Finding Primes
Exposition by William Gasarch

1 Introduction

For the Diffie-Helman protocol we need to be able to, given n, find a prime $p \in [n, 2n]$. It is known that such a prime exists.

Assume for now that we can test if a number is prime. We call that procedure $TEST$.

2 An Idiotic Solution

We could do the following:

FOUND=FALSE
While NOT FOUND
    Pick a random $m \in [n.2n]$
    If TEST(m)=TRUE then
        FOUND=TRUE
        ANS=m

There are $\frac{n}{\log n}$ primes between n and $2n$ (the log is base e) so this takes, on average $\log n$ steps.

Can we do better? Yes- we should never pick an even number.

3 Only Consider $n \not\equiv 0 \pmod 2$

If we want to pick only odd numbers then we pick $k \in [n/2, n]$ and then let $m = 2k+1$.

If a number n is such that $n \not\equiv 0 \pmod 2$ then it must be of the form $2x + b$ where $b \in \{1\}$. (I wrote it in this funny form since i is analogous to the later cases.)

FOUND=FALSE
While NOT FOUND
    Pick a random $m \in [n/2.n]$
    If TEST($2m + 1$)=TRUE then
        FOUND=TRUE
        ANS=$2m + 1$

We are only looking at half the numbers, hence this will take on average $\frac{\log n}{2}$ steps.

Can we do better?

4 Only Consider $n \not\equiv 0 \pmod{2,3}$

We want to avoid the evens and also avoid the numbers that are divisible by 3. What form do they take? All such numbers are either of the form $6k+1$ or $6k+5$.

If a number n is such that $n \not\equiv 0 \pmod{2,3}$ then it must be of the form $6x+b$ where $b \in \{1,5\}$.

FOUND=FALSE
While NOT FOUND
    Pick a random $m \in [n/6.n/3]$
    Pick a random $b \in \{1,5\}$
    If TEST($6m+b$)=TRUE then
        FOUND=TRUE
        ANS=$6m+b$

We are only looking at 1/3 of hte numbers, hence this will take, on average, $\frac{\log n}{3}$ steps.

Can we do better?

5 Only Consider $n \not\equiv 0 \pmod{2,3,5}$

This is your HW. Here is the FORM of the solution, you need to fill in the parameters.

If a number n is such that $n \not\equiv 0 \pmod{2,3,5}$ then it must be of the form $Ax+b$ where A is a constant and $b \in YYY$ where YYY is a set. (YOU need to find the constant A and the set YYY.)

FOUND=FALSE
While NOT FOUND
    Pick a random $m \in [n/A, n/2A]$
    Pick a random $b \in YYY$
    If TEST($Am+b$)=TRUE then
        FOUND=TRUE
        ANS=$Am+b$