Proof of Fibonacci prime residue property

All primes p divide the $2p(p^2-1)$-th Fibonacci number.

Question taken from Napkin.

Oisín Davey

1 Proof

Theorem 1.1. $p \mid F_{2p(p^2-1)}$ where p is prime and F_n is the n-th Fibonacci number.

Define the Fibonacci group F like so: $\mathrm{F} \triangleq \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \in M^{2\times 2}\left(\mathbf{Z} \setminus p\mathbf{Z}\right) \middle| n \in \mathbf{N}_0 \right\}$

The group axioms hold trivially.

Note that $\det \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = (-1)^n$, and so $\det \Lambda = \pm 1 \ \forall \Lambda \in \mathrm{F}$

Define the alternate special linear group $\mathrm{SL}_n^{\pm}(\mathbf{Z} \setminus p\mathbf{Z})$ as $\left\{\Lambda \in M^{2\times 2}\left(\mathbf{Z} \setminus p\mathbf{Z}\right) \,\middle|\, \det \Lambda = \pm 1\right\}$

Again, the group axioms hold trivially.

$\mathrm{SL}_n^{\pm}(\mathbf{Z} \setminus p\mathbf{Z})$ is a supergroup of $\mathrm{SL}_n(\mathbf{Z} \setminus p\mathbf{Z})$. Define SL_Λ as the coset of $\mathrm{SL}_n(\mathbf{Z} \setminus p\mathbf{Z})$ with some Λ in the supergroup with determinant -1. I claim that this completes the extension.

Suppose, for sake of contradictiotn, that $\exists\ \Pi \in \mathrm{SL}_n^{\pm}(\mathbf{Z} \setminus p\mathbf{Z})$ which is not within $\mathrm{SL}_n(\mathbf{Z} \setminus p\mathbf{Z}) \cup \mathrm{SL}_\Lambda$. By definition $\det \Pi = \pm 1$, but we know $\det \Pi \neq 1$ by the supposition, so $\det \Pi = -1$.

Clearly, $\Pi = (\Pi\Lambda^{-1})\Lambda$, but $\det(\Pi\Lambda^{-1}) = \frac{\det \Pi}{\det \Lambda} = \frac{-1}{-1} = 1$. It follows that $\Pi\Lambda^{-1} \in \mathrm{SL}_n(\mathbf{Z} \setminus p\mathbf{Z})$, and so Π must be in the coset. By contradiction, the alternate special linear group can be formed as a single coset expansion of the special linear group. By Lagrange's theorem, it must then have double the order.

The order of the special linear group is $p(p^2-1)$, and so the order of the alternate special linear group is $2p(p^2-1)$. The Fibonacci group is a proper subgroup and so its order is a proper divisor of $2p(p^2-1)$, again by Lagrange's theorem.

The Fibonacci sequence modulo p is given by $F_n = \left[\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n\right]_{1,1} \mod p$.

The order of $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ is a divisor of the order of F, which is a divisor of $2p(p^2-1)$, so $F_{2p(p^2-1)}$ must have zero residue modulo p. QED.

2 Comments

There may be a much simpler proof of this theorem, but I wanted to use my knowledge of group theory here, and I'm a fan of the Fibonacci group. This proof isn't exactly verbose but it's more for me than anyone else so who cares! I was quite shocked to find that there is no accepted name for $\mathrm{SL}_n^{\pm}(\mathbf{Z} \setminus p\mathbf{Z})$, given how straightforward of a group it is.