MATH 571 ANALYTIC NUMBER THEORY, SPRING 2025, SOLUTIONS 1

1. (i) Prove that $\frac{1}{q}\sum_{a=1}^{q} e(an/q) = \begin{cases} 1 & \text{when } q|n, \\ 0 & \text{when } q \nmid n. \end{cases}$

If $q|n$, then every term in the sum is 1. If $q \nmid n$, then the sum is the sum of the terms of an geometric progression with common ration $e(a/q) \neq 1$. Thus the sum is $\dfrac{e\big((q+1)a/q\big) - e(a/q)}{e(a/q)-1} = 0$.

(ii) Let $\sigma(n) = \sum_{m|n} m$ denote the sum of the divisors of n. Prove that $\sigma(n)$ is a multiplicative function.

$\sigma = 1 * N$ and both 1 and $N \in \mathcal{M}$.

(iii) Prove that $\sigma(n) = n\sum_{m|n}\frac{1}{m}$.

Note the bijection $m \leftrightarrow n/m$ as $m|n$.

(iv) (Ramanujan) Prove that $\sigma(n) = \dfrac{\pi^2 n}{6}\sum_{q=1}^{\infty} q^{-2}c_q(n)$ where $c_q(n)$ denotes Ramanujan's sum $\sum_{\substack{a=1\\(a,q)=1}}^{q} e(an/q)$.

By (iii) and (i) $\sigma(n) = n\sum_{\substack{q=1\\q|n}}^{\infty} q^{-1} = \sum_{q=1}^{\infty} q^{-2}\sum_{a=1}^{q} e(an/q)$. We sort the inner sum according to the $\mathrm{GCD}(q,a) = q/r$ where $r|q$. Thus $\sigma(n) = \sum_{q=1}^{\infty} q^{-2}\sum_{r|q}\sum_{\substack{a=1\\(q,a)=q/r}}^{q} e(an/q) = \sum_{q=1}^{\infty} q^{-2}\sum_{r|q}\sum_{\substack{b=1\\(r,b)=1}}^{r} e(an/q)$. It can be shown that $|c_r(n)| \le \sigma(n)$, so we have absolute convergence. Then interchanging the order and writing $q = mr$ gives

$$\sigma(n) = \sum_{r=1}^{\infty} r^{-2}\sum_{m=1}^{\infty} m^{-2}\sum_{\substack{b=1\\(m,b)=1}}^{r} e(bn/m).$$

To establish the bound for $c_r(n)$, fix n and write $f(q) = \sum_{a=1}^{q} e(an/q)$ and $g(q) = c_q(n)$. Then $f = g*\mathbf{1}$, so $g = f*\mu$, and $|c_q(n)| \le \sum_{r|(q,n)} r \le \sigma(n)$.

2. Let $n \in \mathbb{Z}$ and $m \in \mathbb{Z}$ with $n \ge 0$, $m \ge 0$. The binomial coefficient $\binom{n}{m}$ is defined inductively by $\binom{0}{0} = 1$, $\binom{n}{-1} = \binom{0}{m} = 0\,(m > 0)$, $\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$.

(i) Prove that $\binom{n}{m} \in \mathbb{N}$.

We have $\binom{1}{m} = \binom{0}{m-1} + \binom{0}{m} = 1$ when $m = 0$ or 1 and is 0 otherwise. Then the general result follows immediately by induction on n.

(ii) Prove that if p is a prime and $1 \le m \le p-1$, then $p|\binom{p}{m}$.

Clearly the binomial coefficients are uniquely determined. But $\binom{n}{m} = \frac{n!}{(n-m)!m!}$ also satisfies the defining relationship. Then $\binom{p}{m}(p-m)!m! = p!$. This is divisible by p, but $(p-m)!m!$ is not.

3. Prove that the number $\rho(n)$ of solutions of the equation $x_1 + \ldots + x_k = n$ in non-negative integers $x_1, \ldots, x_k$ is $(-1)^n\binom{-k}{n} = \binom{k+n-1}{n}$.

When $|z| < 1$, $\rho(n)$ is the coefficient of z^n in $(1 + z + z^2 + \cdots)^k = (1-z)^{-k}$. This gives the first formula. By the residue theorem this is also

$$\frac{1}{2\pi i}\int_{\mathcal{C}} (-1)^k (z-1)^{-k} z^{-n-1} dz$$

where $\mathcal{C}$ is the circle centred at 0, of radius $\frac{1}{2}$ and traversed in the positive sense. Expanding the radius of the circle to infinity we see that this is also $-R$ where R is the residue of the integrand at 1, and this is $\frac{(-1)^{k-1}}{(k-1)!}\left(\frac{d}{dz}\right)^{k-1} z^{-n-1}\Big|_{z=1} = \frac{(-1)^{k-1}}{(k-1)!}(-n-1)\ldots(-n-k+1) = \frac{(n+k-1)!}{n!(k-1)!}$

4. Prove that no polynomial $f(x)$ of degree at least 1 with integral coefficients can be prime for every positive integer x.

Suppose that $f(a) = p$. Let $x = a + mp$ where m is arbitrarily large. Then $f(x)$ is arbitrarily large and $f(x) \equiv f(a) \equiv 0 \pmod{p}$.