Name: Solutions

Directions: Show all work. No credit for answers without work.

1. **[2 points]** Give a definition of $\text{ord}_p(n)$. (There are several equivalent ways to define this; give only one.)

(•) $\text{ord}_p(n)$ is the exponent of p in the prime factorization of n

(•) $\text{ord}_p(n)$ is the highest power of p dividing n

(•) $\text{ord}_p(n)$ is the integer k such that $p^k \mid n$ but $p^{k+1} \nmid n$.

2. **[2 points]** Find $\text{ord}_7(4900)$.

$4900 = 7^2 \cdot 100$, so $\text{ord}_7(4900) = \boxed{2}$

3. **[2 points]** Give 3 different examples of an integer n that satisfies $\text{ord}_2(n) = 3$.

• We need integers of the form $2^3 u$, where u is odd:

8, 24, 40, 56, 72, ...

4. **[2 points]** Let m be a positive integer and let p be a prime. For each algebraic structure below, circle the arithmetic operations that are well-behaved.

(a) $\mathbb{Z}_m^*$ $+ \; - \; (\times) \; \div$

(b) $\mathbb{F}_p$ $(+) \; (-) \; (\times) \; (\div)$

(c) $\mathbb{Z}_m$ $(+) \; (-) \; (\times) \; \div$

5. **[2 points]** Let a and b be positive integers such that $\text{ord}_2(a) = \text{ord}_2(b)$. Let k be the common order of 2 in both a and b; that is, $k = \text{ord}_2(a)$ and $k = \text{ord}_2(b)$. Prove that if $\text{ord}_2(a+b) \geq k+1$.

Since $\text{ord}_2(a) = \text{ord}_2(b) = k$, it follows that

$$a = 2^k a'$$
$$b = 2^k b'$$

for some integers a' and b' that are not divisible by 2. This means that a' and b' are odd.

We compute

$$a+b = 2^k a' + 2^k b' = 2^k(a'+b').$$

Since the sum of two odd integers is even, it follows that $a'+b' = 2u$ for some integer u. Therefore

$a+b = 2^k(a'+b') = 2^k \cdot 2u = 2^{k+1} u$ and so $2^{k+1} \mid a+b$.

Since $\text{ord}_2(a+b)$ is the ~~largest~~ highest power of 2 that divides $a+b$, we conclude that $\text{ord}_2(a+b) \geq k+1$. ∎