Towards a problem of Cohn.

Dan Fretwell
University of Bristol
(daniel.fretwell@bristol.ac.uk)

Let p be an odd prime. Consider the unique quadratic character:

$$\chi : \mathbb{F}_p^\times \to \{0, \pm 1\}.$$

Then of course χ is the Legendre symbol. We extend to $\mathbb{F}_p$ by defining $\chi(0) = 0$.

It can be shown that:

$$(\chi \star \chi)(k) = \sum_{x \in \mathbb{F}_p} \chi(x)\chi(x+k) = \begin{cases} p-1 & \text{if } k = 0 \\ -1 & \text{if } k \neq 0 \end{cases}$$

Question

Does convolution characterise the Legendre symbol?

Let p be an odd prime. Consider the unique quadratic character:

$$\chi : \mathbb{F}_p^\times \to \{0, \pm 1\}.$$

Then of course χ is the Legendre symbol. We extend to $\mathbb{F}_p$ by defining $\chi(0) = 0$.

It can be shown that:

$$(\chi \star \chi)(k) = \sum_{x \in \mathbb{F}_p} \chi(x)\chi(x+k) = \begin{cases} p-1 & \text{if } k = 0 \\ -1 & \text{if } k \neq 0 \end{cases}$$

Question

Does convolution characterise the Legendre symbol?

Let p be an odd prime. Consider the unique quadratic character:

$$\chi : \mathbb{F}_p^\times \to \{0, \pm 1\}.$$

Then of course χ is the Legendre symbol. We extend to $\mathbb{F}_p$ by defining $\chi(0) = 0$.

It can be shown that:

$$(\chi \star \chi)(k) = \sum_{x \in \mathbb{F}_p} \chi(x)\chi(x+k) = \begin{cases} p-1 & \text{if } k = 0 \\ -1 & \text{if } k \neq 0 \end{cases}$$

Question

Does convolution characterise the Legendre symbol?

Cohn's Conjecture

Let $f : \mathbb{F}_p \to \mathbb{C}$ be a function satisfying:

- $f(0) = 0$,
- $f(1) = 1$,
- $|f(x)| = 1$ for all $x \neq 0$,
- $f \star f = \chi \star \chi$.

Then $f = \chi$.

This is still an open problem. However if we assume $\mathrm{im}(f) = \{0, \pm 1\}$ then it is possible to prove this conjecture quite easily using Tao's uncertainty principle.

Cohn's Conjecture

Let $f : \mathbb{F}_p \to \mathbb{C}$ be a function satisfying:

- $f(0) = 0$,
- $f(1) = 1$,
- $|f(x)| = 1$ for all $x \neq 0$,
- $f \star f = \chi \star \chi$.

Then $f = \chi$.

This is still an open problem. However if we assume $\mathrm{im}(f) = \{0, \pm 1\}$ then it is possible to prove this conjecture quite easily using Tao's uncertainty principle.

Recall that a function $f : \mathbb{F}_p \to \mathbb{C}$ has a Fourier transform $\hat{f} : \mathbb{F}_p \to \mathbb{C}$ where:

$$\hat{f}(y) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} f(x) \zeta_p^{-xy}.$$

Also recall that $\widehat{f_1 \star f_2} = \hat{f_1} \hat{f_2}$ for any two such functions f_1, f_2.

Tao's uncertainty principle

Let $f : \mathbb{F}_p \to \mathbb{C}$ be non-zero, then $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geq p + 1$.

Recall that a function $f : \mathbb{F}_p \to \mathbb{C}$ has a Fourier transform $\hat{f} : \mathbb{F}_p \to \mathbb{C}$ where:

$$\hat{f}(y) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} f(x) \zeta_p^{-xy}.$$

Also recall that $\widehat{f_1 \star f_2} = \hat{f_1} \hat{f_2}$ for any two such functions f_1, f_2.

Tao's uncertainty principle

Let $f : \mathbb{F}_p \to \mathbb{C}$ be non-zero, then $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geq p + 1$.

Recall that a function $f : \mathbb{F}_p \to \mathbb{C}$ has a Fourier transform $\hat{f} : \mathbb{F}_p \to \mathbb{C}$ where:

$$\hat{f}(y) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} f(x) \zeta_p^{-xy}.$$

Also recall that $\widehat{f_1 \star f_2} = \hat{f_1} \hat{f_2}$ for any two such functions f_1, f_2.

Tao's uncertainty principle

Let $f : \mathbb{F}_p \to \mathbb{C}$ be non-zero, then $|\mathrm{supp}(f)| + |\mathrm{supp}(\hat{f})| \geq p + 1$.

Theorem

Let $f, g : \mathbb{F}_p \to \mathbb{C}$ satisfy $\text{supp}(f) = \text{supp}(g) = \mathbb{F}_p^\times$ and $f \star f = g \star g$. Then $f = \pm g$.

Corollary

Cohn's conjecture is true under the assumption that $\text{im}(f) = \{0, \pm 1\}$.

Theorem

Let $f, g : \mathbb{F}_p \to \mathbb{C}$ satisfy $\text{supp}(f) = \text{supp}(g) = \mathbb{F}_p^\times$ and $f \star f = g \star g$. Then $f = \pm g$.

Corollary

Cohn's conjecture is true under the assumption that $\text{im}(f) = \{0, \pm 1\}$.

To prove the Theorem we define two functions, $F = f - g$ and $G = f + g$.

Note that $FG \equiv 0$ so that for each x at least one of $F(x), G(x)$ is 0. For $x = 0$ we have $F(0) = G(0) = 0$ and for $x \neq 0$ we must have $F(x) \neq G(x)$. Thus $|\text{supp}(F)| + |\text{supp}(G)| = (p - 1)$.

We do the same for the Fourier transforms. The convolution condition gives $\hat{F}^2 = \hat{G}^2$ so that $\hat{F}\hat{G} \equiv 0$. By the same argument as above we conclude that $|\text{supp}(\hat{F})| + |\text{supp}(\hat{G})| \leq p$.

To prove the Theorem we define two functions, $F = f - g$ and $G = f + g$.

Note that $FG \equiv 0$ so that for each x at least one of $F(x), G(x)$ is 0. For $x = 0$ we have $F(0) = G(0) = 0$ and for $x \neq 0$ we must have $F(x) \neq G(x)$. Thus $|\text{supp}(F)| + |\text{supp}(G)| = (p - 1)$.

We do the same for the Fourier transforms. The convolution condition gives $\hat{F}^2 = \hat{G}^2$ so that $\hat{F}\hat{G} \equiv 0$. By the same argument as above we conclude that $|\text{supp}(\hat{F})| + |\text{supp}(\hat{G})| \leq p$.

To prove the Theorem we define two functions, $F = f - g$ and $G = f + g$.

Note that $FG \equiv 0$ so that for each x at least one of $F(x), G(x)$ is 0. For $x = 0$ we have $F(0) = G(0) = 0$ and for $x \neq 0$ we must have $F(x) \neq G(x)$. Thus $|\text{supp}(F)| + |\text{supp}(G)| = (p - 1)$.

We do the same for the Fourier transforms. The convolution condition gives $\hat{F}^2 = \hat{G}^2$ so that $\hat{F}\hat{G} \equiv 0$. By the same argument as above we conclude that $|\text{supp}(\hat{F})| + |\text{supp}(\hat{G})| \leq p$.

Now consider:

$$S = |\text{supp}(F)| + |\text{supp}(G)| + |\text{supp}(\hat{F})| + |\text{supp}(\hat{G})|.$$

Then by the previous slide we know $S \leq (p-1) + p = 2p - 1$.

However, if neither $F, G \equiv 0$ then the uncertainty principle gives $S \geq 2(p+1)$. This is a contradiction, and hence either $F = f - g \equiv 0$ or $G = f + g \equiv 0$. Thus $f = \pm g$.

Now consider:

$$S = |\text{supp}(F)| + |\text{supp}(G)| + |\text{supp}(\hat{F})| + |\text{supp}(\hat{G})|.$$

Then by the previous slide we know $S \leq (p-1) + p = 2p - 1$.

However, if neither $F, G \equiv 0$ then the uncertainty principle gives $S \geq 2(p+1)$. This is a contradiction, and hence either $F = f - g \equiv 0$ or $G = f + g \equiv 0$. Thus $f = \pm g$.

Question

Can we classify other characters via convolution?

The answer is yes, but now we must use repeated convolutions.

Theorem

Let p be an odd prime and $d \mid p-1$. If $f, g : \mathbb{F}_p \to \mu_d \cup \{0\}$ are functions satisfying $\operatorname{supp}(f) = \operatorname{supp}(g) = \mathbb{F}_p^\times$ and $f^{\star d} = g^{\star d}$ then $f = \zeta_d^i g$ for some i.

Thank you for listening!