2/26 Spring 2025, Number Theory II Test I solutions Sitaraman
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 $b = 15$].
   False. 2 is not a square mod 15 but its Jacobi symbol is 1 because 15 is 7 mod 8.

   (b) $3^n + 2$ is always prime for $n = 1, 2, 3, ...$
   False. Even $3^5 + 2 = 245$ is not prime.

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

   (a) A Carmichael number bigger than 1000 (use Korselt's criterion).
   We look at $5 \times 13 \times 17 = 1105$ and it satisfies Korselt's criterion.

   (b) A prime ideal in $\mathbb{Z}[i]$.
   $1 + i$ generates a prime ideal because its norm is $(1 + i)(1 - i) = 2$ which is a prime. You can also prove it by showing it is irreducible: write it as a product of two Gaussian integers, show that one of them has to be a unit.

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

   Solution: $49 - 1 = 48 = 2^4 \times 3$. So we look at a^3, a^6, a^{12}, a^{24} for some a not divisible by 49. Here we can take $a = 2$. Then we get $2^3 = 8 \equiv 8 \bmod 49$, $2^6 \equiv 64 \equiv 15 \bmod 49$, $2^{12} \equiv 15^2 \equiv 29 \bmod 49$, $2^{24} \equiv 29^2 \equiv (-20)^2 \equiv 8 \bmod 49$. So 49 must be 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 $p \equiv 7 \bmod 12$ of this form? If you believe it true, how would you prove it? Heuristics are enough.

   Solution: Clearly such primes are squares mod 3. Now from $p = a^2 + 3b^2$ we get -3 is a square mod p. Now we have

   $$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$$

   So either -1 is a square mod p and so $p \equiv 1 \pmod 4$ and so $(3/p) = (p/3) = 1$, or -1 is not a square and $p \equiv 3 \pmod 4$ and so $(3/p) = -(p/3) = -1$. In the first case we get $p \equiv 1 \pmod{12}$ and in the second we get $p \equiv 7 \pmod{12}$.

Now, we can see that 7, 13, 19, 31, 37, ... are all of the desired form. To prove it we can try working in the ring $\mathbb{Z}[\sqrt{-3}]$ in which every element is of the form $a+i\sqrt{3}b$ and the norms are $(a+i\sqrt{3}b)(a-i\sqrt{3}b) = a^2+3b^2$. If this ring is a UFD then as in the case of a^2+b^2 we could show that a prime element divides p and then by multiplying by conjugate get that $a^2+3b^2 = p$ for some a, b. In reality, this is done by looking at $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ which happens to be a UFD.

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

   Solution: The discriminant of $x^2 - 2x - 4 \equiv 0$ is $4 + 16 = 20 = 2^2 \times 5$. This will be a square if 5 is a square mod 29. By quadratic reciprocity it is. We check the numbers that are congruent to 5 mod 29: 34, 63, 92, 121 and the first square is 121. We see that $5 \equiv 11^2 \pmod{29}$. So $20 \equiv 22 \equiv -7 \pmod{29}$. The solution of the equation will be $(2 \pm \sqrt{20})/2 = 1 \pm 7(2^{-1}) \equiv 1 \pm 7(15) \equiv 12, 19$. $(x-12)(x-19) \equiv x^2 - 2x - 4$ so the answer is correct.