1. Let 

\[ \sigma_2(n) = \sum_{d|n} d^2. \]

Using Problem 6 from Assignment 1 and the fact that for \( r \in (1, \infty) \) we have

\[ \sum_{n \leq x} \frac{1}{n^r} = \zeta(r) + O \left( \frac{1}{x^{r-1}} \right), \]

which you don’t have to prove, prove that

\[ \sum_{n \leq x} \sigma_2(n) = \frac{\zeta(3)}{3} x^3 + O(x^2). \]

**Solution:** We see that

\[ \sum_{n \leq x} \sigma_2(n) = \sum_{n \leq x} d^2 = \sum_{md \leq x} d^2 = \sum_{m \leq x} \sum_{d \leq \frac{x}{m}} d^2 \]

and that by Problem 6 we have

\[ \sum_{d \leq \frac{x}{m}} d^2 = \frac{\left\lfloor \frac{x}{m} \right\rfloor + 1}{6} \left( \frac{2 \left\lfloor \frac{x}{m} \right\rfloor + 1}{3} \right) = \frac{1}{3} \left( \frac{x}{m} \right)^3 + O \left( \left( \frac{x}{m} \right)^2 \right). \]

So

\[ \sum_{n \leq x} \sigma_2(n) = \sum_{m \leq x} \left( \frac{1}{3} \left( \frac{x}{m} \right)^3 + O \left( \left( \frac{x}{m} \right)^2 \right) \right) = \frac{x^3}{3} \sum_{m \leq x} \frac{1}{m^3} + O(x^2) \]

\[ = \frac{\zeta(3)}{3} x^3 + O \left( \frac{1}{x^2} \right) + O(x^2) = \frac{\zeta(3)}{3} x^3 + O(x^2). \]

2. As an alternative means of finding the Euler Product for \( \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \), note that for \( \text{Re}(s) > 1 \),

\[ \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \sum_{k=0}^{\infty} \frac{1}{p^{sk}} = \prod_{p \text{ prime}} \varphi_p(s). \]

where \( \varphi_p(s) = \sum_{k=0}^{\infty} \frac{1}{p^{sk}} \) for \( \text{Re}(s) > 1 \). Ignoring issues of convergence, we can give a formula for \( \varphi_p(s) \) as a rational function in \( p^{-s} \) by using the recursion:

\[ \frac{1}{p^s} \varphi_p(s) = \sum_{k=0}^{\infty} \frac{1}{p^{s(k+1)}} = \sum_{k=1}^{\infty} \frac{1}{p^{sk}} = \sum_{k=0}^{\infty} \frac{1}{p^{sk}} - 1 = \varphi_p(s) - 1 \]
and then solving the recursion $p^{-s} \varphi_p(s) = \varphi_p(s) - 1$ to get $\varphi_p(s) = (1 - p^{-s})^{-1}$, we have $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ for $\text{Re}(s) > 1$.

Now, let $f : \mathbb{N} \to \mathbb{R}$ (or $\mathbb{C}$) be a multiplicative function such that for $r, p \in \mathbb{N}$ with $p$ prime we have $f(p^{r+1}) = f(p) f(p^r) - f(p^{r-1})$. Ignoring issues of convergence, use similar methods to find an Euler Product for $L(s, f) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$.

Solution: We see that

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \text{ prime}} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{sk}} = \prod_{p \text{ prime}} \psi_p(s),$$

where $\psi_p(s) = \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{sk}}$. We observe that

$$\frac{f(p)}{p^s} \psi_p(s) = \sum_{k=0}^{\infty} \frac{f(p) f(p^{k+1})}{p^{sk(k+1)}} = \sum_{k=0}^{\infty} \frac{f(p^{k+1})}{p^{sk(k+1)}} + \sum_{k=1}^{\infty} \frac{f(p^{k-1})}{p^{sk(k+1)}} = \sum_{k=1}^{\infty} \frac{f(p^k)}{p^{sk}} + \frac{1}{p^{2s}} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{sk}}$$

so

$$1 = \psi_p(s) - f(p) p^{-s} \psi_p(s) + p^{-2s} \psi_p(s) \quad \rightarrow \quad \psi_p(s) = (1 - f(p) p^{-s} + p^{-2s})^{-1}$$

and so, ignoring issues of convergence, we have

$$L(s, f) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \text{ prime}} (1 - f(p) p^{-s} + p^{-2s})^{-1}.$$

3. Recall the derivative $\frac{d}{dx} \log(f(x)) = \frac{f'(x)}{f(x)}$ (remember in Number Theory all logarithms are base $e$) as well as the Taylor Series expansion

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n} \text{ when } |x| < 1.$$

Using these facts together with the Euler Product of $\zeta(\sigma)$ give a formula for $c : \mathbb{N} \to \mathbb{R}$ where $c(n)$ is such that

$$\frac{-\zeta'(\sigma)}{\zeta(\sigma)} = \sum_{n=1}^{\infty} \frac{c(n)}{n^\sigma} \text{ when } \sigma > 1.$$

Don’t worry about issues of convergence or differentiability, it all checks out. [Hint: You’ve seen $c(n)$ before.]
**Solution:** We see that
\[
\log(\zeta(\sigma)) = \log \left( \prod_p \left( 1 - \frac{1}{p^\sigma} \right)^{-1} \right) = \sum_p - \log(1 - \frac{1}{p^\sigma}) = \sum_p \sum_{n=1}^{\infty} \frac{1}{n p^{n \sigma}}
\]
so taking the derivative of the left and right-hand sides we get
\[
\frac{\zeta'(\sigma)}{\zeta(\sigma)} = - \sum_p \sum_{n=1}^{\infty} \frac{n \log(p)}{np^{n \sigma}}
\]
so
\[
-\frac{\zeta'(\sigma)}{\zeta(\sigma)} = \sum_p \sum_{n=1}^{\infty} \frac{\log(p)}{(p^n)^\sigma} = \sum_{m=1}^{\infty} \frac{c(m)}{m^\sigma}
\]
\[
= \left( \frac{\log(2)}{2^\sigma} + \frac{\log(2)}{4^\sigma} + \cdots \right) + \left( \frac{\log(3)}{3^\sigma} + \frac{\log(3)}{9^\sigma} + \cdots \right) + \left( \frac{\log(5)}{5^\sigma} + \frac{\log(5)}{25^\sigma} + \cdots \right) + \cdots
\]
and so we see \(c(m) \neq 0\) only when \(m = p^n\) for some prime \(p\), in which case \(c(m) = \Lambda(m)\).

4. Show that for the polynomial \(f(x) = x^5 + 115x^3 + 124x\), \(f(n)\) is divisible by 120 for all \(n \in \mathbb{Z}\). [Hint: Reduce and factor.]

**Solution:** If we reduce the polynomial modulo 120 we see \(f(x) \equiv x^5 - 5x^3 + 4x \pmod{120}\) which factors:
\[
x^5 - 5x^3 + 4x = x(x^4 - 5x^2 + 4) = x(x^2 - 1)(x^2 - 4) = (x - 2)(x - 1)x(x + 1)(x + 2)
\]
So \(\forall n \in \mathbb{Z}, f(n) \equiv (n - 2)(n - 1)n(n + 1)(n + 2) \pmod{120}\), and we see that \((n - 2), (n - 1), n, (n + 1), \) and \((n + 2)\) will run through at least one representative of every equivalence class \(\pmod{2}, \pmod{3}, \pmod{4}\) and \(\pmod{5}\). In the case of \(\pmod{2}\) we see every equivalence class is hit at least twice. So this means that \(f(n) \equiv 0 \pmod{3}, \pmod{5}\), and even \(\pmod{8}\) since though maybe only one of the five factors divisible by 4 there is another factor divisible by 2. So \(\forall n \in \mathbb{Z}, f(n) \equiv 0 \pmod{3 \cdot 5 \cdot 8}\) and \(3 \cdot 5 \cdot 8 = 120\).

An alternative method would be to reduce \(f(x) \pmod{3}, \pmod{5}\) and \(\pmod{8}\) and check all 16 cases that \(f(n) \equiv 0\).

5. For any \(n\) with decimal notation (base 10) of the form \(n = a_m \cdots a_5 a_4 a_3 a_2 a_1 a_0\) with \(a_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}\) and \(a_m \neq 0\), let
\[
s_n = a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5 + \cdots + (-1)^m c_m a_m = \sum_{k=0}^{m} (-1)^k c_k a_k
\]
where \( c_k = 1, 3, \) or \(-4\) if \( k \equiv 0, 1 \) or \(2 \pmod{3}\) respectively. Show that \(13|n\) iff \(13|s_n\).

**Solution:** Taking \( n = a_0 + a_1(10) + a_2(10^2) + a_3(10^3) + \cdots + a_m(10^m)\) and noting that \(10 \equiv -3 \pmod{13}\) we have that \( n \equiv a_0 + a_1(-3) + a_2(-3)^2 + a_3(-3)^3 + \cdots + a_m(-3)^m \pmod{13}\). Now \( 3^3 \equiv 1 \pmod{13} \) so

\[
\begin{align*}
    n &\equiv a_0 + (-1)(3)a_1 + 9a_2 + (-1)a_3 + \cdots + (-1)^m(3^m)a_m \\
    &\equiv \sum_{k=0}^{m} (-1)^m 3^r a_k \pmod{13}
\end{align*}
\]

where \( k \equiv r_k \pmod{3} \). Since \( 3^2 = 9 \equiv -4 \pmod{13} \) we get that

\[
    n \equiv \sum_{k=0}^{m} (-1)^m c_k a_k \pmod{13}
\]

where \( c_k \) is as in the problem, giving \( n \equiv s_n \pmod{13} \) so \(13|n\) iff \(13|s_n\).

6. Find all \( x \in \mathbb{Z} \) such that \(8x \equiv 2 \pmod{14}, 21x \equiv 6 \pmod{51}\) and \(6x \equiv 8 \pmod{22}\), simultaneously.

**Solution:** Each of these equalities reduces:

\[
\begin{align*}
    8x &\equiv 2 \pmod{14} \iff 4x \equiv 1 \pmod{7} \\
    21x &\equiv 6 \pmod{51} \iff 7x \equiv 2 \pmod{17} \\
    6x &\equiv 8 \pmod{22} \iff 3x \equiv 4 \pmod{11}
\end{align*}
\]

and each has a unique solution per their modulus:

\[
\begin{align*}
    4x &\equiv 1 \pmod{7} \iff x \equiv 2 \pmod{7} \\
    7x &\equiv 2 \pmod{17} \iff x \equiv 10 \pmod{17} \\
    3x &\equiv 4 \pmod{11} \iff x \equiv 5 \pmod{11}
\end{align*}
\]

and then we can solve these family of equalities via the Chinese Remainder Theorem. We just have to find \( x_j \) such that

\[
\begin{align*}
    (17)(11)x_1 &\equiv 2 \pmod{7} \iff 5x_1 \equiv 2 \pmod{7} \iff x_1 \equiv 6 \pmod{7} \\
    (7)(11)x_2 &\equiv 10 \pmod{17} \iff 9x_2 \equiv 10 \pmod{17} \iff x_2 \equiv 3 \pmod{17} \\
    (7)(17)x_3 &\equiv 5 \pmod{11} \iff 9x_3 \equiv 5 \pmod{11} \iff x_3 \equiv 3 \pmod{11}
\end{align*}
\]

and so one solution is

\[
\]

and this solution is unique \( \pmod{7 \cdot 11 \cdot 17} \) so all integer solutions are of the form \( 1710 + 1309n \) for \( n \in \mathbb{Z} \). If you prefer to have the solution be less than the modulus we can also take the form \( 401 + 1309n \) for \( n \in \mathbb{Z} \).
7. Show that if \( n > 4 \) is composite then \((n - 2)! \equiv 0 \pmod{n}\).

**Solution:** If \( n > 4 \) is composite then either \( n = ab \) with \( n > a > b > 1 \) of \( n = a^2 \) for \( a > 2 \). In the prior case, both \( a \) and \( b \) appear in \((n - 1)! = 1 \cdot 2 \cdot 3 \cdots (n - 1)\) and so \( n \mid (n - 1)! \) and so \((n - 1)! \equiv 0 \pmod{n}\). In the latter case \( n > 2a > a > 1 \) and so \( a^2 = n \mid (n - 1)! \) as well. So for all composite \( n > 4 \) we have \((n - 1)! \equiv 0 \pmod{n}\). But \((n, n - 1) = 1\) so \((n - 1)\) is invertible \(\pmod{n}\) and so we can say

\[
(n - 1)^{-1}(n - 1)! \equiv (n - 1)^{-1}0 \pmod{n} \iff (n - 2)! \equiv 0 \pmod{n}.
\]

and we’re done.

8. Let \( a \in \mathbb{Z} \) with \((a, 9139) = 1\), show that \( a^{1332} \equiv 1 \pmod{9139} \). [Hint: Factor 9139.]

**Solution:** We see that 9139 = 13 \cdot 19 \cdot 37. So by Fermat’s Little Theorem, for any \( a \in \mathbb{Z} \),

\[
a^{12} \equiv 1 \pmod{13}, \quad a^{18} \equiv 1 \pmod{19}, \quad \text{and} \quad a^{36} \equiv 1 \pmod{37}
\]

since 12|36 and 18|36, this means \( a^{36} \equiv 1 \pmod{13} \), \( \pmod{19} \) and \( \pmod{37} \). Thus 13, 19 and 37 all divide \( a^{36} - 1 \) and so \( a^{36} \equiv 1 \pmod{9139} \). Since 36|1332, we have \( a^{1332} \equiv 1 \pmod{9139} \).

9. Find all \( x \in \mathbb{Z} \) such that the set \( \{\frac{n^5}{5} + \frac{n^{13}}{13} + \frac{x n}{65} \mid n \in \mathbb{Z}\} \) is a set of integers.

**Solution:** Taking a common denominator and factoring we see that

\[
\frac{n^5}{5} + \frac{n^{13}}{13} + \frac{x n}{65} = \frac{n(13n^4 + 5n^{12} + x)}{65}
\]

which is an integer iff \( n(13n^4 + 5n^{12} + x) \equiv 0 \pmod{65} \) which holds iff \( n(13n^4 + 5n^{12} + x) \equiv 0 \pmod{5} \) and \( \pmod{13} \). Since \( n^4 \equiv 1 \pmod{5} \) when \((n, 5) = 1\) and \( n^{12} \equiv 1 \pmod{13} \) when \((n, 13) = 1\) we have

\[
n(13n^4 + 5n^{12} + x) \equiv n(13 + x) \pmod{5}
\]

and

\[
n(13n^4 + 5n^{12} + x) \equiv n(5 + x) \pmod{13}.
\]

in either respective case. In fact these are still true if \((n, 5) \neq 1 \) or \((n, 13) \neq 1 \) respectively for then both sides are equivalent to zero in either case. Since we require \( n(13 + x) \equiv 0 \pmod{5} \) and \( n(5 + x) \equiv 0 \pmod{13} \) for all \( n \in \mathbb{Z} \), and these equivalences must hold when \((n, 65) = 1\), this means that we have the desired condition exactly when \( x \equiv -13 \equiv 2 \pmod{5} \) and \( x \equiv -5 \equiv 8 \pmod{13} \). We use the Chinese Remainder Theorem to find the unique solution \( \pmod{65} \):

\[
13x_1 \equiv 2 \pmod{5} \quad \text{and} \quad 5x_2 \equiv 8 \pmod{13}.
\]
So $x_1 \equiv 4 \pmod{5}$ and $x_2 \equiv 12 \pmod{13}$. So $x = 13(4) + 12(5) = 112$ is a solution and is unique (mod 65). So all solutions $x \in \mathbb{Z}$ are of the form $x = 47 + 65m$ for $m \in \mathbb{Z}$.

10. Let $p$ be a prime greater than 3, show that the numerator of

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1},$$

when written in lowest terms, is divisible by $p^2$.

[Hint: Use that $\frac{1}{j} + \frac{1}{p-j} = \frac{p}{j(p-j)}$, and also Wilson’s Theorem. It may also be helpful to recall Problem 6 in Assignment 1, or the Proof of Euler’s Theorem.]

Solution: As per the hint we have that

$$2 \left( 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \right) = \left( \frac{1}{1} + \frac{1}{p-1} \right) + \left( \frac{1}{2} + \frac{1}{p-2} \right) + \cdots + \left( \frac{1}{p-1} + \frac{1}{1} \right)$$

$$= \frac{p}{1 \cdot (p-1)} + \frac{p}{2 \cdot (p-2)} + \cdots + \frac{p}{(p-2) \cdot 2} + \frac{p}{(p-1) \cdot 1} = p \sum_{j=1}^{p-1} \frac{1}{j(p-j)}$$

and we see that we can take $(p-1)!$ as a common denominator since every denominator divides it (we never have $p-j = j$ because $p$ is odd). So we get

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{p \sum_{j=1}^{p-1} \frac{(p-1)!}{j(p-j)}}{2(p-1)!}$$

By Wilson’s Theorem, $(p-1)! \equiv -1 \pmod{p}$ so $(p, (p-1)!) = 1$. Also $(p, 2) = 1$. Thus if we reduce this fraction to lowest terms, any prime powers of $p$ in the numerator will remain. Thus if $p$ divides the sum in the numerator, which is a sum of integers, then we are done. But

$$\frac{(p-1)!}{j(p-j)} \equiv j^{-1}(p-j)^{-1}(p-1)! \equiv j^{-2} \equiv (j^{-1})^2 \pmod{p}$$

so

$$\sum_{j=1}^{p-1} \frac{(p-1)!}{j(p-j)} \equiv \sum_{j=1}^{p-1} (j^{-1})^2 \pmod{p}$$

but summing over inverse residues is the same as just summing over residues since every nonzero residue is a unique inverse (mod $p$), so

$$\sum_{j=1}^{p-1} \frac{(p-1)!}{j(p-j)} \equiv \sum_{j=1}^{p-1} j^2 \pmod{p}$$
but by Problem 6 of Assignment 1 we have that

$$\sum_{j=1}^{p-1} j^2 = \frac{(p-1)p(2p-1)}{6} \equiv 0 \pmod{p}$$

since $2, 3 \nmid p$. So $p$ divides the sum and we’re done. Alternately, we can use that for $p > 2$ we have that $2 \cdot 1, 2 \cdot 2, 2 \cdot 3, \ldots, 2(p-1)$ are another complete set of invertible residues and so

$$\sum_{j=1}^{p-1} j^2 \equiv \sum_{j=1}^{p-1} (2j)^2 \equiv 4 \sum_{j=1}^{p-1} j^2 \pmod{p},$$

But $4 \not\equiv 1 \pmod{p}$ when $p > 3$ so $\sum_{j=1}^{p-1} j^2 \equiv 0 \pmod{p}$. This method is very similar to the proof of Euler’s Theorem.