MATH 236: Discrete Mathematics with Applications

TUTORIAL 5: 11 March, 2011

1. Calculate each of the following.
   (a) $\phi(10), \phi(11), \cdots, \phi(20)$
   (b) $\phi(243)$
   (c) $\phi(150)$
   (d) $\phi(475)$
   (e) $\phi(159)$.
2. Use the Fermat's Little Theorem to find the remainder when
   (a) 5^{150} is divided by 7
   (b) $3^{9,999,999}$ is divided by 7
3. Use Euler's Theorem to find.
   (a) 22^{-1} in $\mathbb{Z}_{39}$
   (b) 4^{-1} in $\mathbb{Z}_{19}$
   (c) $x \in \mathbb{Z}_6$ such that $5x \equiv 4(\text{mod } 6)$.
4. Use the square and multiply algorithm to find each of the following.
   (a) $6^{13}(\text{mod } 17)$
   (b) $47^{53}(\text{mod } 71)$
5. Prove the following:
   (a) For all integers a, b and c, if $\gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.
   (b) For all integers a, b, c and n, if $\gcd(c, n) = 1$ and $ac \equiv bc(\text{mod n})$, then $a \equiv b(\text{mod n})$.
   (c) For all integers a, b, c and n, where $n \geq 2$ and $\gcd(a, n) = 1$, if $ab \equiv c(\text{mod n})$, then $b \equiv a^{-1}c(\text{mod n})$, where a^{-1} is the multiplicative inverse of a in $\mathbb{Z}_n$.
   (d) For all integers a, b and n, where $n \geq 2$, if $a \equiv 1(\text{mod n})$, then $b \equiv ab(\text{mod n})$.
6. For each integer n below:
   (i) Find the elements of $\mathbb{Z}_n^*$
   (ii) Determine the multiplication table of $\mathbb{Z}_n^*$
   (iii) Determine which elements of $\mathbb{Z}_n^*$ are generators.
   (a) $n = 4$
   (b) $n = 7$
   (c) $n = 16$.
7. Verify that 2 generates $\mathbb{Z}_{37}^*$.
8. Determine a generator of $\mathbb{Z}_{17}^*$.