I have been asked to write up solutions to problems 10 and 16 in §3.2 and problem 7, 9 and 10 in §3.3.  

**Problem 10 of §3.2:** Consider the map \( \alpha : G/(H \cap K) \to G/H \) sending \( g(H \cap K) \) to \( gH \); this is well defined because \( H \cap K \) is a subgroup of \( H \). Similarly, there’s a map \( \beta : G/(H \cap K) \to G/K \). The map \( \alpha \times \beta : G/(H \cap K) \to G/H \times G/K \) is injective because an element of \( G \) that is in both \( H \) and \( K \) is in \( H \cap K \). Note that these maps are merely maps of sets because \( H \) and \( K \) were not assumed to be normal. The target set \( G/H \times G/K \) has \( mn \) elements, so \( G/(H \cap K) \) has at most \( mn \) elements. The map \( \alpha \) is clearly surjective. The elements of \( G/(H \cap K) \) that map to a given element \( gH \) of \( G/H \) are the cosets \( gh(H \cap K) \) with \( h \) running through \( H \). These are in bijection (under the map “multiplication by \( g \)” with the cosets \( h(H \cap K) \), i.e., with the elements of the quotient \( H/(H \cap K) \). Hence the index \( (G : H \cap K) \) may be written \( (G : H) \cdot (H : H \cap K) \); this is something that we probably knew before! Hence \( (G : H \cap K) \) is divisible by \( m \); analogously, it is divisible by \( n \). Hence it is divisible by the least common multiple of \( m \) and \( n \); in particular, it is at least as big as this lcm.

**§3.2, problem 16:** Take an integer \( a \) and suppose first that \( a \) is prime to \( p \). If \( g \) is the image of \( a \) in \((\mathbb{Z}/p\mathbb{Z})^*\), then the order of \( g \) divides \( p - 1 \). This follows from the general statement that if \( g \) is an element of a finite group \( G \), then the order of \( g \) divides the order of \( G \). Indeed, the order of \( g \) is the order of the cyclic subgroup \( \langle g \rangle \) generated by \( g \), and this order divides the order of \( G \) by Lagrange’s theorem. In our specific application, the order of \( g \) divides \( p - 1 \), so that \( g^{p-1} = 1 \) in \((\mathbb{Z}/p\mathbb{Z})^*\). In terms of congruences, this statement means that we have \( a^{p-1} \equiv 1 \mod p \). We get the required congruence \( a^p \equiv a \mod p \) by multiplying both sides by \( a \). If \( a \) is now not prime to \( p \), then \( a \mod p = 0 \), and the congruence \( a^p \equiv a \mod p \) holds for trivial reasons. This congruence holds then for all integers \( a \).

**Problem 7 of §3.3:** Consider the homomorphism \( \varphi \) from \( G \) to \( G/M \times G/N \) that sends \( g \in G \) to \((gM, gN)\). The kernel of this homomorphism is the set of \( g \) that are in both \( M \) and \( N \); it is \( M \cap N \). Thus the image of \( \varphi \) may be identified with \( G/(M \cap N) \). We need to show that this image is all of \( G/M \times G/N \), i.e., that \( \varphi \) is surjective. A typical element of \( G/M \times G/N \) is \((xM, yN)\) for some \( x, y \in G \). This is the product \((xM,N) \cdot (M,yN)\). It suffices to show that both factors are in the image. Since \( G = MN \), we can write \( y = mn \) with \( m \in M \), \( n \in N \). Then \((M,yN) = (M,mnN) = (M,mN) = (mM,mN) = \varphi(m)\). Similarly we have \( G = NM \) because of the normality. Write \( x = n'm' \); then \((xM,N) = (n'M,n'N) = \varphi(n')\).

**#9 of §3.3:** Let’s say that the \( p \)-part of a positive integer is the highest power of \( p \) dividing that integer. The \( p \)-part of the order of \( G \) is \( p^a \), for instance. Consider the subgroup \( PN \). The \( p \)-part of its order is at least \( p^a \) (the order of \( P \)) but also at most \( p^a \), which is the
$p$-part of the order of $G$. Hence the $p$-part of the order of $PN$ is $p^a$. Now the order of $PN$ is $\#(P)\#(N)/\#(P \cap N)$. Looking at $p$-parts, we see that the $p$-part of the order of $P \cap N$ coincides with the $p$-part of the order of $N$, which is $p^b$ (by definition). Since $P \cap N$ is a subgroup of $P$, its order is actually a power of $p$. Hence the order of $P \cap N$ is $p^b$, which is one thing that we were supposed to prove. For the other, look at the isomorphism $P/(P \cap N) \sim PN/N$. The order of $PN/N$ is seen to be $p^{a-b}$ because the orders of $P$ and $P \cap N$ are $p^a$ and $p^b$, respectively.

§3.3, Problem 10: We are given, for each prime $p$, that if $p$ divides $|H|$, then $|H|$ is divisible by the $p$-part of $|G|$. We have to prove the same statement for $H \cap N$ relative to $N$ and for $HN/N$ relative to $G/N$. If $p$ does not divide the order of $H$, then $p$ does not divide the order of $N \cap H$; also, $p$ does not divide the order of $HN/N$, which is a quotient of $H$. (It is $H/(H \cap N)$.) Assume now that $p$ does divide the order of $H$. Then the $p$-part of the order of $H$ coincides with the $p$-part of the order of $G$, which we’ll call $p^a$. Let $p^b$ be the $p$-part of the order of $N$. As in the previous problem, the $p$-part of the order of $HN$ is $p^a$. We again look at the formula giving the order of $HN$ in terms of the orders of $N$, $H$ and $H \cap N$. We see that the $p$-parts of the orders of $N$ and $H \cap N$ must be the same. This shows that $H \cap N$ verifies the Hall subgroup condition as a subgroup of $N$ at the prime number $p$. As above, the groups $H/(H \cap N)$ and $HN/N$ are isomorphic. The $p$-part of the order of $HN/N$ is thus $p^{a-b}$. The number $p^{a-b}$ is also the $p$-part of the order of $G/N$.  

2