10/3 Fall 2022, Number Theory I Test I solutions Sitaraman

Howard University Math Department

1. (20 points) Find GCD of 198 AND 121 using (a) unique factorization (b) Euclidean algorithm and then (c) find x, y such that $121x + 198y = gcd(121, 198)$.

   Solution: 11, using the Euclidean algorithm.$198 = 121 + 77, 121 = 77 + 44, 77 = 44 + 33, 44 = 33 + 11, 33 = 3(11) + 0$.

   Working backwards, $11 = 44 - 33 = 2(44) - 77 = 2(121) - 3(77) = 5(121) - 3(198)$.

2. (20 points) Can there be infinitely many primes of the following forms: $n^3 - 1, n^3 + 1, n^4 - 1, n^4 + 1, n^2 + n + 2$?

   Solution: The first 3 can be factored, so they won't produce infinitely many primes. $n^4 + 1$ could possible produce infinitely many primes. The last one will always be divisible by 2 because $n(n + 1)$ is always even.

3. (20 points) Show that GCD of three integers a, b, c is the minimum positive of all linear combinations $ax + by + cz$.

   Solution: We showed in class that $G = gcd(a, b, c) = gcd(a, g)$ where $g = gcd(b, c)$. So $G = ax + gy = ax + bu + cv$ for some integers x, y, u, v because g is a linear combination of b, c. Now just as in the case of 2 integers, we can show that G divides any linear combination of a, b, c, so it would have to be the smallest such.

4. (20 points) (a) Solve the equation $ax \equiv 1 \pmod 5$ for $a = 1, 2, 3, 4$ using any method, with $x \in \{1, 2, 3, 4\}$. (b) Why are the solutions unique? (c) Show that the set $\{0, 1, 2, 3, 4\}$ is a field under addition and multiplication mod 5.

   Solution: The solutions will be unique from the theorem: $ax \equiv c \pmod m$ has unique solution if $gcd(a, m) = 1$. The solutions for $1, 2, 3, 4$ are $1, 3, 3, 4$ respectively. These are the multiplicative inverses. Closure under addition and multiplication are consequences of congeuence properties. Additive identiity is 0 and multiplicative identity is 1. Associativity follows from associativity in integers and congruence properties.

5. (20 points) Explain how you parametrize rational points on the unit circle using rational points on the y-axis. Find a Pythagorean triple by mapping $P = (0, 5/6)$ to the unit circle under the parametrization map.

   Solution: First part is in textbook. P would be mapped mapped to (x, y) such that $x^2 + y^2 = 1, y = m(x + 1)$, with $m = 5/6$. You can also get them as $\cos 2t, \sin 2t$ where $m = \tan t$. If $\tan t = 5/6$, we can let $\cos t = 5/\sqrt{61}, \sin t = 6/\sqrt{61}$, then the required point is

   $$(\cos 2t, \sin 2t) = (\cos^2 t - \sin^2 t, 2 \sin t \cos t) = (-11/61, 60/61)$$

   The Pythagorean triple we get from this is (11,60, 61) and it happens to be primitive as well!