Week 5 - Exercise 3. (Midterm - 3rd problem something similar to some part).

About quadratic numbers for the most part.

(1) Write down times tables for $\mathbb{F}_3[x]/(x^2+1)$ and $\mathbb{Z}[i]/(3)$.

$\mathbb{F}_3[x]/(x^2+1)$

$\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$

elements of $\mathbb{F}_3$ are $0, 1, 2$.

$\mathbb{F}_3[x] \leftarrow$ elements look like

$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$

$a_i \in \mathbb{F}_3$ i.e. $a_i = 0, 1, 2$.

e.g. $x^{17}+2x^2+1$ is an element of $\mathbb{F}_3[x]$

$$2x(x^{17}+2x^2+1) = 2x^{18}+x^3+2x$$

$$2x\cdot 2x^2 = (2\cdot 2)(x\cdot x^2) = 1x^3$$

working with coefficients in $\mathbb{F}_3$.

$\mathbb{F}_3[x]/(x^2+1)$ means we identify polynomials that differ by a multiple of x^2+1

e.g. $x^3+\underbrace{2x^2+2}_{2(x^2+1)} \equiv x^3 \mod (x^2+1)$

Recall by long division, any $f(x) \in \mathbb{F}_3[x]$

can be written as $f(x) = q(x)(x^2+1) + r(x)$

where degree of $r(x) < \deg(x^2+1)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad = 2.$

To compute $r(x)$ just do $x^2+1 \overline{\smash{\big)}\, f(x)}$ with quotient $q(x)$

$$f(x) = \underline{q(x)(x^2+1)} + r(x)$$

$$\Rightarrow \quad f(x) \equiv r(x) \mod (x^2+1).$$

Payoff: The elements of $\mathbb{F}_3[x]/x^2+1$ can be represented unique using polynomials of degree <2.

All of the form $ax + b$

with $a, b \in \mathbb{F}_3$.

All of them:

$0x + 0 = 0$

just listed all possibilities for a, b.

$0x + 1 = 1$

$0x + 2 = 2$

$1x + 0 = x$

$1x + 1 = x + 1$

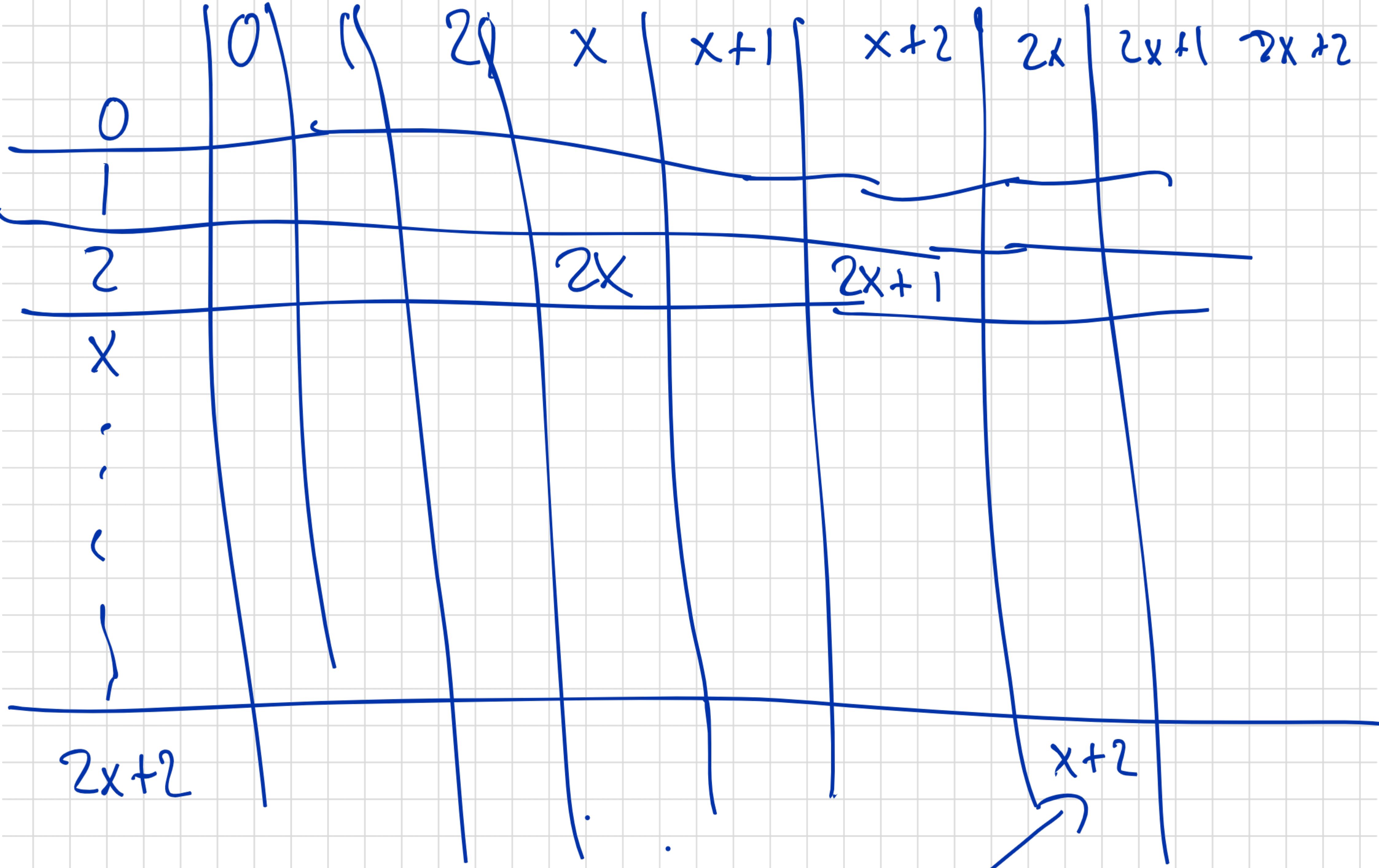
$1x + 2 = x + 2$

$2x + 0 = 2x$

$2x + 1 = 2x + 1$

$2x + 2 = 2x + 2$

Once listed, you can write this table.



$$(2x+2)(2x) = x^2 + x$$

I eyeballed, but can always compute w/ long division.

$$\underline{x^2+x} = \underline{(x^2+1)} + \underline{x+2}$$

$$x^2+x \equiv x+2 \mod x^2+1,$$

what about, e.g. $\mathbb{F}_3[x]/(x^3+x+2.)$

Elements are ax^2+bx+c.

$a, b, c \in \mathbb{F}_3$.

Determining if $f(x) \in \mathbb{K}[x]$ is prime/irreducible.
(Not needed for above - digression)

i.e. when does $f(x)$ have no factors of smaller degree?

1) If $f(x)$ has degree ≤ 3 then it is irreducible/prime $\iff$ it has no roots, i.e. not $a \in \mathbb{K}$ s.t. $f(a)=0$.

Example: $f(x) = x^2 + x + 2$ in $\mathbb{F}_3[x]$.

$f(0) = 2$

$f(1) = 1$

$f(2) = 2+2+2=0$ ← is a root. So this is ~~not~~ prime.

(2) If $f(x)$ has degree n, to check if it's prime, just try dividing by every polynomial of degree $\leq \lfloor \frac{n}{2} \rfloor$.

E.g. if $f(x) = x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.

it's not enough to check if it has no roots.

wouldn't be on the exam.

Back to Week 5 - Exercise 3.

2nd part of part (1) times table.

for $\mathbb{Z}[i]/(3)$

An element of $\mathbb{Z}[i]$ is $a+bi$ where $a, b \in \mathbb{Z}$.

any such can be shifted by a multiple of 3 to get

$a+bi \quad a, b \quad 0, 1, 2.$

(i.e. $a, b \in \mathbb{F}_3$)..

$0+0i = 0$

$0+1i = i$

$0+2i = 2i$

$1+0i = 1$

$1+1i = 1+i$

$1+2i = 1+2i$

$2+0i = 2$

$2+1i = 2+i$

$2+2i = 2+2i$

2). $N(a+b\sqrt{D}) = a^2 - b^2 D$

$= (a+b\sqrt{D})(a-b\sqrt{D})$

This is what shows up when you clear square roots from a denominator.

Check $N(x)N(y) = N(xy)$. ← just expand out both sides.