M328K Homework 8

Joshua Dong

March 31, 2014

0.1 6.1.16

Show that if n is a composite integer with $n \neq 4$, then $(n-1)! \equiv 0 \pmod{n}$

If n is composite, then there two possibilities:
Case 1:
There exist different prime integers a and b where $ab = n$ and $2 \leq a < b \leq n-2$.
Both a and b are in the product $(ab-1)!$.
Therefore $(ab-1)!$ is divisible by ab.

Case 2:
If n cannot be expressed as a product of two different primes, then n is a square where $n = p^2$.
p appears in the factorial product of $(n-1)!$, therefore $p \mid (n-1)!$.
We can say $2p \mid (n-1)!$ if $2p < n$, which is true for all squares where $n \neq 4$.
If $2p \mid (n-1)!$ and $p \mid (n-1)!$, then $2p^2 \mid (n-1)!$.
Therefore $2n \mid (n-1)!$.
Therefore $n \mid (n-1)!$.

Therefore, $(n-1)! \equiv 0 \pmod{n}$ for all composites n, $n \neq 4$.

0.2 6.1.22

Show that $30 \mid (n^9 - n) \;\; \forall n \in \mathbb{Z}^+$.
$(n^9 - n) = n(n-1)(n+1)(n^2+1)(n^4+1)$
If we can show that $30 \mid n(n-1)(n+1)(n^2+1)$,
then $30 \mid n(n-1)(n+1)(n^2+1)(n^4+1)$.
If we can show that 2, 3, and 5 divide $n(n-1)(n+1)(n^2+1)$,
then 30 divides $n(n-1)(n+1)(n^2+1)$.
$n(n-1)$ is always even (the product of an even and odd is odd).
Therefore 2 divides $n(n-1)(n+1)(n^2+1) \;\; \forall n \in \mathbb{Z}^+$.

$n(n-1)(n+1)$ forms a sequence of three consecutive integers.
Therefore, one of them must divide 3 (this could be shown with an enumeration of possibilities)
Therefore 3 divides $n(n-1)(n+1)(n^2+1) \;\; \forall n \in \mathbb{Z}^+$.

Suppose 5 does not divide $k(k-1)(k+1)$.
k must then be in the form $5t+2$ or $5t+3$ for some $t \in \mathbb{Z}^+$, as a form of $5t+0$, $5t+1$, or $5t+4$ would result in the product having a term divisible by 5.
If k is in the form $5t+2$ or $5t+3$, then (k^2+1) is in the form $25t+4+1$ or $25t+9+1$, both which are divisible by 5.
Therefore 5 divides $n(n-1)(n+1)(n^2+1) \;\; \forall n \in \mathbb{Z}^+$.

Therefore 30 divides $(n^9 - n) \;\; \forall n \in \mathbb{Z}^+$.
However, it is worth noting that if $n < 2$, then the product is 0.

0.3 6.3.4

Show that if $a, m \in \mathbb{Z}^+$, $(a, m) = (a-1, m) = 1$, then $1 + a + a^2 + ... + a^{\phi(m)-1} \equiv 0 \pmod{m}$.

We split the proof into two cases.
Case 1: m is prime.
$\phi(m) = m - 1$.
$\therefore$ there are m-1 terms in the sequence.
If we can show that the series forms a complete set of residues modulo m (the 0 term is omissible), then that is sufficient to prove the assertion, as the sum of all residues is 0 modulo m.
We can rewrite each term with respect to the reverse index i from $a^{\phi(m)-i}$ to $\bar{i}$.
$\bar{i}$ exists because m is prime, and is unique for each i.
Therefore, for prime moduli m, the sum is equivalent to 0 modulo m.
Case 2: m is composite.

0.4 6.3.10

–