Department of Basic Sciences — Philadelphia University

Final Exam **Number Theory** **06–02–2022**

1. (3 points) Compute 5^{57} % 11 using SSA.
2. (4 points) Compute 2^{3491} % 35 using Euler's theorem.
3. (2 points) Evaluate $\phi(7920)$.
4. (4 points) Solve the root mod congruence $x^9 \equiv 3 \pmod{23}$.
5. (2 points) Evaluate $|4^{45}|_{13}$.
6. (2 points) Find all the primitive roots mod 13.
7. (4 points) Solve the discrete log problem $7^x \equiv 5 \pmod{13}$.
8. (2 points) Count how many primitive roots mod 313 (prime) exist.
9. (4 points) Find the 4 solution classes to $x^2 \equiv 130 \pmod{133}$. Note $133 = 7 \times 19$.
10. (2 points) Find all the NR mod 13.
11. (2 points) Determine 32 is QR or NR mod 113.
12. (3 points) Evaluate the Legendre symbol $\left(\frac{97}{313}\right)$.
13. (2 points) Prove the theorem: If $\{g, g^2, \ldots, g^{\phi(n)}\}$ is RRS mod n, then g is primitive root mod n.
14. (2 points) Prove the theorem: If $x^e \equiv a \pmod{n}$, then a particular solution is $x_0 = a^d$ where $d = e^{-1} \,\%\, \phi(n)$. Assume $\gcd(a, n) = 1$.
15. (2 points) Prove the theorem: If g is a primitive root mod a prime $p > 2$, then $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

–Amin Witno