Solutions to problem set TWO

Problem 1:
(a): Suppose \( p^r \) is the largest \( p - \text{power} \) in the first \( N \) nature numbers, then \( \text{ord}_p(d_N) = r \). From \( p^r \leq n < p^{r+1} \), we have \( r \leq \frac{\log N}{\log p} < r+1 \), \( r = \lfloor \frac{\log N}{\log p} \rfloor \). Therefore

\[
d_N = \prod_{p \leq N} p^{\left\lfloor \frac{\log N}{\log p} \right\rfloor}
\]

\[
\log d_N = \sum_{p \leq N} \left\lfloor \frac{\log N}{\log p} \right\rfloor \cdot \log p \leq \sum_{p \leq N} \frac{\log N}{\log p} \cdot \log p = \pi(N) \log N
\]

(b): \( d_N \int_0^1 f(x)dx = \sum_{i=1}^N \frac{d_N}{i} a_{i-1} \). By the definition of \( d_N \), each \( \frac{d_N}{i} \) is an integer. Hence the foregoing formula is an integer.

(c): This is obvious by (b).

(d): By the arithmetic-geometric inequality, we have for \( x \in [0,1] \),

\[
f(x) = x^N(1-x)^N \leq \left( \frac{N \cdot x + N \cdot (1-x)}{2N} \right)^{2N} = 4^{-N}
\]

Combining this inequality with the results in (a) and (c), we get

\[
(2N + 1) \exp \pi(2N + 1) \cdot 4^{-N} \geq d_{2N+1} \cdot 4^{-N} \geq d_{2N+1} \int_0^1 f(x)dx \geq 1
\]

Taking logarithm of the above inequality, we have

\[
\pi(2N + 1) \geq \frac{(2 \log 2)N}{\log 2N + 1}
\]

Problem 2:
Suppose \( a \) is a point in this disc \( D = \{ x \in \mathbb{Q} : |x|_p < 1 \} \). Our aim is to prove \( A = \{ x \in \mathbb{Q} : |x-a|_p < 1 \} \) equals \( D \).

Since \( a \in D, |a|_p < 1 \), for any \( b \in A \), we have by the strong triangle inequality: \( |b|_p \leq \max\{ |b-a|_p, |a|_p \} < 1 \). Hence \( A \subseteq D \).

Conversely, for any \( c \in D \), we have by the strong triangle inequality: \( |b-a|_p \leq \max\{ |b|_p, |a|_p \} < 1 \). Hence \( D \subseteq A \).

Problem 3:
When \( p = 2, 3 \), the result is obvious.

We suppose \( p > 3 \). Let \( k = \frac{p-1}{2} \), then

\[
1 + 2 + \cdots + (p-1) = kp
\]
Our purpose is to prove $kp|((p-1)!-(p-1))$. Because $k$ and $p$ are co-prime, this is equivalent to $k|((p-1)!-(p-1))$.

First, \((p-1)!/(p-1) - 1 = 2 \cdot ((p-2)! - 1) \in \mathbb{Z}\).

Second, the \(p-3\) numbers \(2, 3, \ldots, p-2\) can be partitioned to \((p-3)/2\) pairs, each pair consists of two integers whose product is congruent to \(1\) mod \(p\). Therefore

\[
(p-2)! = 2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p}
\]

\[
(p-1)! = (p-1) \cdot (p-2)! \equiv p-1 \pmod{p}
\]

Hence the result.

Problem 4:
Since \(a\) is co-prime to \(p\), Fermat’s Little theorem tells us that \(a^{p-1} - 1 = (a-1)(1 + a + a^2 + \cdots + a^{p-2})\) is a multiple of \(p\). Now the assumption says that the first factor \(a-1\) is not divisible by \(p\), hence the second factor \(1 + a + a^2 + \cdots + a^{p-2}\) must be divisible by \(p\).

Problem 5: \(u_1 \equiv v_1, u_2 \equiv v_2 \pmod{m}\) implies \(u_1 + u_2 \equiv v_1 + v_2 \pmod{m}\). In proving \(f(a + tm) \equiv f(a) \pmod{m}\), we can assume that \(f\) is a monomial. In this case, \(f(x) = cx^k, c \in \mathbb{Z}\), we have

\[
f(a + tm) - f(a) = c(a + tm)^k - ca^k = c(C_m^1 a^{m-1} tm + C_m^2 a^{m-2} (tm)^2 + \cdots + C_m^m (tm)^m)
\]

Each summand is a multiple of \(m\), hence the sum itself is a multiple of \(m\).

Suppose the degree of \(f\) is \(n\). Then there are at most \(2n\) different integer value of \(x\) satisfying \(f(x) = \pm 1\). Thus there exist some \(a \in \mathbb{Z}\) such that \(f(a) \neq \pm 1\), take a prime factor of \(f(a)\), say, \(p\). By the foregoing result, each integer \(f(a + tp)\) is a multiple of \(p\). But the number of solutions for the equation \(f(X) = \pm p\) is at most \(2n\), there must be some \(t_0 \in \mathbb{Z}\) such that \(f(a + t_0 p) \neq \pm p\). Then \(f(a + t_0 p)\) is not a prime.