RSA encryption

Problem 182

The RSA encryption is based on the following procedure:

Generate two distinct primes p and q.
Compute $n=pq$ and $\varphi=(p-1)(q-1)$.
Find an integer e, $1<e<\varphi$, such that $\gcd(e,\varphi)=1$.

A message in this system is a number in the interval $[0,n-1]$.
A text to be encrypted is then somehow converted to messages (numbers in the interval $[0,n-1]$).
To encrypt the text, for each message, m, $c=m^e \bmod n$ is calculated.

To decrypt the text, the following procedure is needed: calculate d such that $ed=1 \bmod \varphi$, then for each encrypted message, c, calculate $m=c^d \bmod n$.

There exist values of e and m such that $m^e \bmod n=m$.
We call messages m for which $m^e \bmod n=m$ unconcealed messages.

An issue when choosing e is that there should not be too many unconcealed messages.
For instance, let $p=19$ and $q=37$.
Then $n=19*37=703$ and $\varphi=18*36=648$.
If we choose $e=181$, then, although $\gcd(181,648)=1$ it turns out that all possible messages
m $(0\le m\le n-1)$ are unconcealed when calculating $m^e \bmod n$.
For any valid choice of e there exist some unconcealed messages.
It's important that the number of unconcealed messages is at a minimum.

Choose $p=1009$ and $q=3643$.
Find the sum of all values of e, $1<e<\varphi(1009,3643)$ and $\gcd(e,\varphi)=1$, so that the number of unconcealed messages for this value of e is at a minimum.