Midsemestral examination
First Semester 2012
M.Math. IInd year
Number Theory
Instructor - B.Sury

Q 1.
If $p = 2^n + 1 > 3$ is a prime, prove that 3 is a primitive root modulo p.

OR

Let $p \equiv 3$ modulo 4 be a prime > 3 such that $2^p - 1$ is also a prime. Show that $2p + 1$ cannot be prime.

Q 2.
Let $p = a^2 + b^2$ be an odd prime, where a is odd. Prove:
(i) $\left(\frac{a}{p}\right) = 1$;
(ii) $\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$;
(iii) $(a+b)^2 \equiv 2ab$ modulo p.
Further, if 2 is a 4-th power modulo p, use the above results to show that p can be written as $c^2 + 64d^2$ for some c, d.

Q 3.
Let a, n be positive integers. Prove $a^n \equiv a^{n-\phi(n)}$ modulo n.

OR

Prove that $\sum_{r=1}^{n}(r!)^2$ is not a square if $n > 1$.

Q 4.
If p is a prime ≥ 7, show that $(p-1)! + 1$ is not a power of p.

OR

For a prime power p^n and $0 \leq r \leq p^n$, determine the residue of $\binom{p^n-1}{r}$ modulo p.

Q 5.
Show that for each positive integer n, $\mu(n) = \sum_{(k,n)=1} e^{2k\pi i/n}$.

OR

Prove that the first digit of 5^n is 1 if and only if the first digit of 2^{n+1} is also 1.

Q 6.
(i) Prove that the equation $x^2 + 5x + 12 = 31y$ has solutions in integers x, y.
(ii) Prove that the equation $u^2 + 6u + 7 = 317v$ has no solutions in integers u, v.