for p a prime, $\mathbb{Z}_p^*$ is cyclic

To establish the result of the title, we need three facts. First:

Fermat's Little Theorem: If p is prime and $(a,p)=1$, then $p|a^{p-1}-1$ (i.e., $a^{p-1}\equiv_p 1$).

Main ingredients:

(1) If p is prime, $(a,p)=1$, and $ab\equiv_p ac$, then $b\equiv_p c$

[multiply both sides by a^{-1}]

(2) If $(a,n)=1$ and $(b,n)=1$, then $(ab,n)=1$

[multiply the equations $1=ax+ny$ and $1=bz+nw$ together and collect multiples of n together]

Then to prove FLT, look at $N=(p-1)!a^{p-1}=(1\cdot a)(2\cdot a)\cdots((p-1)\cdot a)$.

If we show that $N\equiv_p (p-1)!$, then since $((p-1)!,p)=1$ (by (2) and induction), we have $a^{p-1}\equiv_p 1$ by (1). But, again by (1), if $xa\equiv_p ya$ then $x\equiv_p y$, so each of $1\cdot a, 2\cdot a,\ldots,(p-1)\cdot a$ are distinct, mod p. That is, this list is the same, mod p, as $1,2,\ldots,p-1$, except for possibly being written in a different order. But then the products of the two lists are the same (mod p), as desired.

FLT tells us that $a^{p-1}\equiv 1 \pmod p$ is always true, when p is prime. In the language of groups, this means that the order of any $a\in\mathbb{Z}_p^*$ with $a\neq 0$ has order dividing $p-1=|\mathbb{Z}_p^*|$. To establish that $\mathbb{Z}_p^*$ is cyclic, we need to show that at least one of them has order <u>equal</u> to $p-1$. In order to show this, we need a bit more machinery:

Lagrange's (other) Theorem: If $f(x)$ is a polynomial with integer coefficients, of degree n, and p is prime, then the equation $f(x)\equiv 0 \pmod p$ has at most n mutually incongruent solutions, unless $f(x)\equiv 0 \pmod p$ for <u>all</u> x.

To see this, do what you would do if you were proving this for real or complex roots; given a solution a, write $f(x)=(x-a)g(x)+r$ with r=constant (where we understand this equation to have coefficients in $\mathbb{Z}_p$) using polynomial long division. This makes sense because $\mathbb{Z}_p$ is a *field*, so division by non-zero elements works fine. Then $0=f(a)=(a-a)g(a)+r=r$ means $r=0$ in $\mathbb{Z}_p$, so $f(x)=(x-a)g(x)$ with $g(x)$ a polynomial with degree $n-1$. Structuring this as an induction argument, we can then assume that $g(x)$ has at most $n-1$ roots, so f has at most (a and the roots of g, so) n roots, because, *since p is prime*, if $f(b)=(b-a)g(b)\equiv 0 \pmod p$, then either $b-a\equiv 0$ (so a and b are congruent mod p), or $g(b)=0$, so b is among the roots of g. [This is because $p|xy$ and p prime implies that $p|x$ or $p|y$.]

This in turn leads us to

Corollary: If p is prime and d is a factor of $p-1$ (i,e, $d|p-1$), then the equation $x^d-1\equiv 0 \pmod p$ has *exactly* d solutions mod p.

This is because, writing $p-1=ds$, $f(x)=x^{p-1}-1\equiv 0$ has exactly $p-1$ solutions (namely, 1 through $p-1$), and

$$x^{p-1}-1==(x^d-1)(x^{d(s-1)}+x^{d(s-2)}+\cdots+x^d+1)=(x^d-1)g(x)\ .$$

But $g(x)$ has *at most* $d(s-1) = (p-1) - d$ roots, and $x^d - 1$ has at most d roots, and together (since p is prime) they make up the $p-1$ roots of f. So in order to have enough, they both must have *exactly* that many roots.

To finish our proof that for p prime, there must be an a with $\mathrm{ord}_p(a) = p-1$: we introduce the notation $p^k||N$, which means that $p^k|N$ but $p^{k+1} \not| N$.

For each prime p_i dividing $p-1$, $1 \leq i \leq s$, we let $p_i^{k_i}||p-1$. So $p-1 = p_1^{k_1} \cdots p_r^{k_r}$. Then:

the equation (*) $x^{p_i^{k_i}} \equiv 1 \pmod p$ has $p_i^{k_i}$ solutions, while

(†) $x^{p_i^{k_i-1}} \equiv 1 \pmod p$ has only $p_i^{k_i-1} < p_i^{k_i}$ solutions.

Pick a solution, a_i, to (*) which is not a solution to (†) . [In particular, $\mathrm{ord}_n(a_i) = p_i^{k_i}$, since if it were smaller, it would have to divide $p_i^{k_i-1}$, which, by our choice of a_i, it doesn't!] Then set $a = a_1 \cdots a_r$. Then a computation yields that, mod p, $(a_1 \cdots a_r)^k = a_1^k \cdots a_r^k$, and $a_j^{\frac{p-1}{p_i}} \equiv_p 1$ for $j \neq i$, since $p_j^{k_j} | \frac{p-1}{p_i}$. This implies that

$$a^{\frac{p-1}{p_i}} \equiv a_i^{\frac{p-1}{p_i}} \not\equiv 1,$$

since otherwise $\mathrm{ord}_p(a_i) | \dfrac{p-1}{p_i}$, and so $\mathrm{ord}_p(a_i) | \gcd(p_i^{k_i}, \dfrac{p-1}{p_i}) = p_i^{k_i-1}$, a contradiction. So $p_i^{k_i}||\mathrm{ord}_n(a)$ for every i, so $p-1|\mathrm{ord}_p(a)$, so $\mathrm{ord}_p(a) = p-1$.

Actually finding a primitive root a for $\mathbb{Z}_p^*$ is a much more challenging task than proving one exists! The above procedure will do it, but you need to completely factor $p-1$ in order to find the a_i and then assemble the resulting product a. In practice, if you can factor $p-1$ completely, what one really does is start with $a = 2$, and compute $a^{\frac{p-1}{p_i}} \pmod p$ for every prime factor p_i of $p-1$. If the result is never 1, then we know that the order or a is $p-1$ and so $\mathbb{Z}_p^* = \langle a \rangle$. In practice it doesn't require too many attempts with (small) numbers relatively prime to p before this stumbles across a generator for $\mathbb{Z}_p^*$ ....