## Math for dh parameters

* [A Computational Introduction to Number Theory and Algebra (Version 2) (shoup.net)](https://shoup.net/ntb/ntb-v2.pdf)
  + Euler’s totient
  + Primitive root
  + Quadratic residues
  + Legendre symbol
* [BigNum Math | ScienceDirect](https://www.sciencedirect.com/book/9781597491129/bignum-math)
  + Miller rabin primality test
  + Exponentiation

## Bernardo email about DH params

1. If q is prime, then p=2q+1 is \*not\* automatically prime. This is easy to see with a counter-example. Let q = 7, then p = 2\*7+1 = 15 which is not a prime.  
   Thus, a safe prime p is a prime number p=2q+1 such that q is also prime.
2. P will indeed be the modulus for your DH
3. This is what I was missing last time, when your modulus is a safe prime it’s easier to find a generator. However you are not quite correct in what you said here.  
   A generator in this group mod p is any quadratic non-residue, i.e., any number with Legendre value of -1 (exc. So to find a generator in this group you sample a random value and compute its Legendre value; if it’s -1 then you are done, otherwise you try another one. You will find a generator in the first try with about 50% probability.

I’m adding some extra references here so you can understand better the problem. This is a nice discussion to add to the report, because most of the times those details are swept under the rug.

<https://en.wikipedia.org/wiki/Legendre_symbol>

<https://en.wikipedia.org/wiki/Quadratic_residue>

<https://math.stackexchange.com/questions/145578/what-are-the-generators-for-mathbbz-p-with-p-a-safe-prime>

<https://en.wikipedia.org/wiki/Safe_and_Sophie_Germain_primes>