Problem 1  (a) It is very easy to find the sequence which satisfies given condition. For example,

\[ a_n := \frac{1}{n} \]

(Note that this sequence has no zero term.) Then \[ P_N = \prod_{n=1}^{N} a_n = \frac{1}{n!} \], and the limit of \( P_n \) is clearly 0.

(b) Write as following :

\[ \prod_{n=1}^{\infty} a_n = \prod_{n=1}^{\infty} (1 + (a_n - 1)). \]

Let \( b_n := a_n - 1 \), then to show \( \lim_{n \to \infty} b_n = 0 \) is equivalent to show that \( \lim_{n \to \infty} a_n = 1 \). For the convergent infinite product, by our definition, \( \lim_{n \to \infty} P_n = \alpha \) where \( \alpha \neq 0 \). Then

\[ \lim_{n \to \infty} a_n = \lim_{n \to \infty} \frac{P_n}{P_{n-1}} = \frac{\lim_{n \to \infty} P_n}{\lim_{n \to \infty} P_{n-1}} = \frac{\alpha}{\alpha} = 1, \]

as desired.

(c) Think of \( b_n = \frac{1}{n} \). Then \( 1 + b_n = \frac{n+1}{n} \), and we have

\[ P_N = \prod_{n=1}^{N} \frac{n+1}{n} = \frac{2}{1} \cdot \frac{3}{2} \cdots \frac{N+1}{N} = N + 1. \]

As \( N \to \infty \), \( P_N \to \infty \), so it does not converge.

(d) When \( a_n > 0 \) for all \( n \), we can say that \( \log(P_N) = \sum_{n=1}^{N} \log a_n \). Hence, \([P_n \text{ converges nonzero number}]\) is equivalent to \([\sum_{n=1}^{\infty} \log a_n \text{ converges}]\). Therefore it is enough to show that

\[ \sum_{p} \log([1 - p^{-s}]^{-1}) = \sum_{p} \log \left( \frac{p^s}{p^s - 1} \right) = \sum_{p} \log \left( 1 + \frac{1}{p^s - 1} \right) < \infty. \]

To show that, I claim that

\[ \text{If } x > 0, \text{ then } \log(1 + x) \leq x. \]
Problem 2 When we try to prove the Dirichlet’s theorem on primes in general modulus \( d \), we need to find a good method to express \( \chi \), as similar as the character used in the proof for prime modulus. Note that we used a primitive root to define that character. But for general modulus \( d \), the problem is that \( d \) may not have a primitive root.

To resolve this problem, let’s think \( d = 2^k p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \), where \( p_i \) is a prime divisor of \( d \). Then each \( p_i^{e_i} \) has a primitive root, so let \( g_i \) be the primitive root of \( p_i^{e_i} \) for each \( i \). As the case of prime modulus, take complex \( \phi(p_i^{e_i}) \) th root of unity \( w_i \), and let \( v_i \) be the index function for each \( w_i \).

First consider the case \( k = 0 \). (i.e, \( d \) is odd.) By Chinese remainder theorem, residue class \( n \) in modulus \( d \) such that \( \gcd(n, d) = 1 \) is defined by residue class \( n_i \) in modulus \( p_i^{e_i} \) such that \( \gcd(n_i, p_i) = 1 \) for each \( i \). Then define \( \chi(n) = w_1^{v_1(n_1)} w_2^{v_2(n_2)} \cdots w_r^{v_r(n_r)} \). (Actually, we can just write that \( \chi(n) = w_1^{v_1(n)} w_2^{v_2(n)} \cdots w_r^{v_r(n)} \).) It can be easily verified that this is actually a character, and all the character are coming from this, depending on choice of \( w_i \). Then we have

\[
\sum_{\chi} \chi(n) = \sum_{i=1}^r \sum_{w_i} w_i^{v_1(n)}.
\]

For each \( i \), \( \sum_{w_i} w_i^{v_1(n)} = 0 \) if \( \phi(p_i^{e_i}) \nmid n \) and \( \sum_{w_i} w_i^{v_1(n)} = \phi(p_i^{e_i}) \) if \( n \equiv 0 \pmod{\phi(p_i^{e_i})} \).

With use of Chinese remainder theorem properly, this formation gives desired result.

When \( k \geq 1 \), it is more complicated. The problem is that \( 2^k \) does not have a primitive root. But we can resolve this problem to find values which play roles similar with the primitive root. More precisely, we will show that any reduced residue class of \( 2^k \) can be expressed by \((-1)^{i}5^j \) where \( i = 0, 1 \) and \( j = 1, \cdots, 2^{k-2} = \frac{\phi(2^k)}{2} \). When we prove this, all the cases will be proved by similar argument.

We use the following fact to prove this.

Let \( f(n) \) is the largest integer \( x \) such that \( 2^x \mid n \). Then for each \( 0 \leq i \leq 2^k \),

\[
f\left(\binom{2^k}{i}\right) = k - f(i).
\]

(This can be proved using \( f(2^k - i) = f(i) \) for \( 0 < i < 2^k \), and expansion of \( \binom{2^k}{i} \).)
We can write as following:

\[ 5^{2^k} = (2^2 + 1)^{2^k} = \sum_{i=0}^{2^k} \binom{2^k}{i} 2^{2i}. \]

Now using the above fact, we can conclude that \( f \left( \binom{2^k}{i} 2^{2i} \right) = k - f(i) + 2i. \) Since \( i \geq f(i) \) is clear, we have \( 5^{2^k} \equiv 2^{2k+2} + 1 \pmod{2^{k+3}}. \) By squaring this, \( 5^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}. \)

Note that \( \phi(2^k) = 2^{k-1}. \) Now what we have observed gives us following facts.

1. The order of 5 in modulus \( 2^k \) is \( 2^{k-2}. \)
2. \( 5^{2^{k-3}} \equiv 2^{k-1} + 1 \not\equiv -1 \pmod{2^k}. \)

Consider the set \( \{ \pm 5^j \} \) \((j = 1, 2, \cdots, 2^{k-2})\). By above two facts, all elements are distinct in modulus \( 2^k \). (Only nontrivial part is proving \( 5^i + 1 \not\equiv 0 \pmod{2^k} \) for \( i = 0, 1, \cdots, 2^{k-2} - 1. \) If \( 5^i + 1 \equiv 0, 5^{2i} \equiv 1, \) hence by (1), \( 2^{k-2} \mid 2i, \) so only possible \( i \) is \( 2^{k-3}, \) but this is a contradiction because of (2).) Thus comparing the number of elements, this is same with reduced residue class of \( 2^k, \) as desired. □

**Problem 3** Let’s calculate this sum for several primes \( q \equiv 3 \pmod{4}. \)

For \( q = 3, \) \( \sum_{m=1}^{q-1} m \left( \frac{m}{q} \right) = 1 - 2 = -1. \)

For \( q = 7, \) \( \sum_{m=1}^{q-1} m \left( \frac{m}{q} \right) = 1 + 2 - 3 + 4 - 5 - 6 = -7. \)

For \( q = 11, \) \( \sum_{m=1}^{q-1} m \left( \frac{m}{q} \right) = 1 - 2 + 3 + 4 - 5 - 6 - 7 - 8 + 9 - 10 = -11. \)

For \( q = 19, \) \( \sum_{m=1}^{q-1} m \left( \frac{m}{q} \right) = 1 - 2 - 3 + 4 + 5 + 6 + 7 - 8 + 9 - 10 + 11 - 12 - 13 - 14 - 15 + 16 + 17 - 18 = -19. \)

For \( q = 23, \) \( \sum_{m=1}^{q-1} m \left( \frac{m}{q} \right) = \cdots = -69. \)

From above, we may guess that this sum is divisible by \( q. \) Actually it is. Let \( A \) is the sum of quadratic residue of \( q \) and \( B \) is the sum of quadratic nonresidue, then \( A + B = 1 + 2 + \cdots + q - 1 = q \cdot \frac{q-1}{2}. \) Let \( g \) be the primitive root of \( q. \) Then \( B \equiv g^1 + g^3 + \cdots + g^{q-2} \)
(mod q) and \( A \equiv g^2 + g^4 + \cdots + g^{q-1} \) (mod q). Therefore, \( A \equiv gB \) (mod q), and we can conclude that \( 0 \equiv A + B \equiv (g + 1)B \) (mod q). If q is not 3, \( g \not\equiv -1 \) (mod q) clearly, so \( B \equiv 0 \) (mod q). This implies that \( A \equiv 0 \) (mod q), so \( S := \sum_{m=1}^{q-1} m \left( \frac{m}{q} \right) = A - B \equiv 0 \) (mod q).

In the class, we already prove that this sum is not equal to zero using parity. (More over, \( S \) is an odd integer.) Therefore, if \( S \geq 0 \), then \( S \geq q \).

But it is still hard to make the conclusion.... I can’t find elementary solution, but I think there will be a simple solution. If you find something nice, please let me know.

*If you have any question, please contact me : Yoonsuk Hyun (yshyun@math.mit.edu)*