

## Homework 4 Partial Solutions

### Question 9A # 16

Let  $n$  be an integer such that  $41 \nmid n$  and  $n$  has order 2 mod 41. This last statement implies that  $[n]_{41}^2 = [1]_{41}$  in  $\mathbb{Z}/41\mathbb{Z}$ . Since 41 is prime,  $\mathbb{Z}/41\mathbb{Z}$  is a field, and hence also a commutative ring with no zero divisors. Since  $41 \nmid n$ ,  $n$  is a unit in  $\mathbb{Z}/41\mathbb{Z}$ . Thus we can apply 8A E18 to get that  $[n]_{41} = [1]_{41}$  or  $[n]_{41} = [-1]_{41}$ . However, if  $[n]_{41} = [1]_{41}$  then  $n$  would have order 1 mod 41. But this is a contradiction, so  $[n]_{41} = [-1]_{41} = [40]_{41}$ . This implies that  $n = 40 + 41k$  for some  $k \in \mathbb{Z}$ .

### Question 9B # 12

$\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} = \frac{15}{15} \left( \frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} \right) = \frac{1}{15} (3n^5 + 5n^3 + 7n)$ . So  $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$  is an integer if and only if  $3n^5 + 5n^3 + 7n$  is divisible by 15 or  $3n^5 + 5n^3 + 7n \equiv 0 \pmod{15}$ . By property (v) on pg. 71, we can show this by showing that  $3n^5 + 5n^3 + 7n \equiv 0 \pmod{3}$  and  $3n^5 + 5n^3 + 7n \equiv 0 \pmod{5}$ , since  $15 = [3, 5]$ .

If  $3|n$ , then  $3n^5 + 5n^3 + 7n \equiv 0 \pmod{3}$ . Otherwise, by Fermat's theorem,  $n^2 \equiv 1 \pmod{3}$ . In this case,  $3n^5 + 5n^3 + 7n \equiv 3(n^2)^2n + 5n^2n + 7n \equiv 3(1)^2n + 5(1)n + 7n \equiv 15n \equiv 0 \pmod{3}$ .

If  $5|n$ , then  $3n^5 + 5n^3 + 7n \equiv 0 \pmod{5}$ . Otherwise, by Fermat's theorem,  $n^4 \equiv 1 \pmod{5}$ . In this case,  $3n^5 + 5n^3 + 7n \equiv 3(n^4)n + 5n^3 + 7n \equiv 3(1)n + 5n^3 + 7n \equiv 10n + 5n^3 \equiv 5(2n + n^3) \equiv 0 \pmod{5}$ .

Therefore,  $3n^5 + 5n^3 + 7n \equiv 0 \pmod{3}$  and  $3n^5 + 5n^3 + 7n \equiv 0 \pmod{5}$ , so  $3n^5 + 5n^3 + 7n \equiv 0 \pmod{15}$ , and hence  $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$  is an integer.

### Question 9C # 7

(i) If  $p$  is prime, then for all  $1 \leq a \leq p-1$ ,  $(a, p) = 1$ . This implies that  $[a]$  is a unit in  $\mathbb{Z}/p\mathbb{Z}$ .  $\phi(p)$  is the number of units in  $\mathbb{Z}/p\mathbb{Z}$ , so  $\phi(p) = p-1$ .

(ii)  $\phi(p^n)$  is the number of integers  $a$ , where  $1 \leq a \leq p^n$  and  $(a, p^n) = 1$ . Since  $p$  is prime,  $(a, p^n) = 1$  if and only if  $p \nmid a$ . So  $\phi(p^n)$  counts all number between 1 and  $p^n$ , inclusive, that are not multiples of  $p$ . Since  $p^n = p^{n-1}p$ , then there are  $p^{n-1}$  multiples of  $p$  between 1 and  $p^n$  inclusive. Therefore,  $\phi(p^n) = p^n - p^{n-1}$  if  $p$  is prime.