Finite fields

field a set of elements with $+, -, \cdot, \div$
according to the usual rules

EG not a field: $\mathbb{Z}$ (integers), polynomials

fields: $\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), $\mathbb{C}$ (complex numbers), rational functions (= quotients of polynomials) — all infinite

EG residues mod 21 not a field
cannot divide by 3, 6, 7, 9, ...

residues mod p are a field — $GF(p)$ Galois field
all nonzero residues are invertible mod p

$GF(p^n)$ "the" field with p^n elements
Up to isomorphism (i.e. relabeling), these are the only finite fields.

how to construct:
- fix polynomial $m(x)$ of degree n which is irreducible mod p
- elements of $GF(p^n)$ are polynomials
  - modulo $m(x)$, and
  - modulo p

EG AES based on $GF(2^8)$
- $m(x) = x^8 + x^4 + x^3 + x + 1$
- each element of $GF(2^8)$ is a polynomial

$$a_7 x^7 + a_6 x^6 + \dots + a_1 x + a_0 \xrightarrow[\text{1 byte}]{\text{8 bits}} a_7 a_6 \dots a_1 a_0$$

$$x^6 + x^2 + 1 \qquad 01000101$$