1 Prime Factorization

Prime factorization is the method by which we factor an integer into its canonical prime factorization. For relatively small integers, this is trivial to do by hand. As these integers scale, however, this task becomes prohibitively expensive to compute by our modern day algorithms. In fact, the security of the RSA cryptographic algorithm relies on the difficulty of factoring large algorithms.

Because factoring large integers is so computationally expensive, it is better to first determine that the number we want to factor is, indeed, a composite. To do this, we can use the variety of primality tests to ensure that our number is factorable before we start down this path.

2 Classical Factorization Methods

2.1 Trial Division

As a factorization method, trial division is repeated division of our number N by small primes. We store the pre-computed primes and their number in some table. This would be very speedy, albeit at the cost of the storage. Alternatively, we could save space by generating our primes along the way, using the form $6k \pm 1$ (including 2 and 3).

2.2 Euclid's Algorithm

Interestingly enough, we can also use Euclid's algorithm to search for the factors of a number.

2.3 Fermat

2.4 A Revisit of The Sieve of Eratosthenese

2.4.1 Construction of a Factor Table