MATH453M Homework Solutions Week3

Nick Inglis
ninglis@math.purdue.edu

1.4.2 a In $\mathbb{Z}_7$, $\overline{5}^{-1} = (-\overline{2})^{-1} = \overline{3}$ and $\overline{3}^{-1} = -\overline{2}$ so $\overline{3}.\overline{5}^{-1} + \overline{4}.\overline{3}^{-1} = \overline{3}.\overline{3} + \overline{4}(-\overline{2}) = \overline{9} - \overline{8} = \overline{1}$.

1.4.2 b Modulo 11, $7^2+8^2+9^2+10^2 \equiv (-4)^2+(-3)^2+(-2)^2+(-1)^2 \equiv 4^2+3^2+2^2+1^2 = 16+9+4+1 = 30 \equiv 8 \pmod{11}$ so the denominator and numerator have the same non-zero value, so the value of the quotient is $\overline{1}$.

1.4.2 c By 1.1.4 c we have

$$1^2 + 2^2 + \cdots + \left(\frac{p-1}{2}\right)^2 = \frac{n(n+1)(2n+1)}{6},$$

where $n = (p-1)/2$. Now $2n+1 = p$ so the numerator is $\overline{0}$, but $p \geqslant 5$ so the denominator is $\overline{6} \neq \overline{0}$ and hence the quotient is $\overline{0}$.

1.4.4 For a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ if we let $\widehat{A} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ and $\det A = ad - bc$ then $A\widehat{A} = \det(A)I$. It follows that A is a zero-divisor if $\det A = 0$ and $A \neq 0$. If $\det A \neq 0$ then A has inverse $A^{-1} = (\det A)^{-1}\widehat{A}$ in $M_2(\mathbb{Q})$, so A is not a zero-divisor. If $\det A = \pm 1$ the $A^{-1} \in M_2(\mathbb{Z})$ and A is a unit.
a $\det A = 1$ so A is a unit. **b** $\det A = -1$ so A is a unit. **c** $\det A = 3$ so A is neither a unit nor a zero-divisor. **d** $\det A = 0$ so A is a zero-divisor. **e** $\det A = 0$ so A is a zero-divisor.

1.4.5 a $\gcd(a, m) = 1 \iff$ there exist $x, y \in \mathbb{Z}$ with $ax + my = 1 \iff$ there exists $x \in \mathbb{Z}$ with $ax \equiv 1 \pmod{m} \iff$ there exists $\overline{x} \in \mathbb{Z}_m$ with $\overline{ax} = \overline{1} \iff \overline{a}$ is a unit.

1.4.5 b If $\overline{a}$ is a zero-divisor then it is not a unit (see (d)) so $\gcd(a, m) \neq 1$ by (a). If $d = gcd(a, m) > 1$ and $m \nmid a$ then $m = cd$ with $c, d > 1$ and d divides a so $m = cd$ divides ac and hence $\overline{ac} = \overline{0}$. But $\overline{a}, \overline{c} \neq \overline{0}$ so $\overline{a}$ is a zero-divisor.

1.4.5 c If $\overline{a} \neq \overline{0}$ then $m \nmid a$ and either $\gcd(a, m) = 1$ in which case $\overline{a}$ is a unit by (a), or $\gcd(a, m) > 1$ and $\overline{a}$ is a zero-divisor by (b).

1.4.5 d Suppose that a is a unit and $ab = 0$. Then $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$, so a is not a zero-divisor. (c) is false for the ring $\mathbb{Z}$, where 2 is neither a zero-divisor, nor a unit.

1.4.6 a $0.a = 0.a + 0 = 0.a + (1.a - 1.a) = (0.a + 1.a) - 1.a = (0+1).a - 1.a = 1.a - 1.a = 0$.

1.4.6 b $(-1)a = (-1)a + 0 = (-1)a + (a + (-a)) = ((-1)a + 1.a) + (-a) = (-1+1).a + (-a) = 0.a + (-a) = 0 + (-a) = -a$.

1.4.6 c Similarly to (b) we have $a(-1) = -a$ so $(-a)(-b) = [a(-1)][(-1)b] = a(-1)^2 b = a.1.b = ab$.

1.4.6 d Suppose that $e.a = a$ for all $a \in R$. Then $e = e.1 = 1$.

1.4.7 $0 = cx - cy = c(x - y)$, but $c \neq 0$ so $x - y = 0$, hence $x = y$.

1.4.9 Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$. Then $x + y = (a + c) + (b + d)\sqrt{2} \in R$ and

$$xy = ac + ad\sqrt{2} + bc\sqrt{2} + bd(\sqrt{2})^2 = (ac + 2bd) + (ad + bc)\sqrt{2} \in R.$$

Therefore the addition and multiplication are defined on R. The associativity and commutativity of $+$ and $.$ and the distributive law are all inherited from the real numbers since $R \subset \mathbb{R}$. Also $0 = 0+0\sqrt{2} \in R$ and $1 = 1+0\sqrt{2} \in R$ so R has additive and multiplicative identities. Finally, if $x = a + b\sqrt{2} \in R$ then $-x = (-a) + (-b)\sqrt{2} \in R$ so there are additive inverses in R. Thus R is a commutative ring.

For $x = a+b\sqrt{2} \in R$ we define $x^* = a-b\sqrt{2} \in R$ and $N(x) = xx^* = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$. Now for $x, y \in R$, we have $(xy)^* = x^* y^*$ and $N(xy) = N(x)N(y)$. It follows that if x is a unit in R, then $N(x)$ is a unit in $\mathbb{Z}$, so $N(x) = \pm 1$. But if $N(x) = \pm 1$ then x has inverse $\pm x^* \in R$. Thus $x = a + b\sqrt{2}$ is a unit if and only if $a^2 - 2b^2 = \pm 1$. [In fact there are infinitely many such units.]

1.4.12 Given $a \neq 0$ we let $S = \{ab : b \in R\}$. Now for $b \neq c$ we have $ab \neq ac$ (from question 7) so $|S| = |R|$. But $S \subset R$ so we must have $S = R$ and hence $1 \in S$. Therefore there is some $b \in R$ with $ab = 1$.

1.4.13 For $\overline{a} \in \mathbb{Z}_p$ with $\overline{a} \neq \overline{0}$ there is an inverse $\overline{a}^{-1}$ with $\overline{a}\overline{a}^{-1} = \overline{1}$. Now $\overline{a} = \overline{a}^{-1} \iff \overline{a}^2 = 1 \iff (\overline{a} - \overline{1})(\overline{a} + \overline{1}) = \overline{a}^2 - \overline{1} = \overline{0} \iff \overline{a} = \overline{1}$ or $\overline{a} = -\overline{1}$. Therefore the non-zero elements of $\mathbb{Z}_p$ come in $\{\overline{a}, \overline{a}^{-1}\}$ pairs except for $\overline{1}$ and $-\overline{1}$. The pairs contribute $\overline{1}$ to the product $\overline{(p-1)!} = \prod_{\overline{a} \neq \overline{0}} \overline{a}$ so the product reduces to $\overline{(p-1)!} = \overline{1}(-\overline{1}) = -\overline{1}$ and hence $(p-1)! \equiv -1 \pmod{p}$.