Ring Learning w/ Errors

Ring $+, -, \times$

Dfn: a ring is a set R
2 operations $+, \cdot,$ s.t.

1) R is an ab gp under $+$
 w/ identity 0.
2) $\cdot$ is comm, id 1
3) $k(x+y) = kx + ky$

ex:

1) $\mathbb{Z}$
2) Fields $(\mathbb{Q})$
3) $\mathbb{Z}/m\mathbb{Z}$
4) $\{f: \mathbb{R} \to \mathbb{R}\}$
 pointwise $+, \cdot$
5) set of polynomials
 w/ $\mathbb{Q}$ coeffs

 $\mathbb{Q}[x]$

 $= \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{Q}\}$

6) $R[x]$ for any ring R

not matrices
ab gp under $+$
but $\cdot$ not comm
"non-commutative ring"

other non-example
$2\mathbb{Z}$ - no 1
this is a Rng (no I)

Fields
$\cup\!\!\!/$
Rings
$\cup\!\!\!/$
ab gp
$\cup\!\!\!/$
gp

ED
PID
UFD

Pring
|
non-com ring

$\mathbb{Z}[x] = \{ a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{Z} \}$

$\mathbb{Z}/m\mathbb{Z}[x] = \{ a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{Z}/m\mathbb{Z} \}$

$\mathbb{Z}/5\mathbb{Z}[x]$

$f(x) = x^2 + 3x + 1 = x^2 - 2x + 6 \pmod 5$

$g(x) = x^3 + 2x^2 + 4$

$f(x) + g(x) = x^3 + 3x^2 + 3x.$

$(f \cdot g)(x) = (x^2 + 3x + 1)(x^3 + 2x^2 + 4)$

$= x^5 + 2x^4 + 4x^2$
$+ 3x^4 + 6x^3 + 12x$
$+ x^3 + 2x^2 + 4$

$= x^5 + 0x^4 + 2x^3 + x^2 + 2x + 4$

$f(1) \cdot g(1) = 5 \cdot 7 = 35$
$\equiv 0 \bmod 5$

$f \cdot g\,(1) = 10 \equiv 0 \bmod 5$

$\mathbb{Z}/5\mathbb{Z}[x]$ has

5 constant polys

5^2 linear polys

5^3 quadratic polys

5^{n+1} degree n polys

∞ total polys

---

how do I cap the degree?

polys of deg ≤ 5

not closed under $\cdot$

$x^4 \cdot x^3 = x^7 \notin$ this set.

Dfn: R a ring
$r_1, \dots, r_n \in R$
the ideal generated by r_i
is $\langle r_1, \dots, r_n \rangle$

$= \{ r_1 s_1 + r_2 s_2 + \dots + r_n s_n \mid s_i \in R \}$.

In particular, if $f \in \mathbb{Z}/m\mathbb{Z}[x]$
$\langle f \rangle = \{ f(x) g(x) \mid g(x) \in \mathbb{Z}/m\mathbb{Z}[x] \}$

1) I is an ab gp
2) closed under mult
in fact, if $g \in \langle f \rangle$
then $gh \in \langle f \rangle$
even if h is not.

3) this is a subring
not a subring.

ex: $2\mathbb{Z} = \langle 2 \rangle$ is an ideal in $\mathbb{Z}$.

If R a ring, I an ideal, and $r, s \in R$,
say $r \equiv s + I$ if $r - s \in I$
write R/I for set of equivalence classes.
This is a ring.

$R = \mathbb{Z}$, $I = \langle m \rangle = m\mathbb{Z}$

$a \equiv b \bmod m$ if $m \mid a - b$
$(a - b \in \langle m \rangle)$

$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\langle m \rangle$

$0, m, 3m, -17m \in I = \langle m \rangle$

Ex: $R = \mathbb{Z}[x]$, $I = \langle m \rangle = mR = m\mathbb{Z}[x]$
$0, m, 34m, mx, 12mx^2 - 3mx + m \in I$
$mx + 1, x + m \notin I$.

$R/I = \mathbb{Z}[x] / m\mathbb{Z}[x] = \mathbb{Z}/m\mathbb{Z}[x]$

$R = \mathbb{Z}/m\mathbb{Z}[x]$

$I = \langle x^n + 1 \rangle \qquad n = 2^k$

(roots of this poly in $\mathbb{C}$ are 2^{k+1}th roots of 1 $e^{2\pi r i / 2^{k+1}}$)

R/I sets $x^n = -1$

$x^{n+1} = x^n \cdot x$

$= (-1)x = -x.$

$x^{n+2} = -x^2$

$\vdots$

$\mathbb{Z}[x]/\langle m, x^n+1 \rangle$

$R/I = \{ a_0 + a_1 x + \cdots + a_n x^{n-1} \mid a_i \in \mathbb{Z}/m\mathbb{Z} \}$

$\# R/I = m^n < \infty$

$k = 2$
$n = 4$

$x^3 \cdot x^3 = x^6 = x^4 \cdot x^2 = -x^2.$

$R = \mathbb{Z}/5\mathbb{Z}[x] / \langle x^4 + 1 \rangle$ $\qquad k=2$, $n=4$ $\qquad \mathbb{Z}[x]/\langle 5, x^4+1 \rangle$

$f(x) = x^2 + 3x + 1$

$g(x) = x^3 + 2x^2 + 4$

$(f+g)(x) = x^3 + 3x^2 + 3x$

$(fg)(x) = x^5 + 2x^3 + x^2 + 2x + 4$

$= -x + 2x^3 + x^2 + 2x + 4$

$= 2x^3 + x^2 + x + 4.$

Ring Learning with Errors

Let $f(x) = x^n + 1$, $n = 2^K$

q large prime, $q \equiv 1 \bmod 2n$

$R_q = \mathbb{Z}/q\mathbb{Z}[x]/\langle f \rangle$

Dfn: for $g(x) \in R$,

write $g(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

$a_i \in \left\{ \frac{-(q-1)}{2}, \dots, -1, 0, 1, \dots, \frac{q-1}{2} \right\}$

as close to 0 as possible

define $\|g\|_\infty = \max\{|a_i|\}$.

ex: $g(x) = 2x^3 + x^2 + x + 4 \in \mathbb{Z}[x]/\langle 5, x^4+1 \rangle$

$= 2x^3 + x^2 + x - 1$

$\|g\|_\infty = 2$

prob dist giving small poly's

choose bound b, choose coeffs at random from $\{0, 1, \dots, b\}$

Ring LWE:

1) Let a_i random known $\in R_q$
2) e_i random unknown small $\in R_q$
3) s unknown small poly $\|s\|_\infty \le b$
4) set $b_i = (a_i s) + e_i$

Q: given (a_i, b_i), what is s?

Thm: This is at least as hard as worst-case approx SV problem, even on a QC.