

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 $x^3 + 4x + 8 \equiv 0 \pmod{15}$.

Answer. Using the Chinese remainder theorem, we see that this congruence has a solution if and only if it has one solution modulo 3 and one solution modulo 5. Now by hand one can realize that the congruence modulo 5 has no solution, so the problem has no solution.

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

Answer. Just write $n = p_1^{r_1} \dots p_k^{r_k}$ and $m = p_1^{s_1} \dots p_k^{s_k} \cdot m'$ where m' is coprime with n . Now one has

$$\phi(n \cdot m) = \phi(p_1^{r_1+s_1} \dots p_k^{r_k+s_k} \cdot m') = (p_1^{r_1+s_1} - p_1^{r_1+s_1-1}) \dots (p_k^{r_k+s_k} - p_k^{r_k+s_k-1}) \cdot \phi(m'),$$

but this is also $(p_1^{r_1} \dots p_k^{r_k}) \cdot (p_1^{s_1} - p_1^{s_1-1}) \dots (p_k^{s_k} - p_k^{s_k-1}) \cdot \phi(m') = n \cdot \phi(m)$.

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 $\mathbb{Z}/p \cdot q\mathbb{Z}$ (where p, q are two distinct primes)?

Answer. Since $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ are fields, the equation $X^2 - 1 = 0$ has exactly two roots ± 1 . Now because of the chinese remainder theorem, we know the existence of the isomorphism

$$\mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Since this map is a ring morphism there is a bijection between the roots of $X^2 - 1 \pmod{15}$ and the ordered pairs $(a, b) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, where $a^2 - 1 \equiv 0 \pmod{3}$, and $b^2 - 1 \equiv 0 \pmod{5}$. So we get 4 such roots. The same thing is true for $\mathbb{Z}/p \cdot q\mathbb{Z}$

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 $\mathbb{Z}/p\mathbb{Z}$?

Answer. If there is such a square root y of x , then one could write it as $y = x^k$ for some $1 \leq k \leq p-1$ because x is a generator. But then one has $x = y^2 = x^{2k}$, so $x^{2k-1} - 1 \equiv 0$. Since the order of x is $p-1$ this implies $p-1 \mid 2k-1$, but since $2k-1 < 2p-1 < 2(p-1)$, the only possibility is $2k-1 = p-1$ (absurd: p must be odd).

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 $\left(\frac{a}{p}\right)$ is equal to $+1$ if the integer a has a square root modulo p , and is equal to -1 otherwise.

Answer. • If $\left(\frac{a}{p}\right) = -1$, then clearly $x^2 \equiv a \pmod{p^\alpha}$ has no root (otherwise it would have a root modulo p);

- now assume $\left(\frac{a}{p}\right) = +1$: if the equation $x^2 = a \pmod{p^\alpha}$ has one solution b , then automatically it has also the solution $-b$ (just because $(-1)^2 = 1$!). Let's show that it can't have a third root c with $c \neq b$ and $c \neq -b$. Indeed one would have $b^2 = a = c^2$, and therefore $p^\alpha | (b - c)(b + c)$. But since modulo p^α one has $c \neq b$ and $c \neq -b$, this would imply that p divides both $b - c, b + c$ and therefore p would divide b and also a (impossible because a and p are coprime). At this point we have proved that if there is one solution, then there are actually exactly two solutions. So it remains to prove the existence of one solution modulo p^α , knowing that there is a solution modulo p . Here the integer a is fixed, and we can assume that it is less than p^α . By successive euclidian divisions by the power of p , one can write it as $a = a_0 + pa_1 + \dots + p^{\alpha-1}a_{\alpha-1}$. (Replace p by 10 and this is just the usual form of an integer in base 10...). There is a solution modulo p , so there is an $x, x \leq p$ such that $x^2 \equiv a \pmod{p}$. As an integer one has $x^2 = c + p.d$. Necessarily $c = a_0$. Now replace x by $x + b.p$, where $b < p$: then $(x + p.b)^2 = x^2 + 2b.x.p + b^2.p^2$. Since $2.b.x$ can take all the possible values modulo p , one can find a b such that $x^2 \equiv a \pmod{p^2}$. Let's prove by induction that one can find a solution modulo p^α : Assume one has a solution x modulo p^k , with $x < p^k$. Then $x^2 = a_0 + \dots + a_{k-1}p^{k-1} + C.p^k$, where C can be expanded in powers of p as a finite sum $C_0 + pC_1 + \dots$. The only thing we have to do is to replace x by $x' = x + t.p^k$, so that now $x'^2 = a_0 + \dots + a_{k-1}p^{k-1} + a_k.p^k + C'.p^{k+1}$. But again, just write $x' = x + t.p^k$, notice that since $2x$ is prime with p , the multiples $2t.x$ can take any value modulo p , and therefore $x^2 + 2t.x.p^k + t^2.p^{2k}$ can be made congruent to a modulo p^{k+1} . Thus we proved that if there is one square root modulo p then there are exactly two $(2 = 1 + \left(\frac{a}{p}\right))$ square roots modulo p^α .

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

- 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).

Answer. The only thing to realize is that the product $j.j = j^2 = -1 - j$ is in the ring. Now the square of the modulus of $a + b.j$ is $a^2 + b^2 - ab$ and it must be a positive invertible integer, so it must be 1. Now $a \geq 2, b \geq 2$ are impossible, so a, b must be in $\{-1, 0, 1\}$. This leaves only six possibilities: $\{1, -1, j, j^2, 1 + j, -1 - j\}$.

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...

Answer. You just need to prove that around the origin there is a disk containing only the origin as a point of R , and that there exists for any complex number z in the plane an element λ of R such that $|z - \lambda| < 1$.