Computer Science & Engineering Department

IIT Kharagpur

Computational Number Theory: CS60094

Tutorial V

Instructor: Goutam Biswas — *Spring Semester 2014-2015*

1. Prove that for any positive integer c, $n! = \Omega(c^n)$.
2. Prove that $\frac{2^{2n}}{2n} < \binom{2n}{n} < 2^{2n}$, for all $n \geq 1$.
3. If n is a positive integer and p is a prime, then $\nu_p(n) = k$, is the largest positive integer such that $p^k|n$.
   Prove that for all integers $n \geq 1$ and for all primes p, $\nu_p(n!) = \sum_{i\geq 1}\lfloor\frac{n}{p^i}\rfloor$.
4. If $l = \nu_p(\binom{2n}{n})$ then $p^l \leq 2n$.
5. Prove that $\binom{2n}{n} \leq (2n)^{\pi(2n)}$, where $\pi(x)$ is the number of primes $\leq x$.
6. Prove that for all integers $n \geq 2$, $\pi(n) \geq \frac{n}{\log n} - 2$
7. A *Carmichale number* is an odd positive integer $n > 1$ such that for all $a \in \mathbb{Z}_n^*$, $a^{n-1} \equiv 1 (\bmod\ n)$. Prove that the following two conditions are equivalent to the given definition (d). Note that $\mathbb{Z}_{p^k}^*$ is a *cyclic group* when p is an odd prime.
   (a) $a^n \equiv a (\bmod\ n)$ for all $a \in \mathbb{Z}$.
   (b) n is starfree and for all prime p, if $p|n$, then $p - 1|n - 1$.