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 $x \in \mathbb{Z}_p^* = \mathbb{Z}_p \quad \{0\}$ 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 $\phi(p) = p - 1$.

4.3 Ex 1.4

$$q \geq 1 \implies r_1 = qr_2 + r_3 > r_2 + r_3$$
$$r_2 > r_3 \implies r_1 > r_3 + r_3$$

4.4 Ex 1.9

This question has a notation error. Let $s \equiv -2 \mod p$.

```
sage: x, y, p, s, q
(910833, 840626, 2242920897641, 141238812168, 8893939186)
sage: s^2 + 2 == p*q
True
sage: N = lambda a, b: a^2 + 2*b^2
sage: N(s, 1)*N(s, 1) == N(p, 0)*N(q, 0)
True
sage: N(x, y)
2242920897641
sage: N(x, -y)
2242920897641
sage: p
2242920897641
sage: N(x, y) == N(x, -y), N(x, y) == p
(True, True)
```

The rest follows from the previous page. In short because $(s \pm \sqrt{-2})/p \notin \mathbb{Z}[\sqrt{-2}]$, we conclude that $N(\alpha) = N(\beta) = p$. So therefore p can be factored inside $\mathbb{Z}[\sqrt{-2}]$.

4.5 Ex 1.13

4.5.1 1

Each normal involution has two elements from S whereas the fixed ones $s = f(s)$.

4.5.2 2

First rewrite the relations for each case as:

$$f(x,y,z) = \begin{cases} (x+2z, z, y-x-z) & \text{if } 0 < y-x-z \\ (-(x-2y), y, -(y-x-z)) & \text{if } y-x-z < 0 \text{ and } x-2y < 0 \\ (x-2y, x-y+z, y) & \text{if } 0 < x-2y \end{cases}$$

We can see that when #2 is false, then either #1 or #3 will be true. So each of the cases are exclusive.

By looking at the relations we can also confirm that $f : S \to S$ where $(x,y,z) \in S \subset \mathbb{N}^3$.

By testing each case like below we can see how they map onto each other.

```
sage: z - (x + 2*z) - (y - x - z)
-y
sage: (2*y - x) - 2*y
-x
sage: y - (2*y - x) - (x - y + z)
-z
sage: (x - 2*y) - 2*(x - y + z)
-x - 2*z
sage: (x - y + z) - (x - 2*y) - y
z
```

$1 \longrightarrow 3$

$2 \longrightarrow 2$

$3 \longrightarrow 1$

4.5.3 3

Let $x = 1, y = 1, z = k$, then $p = x^2 + 4yz = 1 + 4k$ as desired.

Then $y - x - z = -k < 0$ and $x - 2y = -1 < 0$ which means condition 2 is correct.

Condition 2 is fixed.

4.5.4 4

Obvious

4.5.5 5

y and z are interchangable by previous answer so $p = x^2 + (2y)^2$ for some y.