

Math 558 Spring 2009

First exam

(7 points) 1. What's $(1+i)^{64}$?

Answer: $(1+i) = \sqrt{2}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})$. $(1+i)^{64} = (\sqrt{2})^{64}(\cos 16\pi + i \sin 16\pi) = 2^{32}$.

(7 points) 2. What's 2^{1000} in \mathbb{Z}_7 ?

Answer: In \mathbb{Z}_7 , $2^{1000} = 2^{6 \cdot 166 + 4} = (2^6)^{166} \cdot 2^4 = 2^4 = 2$.

(14 points) 3. Consider the root of unity $\zeta = \frac{1}{\sqrt{2}}(i-1)$.

(a) What's $o(\zeta)$?

Answer: $\arg \zeta = \frac{3\pi}{4}$, so $o(\zeta) = 8$.

(b) What's $o(\zeta^{28})$?

Answer: $\frac{8}{(28,8)} = \frac{8}{4} = 2$.

(7 points) 4. Which elements of \mathbb{Z}_{20} have multiplicative inverses?

Answer: 3,7,9,11,13,17,19

(14 points) 5. (a) what's $o(2)$ in \mathbb{Z}_{63} ?

Answer: $2^6 = 64 \equiv 1 \pmod{63}$, so $o(2) = 6$.

(b) what's 2^{-1} in \mathbb{Z}_{63} ?

Answer: $2 \cdot 32 = 64$, so $2^{-1} = 32$.

(7 points) 6. Find $(192, 54)$ using the Euclidean algorithm.

Answer: $(192, 54) = (54, 30) = (30, 24) = (24, 6) = 6$.

(7 points) 7. Find the quotient and remainder when $x^5 + 3x^3 + x^2$ is divided by $x^3 + 2$ in $\mathbb{Z}_5[x]$.

Answer: Quotient = $x^2 + 3$. Remainder = $4x^2 + 4$.

(7 points) 8. (a) Is \mathbb{Z}_5 a field? If not, is it a ring?

Answer: Field.

(b) Is $\mathbb{Z}_5[x]$ a field? If not, is it a ring?

Answer: Ring, not field.

(c) Is $\sqrt[3]{1}$ a field? If not, is it a ring?

Answer: Neither.

(7 points) 9. Define the order of r , where r is a root of unity.

Answer: $o(r)$ is the least $n \in \mathbb{N}$ with $n > 0$ so $r^n = 1$.

(7 points) 10. Prove that if r is a root of unity, then $r^n = 1$ iff $o(r)$ divides n .

Answer. Assume $o(r)$ divides n . Then there is k with $n = k \cdot o(r)$. So $r^n = r^{k \cdot o(r)} = (r^{o(r)})^k = 1$.

For the other direction, we use the contrapositive. Suppose $o(r)$ does not divide n . Then there are k, m with $n = m \cdot o(r) + k$ where $0 < k < o(r)$. Hence $r^n = r^{m \cdot o(r)} r^k = (r^{o(r)})^m r^k = r^k$. Since $0 < k < o(r)$, $r^k \neq 1$.

(7 points) 11. Let p be prime. Prove that in \mathbb{Z}_p , $m^{-1} = k$ iff $(p - m)^{-1} = (p - k)$.

Answer In \mathbb{Z}_p , $(p - m)(p - k) = p^2 - (m + k)p + mk = mk$. So $mk = 1$ iff $(p - m)(p - k) = 1$.

(9 points) 12. Prove the following by induction: If p is prime and $a \in \mathbb{Z}_p$ then, in \mathbb{Z}_p , $a^{(p^n)} = a$ for all $n \in \mathbb{N}$ with $n > 0$.

Answer: Base case: $n = 1$: By Fermat's little theorem, $a^p = a$.

IH: For some n , $a^{(p^n)} = a$.

IS: $a^{(p^{n+1})} = a^{(p^n \cdot p)} = (a^{(p^n)})^p = a^p = a$. By induction hypothesis $(a^{(p^n)})^p = a^p = a$.