Sample homework solutions for 1.4

Jim Brown

2. Compute the following in the indicated $\mathbb{Z}_p$.
(b)

$$\frac{1^2+2^2+3^2+4^2}{7^2+8^2+9^2+10^2} \in \mathbb{Z}_{11}.$$

Observe that $7^2+8^2+9^2+10^2 = 294 \equiv 8 \pmod{11}$. Now we compute that $1^2+2^2+3^2+4^2 = 30 \equiv 8 \pmod{11}$, so we have that

$$\frac{1^2+2^2+3^2+4^2}{7^2+8^2+9^2+10^2} \equiv 8(8^{-1}) \equiv 1 \pmod{11}.$$

5. (b) Prove that if $\bar{a} \in \mathbb{Z}_m$ is a zero-divisor, then $\gcd(a,m) > 1$, and conversely, provided $m \nmid a$.

Proof: Let $\bar{a} \in \mathbb{Z}_m$ be a zero-divisor, i.e., $\bar{a} \neq \bar{0}$ and there exists a $\bar{b} \in \mathbb{Z}_m$ so that $\bar{a}\bar{b} = \bar{0}$ and $\bar{b} \neq \bar{0}$. Translated back into the integers, this means that $m|ab$, i.e., there exists $c \in \mathbb{Z}$ so that $cm = ab$. Suppose that $\gcd(a,m) = 1$. Then there exists integers $s,t \in \mathbb{Z}$ so that $1 = as + mt$. Multiplying this through by b we obtain $b = abs + mbt$, i.e., $b = m(cs + bt)$. Thus, $m|b$ and so $\bar{b} = \bar{0}$, a contradiction. Thus it must be that $\gcd(a,m) > 1$.
Conversely, suppose that $m \nmid a$ but $\gcd(a,m) > 1$. Note that these conditions show that $\gcd(a,m) \neq m$. Let $d = \gcd(a,m)$. Since $d|m$, there exists $s \in \mathbb{Z}$ so that $ds = m$ and similarly there exists $t \in \mathbb{Z}$ so that $dt = a$. Since $d \neq 1$, we know that $\bar{s} \neq \bar{0}$. Now consider $\bar{a}\bar{s}$:

$$\begin{aligned} \bar{a}\bar{s} &= \bar{d}\bar{t}\bar{s} \\ &= \bar{t}\bar{d}\bar{s} \\ &= \bar{t}\bar{m} \\ &= \bar{0}. \end{aligned}$$

Since $\bar{s} \neq \bar{0}$, this shows $\bar{a}$ must be a zero-divisor. ■

6. Prove that in any ring R:
(a) $0 \cdot a = 0$

Proof: Just copy down Lemma 1.1. ■

(c) $(-a)(-b) = ab$ for all $a, b \in R$.

Proof: We first show that $-(-a) = a$ for any $a \in R$. We use here that additive inverses are unique. So $-(-a)$ is the additive inverse of the element $-a$, i.e., the unique solution of the equation $x + (-a) = 0$. However, we also know that a satisfies this equation since $-a$ is the additive inverse of a, thus $a = -(-a)$ by the uniqueness.
Now we show that $(-a)b = -(ab) = a(-b)$. Note that $-(ab)$ is the unique solution of the equation $x + ab = 0$. However, $a(-b)$ is also a solution because $a(-b) + ab = a(-b+b) = a(0) = 0$ where we have used the distributive property and part (a). Thus we must have $a(-b) = -(ab)$. A similar argument shows that $(-a)b = -(ab)$.
Now we are in a position to prove that $(-a)(-b) = ab$. First observe that by what we have just shown we have $(-a)(-b) = -a(-b)$. Applying it again we get $-a(-b) = -(-ab)$. Now we use the first part to see that $-(-ab) = ab$. Thus, $(-a)(-b) = ab$. ■

7. Suppose that R is an integral domain, $c, x, y \in R$, and $c \neq 0$. Prove that if $cx = cy$, then $x = y$.

Proof: Using that $cx = cy$, we can add $-cy$ to both sides of the equation to obtain $cx - cy = 0$. Now we use the distributive property to get that $c(x - y) = 0$. Since we are in an integral domain there are no zero divisors, so either $c = 0$ or $x - y = 0$. However we assumed $c \neq 0$, so it must be that $x - y = 0$, i.e., $x = y$. ■