$$

for some k. In this representation, the d_i are the digits of n in base 10. Also, for any value of $i \geq 1$, $10^i - 1$ is divisible by 3 and 9, because:

$$10^k - 1 = \sum_{i=0}^{k-1} 9(10^i)$$

As an example, $k = 3$:

$$10^3 - 1 = 999 = 9(10^0) + 9(10^1) + 9(10^2) = \sum_{i=0}^{2} 9(10^i)$$

Then:

$$n = \sum_{i=0}^{k} d_i(10^i - 1) + d_i$$

And since:

$$\sum_{i=0}^{k} d_i(10^i - 1)$$

is divisible by 3 and 9, because all the $10^i - 1$ are divisible by 3 and 9. Then, n is divisible by 9 if:

$$\sum_{i=0}^{k} d_i$$

is divisible by 9, giving the rule.

Note, we say a number is divisible by another number if under Euclid's division algorithm, it has remainder 0 (see the Project Euler 1 solution). Or:

$$n = qp + r$$

$p > 0$, $q > r \geq 0$, n is divisible by p if $r = 0$. Consider $a = b + c$. Observe:

$$\begin{aligned} b &= q_b d \\ c &= q_c d \\ a = b + c &= (q_b d + q_c d) = (q_b + q_c) d \end{aligned}$$

So if b and c are divisible then a is divisible. Thus, in the proof above, since a b and c were found, the number $n4$ must be divisible as well.