

For $n = 1$, p arbitrary, $M = 1$, $v = 1$, does the job. So from now on, assume $n \geq 2$, and that M and v give an appropriate G . The condition says that starting from 0 and applying G several times, we obtain all elements of $V = \mathbb{F}_p^n$.

Step 1. M is invertible. Indeed, otherwise, $|\text{im } M| < p^n$. Then for $k \geq 1$, $G^{(k)}(0) \in \text{im } M + v$, which has cardinality less than p^n , a contradiction.

Then $Gx = u$ can be solved for any u , indeed, $x = M^{-1}(u - v)$ is the solution. This shows that $G^{(p^n)}(0) = 0$ and for $0 < i < p^n$, $G^{(i)}(0) \neq 0$. Then the sequence $G^{(i)}(0)$ of i has period p^n .

Step 2. $M - \text{id}$ is not invertible. Indeed, otherwise $Gx = x$ has the solution $x = (M - \text{id})^{-1}(-v)$, so after getting x , we stay at x , a contradiction.

Step 3. There are no proper subspaces U_1, U_2 with the properties $V = U_1 \oplus U_2$, U_1, U_2 are invariant under M . Assume not. Then let $M = M_1 + M_2$, $v = v_1 + v_2$, $G = G_1 + G_2$ be the decompositions with respect to $U_1 \oplus U_2$. Denote by k_1 the smallest positive number such that $G^{(k_1)}(0) = 0$, and define similarly k_2 . Since $|U_1|, |U_2| < p^n$, $k_1, k_2 < p^n$. Then $\text{lcm}(k_1, k_2) < p^n$, and $G^{(\text{lcm}(k_1, k_2))}(0) = 0$ shows a contradiction.

Step 4. The minimal polynomial q of M is $(1 - x)^k$. We know that the minimal polynomial has a factor $(1 - x)$, since $M - \text{id}$ is not invertible (recall the Jordan normal form in the algebraic closure). We prove below that if q could be factorized as $q = q_1 q_2$, where $\text{gcd}(q_1, q_2) = 1$, then there would be an invariant subspace decomposition, which would lead to a contradiction. Then $q(x)$ must be $(1 - x)^k$, indeed.

Assume hence $q = q_1 q_2$ with $\text{gcd}(q_1, q_2) = 1$. We claim $V = \ker q_1(M) \oplus \ker q_2(M)$. First, $\ker q_1(M) \supseteq \text{im } q_2(M)$, which is trivial: for any $u \in V$, $0 = q(M)u = q_1(M)q_2(M)u$, and $q_2(M)u$ runs through $\text{im } q_2(M)$. Similarly, $\ker q_2(M) \supseteq \text{im } q_1(M)$. Now we prove that (a) $\ker q_1(M) \cap \ker q_2(M) = \{0\}$, and (b) $\text{im } q_1(M) + \text{im } q_2(M) = V$. To see this, take polynomials r_1, r_2 such that $q_1 r_1 + q_2 r_2 = 1$. Then if $u \in \ker q_1(M) \cap \ker q_2(M)$, then $0 = r_1(M)q_1(M)u + r_2(M)q_2(M)u = u$ shows (a); and for any $u \in V$, $u = q_1(M)r_1(M)u + q_2(M)r_2(M)u$, the first term is in $\text{im } q_1(M)$, the second is in $\text{im } q_2(M)$, which shows (b). Then $\ker q_1(M) = \text{im } q_2(M)$, $\ker q_2(M) = \text{im } q_1(M)$. Since kernels are invariant, images are nonzero, we have a proper invariant subspace decomposition, so we are done. (This is a highly standard argument, but I decided to work out the details for your convenience!)

So the minimal polynomial is $(1 - x)^k$, then the characteristic polynomial is $(1 - x)^n$ (in the Jordan normal form in the algebraic closure, every block has diagonal $(1, \dots, 1)$). Then $M = \text{id} + N$, where $N^n = 0$.

Step 5. We prove $p^{n-2} < n$ by contradiction. Assume $p^{n-2} \geq n$. Then $M^{p^{n-2}} = I^{p^{n-2}} + N^{p^{n-2}} = I$. Therefore,

$$\begin{aligned} G^{(p^{n-1})}(0) &= M^{p^{n-1}-1}v + \dots + Mv + v \\ &= (M^{(p-1)p^{n-2}} + M^{(p-2)p^{n-2}} + \dots + M^{p^{n-2}} + \text{id})(M^{p^{n-2}-1} + \dots + M + \text{id})v \\ &= 0, \end{aligned}$$

which is a contradiction.

Step 6. $p^{n-2} < n$. This holds in the cases (A) $n = 2$, (B) $n = 3$, $p = 2$.

Case (A). Since there is no proper invariant subspace decomposition, $M \neq \text{id}$, hence in a suitable basis, $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Assume that in this basis $v = \begin{pmatrix} a \\ b \end{pmatrix}$. By induction, $M^i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$, so $M^i v = \begin{pmatrix} a+ib \\ b \end{pmatrix}$. Then

$$G^{(k)}(0) = \sum_{i=0}^{k-1} \begin{pmatrix} a+ib \\ b \end{pmatrix} = \begin{pmatrix} ka + \frac{k(k-1)}{2}b \\ kb \end{pmatrix}.$$

Therefore, if $p > 2$, $G^{(p)}(0) = 0$, and it is easy to check that for $p = 2$, $v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ does the job. So in the case $n = 2$, only $p = 2$ gives a solution.

Case (B). Again, since there is no proper invariant subspace decomposition, in a suitable basis, $M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Assume that in this basis $v = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. It is easy to check that $Mv = \begin{pmatrix} a+b \\ b+c \\ c \end{pmatrix}$, $M^2v = \begin{pmatrix} a+c \\ b \\ c \end{pmatrix}$, $M^3v = \begin{pmatrix} a+b+c \\ b+c \\ c \end{pmatrix}$, showing that $G^{(4)}(0) = (M^3 + M^2 + M + \text{id})v = 0$, that is, no solution here.

To sum up, there are appropriate M and v if and only if ' $n = 1$ and p is arbitrary' or ' $n = p = 2$ '.