Claim

$\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has a cyclic subgroup of order p^2-1.

Proof. Idea: construct a field $\mathbb{F}_{p^2}$ of order p^2 and identify $\mathbb{F}_{p^2}$ with $(\mathbb{Z}/p\mathbb{Z})^2$. Then $\mathrm{GL}_1(\mathbb{F}_{p^2}) \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and $\mathrm{GL}_1(\mathbb{F}_{p^2}) \cong C_{p^2-1}$ so we're done.

For $p=3$ we set $F_9 = (\mathbb{Z}/3\mathbb{Z}) + (\mathbb{Z}/3\mathbb{Z})i$ where $i^2=-1$. Also, lets denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$. Another way to see this is

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)\mathbb{F}_3[x]$$

We will prove in 494 that if k is a field and $p(x)$ is an irreducible polynomial then $k[x]/p(x)k[x]$ is a field. The key ideas are the same as the ideas used to prove $\mathbb{Z}/p\mathbb{Z}$ is a field–the division algorithm!!!

In general, if p is odd then the squaring map $\mathbb{F}_p \to \mathbb{F}_p$ is not injective because $(-1)^2 \equiv_p 1^2$, and so it cannot be surjective. Pick some $d \in \mathbb{F}_p$ without a square root. Then of course x^2-d is an irreducible polynomial (as it has no roots). We then take

$$\mathbb{F}_{p^2} \coloneqq \mathbb{F}_p[x]/(x^2-c)\mathbb{F}_p[x]$$

Every $f \in \mathbb{F}_p[x]$ can be written in exactly one way as

$$f(x) = q(x)\cdot(x^2-d) + r(x)$$

where $q, r \in \mathbb{F}_p[x]$ and $\deg r \leq 1$. Then each coset contains exactly one polynomial of degree ≤ 1. There are then p^2 ways to pick the coefficients and $\left|\mathbb{F}_{p^2}\right| = p^2$. (Note: $\mathbb{F}_{p^2} \cong C_p \times C_p$ as a group under addition).

Now we need the multiplication, both that it's well-defined and it is invertible. Start with

$$f_1(x) \equiv f_2(x) \mod x^2-d \quad g_1(x) \equiv g_2(x) \mod x^2-d$$

where $f_1, f_2, g_1, g_2 \in \mathbb{F}_p[x]$. Then we should show that $f_1(x)g_1(x) \equiv f_2(x)g_2(x) \mod x^2-d$. To do this we see that for some $A, B \in \mathbb{F}_p[x]$ we have

$$\begin{aligned} f_1(x) &= f_2(x) + (x^2-d)A(x) \\ g_1(x) &= g_2(x) + (x^2-d)B(x) \\ f_1(x)g_1(x) &= f_2(x)g_2(x) + (x^2-d)(f_2(x)B(x) + A(x)g_2(x)) + (x^2-d)^2A(x)B(x) \end{aligned}$$

And thus the multiplication is well-defined, commutative, associative, distributes with respect to addition, and has an identity element 1 because these hold in $\mathbb{F}_p[x]$.

Now we show it has multiplicative inverses. This is clear for nonzero elements of $\mathbb{F}_p$. Now we want to find the inverse of $c+\overline{x}$, where $\overline{x}$ is the image of x in $\mathbb{F}_{p^2}$. Well

$$(c+\overline{x})(c-\overline{x}) = c^2 - \overline{x}^2 = c^2 - d \in \mathbb{F}_p$$

and this is nonzero as d is not a square in $\mathbb{F}_p$. We then have that

$$(c+\overline{x})\cdot\frac{c-\overline{x}}{c^2-d} = 1$$

Similarly, $a + b\overline{x}$ has an inverse in $\mathbb{F}_{p^2}$ for $b \neq 0$, as we can multiply by b^{-1} and then multiply by the inverse of $\frac{a}{b} + \overline{x}$.

Proposition .0.1

If k is a finite field with n elements then $k^\times$ is a cyclic group of order $n-1$.

Proof. Fact: In $k[x]$ for any field k a degree-n polynomial has at most n roots. The reason being that for c a root

$$f(x) = (x-c)g(x) + r$$

where $r \in \mathbb{F}_p$, this implies since $f(c) = 0$ that $r = 0$. Then if $c \neq c'$ and $f(c) = f(c')$ then

$$f(c') = (c'-c)g(c')$$

And so $g(c') = 0$, and we can factor it as well. Because degrees add when multiplying this implies the fact.

In C_{n-1} all elements have order dividing $n-1$, and the # of elements of order dividing d (for any d dividing $n-1$) is d.

In $k^\times$, all elements have order dividing $n-1$, and if $d \mid n-1$ then every $c \in k^\times$ of order dividing d is a root of $x^d - 1$. But this means there are at most d elements of order dividing d in $k^\times$.

Now we just compare.

C_{n-1}	Both	$k^\times$
	size $= n-1$	
	all elements have order dividing $n-1$	
exactly d elements of order dividing d		at most d elements of order dividing d

It follows that C_{n-1} and $k^\times$ have the same number of elements of each order. Thus $k^\times$ has an element of order $n-1$ and hence is cyclic.