GALOIS FIELDS

BURTON ROSENBERG
UNIVERSITY OF MIAMI

Contents

1. Overview

The field of cryptography is very creative in making use of what might be considered "alternative" number systems, exploiting their unique algebraic structures and computational potential. Everyday experience provides examples of applications of the real number system, as it measures and describes our reality completely. The complex number system is an abstraction with the inclusion of "imaginary" numbers as supplement to the reals. The imaginaries provide an additional dimension attached to each real location that better describes that location for the purpose of physics. For instance, a value that as always been recognized to have an intensity, registered as a real, can also have a phase, registered as an imaginary.

The pure mathematical facts of a number system can be stated in the abstract, estranged any example, and other models made of those abstract facts. One then develops an intuition of when certain phenomena are due to the abstract structure, and are therefore valid intuitions when applied to any model, or are specifics introduced by a particular model, that is, that the model does more than narrowly implement the abstract structure.

For instance, the points of the real number system not only admit to the operations of addition, multiplication, etc.., but are part of an "analytic completion" whose essence is in the idea of convergence sequences of approximations. To converge means to lay over the numbers system a conception of distance and, eventually, of continuity. There is no rational whose square is 2, there is a sequence of rationals whose squares converge towards 2. This is an analytic approach that depends on

Date: March 22, 2018.

distance, neighborhoods, and continuity, and it discovers, or creates, $\sqrt{2}$ as the limit to an infinitely refining sequence of approximations.

The integers modulo a prime have the algebraic structure of the reals, they are both *commutative fields*, but the modular field does not have the analytic structure. It is discrete and there is no possibility for endlessly refined approximation, and not metric to judge convergence. In these fields we investigate the roots of algebraic equations, and introduce square roots what are analogies of non-rational reals, and numbers that act like the complex. To keep the perspective, we also look at algebraic integers, such as Gaussian Integers, to contrast the finite and infinite cases.

2. Quadratic Extensions

Definition 2.1. An element y of a finite field $\mathcal{F}_p$, for p an odd prime, is a *quadratic residue* if it is in the image of the squaring map,

$$\mathcal{Q} = \{\, x^2 \,|\, x \in \mathcal{F} \,\}.$$

The elements which are not residues, and called *quadratic non-residues*.

The set $\mathcal{Q}$ is a subgroup of $\mathcal{F}$, and therefore there is the quadratic character map χ,

$$\mathcal{F}_p \xrightarrow{x^2} \mathcal{F}_p \xrightarrow{\chi} \mathcal{F}_p/\mathcal{Q} \cong \mathcal{F}_2 \longrightarrow 0,$$

that can be simply stated as $\chi(x) = x^{(p-1)/2}$.

Note: The above exact sequence reads as follows. The squaring map $x \mapsto x^2$ has an image $\mathcal{Q}$ in $\mathcal{F}_p$ that maps under χ to 1, and all other elements map by χ to -1. The map is a homomorphism of groups, hence such facts as the product of residues is a non-residue, since $-1 \cdot -1 = 1$, or the product of a non-residue with a residue is a non-residue, as $1 \cdot -1 = -1$.

In the case that x is the square root of y, evidently so is $-x$. This gives a two fold cover of $\mathcal{F}_p$, leaving half of the elements as non-residues. Taking any non-residue a, its square root can be adjoined to the field, and closed by field operations, to make a degree two extension,

$$\mathcal{F}_{p^2} = \{\, x + y\,\alpha \,|\, x, y \in \mathcal{F}_p \,\}$$

where α is a new element such that $\alpha^2 = a$, the non-residue.

Theorem 2.1. $\mathcal{F}_{p^2}$ is a field.

Define the conjugate of $s = x + y\,\alpha$ to be $s^* = x - y\,\alpha$ and the norm of $s = x + y\,\alpha$ to be $N(s) = x^2 - a\,y^2$, where $\alpha^2 = a$. Then,

$$s^{-1} = N(s)^{-1}\, s^*,$$

as can be verified,

$$s\,s^{-1} = N(s)^{-1} s\,s^* = (x^2 - a\,y^2)^{-1}(x + y\,\alpha)(x - y\,\alpha) = (x^2 - a\,y^2)^{-1}(x^2 - a\,y^2) = 1$$

Theorem 2.2. The field $\mathcal{F}_{p^2}$ in the above construction does not depend on the choice of non-residue a.

Let b be any other non-residue, with proposed square root β. Solving $k\alpha = \beta$ gives $k = \sqrt{b/a}$, noting that b/a is the product of two non-residues, and is therefore a quadratic residue.