Melbourne High School
Maths Extension Group 2023
Term 2 Week 5 Handout Solutions

The Fundamental Theorem of Arithmetic

1. (a) If the divisors of m are

$$a_1, a_2, \dots, a_r$$

and the divisors of n are

$$b_1, b_2, \dots, b_s$$

the divisors of mn are exactly all the products of all pairs of a's and b's. Therefore

$$\begin{aligned}\sigma(mn) &= a_1 \sum_{k=1}^{s} b_k + a_2 \sum_{k=1}^{s} b_k + \cdots + a_r \sum_{k=1}^{s} b_k \\ &= \sum_{k=1}^{r} a_k \cdot \sum_{k=1}^{s} b_k \\ &= \sigma(m)\sigma(n).\end{aligned}$$

(b) Since

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$$

the formula for $\sigma(n)$ is just the product of these terms for all powers of primes that divide n. Therefore if

$$n = \prod_{k=1}^{r} p_k^{a_k}$$

then

$$\sigma(n) = \prod_{k=1}^{r} \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

2. (a) Let p be a prime and a be a number less than p. Suppose that the proposition is false and that there exist numbers $x \equiv b, b', b'', \ldots$ all less than p such that

$$ax \equiv 0 \pmod{p}.$$

Let b be the smallest of these.

Since $b < p$, it must be that p lies between two successive multiples of b; that is, there exists some m such that

$$bm < p < b(m+1).$$

From $bm < p$ it follows that $p - bm > 0$, and from $p < bm + b$ it follows that $p - bm < b$. Put $c = p - bm$. Then we have $0 < c < b$. But

$$ac \equiv a(p - bm) \equiv ap - abm \equiv 0 \pmod{p}$$

because clearly $ap \equiv 0$, and by hypothesis $ab \equiv 0$ too. Therefore $ac \equiv 0$, which contradicts the minimality of b because $c < b$. This contradiction completes the proof.

(b) If $a \not\equiv 0$ and $b \not\equiv 0$, their least positive residues, say α and β, are also not congruent to 0. If

$$ab \equiv 0 \pmod{p}$$

then

$$\alpha\beta \equiv 0 \pmod{p},$$

but this contradicts the previous result as $0 < \alpha, \beta < p$.

3. (a) Let the two sets of prime factors be arranged in ascending order, so that

$$p_1 < p_2 < \cdots < p_r$$

and

$$q_1 < q_2 < \cdots < q_s.$$

None of the p's can be a q because otherwise it could be cancelled out, and we know the resulting number cannot have two different factorisations because it is smaller than n. Therefore either $p_1 < q_1$ or $q_1 < p_1$. Since $p_1^2 \leq n$ and $q_1^2 \leq n$, we have $p_1 q_1 < n$, which implies $n - p_1 q_1 > 0$.

(b) Since both p_1 and q_1 divide n, they also divide $N = n - p_1 q_1$. Rearranging for n, we get $n = N + p_1 q_1$, and so $p_1 q_1$ divides n.

(c) If $p_1 q_1$ divides n, then q_1 divides $p_2 \ldots p_r$. This is impossible because n/p_1, being less than n, has a unique factorisation consisting of exactly those primes p_2 up to p_r, and since no q is a p, it cannot be that q_1 occurs in the factorisation. This contradiction completes the proof.