

Math 558 S09

Answers to first exam review problems.

I. Calculations

1. Let r be the other root. (a) $3r = 15$ so $r = 5$. (b) Hence $a = -(3 + 5) = -8$.
2. $45(\cos 3.4\pi + i \sin 3.4\pi)$
2. (apologies for the typo of two problem 2's) (a) $1 - i = \sqrt{2}(\cos \frac{7\pi}{4} + i \sin \frac{7\pi}{4})$. $(1 - i)^{25} = (\sqrt{2})^{25}(\cos \frac{175\pi}{4} + i \sin \frac{175\pi}{4}) = \sqrt{2^{24}}\sqrt{2}(\cos \frac{7\pi}{4} + i \sin \frac{7\pi}{4}) = 2^{12}(1 - i)$.
(b) $[2(\cos \frac{5\pi}{9} + i \sin \frac{5\pi}{9})]^6 = 64(\cos \frac{10\pi}{3} + i \sin \frac{10\pi}{3}) = 64(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3}) = -32 - 32\sqrt{3}i$.
3. Start with $3(\cos \frac{5\pi}{16} + i \sin \frac{5\pi}{16})$ and then multiply it by $\cos \frac{2k\pi}{5} + i \sin \frac{2k\pi}{5}$, $0 < k < 5$. This gives a full list of:

$$3(\cos \frac{5\pi}{16} + i \sin \frac{5\pi}{16})$$

$$3(\cos \frac{57\pi}{80} + i \sin \frac{57\pi}{80})$$

$$3(\cos \frac{89\pi}{80} + i \sin \frac{89\pi}{80})$$

$$3(\cos \frac{121\pi}{80} + i \sin \frac{121\pi}{80})$$

$$3(\cos \frac{153\pi}{80} + i \sin \frac{153\pi}{80})$$

4. $\zeta^{200} = (\zeta^{99})^2 \zeta^2 = \zeta^2$
5. $2 + 3 = 5$.
6. (a) 29 is prime, so in \mathbb{Z}_{29} , $3^{30} = 3 \cdot 3^{29} = 3 \cdot 3 = 9$.
(b) 31 is prime, so in \mathbb{Z}_{31} , $3^{30} = 1$.
7. (a) $\frac{5\pi}{9} = \frac{10\pi}{18}$, and $(5, 18) = 1$, so $o(\zeta) = 18$.
(b) $(18, 3) = 3$, so $o(\zeta^3) = \frac{18}{3} = 6$.
(d) $(18, 5) = 1$, so $o(\zeta^5) = 18$.
8. (a) In \mathbb{Z}_5 : $3^2 = 4$, $3^3 = 2$, $3^4 = 1$. So $o(3) = 4$.
(b) $(4, 18) = 2$, so in \mathbb{Z}_5 , $o(3^{18}) = \frac{4}{2} = 2$.
9. (a) In \mathbb{Z}_6 , $5^2 = 1$, so $o(5) = 2$.
(b) $(2, 25) = 1$, so in \mathbb{Z}_6 , $o(5^{25}) = 2$.
10. 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.
11. 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.
12. You only have to check $5 \times a$ where a is relatively prime to 12, i.e., 5, 7, 11. $5 \cdot 5 = 25 \equiv 1 \pmod{12}$, so in \mathbb{Z}_{12} , $5 = 5^{-1}$. And, since $5 + 7 = 12$, in \mathbb{Z}_{12} , $-5 = 7$.
13. $324 = 13 \cdot 24 + 12$, so $(324, 24) = (24, 12) = 12$.
14. $2^2 3^2 5^2$ (= 900 but I don't care about that)
15. In \mathbb{Z}_4 : $1^3 + 1 = 2$; $2^3 + 2 = 0 + 2 = 2$; $3^3 + 3 = 3 + 3 = 2$. So 1, 2, 3 all satisfy the equation. [Note: because 4 is not prime, we couldn't use $a^3 = 1$; in fact that's false for both $a = 2$ and $a = 3$.]
16. 5 is a prime, so we can use $a^4 = 1$ in \mathbb{Z}_5 . $a^{125} + a^{120} - a^3 - 1 = (a^4)^{31} \cdot a + (a^4)^{30} - a^3 - 1 = a + 1 - a^3 - 1 = a - a^3$. So let $f(a) = a - a^3$. In \mathbb{Z}_5 , $f(0) = 0$; $f(1) = 0$; $f(2) = 1 \neq 0$; $f(3) = 4 \neq 0$; $f(4) = 0$.

I.e., there are three solutions: $a = 0, 1, 4$. [Note: I used bad notation here: I should have written $a^{125} + a^{120} + 4a^3 + 4$, because in \mathbb{Z}_5 , $-1 = 4$.]

17. (a) $-2x^2 - 2$; (b) $3x^2 + 3$ (because in \mathbb{Z}_5 , $-2 = 3$); (c) $x^2 + 1$ (because in \mathbb{Z}_3 , $-2 = 1$)

True/false

1. (a) F (b) T (c) T (d) F (e) T
2. (a) F (b) T (c) F
3. T
4. (a) T (b) T (c) F (d) F
5. (a) T (b) F
6. (a) F (b) T (c) T (d) T

Finish the sentence

1. n
2. (a) -3 ; (b) -5
3. n
4. prime
5. a
6. $p - 1$

Fairly short proofs

1. Suppose $n = km$ where $1 < k \leq m < n$. Let $\zeta = \cos \frac{2m\pi}{n} + i \sin \frac{2m\pi}{n}$. Then $\zeta^k = \cos \frac{2n\pi}{n} + i \sin \frac{2n\pi}{n} = 1$. So $o(\zeta) \leq k < n$.
2. If $\zeta \in \sqrt[12]{1}$ then $o(\zeta)$ divides 12. Since 12 divides 60, $o(\zeta)$ divides 60. But 60 is a divisor of 60 which does not divide 12, so $o(\zeta) \neq 60$;
3. Let $\zeta \in \sqrt[7]{1}$. Let $S = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6\}$. 7 is prime, so every element of $\sqrt[7]{1}$ has order 7. Hence $o(\zeta) = 7$ and the elements of S are all distinct. Since $o(\zeta^m) = \frac{7}{(m,7)} = 7$ for $0 < m < 7$, $S \subset \sqrt[7]{1}$. Since $\#S = \# \sqrt[7]{1} = 7$, $S = \sqrt[7]{1}$.
4. By way of contradiction, suppose $\sqrt{5} = \frac{k}{m}$ where k, m are relatively prime. Then $5 = \frac{k^2}{m^2}$ so $5m^2 = k^2$. Hence 5 divides k . Let $k = 5n$. $k^2 = 25n^2$, so $m^2 = 5n^2$. Hence 5 divides m . Which contradicts our assumption that $(k, m) = 1$.
5. Let F be a field, $a \in F$ and suppose $ab = ac = 1$. Then $bab = bac$, so $b = c$.
6. Let $n = o(a), m = o(b), g = (n, m) > 1$. There are $r, s \in \mathbb{N}, r < n, s < m$ so $n = gr, m = gs$. Hence $grs < nm$. $(ab)^{grs} = a^{grs}b^{grs} = (a^n)^s(b^m)^r = 1^s \cdot 1^r = 1$. So $o(ab) \leq grs < nm$.
7. Suppose $p = 2^k + 1$ and p is prime. Let $a \in \mathbb{Z}_p, a \neq 0$. $a^{p-1} = 1$. So $o(a)$ divides $p - 1 = 2^k$. Hence $o(a)$ is a power of 2.
8. If $p > 3$ then $p - 1 = 2k$ for some k where $1 < k < p - 1$. Let $a \in \mathbb{Z}_p, a \neq 1$. If $1 < o(a) < p - 1$ we're done. Otherwise $o(a) = p - 1$. So $o(a^2) = k$.

Proofs by induction

1. (a) $\sum_{i=1}^4 (2i - 1) = 2(1 + 2 + 3 + 4) - 4 = 20 - 4 = 16 = 4^2$.

(b) Base case: $n = 1$: $2 - 1 = 1 = 1^2$.

IH: For some n , $\sum_{i=1}^n (2i - 1) = n^2$.

IS: $\sum_{i=1}^{n+1} (2i - 1) = 2(n+1) - 1 + \sum_{i=1}^n (2i - 1) = 2n + 1 + n^2$ (by IH). and $2n + 1 + n^2 = (n+1)^2$.

2. (a) $2^5 = 32 > 25 = 5^2$; $2^6 = 64 > 36 = 6^2$; $2^7 = 128 > 49 = 7^2$. But $2^4 = 16 = 4^2$.

(b) Base case: $n = 5$: done in part (a)

IH: For some n , $2^n > n^2$.

IS: We want to prove $2^{n+1} > (n+1)^2 = n^2 + 2n + 1$. $2^{n+1} = 2 \cdot 2^n = 2^n + 2^n$. So we need to prove $2^n + 2^n > n^2 + 2n + 1$. By induction hypothesis, $2^n > n^2$. Since $n \geq 5$, $n^2 > 3n = 2n + n > 2n + 1$. Putting this all together, $2^{n+1} = 2^n + 2^n > n^2 + n^2 > n^2 + 2n + 1 = (n+1)^2$.

3. (a) $3^2 = 9 > 7 = 2 \cdot 3 + 1$, but $2^2 = 4 < 2 \cdot 2 + 1 = 5$.

(b) If $n > 2$ then $n^2 \geq 3n > 2n + 1$.

(c) $4! = 24 > 16 = 4^2$, but $3! = 6 < 9 = 3^2$.

(d) Base case: $n = 4$: done in (c)

IH: For some n , $n! > n^2$.

IS: $(n+1)! = (n+1)n! > (n+1)n^2$ by IH. By (b), $(n+1)n^2 > (n+1)(2n+1) = 2n^2 + 3n + 1 > n^2 + 2n + 1 = (n+1)^2$.