Howard University Math Department

TOTAL 100 POINTS.

1. (20 points) Explain which of the following statements are true and why. If false, give a counterexample.

   (a) Let a, b be odd integers relatively prime to each other. Then if the Jacobi symbol $\left(\frac{a}{b}\right) = 1$ then a is a square mod b. [Hint: try $b = 15$].

   (b) $3^n + 2$ is always prime for $n = 1, 2, 3, ...$

2. (20 points) For each of the following give an example.

   (a) A Carmichael number bigger than 1000 (use Korselt's criterion).

   (b) A prime ideal in $\mathbb{Z}[i]$.

3. (20 points) State the Miller-Rabin test and explain why it works. Use it to show that 49 is composite.

4. (20 points) Show that if a prime p is of the form $a^2 + 3b^2$ then either $p \equiv 1 \pmod{12}$ or $p \equiv 7 \pmod{12}$. In both cases, we get $p \equiv 1 \pmod{6}$. Give examples of two primes that are 1 mod 6 that are of form $a^2 + 3b^2$.

   (extra credit 20 points) Is every prime $p \equiv 1$ or $p \equiv 7$ mod 12 of this form? If you believe it true, how would you prove it? Heuristics are enough.

5. (20 points) Check whether $x^2 - 2x \equiv 4 \pmod{29}$ has a solution. If it does, find it using modular arithmetic.