# Contents

# 1 Theorem 1.19

$$(-1)^{2k} = ((-1)^2)^k = 1^k = 1$$

$(2k)!$ has $2k$ terms, and can therefore be also written as

$$(2k)! = (-1)(-2)\cdots(-2k+1)(-2k)$$

Now finally note that $-a \equiv p - a \mod p$, and the expression becomes $(p-1)! \mod p$.

## 1.1 Wilson's Theorem

Wilson's theorem in short:

$\mathbb{Z}_p$ is a field so all $x \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ is a unit $\implies \bar{2} \cdot \overline{p-2} = \bar{1}$

$$\begin{aligned}(p-1)! &\equiv (p-1)(p-2)! \mod p \\ &\equiv -1 \cdot 1 \mod p\end{aligned}$$

See also Pinter, 23G.

# 2 Lemma 1.28

The only units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.