MATH 356-01
Solutions to Homework Assignment 5

4.16 (a) $\varphi(7) = 6$, so $3^{27} \equiv 3^{27 \mod 6} \equiv 3^3 \equiv 27 \equiv 6 \pmod 7$.

(b) $\varphi(11) = 10$, so $8^{426} \equiv 8^{426 \mod 10} \equiv 8^6 \equiv 3 \pmod{11}$.

(c) $\varphi(55) = 4 \cdot 10 = 40$, so $12^{682} \equiv 12^{682 \mod 40} \equiv 12^2 \equiv 34 \pmod{55}$.

(d) $\varphi(187) = 10 \cdot 16 = 160$, so $18^{735417} \equiv 18^{735417 \mod 160} \equiv 18^{57} \equiv (18^3)^{19} \equiv 35^{19} \equiv (35^4)^4 \cdot 35^3 \equiv 137^4 \cdot 52 \equiv 171 \pmod{187}$.

4.18 (a) This cannot be a subgroup since it lacks 0.

(b) This could be a subgroup. (In fact, it is.)

(c) This cannot be a subgroup since $4 \not| 9$ (Lagrange's Theorem).

4.32 If p is prime, then by Fermat's Little Theorem, $a^p \equiv a \pmod p$. By Wilson's Theorem, $(p-1)! \equiv -1 \pmod p$. Tuhs $a^p + (p-1)!a \equiv a - a \equiv 0 \pmod p$, so $p | a^p + (p-1)!a$.

4.33 Note that $42 = 2 \cdot 3 \cdot 7$. Since 2 is prime, $a^2 \equiv a \pmod 2$, so $a^7 = a^2a^2a^2a \equiv a \cdot a \cdot a \cdot a \equiv a^2a^2 \equiv a \cdot a \equiv a^2 \equiv a \pmod 2$. Similarly, $a^7 \equiv a^3a^3a \equiv a \cdot a \cdot a \equiv a^3 \equiv a \pmod 3$, and $a^7 \equiv a \pmod 7$. Thus, for each $p \in 2, 3, 7$, $a^7 \equiv a \pmod p$, which is to say, $p | (a^7 - a)$. Since 2, 3, and 7 are relatively prime, we get $2 \cdot 3 \cdot 7 | a^7 - a$, so $42 | a^7 - a$ for all $a \in \mathbb{Z}$.

4.35 (Reflexive) Since G is a group, for $a \in G, a^{-1} \in G$ as well. Since $H \leq G$, $1 \in H$, so $aa^{-1} = 1 \in H$; thus, $a \sim a$.

(Symmetric) Suppose $a \sim b$. Then $ab^{-1} \in H$. Since H is itself a group, $(ab^{-1})^{-1} = ba^{-1} \in H$, so $b \sim a$.

(Transitive) Suppose $a \sim b$ and $b \sim c$. Then $ab^{-1}, bc^{-1} \in H$, so $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$ by closure, and $a \sim c$.

Since $\sim$ is reflexive, symmetric, and transitive, it is an equivalence relation.