T-79.5501
Cryptology

Notes from Lecture 3:

- Euler Φ-function
- Finite fields
- Structure of finite fields
- Galois Fields

Euler Phi-function

See separate text

Vocabulary:

prime: alkuluku

relatively prime, coprime: suhteellinen alkuluku, keskenään jaottomat

multiplicative inverse: käänteisluku

ring: rengas

field: kunta

Finite fields

Let $m \geq 2$ be prime. Then all numbers a, $0 < a < m$, are coprime with m, and hence have multiplicative inverses modulo m. It means that the ring Z_m with modulo m arithmetic is a field.

Fact. The number of elements of a finite field is a prime power p^n, where p is prime and $n \geq 1$. A finite field with $n > 1$ can be constructed as a Galois field (polynomial field),see below.

Structure of a finite field

See: Textbook, Section 5.2.3, and separate text.

$\mathbf{Z}_n^* = \{a \mid 0 < a < n, \gcd(a,n) = 1\}$

multiplicative group of the ring $\mathbf{Z}_n$

$|\mathbf{Z}_n^*| = \Phi(n)$

cyclic subgroup: syklinen aliryhmä

order: kertaluku

primitive: primitiivinen

Galois Field

In Galois fields
full of flowers
primitive elements
dance for hours.

S.B. Weinstein

Textbook, Section 6.4