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 $6k\pm1$ (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. Euclid's algorithm will give us the prime factors of our number N between g and G, where ....

To use Euclid's algorithm to factor a number, start by multiplying together all primes between the two limits. In fact, there even exists precomputed products for primes within certain ranges, to use here should we want to. Next, we apply Euclid's algorithm on the product of the primes and our number N.

The application of Euclid's is fast because it simply is repeated division, multiplication, and subtraction. The only possible tricky thing here is the initial division of our long number by N, but aside from that, it is not too difficult to perform in step-wise fashion.

The use of Euclid's algorithm to factor numbers is not obsolete. In fact, it is used when N is too large to be easily divided by a small prime. It is also used when only small divisors are sought.

2.3 Fermat

The idea behind Fermat's method of factoring is that we can write an odd composite number as a difference between two squares. Once we have that, it naturally gives us a factorization, in that: $N = x^2 - y^2 = (x - y)(x + y)$.

To find the two square numbers, we start by making the observation that any x that satisfies $N = x^2 - y^2$ must be $> \sqrt{N}$. Thus, we start with $m = \sqrt{N} + 1$, which is the smallest x possible (aside from the case where N is x^2).

We consider $x = m^2 - N$, checking to see if it is a square. If it is, then we have found our x and y.

2.4 A Revisit of The Sieve of Eratosthenese

2.4.1 Construction of a Factor Table