Melbourne High School
Maths Extension Group 2023
Term 3 Week 5 Handout Solutions

Euler's Criterion

1. We observe that
$$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$$
since $p - a \equiv -a \pmod{p}$. If $p \equiv 1 \pmod 4$ then $(-1|p) = 1$, and so
$$\left(\frac{p-a}{p}\right) = \left(\frac{a}{p}\right).$$
If $p \equiv 3 \pmod 4$ then $(-1|p) = -1$, and so
$$\left(\frac{p-a}{p}\right) = -\left(\frac{a}{p}\right).$$
This completes the proof.

2. Let $P = (p-1)/2$ and α be the index of a for some primitive root of p that we shall call g. From Fermat's Little Theorem we know that either
$$a^P \equiv 1 \pmod{p}$$
or
$$a^P \equiv -1 \pmod{p};$$
the goal here is to prove that the distinction between the two cases is exactly the distinction between $(a|p) = 1$ and $(a|p) = -1$.

   First consider the case where $(a|p) = 1$. Then $a^P \equiv g^{\alpha P} \pmod{p}$. Since $(a|p) = 1$, it follows that α is even and therefore that αP is a multiple of $p-1$. We know that g raised to any multiple of $p-1$ is unity, so
$$a^P \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$
If $(a|p) = -1$, then α is odd, and so αP cannot be a multiple of $p-1$. Since g is a primitive root, the only powers of g that are congruent to unity are the multiples of $p-1$, and so $g^{\alpha P} \not\equiv 1$; hence
$$a^P \equiv g^{\alpha P} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$
This completes the proof of Euler's Criterion.

3. Since $p = 4k+1$, we have $p-1 = 4k$. By Wilson's Theorem
$$(p-1)! \equiv (4k)! \equiv -1 \pmod{p}.$$
Notice that $4k \equiv -1$, $4k-1 \equiv -2$, $4k-2 \equiv -3$, and so on, all the way down to $2k+1 \equiv -2k$, so we actually have
$$1 \times (-1) \times 2 \times (-2) \times \cdots \times 2k \times (-2k) \equiv -1 \pmod{p}$$
which becomes
$$(2k)!^2 \equiv -1 \pmod{p}.$$
The solution to the congruence is therefore $x \equiv \pm(2k)! \pmod{p}$.