CONSTRUCTION OF A FINITE FIELD OF ORDER p^3

G. MCNINCH

Let p be a prime number which satisfies

$$p \equiv 1 \pmod 3.$$

Let $g \in \mathbb{Z}_p^\times$ be a generator for the unit group; in other words, g is a unit of order $p-1$. Since $3|(p-1)$, the $\frac{p-1}{3}$ power of g is an unit of order 3; lets agree to write u for this unit of order 3.

Consider the function

$$\phi : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$$

given by the rule $\phi(x) = x^3$. Then ϕ is *not* a $1-1$ function, since $\phi(1) = \phi(u) = \phi(u^2) = 1$. Since $\mathbb{Z}_p$ is a finite set, ϕ is therefore not an *onto* function. This means that we can find an element $\alpha \in \mathbb{Z}_p^\times$ so that

$$\alpha \neq x^3 \quad \text{for any } x \in \mathbb{Z}_p^\times.$$

(In fact, there are $\frac{2(p-1)}{3}$ choices for α...do you see why?)

While we are at it, let us observe the following:

Lemma 1. If $\beta \in \mathbb{Z}_p^\times$ is not a cube, then β^2 is also not a cube.

Proof. Let $g \in \mathbb{Z}_p^\times$ be a generator for this cyclic group. Write $\beta = g^k$. Since β is not a cube, k is not divisible by 3. Since $\beta^2 = g^{2k}$ and $2k$ is not divisible by 3, β^2 is not a cube. □

Let F be a vector space over $\mathbb{Z}_p$ of dimension 3, with basis elements $1, \zeta, \zeta^2$. We are going to "teach" vectors in F how to multiply. The idea is that ζ should be a cube root of α (the element above which had no cube root in $\mathbb{Z}_p$). Formally, this means that $\zeta^3 = \zeta \cdot \zeta^2 = \alpha$.

A typical vector in F has the form

$$z = a + b\zeta + c\zeta^2 \quad \text{for } a, b, c \in \mathbb{Z}_p.$$

If z and z' are vectors in F, then by requiring that the distributive law holds, the above rules for multiplication of ζ with itself and ζ^2 more or less determine the multiplication in F.

The formal rule is:

$$\begin{aligned} z \cdot z' = \quad & aa' + \alpha(bc' + b'c) \\ & + (ab' + a'b + \alpha cc')\zeta \\ & + (ac' + a'c + bb')\zeta^2 \end{aligned}$$

which looks worse than it really is!

An alternate way of describing the multiplication is as follows: let

$$M(z) = \begin{bmatrix} a & -\alpha c & -\alpha b \\ b & a & -\alpha c \\ c & b & a \end{bmatrix}.$$

You may check that

$$M(z) \cdot M(z') = M(zz')$$

where the multiplication zz' is as given above.

When $z \in F$ we define the norm $N(z)$ to be the following element of $\mathbb{Z}_p$:

$$N(z) = a^3 + \alpha b^3 + \alpha^2 c^3 - 3\alpha abc.$$

Lemma 2. $N(zz') = N(z) \cdot N(z')$ for all $z, z' \in F$.

Proof. You may check that $N(z) = \det M(z)$ and hence that $N(zz') = N(z)N(z')$. □

Theorem 1. *The vector space F together with the above multiplication forms a field of order p^3.*

Proof. The vector space F evidently has order p^3. That F is a ring we shall leave unchecked – one really needs to verify distributivity and associativity of the multiplication. This actually follows from the fact that we may think about elements z of F as the matrices $M(z)$ so that we can deduce the required properties from those of matrices.

The main thing to check is that elements in F have inverses. As a first step, we claim that $N(z) \neq 0$ for any $0 \neq z \in F$.

We start with the following observation: if $w \in F$ is any element such that $N(w) \neq 0$, then $N(z) \neq 0$ if and only if $N(wz) = N(w)N(z) \neq 0$.

We now find some elements whose norm is known not to be 0. First observe that if $d \in \mathbb{Z}_p^\times$, $N(d) = d^3 \neq 0$, $N(d\zeta) = d^3\alpha \neq 0$, and $N(d\zeta^2) = d^3\alpha^2 \neq 0$.

Let us call a, b, c the *coefficients* of z.

So we know that $N(z)$ is not zero at least in the case that there are two coefficients which are 0.

Suppose now that precisely one coefficient of z is 0. Then multiplying by a suitable power of ζ, we may suppose that $z = a + b\zeta$ or $z = a + b\zeta^2$ for $a, b \in \mathbb{Z}_p^\times$. Notice that

$$N(a + b\zeta) = a^3 + \alpha b^3.$$

If this were 0, we would have $(\frac{-a}{b})^3 = \alpha$ contrary to the fact that α is not a cube.

Similarly,

$$N(a + b\zeta^2) = a^3 + \alpha^2 b^3.$$

If this were 0, we would have $(\frac{-a}{b})^3 = \alpha^2$ contrary to the fact that α^2 is not a cube.

Finally, suppose that $z = a + b\zeta + c\zeta^2$ has no nozero coefficients. We may replace z with $\frac{z}{a}$ and thus suppose that $a = 1$.

Then observe that

$$(1 + b\zeta + c\zeta^2)(1 - b\zeta) = (1 + b\zeta + c\zeta^2) - (\alpha cb + b\zeta + b^2\zeta^2) = (1 - \alpha cb) + (c - b^2)\zeta^2.$$

This product has at most two coeffients. Let us argue that this element is not zero so its norm is not zero. Well, if this element were zero, we would have $c = b^2$ and

$$\alpha = \frac{1}{cb} = \frac{1}{b^3} = \left(\frac{1}{b}\right)^3$$

contrary to the fact that α is not a cube!

This proves that $N(z) \neq 0$ whenever $z \neq 0$.

Since $N(z)$ is the determinant of $M(z)$, we know that $M(z)$ is an invertible matrix. Thus the equation

$$M(z) \cdot \begin{bmatrix} r \\ s \\ t \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

has a solution (r, s, t) with $r, s, t \in \mathbb{Z}_p$. One can then easily check that $z^{-1} = r + s\zeta + t\zeta^2$ is the inverse of z. □

Example: Let $p = 7$; then $p \equiv 1 \pmod 3$. The cubes in $\mathbb{Z}_7$ are $\{1, 6\}$. So take $\alpha = 2$, and

$$\zeta = \sqrt[3]{2}$$

The field F consists of all vectors

$$a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \quad \text{for } a, b, c \in \mathbb{Z}_7;$$

thus F has $7^3 = 343$ elements.

For an explicit inverse computation, take $z = 1 + 2\zeta + \zeta^2$. The reader may check that $N(z) = 2 \in \mathbb{Z}_7$, and that

$$z^{-1} = 6 + 3\zeta + 5\zeta^2.$$