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.

1.2 Factorization of the Norm

$$N : \mathbb{Z}[i] \to \mathbb{Z}$$

Since we have integer factorization in $\mathbb{Z}$, then we have $N(\alpha) \in \{1, p, p^2\}$.

$N(\alpha)$	$N(\beta)$	$\alpha = a + ib$	$\beta = c + id$	$\alpha\beta$
1	p^2	1	p	p
1	p^2	-1	$-p$	p
1	p^2	i	$-ip$	p
1	p^2	$-i$	ip	p
p^2	1	p	1	p
p^2	1	$-p$	-1	p
p^2	1	$-ip$	i	p
p^2	1	ip	$-i$	p

We are writing p in an equivalent way using units with the norm function.

We proved in the previous paragraph that p is *not* prime. Since these factorizations above are just equivalent ways of representing p, that only leaves $N(\alpha) = N(\beta) = p$.

2 Lemma 1.20

We are doing the equivalent of `round(a/b)`. The closest point in 2d will have distance less than $\frac{1}{\sqrt{2}}$.

$N(x) = |x|^2$ are the same thing, except left is "norm" function and right is the "distance" function.

3 Lemma 1.25

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

$\alpha \mid (1+i)^2 \implies a = 1+i$ or $\alpha = (1+i)^2 \implies (1+i) \mid \alpha$.

$\alpha \mid y+i$ and $\alpha \mid y-i \implies \alpha \mid (y+i)(y-i) = x^3$ but $(1+i) \mid \alpha \implies (1+i) \mid x^3$ and $(1+i)$ is prime in $\mathbb{Z}[i]$ so $(1+i) \mid x$.

4 Selected Hints to Exercises

4.1 Ex 1.1

$N \equiv a \mod m$ where a is prime, means also $p \mid N \implies (p \mod m) \mid a$.

4.2 Ex 1.2

Remember that $\phi(p) = p - 1$.