Fourier Analysis Stein: Chapter 8. Problems.

Kelvin Hong
kh.boon2@gmail.com

Xiamen University Malaysia, Asia Pacific University Malaysia — August 11, 2024

1 Problems

1. Prove that there are infinitely many primes by observing that if there were only finitely many, $p_1, \ldots, p_N$, then

$$\prod_{j=1}^{N} \frac{1}{1-1/p_j} \geq \sum_{n=1}^{\infty} \frac{1}{n}.$$

Solution: Assumes there are only finitely many primes $p_1, \ldots, p_N$. Given a positive integer M, each positive integer $n \leq M$ can be expressed as a product of primes $p_1^{k_1} \cdots p_N^{k_N}$ for some integers $k_1, \ldots, k_N$. We let $K_1, \ldots, K_N$ be the maximum values of $k_1, \ldots, k_N$ across all $n \leq M$. Thus, we have

$$\prod_{j=1}^{N} \frac{1}{1-1/p_j} \geq \prod_{j=1}^{N} \left(\sum_{k=0}^{K_j} \frac{1}{p_j^k} \right) \geq \sum_{n=1}^{M} \frac{1}{n}.$$

Taking the limit as $M \to \infty$, we see that the RHS diverges, which is a contradiction to our assumption. $\square$

2. In the text we showed that there are infinitely many primes of the form $4k+3$ by a modification of Euclid's original argument. Adapt this technique to prove the similar result for primes of the form $3k+2$, and for those of the form $6k+5$.

Solution: Assume there are only finitely many primes of the form $3k+2$, and let $p_1, \ldots, p_N$ be all of them in increasing order and $p_1 = 5$. Consider the number $n = 3p_1 \cdots p_N + 2$. This is a number of the form $3k+2$ and $n > p_N$, so it must be composite by our assumption. Since it is not divisible by 3, it must have prime factors of the form $3k+1$ and $3k+2$. If it only has prime factors of the form $3k+1$, the product of these primes would be still of the form $3k+1$, so it will at least has a prime factor of the form $3k+2$. But this is a contradiction since n is not divisible by any of the primes $p_1, \ldots, p_N$.

For another solution, we assume there are only finitely many primes of the form $6k+5$, $q_1, \ldots, q_M$, in increasing order, where $q_1 = 11$. We can let $m = 6q_1 \cdots q_M + 5$, we can argue similarly by noting that if m is composite, it must have prime factors of the form $6k+1$ and $6k+5$, and also it must have at least one prime factor of the form $6k+5$, which create a contradiction. $\square$

3. Prove that if p and q are relatively prime, then $\mathbb{Z}^*(p) \times \mathbb{Z}^*(q)$ is isomorphic to $\mathbb{Z}^*(pq)$.

Solution: Let $\phi : \mathbb{Z}^*(p) \times \mathbb{Z}^*(q) \to \mathbb{Z}^*(pq)$ be defined by $\phi(a,b) = aq + bp \mod pq$. Obviously both sets are groups, so we only need to show the mapping is one-to-one and surjective.

To show ϕ is one-to-one, suppose $\phi(a,b) = \phi(c,d)$, then $aq + bp \equiv cq + dp \mod pq$. There is an integer k such that $(a-c)q + (b-d)p = kpq$. Rearrange to get $(a-c)q = p(kq - b + d)$. Since p and q are relatively prime, p divides $a - c$, hence $a \equiv c \pmod{p}$. Similarly $b \equiv d \pmod{q}$.

To show ϕ is surjective, we first let x, y be integers such that $py + qx \equiv 1 \pmod{p}q$ with $x \in \mathbb{Z}^*(p)$ and $y \in \mathbb{Z}^*(q)$. For any $z \in \mathbb{Z}^*(pq)$, we can write $z = z \cdot 1 = z(py + qx) = zpy + zqx$. We find that $\phi(zx, zy) = z$ just because z is both relatively prime to p and q. $\square$