Math 417: Homework 2 Solutions
Due Friday, February 2, 2018

1. Goodman 1.6.3. Assume that $p$ has the stated property: whenever $p$ divides $ab$, $p$ divides $a$ or $p$ divides $b$. To show that $p$ is prime, we will show that if $d$ is a natural number dividing $p$, then $d = 1$ or $d = p$.

Suppose that $d$ divides $p$. Then we may write $p = dq$ for some natural number $q$. Then $p$ divides $dq$. The assumption implies that either $p$ divides $d$ or $p$ divides $q$.

In the case where $p$ divides $d$, we may write $d = pr$ for some natural number $r$. But then $p = pqr$, and so $1 = qr$, and so both $q$ and $r$ must equal 1. Since $q = 1$, the equation $p = dq$ simplifies to $p = d$, so $d = p$ in this case.

In the case where $p$ divides $q$, we may write $q = ps$ for some natural number $s$. But then $p = dps$, and so $1 = ds$, and so both $d$ and $s$ must equal 1. So $d = 1$ in this case.

This shows that the only natural numbers dividing $p$ are 1 and $p$. So $p$ is prime.

2. Goodman 1.6.4. $60 = 7 \cdot 8 + 4$, $8 = 2 \cdot 4 + 0$. So gcd$(60, 8) = 4$. Also, $4 = 1 \cdot 60 - 7 \cdot 8$ shows 4 as an integer linear combination of 60 and 8.

$32242 = 767 \cdot 42 + 28$, $42 = 1 \cdot 28 + 14$, $28 = 2 \cdot 14 + 0$. So gcd$(32242, 42) = 14$. Then $14 = 42 - 28 = 42 - (32242 - 767 \cdot 42)$, so $(0) \cdot 32242 + 768 \cdot 42$ shows 14 as an integer linear combination of 32242 and 42.

3. Goodman 1.6.6. The proof is based on the following fact: If $a$ and $b$ are natural numbers, and $a$ divides $b$, then $a \leq b$. For if $a$ divides $b$, there is an natural number $q$ such that $b = aq$. Since this $q$ is at least 1, we see that $b$ is at least as big as $a$.

Now let $m$ and $n$ be integers and let $d$ be the greatest common divisor, meaning that $d$ is a natural number that divides both $m$ and $n$, and if $x$ is a natural number that divides $m$ and $n$, then $x$ divides $d$. It follows that if $x$ is a natural number that divides $m$ and $n$, then $x \leq d$ (since “$x$ divides $d$” implies $x \leq d$). This shows that no natural number that divides both $m$ and $n$ can exceed $d$. Since $d$ itself does divide both $m$ and $n$, it is the largest natural number with this property.

4. Goodman 1.6.8. Suppose that $a$, $b$, and $x$ are integers, that $a$ and $b$ are relatively prime, and that $a$ divides $bx$. By Corollary 1.6.15, there are integers $s$ and $t$ such that $sa + tb = 1$. Multiplying this equation by $x$ we find $sax + tbx = x$. It is clear that $a$ divides $sax$, and by hypothesis $a$ divides $bx$ and so divides $txb$. Thus $a$ divides the sum $sax + tbx = x$.

5. Goodman 2.6.1. Let $f : X \to Y$ be a surjective function, and define $x_1 \sim x_2$ if $f(x_1) = f(x_2)$. We check that this is an equivalence relation. For reflexivity, $x \sim x$ since $f(x) = f(x)$. For symmetry, $x \sim x'$, then $f(x) = f(x')$, so $f(x') = f(x)$, and $x' \sim x$. For transitivity, if $x \sim x'$ and $x' \sim x''$, then $f(x) = f(x')$ and $f(x') = f(x'')$. So $f(x) = f(x'')$ and $x \sim x''$.

For the second part, we must show that the equivalence classes are these sets $f^{-1}(y) = \{ x \in X \mid f(x) = y \}$ for $y \in Y$. These sets are called fibers. Denoting the equivalence class of $x$ by $[x]$, we first have a Lemma: if $f(x) = y$ then $[x] = f^{-1}(y)$. To see this, suppose that $x' \in [x]$. Then $x' \sim x$, so $f(x') = f(x) = y$, and so $x' \in f^{-1}(y)$. This shows $[x] \subseteq f^{-1}(y)$. Conversely, if $x' \in f^{-1}(y)$, then $f(x') = y = f(x)$, and so $x' \sim x$, and so $x' \in [x]$. This shows $f^{-1}(y) \subseteq [x]$. The Lemma is proved.
Now suppose we take any equivalence class \([x]\). Set \(y = f(x)\). Then by the Lemma \([x] = f^{-1}(y)\), so each equivalence class is also a fiber. Now take a fiber \(f^{-1}(y)\). Because \(f\) is surjective, there is some \(x\) such that \(f(x) = y\), and so there is some \(x \in f^{-1}(y)\). Applying the Lemma again, we get \(f^{-1}(y) = [x]\). Thus each fiber is also an equivalence class.

6. Goodman 1.7.4. Answer: \(4^{237} \equiv 4 \pmod{12}\). Indeed, \(4^n \equiv 4 \pmod{12}\) for all \(n \geq 1\). The proof is by induction. The base case \(n = 1\) is trivial: \(4 \equiv 4 \pmod{12}\). For the induction step, suppose \(4^k \equiv 4 \pmod{12}\) for some \(k\). Then \(4^{k+1} \equiv 4 \cdot 4^k \equiv 4 \cdot 4 \equiv 16 \equiv 4 \pmod{12}\). This completes the induction.