Theorem. Let R be a ring with multiplicative identity e whose additive group is a free module over $\mathbb{Z}/n\mathbb{Z}$. Then R has a $\mathbb{Z}/n\mathbb{Z}-$basis containing e.

Proof. Let $\{b_i\}_{i\in I}$ be a basis of R, then every element in R can be uniquely written as $x=\sum_{i\in I}x_ib_i$[i], where $0\le x_i<n$, all but finitely many x_i are zero. In particular, write $e=\sum_{i\in I}e_ib_i$.

Let $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ be the canonical factorization of n. We first show that for each $1\le j\le k$, there exists $i_j\in I$ such that p_j does not divide e_{i_j}. Suppose otherwise that p_j divides e_i for all $i\in I$, then there exists $a\in R$ such that $p_ja=e$. For every $x\in R$, we have $\dfrac{n}{p_j}x=e\cdot\dfrac{n}{p_j}x=(p_ja)\cdot\dfrac{n}{p_j}x=nax=0$. In particular, fix $i_0\in I$, we have $\dfrac{n}{p_j}b_{i_0}=0_R$, then 0_R is not a unique linear combination of $\{b_i\}_{i\in I}$, a contradiction.

For each $1\le j\le k$, pick $i_j\in I$ such that p_j does not divide e_{i_j}. Fix $\gamma\in I$. Now construct $\{c_i\}_{i\in I}$ as follows: $c_\gamma=e$; for $i\in I, i\ne\gamma$, $c_i=s_ib_i+t_ib_\gamma$, where $0\le s_i,t_i<n$ satisfy the conditions

$$s_i\equiv\begin{cases}1, & i\ne i_j\\ 0, & i=i_j\end{cases}\pmod{p_j^{a_j}},\quad t_i\equiv\begin{cases}0, & i\ne i_j\\ 1, & i=i_j\end{cases}\pmod{p_j^{a_j}}.$$

We show that $\{c_i\}_{i\in I}$ is a basis. First, for $x\in R$, write $x=\sum_{i\in I}x_ib_i$. For each $i\in I$, pick $0\le y_i<n$ satisfying the condition

$$y_i\equiv\begin{cases}x_i-e_i\dfrac{x_{i_j}}{e_{i_j}}, & i\ne i_j,\gamma\\ \dfrac{x_{i_j}}{e_{i_j}}, & i=\gamma\\ x_\gamma-e_\gamma\dfrac{x_{i_j}}{e_{i_j}}, & i=i_j\ne\gamma\end{cases}\pmod{p_j^{a_j}},$$

Consider $\sum_{i\in I}y_ic_i$, which expands to

$$\begin{aligned}\sum_{i\in I}y_ic_i&=y_\gamma e+\sum_{i\in I,i\ne\gamma}y_i(s_ib_i+t_ib_\gamma)\\&=y_\gamma\sum_{i\in I}e_ib_i+\sum_{i\in I,i\ne\gamma}y_i(s_ib_i+t_ib_\gamma)\\&=(y_\gamma e_\gamma+\sum_{i\in I,i\ne\gamma}y_it_i)b_\gamma+\sum_{i\in I,i\ne\gamma}(y_\gamma e_i+y_is_i)b_i.\end{aligned}$$

It is easy to show that for $1\le j\le k$, $y_\gamma e_\gamma+\sum_{i\in I,i\ne\gamma}y_it_i\equiv x_\gamma\pmod{p_j^{a_j}}$ and $y_\gamma e_i+y_is_i\equiv x_i\pmod{p_j^{a_j}}, i\in I, i\ne\gamma$.[ii] Hence we have $y_\gamma e_\gamma+\sum_{i\in I,i\ne\gamma}y_it_i\equiv x_\gamma\pmod{n}$ and $y_\gamma e_i+y_is_i\equiv x_i\pmod{n}, i\in I, i\ne\gamma$, and it follows that $x=\sum_{i\in I}y_ic_i$.

Moreover, if $\sum_{i\in I}z_ic_i=0_R$, then we have $z_\gamma e_\gamma+\sum_{i\in I,i\ne\gamma}z_it_i\equiv 0\pmod{p_j^{a_j}}$, $z_\gamma e_i+z_is_i\equiv 0\pmod{p_j^{a_j}}, i\in I, i\ne\gamma$. It is not hard to see that these conditions imply that $z_i\equiv 0\pmod{p_j^{a_j}}$ for all $i\in I, 1\le j\le k$[ii], so $z_i\equiv 0\pmod{n}$ for all $i\in I$, and $\{c_i\}_{i\in I}$ are linearly independent. Then we reach the conclusion that $\{c_i\}_{i\in I}$ is a basis of R containing e. ∎

[i] There is a unique way to define scalar multiplication of $\mathbb{Z}/n\mathbb{Z}$ and R, namely for $0\le m<n$, $[m]x=(\underbrace{[1]+[1]+\cdots+[1]}_{m\text{ times}})x=\underbrace{[1]x+[1]x+\cdots+[1]x}_{m\text{ times}}=\underbrace{x+x+\cdots+x}_{m\text{ times}}=mx$. We shall not distinguish accumulated sums and scalar multiplications in the proof.

[ii] There are two cases: $i_j\ne\gamma$ and $i_j=\gamma$.