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 $30 \mid (n^9 - n) \ \ \forall n \in \mathbb{Z}^+$.

$2, 3, 5 \mid n(n-1)(n+1)(n^2+1) \rightarrow$
$30 \mid n(n-1)(n+1)(n^2+1) \rightarrow$
$30 \mid n(n-1)(n+1)(n^2+1)(n^4+1) \rightarrow$
$30 \mid (n^9 - n)$.

$n(n-1)$ forms a sequence of three consecutive integers.
Therefore, one of them must divide 2 (this could be trivially shown with an enumeration of possibilities in the form $2q + r$).
$\therefore 2 \mid n(n-1)(n+1)(n^2+1) \ \ \forall n \in \mathbb{Z}^+$.

$n(n-1)(n+1)$ forms a sequence of three consecutive integers.
We can use the same argument we used to prove divisibility by two.
$\therefore 3 \mid n(n-1)(n+1)(n^2+1) \ \ \forall n \in \mathbb{Z}^+$.

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.
$\therefore 5 \mid n(n-1)(n+1)(n^2+1) \ \ \forall n \in \mathbb{Z}^+$.

$\therefore 30 \mid (n^9 - n) \ \ \forall n \in \mathbb{Z}^+$.
(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 $1 + a + a^2 + ... + a^{\varphi(m)-1} \equiv 0 \pmod{m}$.

Let $x \in \mathbb{Z}$ where $x = 1 + a + a^2 + ... + a^{\varphi(m)-1}$
$ax = a + a^2 + ... + a^{\varphi(m-1)} + a^{\varphi(m)}$
$ax + 1 = 1 + a + a^2 + ... + a^{\varphi(m-1)} + a^{\varphi(m)}$
$ax + 1 = x + a^{\varphi(m)}$
$x = \frac{a^{\varphi(m)}-1}{a-1}$
$1 + a + a^2 + ... + a^{\varphi(m)-1} \equiv \frac{a^{\varphi(m)}-1}{a-1} \pmod{m}$
$\frac{a^{\varphi(m)}-1}{a-1} \equiv \frac{1-1}{a-1} \equiv 0 \pmod{m}$, by Euler's totient theorem, given $a > 1$.
$\therefore 1 + a + a^2 + ... + a^{\varphi(m)-1} \equiv 0 \pmod{m} \ \ \forall a, m \in \mathbb{Z}^+$, $(a, m) = (a-1, m) = 1$.

0.4 6.3.10

Show that $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ given $a \perp b$.

$a^{\varphi(b)} + b^{\varphi(a)} - 1 \equiv b^{\varphi(a)} - 1 \equiv 0 \pmod{a}$ by Euler's totient theorem ($a \perp b$).
Without loss of generality, $a^{\varphi(b)} + b^{\varphi(a)} - 1 \equiv 0 \pmod{b}$.
$\therefore a^{\varphi(b)} + b^{\varphi(a)} - 1 \equiv 0 \pmod{ab}$.
$\therefore a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ for all coprime integers a and b.