Melbourne High School
Maths Extension Group 2023
Term 2 Week 6 Handout Solutions

Fermat's Little Theorem

1. We aim to show that the congruence

$$a^p \equiv a \pmod{p}$$

holds for all a. Clearly $0^p \equiv 0$ and $1^p \equiv 1$. Assume that the congruence holds for $a = k$.

We need to know how to expand $(k+1)^p$ for the inductive step. By the Binomial Theorem

$$(k+1)^p = \sum_{i=0}^{p} \binom{p}{i} k^i.$$

The Binomial coefficient

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}$$

is divisible by p for $0 < n < p$, because $n!$ and $(p-n)!$ are both coprime with p, and so after simplifying the fraction, a factor of p in the $p!$ term remains. Consequently, when considering the expression $(k+1)^p$ modulo p, all the middle terms of the expansion vanish, leaving us with

$$(k+1)^p \equiv k^p + 1^p \pmod{p}.$$

Applying the induction hypothesis, which is that $k^p \equiv k$, we get

$$(k+1)^p \equiv k + 1 \pmod{p}$$

which completes the induction.

2. Since a and m are coprime, the numbers

$$ak_1, ak_2, \ldots, ak_{\phi(m)}$$

reduced modulo m are the numbers

$$k_1, k_2, \ldots, k_{\phi(m)}$$

in some order. The argument is the same as that of Ivory's proof of Fermat's Little Theorem. All the numbers in the first set are clearly coprime with m, and no two are congruent, for if $ak_i \equiv ak_j$ then $k_i \equiv k_j$. Therefore both sets are $\phi(m)$ numbers that are coprime with m, meaning that when both are reduced modulo m, they must be the same sets.

From this we conclude that

$$ak_1 \cdot ak_2 \cdots ak_{\phi(m)} \equiv k_1 \cdot k_2 \cdots k_{\phi(m)} \pmod{m}.$$

On the LHS we have $\phi(m)$ copies of a; hence

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} k_i \equiv \prod_{i=1}^{\phi(m)} k_i \pmod{p}.$$

The product of the k's may be cancelled from both sides as it is clearly coprime with m, and therefore

$$a^{\phi(m)} \equiv 1 \pmod{p}.$$