Quiz 10

(1) Let y be a no. that is $O(2^{m \cdot 2^m})$ and k be a random number from $\{1, 2, \ldots, 2^{2m}\}$.

Let $B_y = \{p : p \text{ is a prime factor of } y\}$

i) Show that $|B_y| = O(m \cdot 2^m)$. [3]

ii) Use (i) & the Prime Number Theorem

[For sufficiently large m, the no. of primes in $\{1, 2, \ldots, 2^{2m}\}$ is atleast $\frac{2^{2m}}{2m}$]

to show that the no. of primes in $\{1, 2, \ldots, 2^{2m}\}$ that are not in B_y is atleast $\frac{2^{2m}}{4m}$. [3]

iii) Use (ii) to choose δ s.t.

$$\Pr_{k \text{ is a rand } [2^{2m}]}[k \text{ is a prime not in } B_y] > \delta$$

[1]

(2) Consider the following randomised algorithm for ZEROP = { $\mathcal{C}$ is an algebraic circuit computing the zero polynomial }

A: On input $\mathcal{C}$

1. $m \leftarrow$ size of $\mathcal{C}$. (i.e. no. of gates)
2. Choose n integers randomly from $[10 \cdot 2^m]$ [say $a_1, \ldots, a_n$.]
3. Choose $20m^2$ integers randomly from $[2^{2m}]$ say $k_1, \ldots, k_{20m^2}$
4. for $i = 1$ to $20m^2$
5. [if k_i is prime and $\mathcal{C}(a) \bmod k_i \neq 0$
6. [[output non-zero
7. output zero

You can assume addition, mult., taking mod is efficiently doable

i) Argue why the algo is efficient. [3]

ii) Use (1) to show the following for sufficiently large m.

a) $\mathcal{C} \in$ ZEROP $\Rightarrow$ Pr [Output is "zero"] $= 1$.

b) $\mathcal{C} \notin$ ZEROP $\Rightarrow$ Pr [Output is "zero"] $\leq 1/3$

[2 + 8]