

Since you will have only one hour for the exam, the actual exam should be shorter than that...I include more problems so that you can practice!

Problem 1. Solve the congruence $x^3 + 4x + 8 \equiv 0 \pmod{15}$.

Problem 2. Show that $\phi(nm) = n\phi(m)$ if every prime that divides n also divides m .

Problem 3. How many square roots of 1 are there in $\mathbb{Z}/3\mathbb{Z}$? in $\mathbb{Z}/5\mathbb{Z}$? in $\mathbb{Z}/15\mathbb{Z}$? in $\mathbb{Z}/p.q\mathbb{Z}$ (where p,q are two distinct primes)?

Problem 4. Let p be an odd prime. Assume that $x \in \mathbb{Z}/p\mathbb{Z}$ is a generator of the (cyclic) multiplicative group of $(\mathbb{Z}/p\mathbb{Z})$. Does x have a square root in $\mathbb{Z}/p\mathbb{Z}$?

Problem 5. Show that if p is an odd prime and $\text{G.C.D.}(a, p) = 1$ then $x^2 \equiv a \pmod{p^\alpha}$ (where α is an integer ≥ 1) has exactly $1 + \left(\frac{a}{p}\right)$ solutions, where the symbol $\left(\frac{a}{p}\right)$ is equal to $+1$ if a has a square root modulo p , and -1 otherwise.

Problem 6. We write $j = e^{\frac{2i\pi}{3}}$ and consider the set $R = \{a + bj \mid a, b \in \mathbb{Z}\}$.

- Show that R is a subring of \mathbb{C} ;
- What are the invertible elements of R ? (Hint: show that the square of the modulus of such an element z , which is $|z|^2 = z\bar{z}$, must be 1).

Problem 7. bonus problem Can you prove that R in the previous problem is a "principal ideal domain" (meaning that any ideal I can be written as the set of all multiples of one single element)? You can use results of the HWs...