Galois Fields

Another view on bytes

<Drahflow>
14. Februar 2018

Stratum 0

Fields

Examples

- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$

Axioms

associative in $+$	$a + (b + c) = (a + b) + c$
associative in $\cdot$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
commutative in $+$	$a + b = b + a$
commutative in $\cdot$	$a \cdot b = b \cdot a$
identity of $+$	$a + 0 = a$
identity of $\cdot$	$a \cdot 1 = a$
	$0 \neq 1$
inverses of $+$	$\exists(-a) : a + (-a) = 0$
inverses of $\cdot$	$a \neq 0 \Rightarrow \exists(a^{-1}) : a \cdot (a^{-1}) = 1$
distributivity	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Finite Fields

$\mathbb{Z}_2 = \mathrm{GF}(2)$

- $\{0, 1\}$
- $0 + 0 = 0$
- $0 + 1 = 1$
- $1 + 1 = 0$
- $0 \cdot 0 = 0$
- $0 \cdot 1 = 0$
- $1 \cdot 1 = 1$

Finite Fields

$$\mathbb{Z}_p = \mathsf{GF}(p)$$

- $\{0, 1, \ldots, p - 1\}$
- $a + b = (a +_{\mathbb{R}} b) \operatorname{mod}_{\mathbb{R}} p$
- $a \cdot b = (a \cdot_{\mathbb{R}} b) \operatorname{mod}_{\mathbb{R}} p$

Finite Fields

$\mathbb{Z}_{256}$?

- $16 \cdot 16 = (16 \cdot_{\mathbb{R}} 16) \mathrm{mod}_{\mathbb{R}} 256 = 256 \mathrm{mod}_{\mathbb{R}} 256 = 0$
- but then… $0 = 0 \cdot (16^{-1}) = 16$.

This is broken (because 256 is not prime).

Finite Fields

$GF(p^n)$

- polynomials of degree $< n$ over $\mathrm{GF}(p)$.
- modulo some fixed irreducible polynomial R of degree n over $\mathrm{GF}(p)$
- all finite fields of equal size are isomorphic, R doesn't matter

Finite Fields

Example: $GF(3^2)$

- Choose $R = (x^2 + 1)$
- $(x + 1) + (2x + 0) = ((1 +_{\mathbb{R}} 2)x + (1 +_{\mathbb{R}} 0)) = (0x + 1) = 1$
- $(x + 1) \cdot (x + 1) = (x^2 + 2x + 1) \text{mod} (x^2 + 1) = (2x)$
- $(x + 1) \cdot (2x + 1) = (2x^2 + ((1 +_{\mathbb{R}} 2) \text{mod}_{\mathbb{R}} 3)x + 1) \text{mod} (x^2 + 1) = (2x^2 + 1) \text{mod} (x^2 + 1) = (2x^2 + 1) - (2x^2 + 2) = (-1) \text{mod}_{\mathbb{R}} 3 = 2.$

Byte-Sized Fields

$GF(2^8)$

- It as 256 elements
- We can represent the 7-degree polynomials with a bit field

$$0 = 0$$
$$x^4 + x + 1 = 0x13$$

- $a + b$ is binary-XOR (and $(-a) = a$).
- $a \cdot b$ is ... complicated

Byte-Sized Fields

Multiplication

- $a \cdot b = (a \cdot_{\mathbb{R}} b) \text{mod}_{\mathbb{R}} R$
- Straightforward: Polynomial multiplication + polynomial division
- Finite fields have generators, such that $a \neq 0 \Rightarrow \exists n : a = g^n$.
- $a \cdot b = g^{\log_g a} \cdot g^{\log_g b} = g^{\log_g a + \log_g b}$
- Store g^a and $\log_a$ in lookup tables.
- Multiply becomes: zero-check; lookup; add; modulo (because $g^{256} = g^1$); lookup

Byte-Sized Fields

Example

- AES field, $R = (x^8 + x^4 + x^3 + x + 1)$, suitable $g = 3$
- $\texttt{0x15} + \texttt{0x05} = \texttt{0x10}$
- $\texttt{0x15} \cdot \texttt{0x05} = 3^{141} \cdot 3^2 = 3^{141+2} = 3^{143} = 65 = \texttt{0x41}$

Applications

Our bytes now have interesting arithmetic properties!

Error Correction

- Reed-Solomon Codes, QR-codes
- Checksum via residues after division by polynomials over $GF(2^8)$.

Cryptography

- AES mix-columns step is matrix multiplication with scalars in $GF(2^8)$.

Bonus: Both use different R for the construction, thus separate log-tables.

Questions?

<Drahflow>
<drahflow@gmx.de>

Stratum 0 e. V. Braunschweig
`https://stratum0.org/`

Stratum 0