On a problem of Perron

Michele Elia

Politecnico di Torino

Trento - March 7, 2019

Outline of the presentation

1. A brief history of the problem
2. Extensions of Perron's original problem
3. Monico's approach and solution for $\mathbb{F}_p$
4. The solution for $\mathbb{F}_{p^m}$ (novel contribution)
5. A problem still open

The problem

In 1952 Oskar Perron found some additive properties of the sets of quadratic residues and non-residues in prime finite fields.
If $\mathfrak{Q}_p$ and $\mathfrak{N}_p$ are the subsets of (non-zero) quadratic residues, and non-residues of $\mathbb{F}_p$, respectively, then

1. Every element of $\mathfrak{Q}_p$ [respectively $\mathfrak{N}_p$] can be written as a sum of two elements of $\mathfrak{Q}_p$ [respectively $\mathfrak{N}_p$] in exactly $d_p - 1 = \lfloor \frac{p+1}{4} \rfloor - 1$ ways
2. Every element of $\mathfrak{Q}_p$ [respectively $\mathfrak{N}_p$] can be written as a sum of two elements of $\mathfrak{N}_p$ [respectively $\mathfrak{Q}_p$] in exactly $d_p = \lfloor \frac{p+1}{4} \rfloor$ ways

Example p=17

$$\mathfrak{Q}_{17} = \{1, 2 = 6^2, 4 = 2^2, 8 = 5^2, 9 = 3^2, 13 = 8^2, 15 = 7^2, 16 = 4^2\}$$
$$\mathfrak{N}_{17} = \{3, 5, 6, 7, 10, 11, 12, 14\}$$
$$\mathfrak{E}_{17} = \{0\}$$

$$1 = 16 + 2,\ 2 + 16,\ 9 + 9 \qquad d_{17} - 1 = 4 - 1 = 3$$
$$13 = 4 + 9,\ 9 + 4,\ 15 + 15 \qquad 13 = 1 \times 13 \bmod 17$$
$$\vdots$$
$$0 = 16 + 1,\ 15 + 2,\ 13 + 4,\ 8 + 9,\ 9 + 8,\ 4 + 13,\ 2 + 15,\ 16 + 1$$
$$3 = 1 + 2,\ 2 + 1,\ 4 + 16,\ 16 + 4$$
$$11 = 2 + 9,\ 9 + 2,\ 13 + 15,\ 15 + 13 \qquad 11 = 3 \times 15 \bmod 17$$
$$\vdots$$
$$14 = 16 + 15,\ 15 + 16,\ 13 + 1,\ 1 + 13$$
$$d_{17} = 4$$

The Problem

In 2005, Chris Monico (unaware of Perron result) re-discovered the above properties concerning the even partitions of $\mathbb{Z}_p$, and gave a formal proof based on an algebra of univariate polynomials.

Contemporarily, he posed the problem whether Perron's additive property uniquely characterizes the partition given by $\mathfrak{Q}_p$ and $\mathfrak{N}_p$.

His positive answer to this question closed the problem.

Observations and Problem extensions

The partition $\mathfrak{Q}_p \cup \mathfrak{N}_p = \mathbb{F}_p^*$ can be formulated in terms of the multiplicative character χ_2 of order 2, i.e. the Legendre symbol, defined over $\mathbb{F}_p^*$.

The partition problem of prime fields was further extended by considering partitions in sub-sets, called cyclotomic cosets, induced by any character χ_n of order n, defined over $\mathbb{F}_p^*$, and was solved almost definitively.

The next extension is to show that the partition induced by any character χ_n, over any finite field $\mathbb{F}_{p^m}$ is the unique partition satisfying Perron's additive property.

In this talk (and in the related paper) only the case of χ_2 is addressed.

Monico's plan in $\mathbb{F}_p$

- Describe the subsets $\mathfrak{Q}_p$ and $\mathfrak{N}_p$ of $\mathbb{F}_p$ by univariate polynomials $r_Q(x)$, $r_N(x)$, and $r_E(x) = 1$ for $\{0\}$.
- Prove that $r_Q(x)$, $r_N(x)$, and $r_E(x)$ generate an algebra of polynomials
- Show that $r_Q(x)$, $r_N(x)$ are roots of a second degree polynomial $Z(w)$ in $\mathbb{F}_p[x]/\langle x^p - 1\rangle$
- Prove that $Z(w)$ has exactly two roots in $\mathbb{F}_p[x]/\langle x^p - 1\rangle$ using a kind of Hensel's lifting argument
- Conclude about the unicity of the partition induced by χ_2

$\mathbb{F}_p$

Consider the univariate polynomials $r_Q(x)$, $r_N(x)$, and $r_E(x)$

$$\mathfrak{Q}_p \to r_Q(x) = \sum_{j\in Q} x^j = \sum_{j\in\mathbb{F}_P^*} \frac{1+(j \mid p)}{2} x^j$$

$$\mathfrak{N}_p \to r_N(x) = \sum_{j\in N} x^j = \sum_{j\in\mathbb{F}_P^*} \frac{1-(j \mid p)}{2} x^j$$

$$\mathfrak{E}_p = \{0\} \to r_E(x) = 1 \quad .$$

$$\mathfrak{Q}_p \cup \mathfrak{N}_p \cup \mathfrak{E}_p = \mathbb{F}_p$$

Main Theorem

Theorem

$$r_Q(x)^2 + r_Q(x) = a_0 + a_1(x + x^2 + \cdots + x^{p-1}) \pmod{x^p - 1}$$
$$r_N(x)^2 + r_N(x) = a_0 + a_1(x + x^2 + \cdots + x^{p-1}) \pmod{x^p - 1}$$
$$r_Q(x) r_N(x) = c_0 + c_1(x + x^2 + \cdots + x^{p-1}) \pmod{x^p - 1}$$

where

$$a_0 = \frac{p-1}{2} \quad , \quad a_1 = \frac{p-1}{4} \textit{ if } p \equiv 1 \bmod 4$$
$$a_0 = 0 \quad , \quad a_1 = \frac{p+1}{4} \textit{ if } p \equiv 3 \bmod 4$$
$$c_0 = 0 \quad , \quad c_1 = \frac{p-1}{4} \textit{ if } p \equiv 1 \bmod 4$$
$$c_0 = \frac{p-1}{2} \quad , \quad c_1 = \frac{p+1}{4} - 1 \textit{ if } p \equiv 3 \bmod 4$$

Proof outline

The representatives of $r_Q(x)^2$ and $r_N(x)^2$ in $\mathbb{F}_p[x]/\langle x^p - 1\rangle$ are

$$r_Q(x)^2 = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1}x^{p-1} \pmod{x^p - 1}$$
$$r_N(x)^2 = b_0 + b_1 x + b_2 x^2 + \cdots + b_{p-1}x^{p-1} \pmod{x^p - 1}$$

where a_j and b_j are non-negative integers smaller than p.
It is observed that a_j [or b_j] is precisely the number of ways in which j can be written as a sum of two quadratic residues [or non-residues].

Key lemma

Lemma

Let p be an odd prime and a_i, b_i as defined above. Then for $i, j \in Z_p$, the following hold:

a) $b_j - a_j = (j \mid p)$.

b) *If* $(i \mid p) = (j \mid p)$, *then* $a_i = a_j$ *and* $b_i = b_j$. $i, j \neq 0$

proof item a)

Observe that

- $r_N(x) + r_Q(x) = x + x^2 + \cdots + x^{p-1} = \frac{x^p-1}{x-1} - 1$
- $r_N(1) - r_Q(1) = 0$ since the number of quadratic residues [quadratic non-residues] is $\frac{p-1}{2}$
- $r_N(x) - r_Q(x) = (x-1)f_p(x)$

$$\begin{aligned} r_N(x)^2 - r_Q(x)^2 &= (x-1)f_p(x)\left[\frac{x^p-1}{x-1} - 1\right] \\ &= f_p(x)(x^p-1) - (x-1)f_p(x) \\ &= -(x-1)f_p(x) \pmod{\langle x^p-1\rangle} \\ &= -(r_N(x) - r_Q(x)) \pmod{\langle x^p-1\rangle} \end{aligned}$$

hence $b_j - a_j = (j \mid p)$, that is, item a).

proof item b)

Suppose $\chi_2(i) = \chi_2(j) = 1$ (i.e. i, j are quadratic residues modulo p).

There exists a quadratic residue $\alpha \in \mathbb{Z}_p$ so that $j = \alpha i \pmod{p}$.

If x, y are quadratic residues with $i = x + y \pmod{p}$, it follows that $j = x\alpha + y\alpha \pmod{p}$ with $x\alpha, y\alpha$ quadratic residues, it follows that

$$a_i = a_j$$

In any case, we get $a_i = a_j$ for $(i \mid p) = (j \mid p)$.
Then, from the first part of the lemma, it follows
$b_i = b_j$ for $(i \mid p) = (j \mid p)$.

Example p=7

$$\begin{array}{lcl} Q = \{1,2,4\} & \rightarrow & r_Q(x) = x + x^2 + x^4 \\ N = \{3,5,6\} & \rightarrow & r_N(x) = x^3 + x^5 + x^6 \\ E = \{0\} & \rightarrow & r_E(x) = 1 \end{array}$$

The polynomials $r_Q(x)$, $r_N(x)$, and $r_E(x)$ are a basis of a tridimensional algebra of polynomials in the ring $\mathbb{F}_7[x]/\langle x^7 - 1\rangle$. It is direct to check

$$\begin{array}{rcl} r_Q(x) \cdot r_Q(x) & = & r_Q(x) + 2r_N(x) \\ r_Q(x) \cdot r_N(x) & = & r_Q(x) + r_N(x) + 3r_E(x) \\ r_N(x) \cdot r_N(x) & = & 2r_Q(x) + r_N(x) \end{array}$$

Only IF

Let $\mathfrak{A}$ and $\mathfrak{B}$ an even partition of $\mathbb{F}_p^*$, with $1 \in \mathfrak{A}$.
$|\mathfrak{A}| = |\mathfrak{B}| = \frac{p-1}{2}$

1. Every element of $\mathfrak{A}$ [respectively $\mathfrak{B}$] can be written as a sum of two elements of $\mathfrak{A}$ [respectively $\mathfrak{B}$] in exactly $d_p - 1$ ways.
2. Every element of $\mathfrak{A}$ [respectively $\mathfrak{B}$] can be written as a sum of two elements of $\mathfrak{B}$ [respectively $\mathfrak{A}$] in exactly d_p ways.

Define

$$r_A(x) = \sum_{j \in \mathfrak{A}} x^j$$

Only IF, cont.

From the assumptions

$$
\begin{aligned}
r_A(x)^2 &= (d_p - 1)r_A(x) + d_p r_B(x) + c_p \pmod{x^p - 1} \\
&= d_p\left(\frac{x^p-1}{x-1} - 1\right) - r_A(x) + c_p \pmod{x^p - 1} \\
&= d_p(-1 + (x-1)^{p-1}) - r_A(x) + c_p \pmod{x^p - 1} \bmod p
\end{aligned}
$$

Lemma

Let p be an odd prime, and $\mathcal{R}_k = \mathbb{F}_p[x]/\langle (x-1)^k \rangle$ for $k \geq 1$. Then each invertible element of $\mathcal{R}_k$ has at most two distinct square roots.

Proof, by recursion, of the Lemma

If $k = 1$, the Lemma is true because $\mathcal{R}_1 = \mathbb{F}_p$.

Suppose that $a(x), b(x), c(x), g(x)$ are invertible modulo $\langle (x-1)^{N+1} \rangle$ and

$$\begin{aligned} a(x)^2 + \langle (x-1)^{N+1} \rangle &= b(x)^2 + \langle (x-1)^{N+1} \rangle \\ &= c(x)^2 + \langle (x-1)^{N+1} \rangle = g(x)^2 + \langle (x-1)^{N+1} \rangle \end{aligned}$$

By canonical projection into $\mathcal{R}_N$ two of these must be equal, say

$$a(x)+\langle (x-1)^N \rangle = b(x)+\langle (x-1)^N \rangle \Rightarrow a(x) = b(x)+(x-1)^N f(x)$$

Proof of the Lemma

$$\begin{aligned} b(x)^2 + \langle (x-1)^{N+1} \rangle &= a(x)^2 + \langle (x-1)^{N+1} \rangle \\ &= (b(x) + (x-1)^N f(x))^2 + \langle (x-1)^{N+1} \rangle \\ &= b(x)^2 + 2b(x)(x-1)^N f(x) + \\ &\qquad (x-1)^{2N} f(x)^2 + \langle (x-1)^{N+1} \rangle \\ &= b(x)^2 + 2b(x)(x-1)^N f(x) + \langle (x-1)^{N+1} \rangle \end{aligned}$$

thus $2b(x)(x-1)^N f(x) \in \langle (x-1)^{N+1} \rangle$.
Since $2b(x)$ is invertible in $\mathcal{R}_{N+1}$, it follows that $(x-1) | f(x)$, then

$$a(x) + \langle (x-1)^{N+1} \rangle = b(x) + \langle (x-1)^{N+1} \rangle$$

Only IF, cont.

It follows that

$$r_A(x)^2 + r_A(x) = -d_p + c_p \pmod{\langle (x-1)^{p-1} \rangle} \bmod p$$

has only two roots.

In conclusion

$$r_A(x) = r_Q(x) \quad , \quad r_B(x) = r_N(x)$$

because $1 \in \mathfrak{A}$ and $1 \in \mathfrak{Q}_p$

The even partition problem in $\mathbb{F}_{p^m}$

Lemma

An element $\beta \in \mathbb{F}_{p^m}$ is a square if and only if its norm $\mathcal{N}(\beta) = \prod_{i=0}^{m-1} \beta^{p^i}$ is a quadratic residue in $\mathbb{F}_p$.

$$\chi_2(\beta) = \left(\frac{\mathcal{N}(\beta)}{p}\right) \quad \forall \beta \in \mathbb{F}_{p^m}^*$$

Then

$$\mathfrak{Q}_{p^m} = \{\beta : \ \beta \in \mathbb{F}_{p^m}^* \wedge \chi_2(\beta) = 1\}$$

$$\mathfrak{N}_{p^m} = \{\beta : \ \beta \in \mathbb{F}_{p^m}^* \wedge \chi_2(\beta) = -1\}$$

Set $d_{p^m} = \frac{p^m-1}{4}$ if $p \equiv 1 \bmod 4$

$d_{p^m} = \frac{p^m-(-1)^m}{4}$ if $p \equiv 3 \bmod 4$.

Generating multivariate polynomials

Given a basis $\{1, \gamma, \gamma^2, \ldots, \gamma^{m-1}\}$ of $\mathbb{F}_{p^m}$, any $\beta \in \mathbb{F}_{p^m}$ is represented by an m-tuple of $\mathbb{F}_p^m$

$$\beta \Leftrightarrow [b_0, b_1, \ldots, b_{m-1}]$$

The following multivariate polynomials uniquely identify the subsets of squares and non-squares

$$r_{\mathfrak{Q}_{p^m}}(\mathbf{x}) = \sum_{\beta \in \mathfrak{Q}_{p^m}} \prod_{i=1}^{m} x_i^{b_i} \quad , \quad r_{\mathfrak{N}_{p^m}}(\mathbf{x}) = \sum_{\beta \in \mathfrak{N}_{p^m}} \prod_{i=1}^{m} x_i^{b_i}$$

It is immediately seen that

$$1 + r_{\mathfrak{Q}_{p^m}}(\mathbf{x}) + r_{\mathfrak{N}_{p^m}}(\mathbf{x}) = \prod_{i=0}^{m-1} \frac{x_i^p - 1}{x_j - 1}$$

cont.

The representatives of $r_{\mathfrak{Q}_{p^m}}(\mathbf{x})^2$ and $r_{\mathfrak{N}_{p^m}}(\mathbf{x})^2$ modulo $\langle (x_1^p - 1), (x_2^p - 1), \cdots, (x_m^p - 1) \rangle$ in $\mathbb{Q}[x]$ are denoted by

$$r_{\mathfrak{Q}_{p^m}}(\mathbf{x})^2 = \sum_{\beta \in \mathfrak{Q}_{p^m}} A_{b_1,\ldots,b_m} \prod_{j=1}^{m} x_j^{b_j} \mod \langle (x_1^p - 1), \cdots, (x_m^p - 1) \rangle$$

$$r_{\mathfrak{N}_{p^m}}(\mathbf{x})^2 = \sum_{\beta \in \mathfrak{N}_{p^m}} B_{b_1,\ldots,b_m} \prod_{j=1}^{m} x_j^{b_j} \mod \langle (x_1^p - 1), \cdots, (x_m^p - 1) \rangle$$

where $A_{b_1,\ldots,b_m}$ and $B_{b_1,\ldots,b_m}$ are non-negative integers smaller than p^m

cont.

It is observed that $A_{b_1,\ldots,b_m}$ [or $B_{b_1,\ldots,b_m}$] is precisely the number of ways in which every $\beta \in \mathbb{F}_{p^m}$ can be written as a sum of two squares [or non-squares].

The numbers $A_{b_1,\ldots,b_m}$ and $B_{b_1,\ldots,b_m}$ can be considered as elements of the set $\mathcal{R} = \{0, 1, 2, \ldots, p^m - 1\}$.

Example p=3, m=2

$p(z) = z^2 + 2z - 1$ primitive polynomial with root α

$$\mathfrak{Q}_{3^2} = \{1, 1+\alpha, 2, 2+2\alpha\} \to r_{\mathfrak{Q}_{3^2}}(x,y) = x + xy + x^2 + x^2y^2$$
$$\mathfrak{N}_{3^2} = \{\alpha, 1+2\alpha, 2\alpha, 2+\alpha\} \to r_{\mathfrak{N}_{3^2}}(x,y) = y + xy^2 + y^2 + x^2y$$
$$\mathfrak{E}_{3^2} = \{0\} \to r_{\mathfrak{E}_{3^2}}(x,y) = 1$$

The polynomials $r_{\mathfrak{Q}_{3^2}}(x,y)$, $r_{\mathfrak{N}_{3^2}}(x,y)$, and $r_{\mathfrak{E}_{3^2}}(x,y)$ are a basis of a tri-dimensional algebra of polynomials in the ring $\mathbb{F}_{3^2}[x,y]/\langle x^3-1, y^3-1\rangle$.
It is direct to check

$$\begin{aligned}
r_{\mathfrak{Q}_{3^2}}(x,y) \cdot r_{\mathfrak{Q}_{3^2}}(x,y) &= r_{\mathfrak{Q}_{3^2}}(x,y) + 2r_{\mathfrak{N}_{3^2}}(x,y) + 4r_{\mathfrak{E}_{3^2}}(x,y) \\
r_{\mathfrak{Q}_{3^2}}(x,y) \cdot r_{\mathfrak{N}_{3^2}}(x,y) &= r_{\mathfrak{Q}_{3^2}}(x,y) + r_{\mathfrak{N}_{3^2}}(x,y) \\
r_{\mathfrak{N}_{3^2}}(x,y) \cdot r_{\mathfrak{N}_{3^2}}(x,y) &= 2r_{\mathfrak{Q}_{3^2}}(x,y) + r_{\mathfrak{N}_{3^2}}(x,y) + 4r_{\mathfrak{E}_{3^2}}(x,y)
\end{aligned} \tag{1}$$

Key lemma

Similalrly to Lemma 2 we have

Lemma

Let p be an odd prime, m be a positive integer, and $A_{b_1,\ldots,b_m}, B_{b_1,\ldots,b_m}$ as defined above. Then for every $\alpha, \beta \in \mathbb{F}_{p^m}$, the following hold:

1. $B_{b_1,\ldots,b_m} - A_{b_1,\ldots,b_m} = (\mathcal{N}(\beta) \mid p)$
2. *If* $(\mathcal{N}(\beta)|p) = (\mathcal{N}(\alpha)|p)$, *then* $A_{b_1,\ldots,b_m} = A_{a_1,\ldots,a_m}$ *and* $B_{b_1,\ldots,b_m} = B_{a_1,\ldots,a_m}$.
3. *If* $(\mathcal{N}(\beta)|p) \neq (\mathcal{N}(\alpha)|p)$, *then*

$$A_{b_1,\ldots,b_m} = A_{a_1,\ldots,a_m} + (\mathcal{N}(\alpha)|p)$$
$$B_{b_1,\ldots,b_m} = B_{a_1,\ldots,a_m} - (\mathcal{N}(\alpha)|p)$$

Proof

Let $\mathbf{e}$ be the all-one m-dimensional vector, then

$$r_{\mathfrak{Q}_{p^m}}(\mathbf{e}) = r_{\mathfrak{N}_{p^m}}(\mathbf{e}) = \frac{p^m - 1}{2}$$

Thus

$$r_{\mathfrak{Q}_{p^m}}(\mathbf{x}) - r_{\mathfrak{N}_{p^m}}(\mathbf{x}) = Q(\mathbf{x}) \prod_{j=1}^{m} (x_j - 1) \quad ,$$

$$r_{\mathfrak{Q}_{p^m}}(\mathbf{x}) + r_{\mathfrak{N}_{p^m}}(\mathbf{x}) = -1 + \prod_{j=1}^{m} \frac{x_j^p - 1}{x_j - 1} \quad ,$$

$$\begin{aligned} r_{\mathfrak{Q}_{p^m}}(\mathbf{x})^2 - r_{\mathfrak{N}_{p^m}}(\mathbf{x})^2 &= -Q(\mathbf{x}) \textstyle\prod_{j=1}^{m} (x_j - 1) + Q(\mathbf{x}) \prod_{j=1}^{m} (x_j^p - 1) \\ &= -Q(\mathbf{x}) \textstyle\prod_{j=1}^{m} (x_j - 1) \mod \prod_{j=1}^{m} (x_j^p - 1) \end{aligned}$$

Proof, cont.

That is

$$r_{\mathfrak{Q}_{p^m}}(\mathbf{x})^2 - r_{\mathfrak{N}_{p^m}}(\mathbf{x})^2 = r_{\mathfrak{Q}_{p^m}}(\mathbf{x}) - r_{\mathfrak{N}_{p^m}}(\mathbf{x}) \bmod \prod_{j=1}^{m}(x_j^p - 1)$$

which proves item 1.

Suppose now that $\chi_2(\alpha) = \chi_2(\beta) = 1$ in $\mathbb{F}_{p^m}$. Then there exists a square $\delta \in \mathbb{F}_{p^m}$ so that $\beta = \delta\alpha$.
If $\chi_2(x) = \chi_2(y) = 1$, with $\alpha = x + y$, it follows that $\beta = \delta x + \delta y$ and $\delta x, \delta y$ are also squares. Thus $A_{b_1,\dots,b_m} = A_{a_1,\dots,a_m}$, and with a similar argument $B_{b_1,\dots,b_m} = B_{a_1,\dots,a_m}$.

Proof, cont.

Suppose $\chi_2(\alpha) = 1$, and that $\alpha = x + y$ is a sum of two non-squares, let β be any non-square, then

$$\eta = \beta\alpha = \beta x + \beta y$$

says that a non-square is the sum of two squares, it follows that $A_\eta = B_\alpha$ with η a non-square and α a square, the same equality holds by exchanging square and non-square.

Let A_1 and A_{-1} denote the common value of the A_α with $(\mathcal{N}(\alpha) \mid p) = 1$ and -1, respectively. Similarly, define B_1 and B_{-1} to be the common values of B_α for $(\mathcal{N}(\alpha) \mid p) = 1$ and -1, respectively.

Observations

From Lemma 5, we have $A_1 = B_{-1}$, and $B_1 = A_{-1}$. Let A_0 denote the number of sums of two squares giving 0, then $A_0 = 0$ if $p \equiv 3 \pmod 4$ and m odd because $\chi_2(-1) = -1$, otherwise $A_0 = \frac{p^m-1}{2}$ because $\chi_2(-1) = 1$, i.e. -1 is a square. A direct counting of the number of sums of two squares gives

$$\frac{p^m-1}{2}A_1 + \frac{p^m-1}{2}A_{-1} + A_0 = \left(\frac{p^m-1}{2}\right)^2 \quad ,$$

therefore, in view of the above observations, we have

$$A_1 + A_{-1} = \begin{cases} \dfrac{p^m-3}{2} & \text{if } p \equiv 1 \pmod 4 \\[2ex] \dfrac{p^m-2-(-1)^m}{2} & \text{if } p \equiv 3 \pmod 4 \end{cases} , \quad (2)$$

furthermore $A_1 + A_{-1} = B_1 + B_{-1}$

Main 2

Theorem

Let $\mathbb{F}_{p^m}$ be a finite field of odd order, and set

$$d_{p^m} = \begin{cases} \dfrac{p^m - 1}{4} & \text{if } p \equiv 1 \pmod 4 \\ \\ \dfrac{p^m - (-1)^m}{4} & \text{if } p \equiv 3 \pmod 4 \,. \end{cases} \tag{3}$$

Then every square [non-square] can be written as a sum of two squares [non-squares] in exactly $d_{p^m} - 1$ ways. Every square [non-square] can be written as a sum of two non-squares in exactly d_{p^m} ways. Moreover, every non-zero element can be written as a sum of a square and a non-square in exactly $p^m - 1 - 2d_p$ ways.

Lemma (a la Hensel)

Lemma

Let p be an odd prime, and $\mathbb{R}_k = \mathbb{F}_{p^m}[x]/\langle \prod_{j=1}^{m}(x_j - 1)^k \rangle$ for $k \geq 1$. Then each invertible element of $\mathbb{R}_k$ has at most two distinct square roots.

Theorem

Theorem

Let p be an odd prime and let d_{p^m} be defined as in Equation (3). Suppose $\mathfrak{A} \in \mathbb{F}_{p^m}^*$ and $\mathfrak{B} = \mathbb{F}_{p^m}^* \backslash \mathfrak{A}$. Then $\mathfrak{A}$ is precisely the set of squares of $\mathbb{F}_{p^m}^*$ if and only if

1. $|\mathfrak{A}| = \frac{p^m - 1}{2}$,
2. $1 \in \mathfrak{A}$,
3. *Every element of $\mathfrak{A}$ can be written as a sum of two elements from $\mathfrak{A}$ in exactly $d_{p^m} - 1$ ways.*
4. *Every element of $\mathfrak{B}$ can be written as a sum of two elements from $\mathfrak{A}$ in exactly d_{p^m} ways.*

References

1. O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, *Mathematische Zeitschrift*, 56(1952), 122-130.
2. C. Monico, M. Elia, Note on an Additive Characterization of Quadratic Residues Modulo p, *Journal of Combinatorics, Information & System Sciences*, 31 (2006), 209-215.
3. C. Monico, M. Elia, An Additive Characterization of Fibers of Characters on ${\mathbb{F}^m}_p$, *International Journal of Algebra*, Vol. 1-4, n.3, 2010, p.109-117.
4. A.A. Albert, *Structure of Algebras*, AMS, Providence, R.I. 2003.
5. M. Elia, On a problem of Perron, *arXiv:1903.00169*, February 2019.

Thank you!