MODEL ANSWERS TO THE FOURTH HOMEWORK

2.1.5. Note that (a, b) divides a and b so that it divides a and bc, that is, (a, b) is a common divisor of a and bc. Thus (a, b) divides (a, bc). By symmetry, (a, c) divides (a, bc). On the other hand, (a, b) divides b and (a, c) divides c so that (a, b) and (a, c) are coprime. Thus $(a, b)(a, c)$ divides (a, bc).

Since (a, bc) divides bc, we may write $(a, bc) = d_1d_2$, where d_1 divides b and d_2 divides c. Then d_1 divides d_1d_2, which divides a. Thus d_1 divides a and it divides b so that it is a common divisor of a and b. Thus d_1 divides (a, b). By symmetry d_2 divides (a, c). Thus $(a, bc) = d_1d_2$ divides $(a, b)(a, c)$. As $(a, bc) = d_1d_2$ divides $(a, b)(a, c)$ and vice-versa, it follows that $(a, bc) = (a, b)(a, c)$, as both sides are natural numbers.

Suppose that $a = bx + cy$. Now if d divides a and b then d certainly divides $a = bx + cy$ and b. Vice-versa, if d divides b and $bx + cy$ then d divides cy. As d divides b and $(b, c) = 1$, it follows that d divides y. Thus the common divisors of $\{a, b\}$ and $\{b, y\}$ are the same, so that $(a, b) = (b, y)$. By symmetry, it follows that $(a, c) = (c, x)$.

By what we already proved,

$$\begin{aligned}(bx + cy, bc) &= (a, bc)\\ &= (a, b)(a, c)\\ &= (b, y)(c, x).\end{aligned}$$

2.2.6. Let

$$u = 3 + \sqrt{10}.$$

Note that if we put

$$v = \sqrt{10} - 3$$

then

$$\begin{aligned}uv &= (\sqrt{10} + 3)(\sqrt{10} - 3)\\ &= (\sqrt{10})^2 - 3^2\\ &= 10 - 9\\ &= 1.\end{aligned}$$

Thus u is a unit, with inverse v. But then

$$\begin{aligned} u^n v^n &= (uv)^n \\ &= 1^n \\ &= 1. \end{aligned}$$

It follows that u^n is a unit for all natural numbers n. In this case

$$u^n = v^{-n},$$

so that $u^{-n} \in \mathbb{Z}[\sqrt{10}]$ for all natural numbers n. From there is follows easily that u^n is a unit for all integers n.

2.3.5. Since $(a, b) = 1$ the linear Diophantine equation

$$ax + by = c$$

has infinitely many integral solutions. The two intercepts are $(c/a, 0)$ and $(0, a/b)$ and the distance between these points is

$$\sqrt{\left(\frac{c}{a}\right)^2 + \left(\frac{c}{b}\right)^2} = \frac{c}{ab}\sqrt{a^2 + b^2}.$$

Now the distance between two successive solutions is

$$\sqrt{a^2 + b^2}.$$

The distance between n solutions is then

$$(n - 1)\sqrt{a^2 + b^2},$$

and this must be at most the distance between the intercepts. Thus

$$(n - 1)\sqrt{a^2 + b^2} \leq \frac{c}{ab}\sqrt{a^2 + b^2},$$

so that cancelling and moving the one over, we get

$$n \leq \frac{c}{ab} + 1.$$

On the other hand, amongst all solutions let (a_0, b_0) be the solution with the largest negative value for a_0 and let (a_{n+1}, b_{n+1}) be the solution with the largest negative value for b_{n+1}. Then the n solutions in the first quadrant are the only solutions between these two solutions. The distance between (a_0, b_0) and (a_{n+1}, b_{n+1}) is then

$$(n + 1)\sqrt{a^2 + b^2},$$

and this must be greater than the distance between the intercepts. Thus

$$(n + 1)\sqrt{a^2 + b^2} \leq \frac{c}{ab}\sqrt{a^2 + b^2},$$

so that cancelling and moving the one over, we get

$$n > \frac{c}{ab} - 1.$$

3.1.1. Suppose that the consecutive integers are a, $a+1$, ..., $a+r-1$. Then the difference between any of these integers is at most $r-1$, so that these none of these r integers are congruent. As there are exactly r congruence classes, it follows that any integer is congruent to exactly one of these r numbers. By assumption $f(a+i)$ is divisible by r, for any $0 \leq i \leq r-1$, so that $f(a+i) \equiv 0 \mod r$.
Suppose that $b \in \mathbb{Z}$ is an integer. Then $b \equiv a+i \mod r$, for some $0 \leq i \leq r-1$. We check below that $f(a+i) \equiv f(b) \mod r$. Assuming this, we have

$$\begin{aligned} f(b) &\equiv f(a+i) \mod r \\ &= 0 \mod r, \end{aligned}$$

so that $f(b)$ is divisible by r.
Note that $f(x) = x^2 + x$ is always even, since both

$$f(0) = 0^2 + 0 = 0 \qquad \text{and} \qquad f(1) = 1^2 + 1 = 2,$$

are even. The coefficients of x^2+x are 1 and 0 and the greatest common divisor is 1, which is not divisbile by 2.
Suppose that a and b are two integers, which are congruent modulo r. We check that $f(a) \equiv f(b) \mod r$. We proceed by induction on n in the expression

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

Let

$$g(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \qquad \text{and} \qquad h(x) = a_n x^n.$$

Then $f(x) = g(x) + h(x)$. Suppose that we know $h(a) \equiv h(b) \mod r$. By induction on n we would have $g(a) \equiv g(b) \mod r$. But then

$$\begin{aligned} f(a) &= g(a) + h(a) \\ &\equiv g(b) + h(b) \mod r \\ &= f(b). \end{aligned}$$

Therefore it suffices to check that $h(a) = h(b) \mod r$. Let $k(x) = x^n$. Note that if $k(a) \equiv k(b) \mod r$ then

$$\begin{aligned} h(a) &= a_n a^n \\ &\equiv a_n b^n \mod r \\ & h(b). \end{aligned}$$

Therefore it suffices to check that $k(a) = k(b) \mod r$. We proceed by induction on n. Assume the result for lower values of n. We have

$$\begin{aligned} k(a) &= a^n \\ &= a \cdot a^{n-1} \\ &\equiv b \cdot b^{n-1} \mod r \\ &= b^n \\ &= k(b). \end{aligned}$$

This completes the induction and the proof. In short, $f(a) \equiv f(b) \mod r$, as equivalence modulo r respects addition and multiplication and a polynomial is built up using just these two operations.
3.1.2. Suppose a is an integer. If we write a in decimal then we get

$$a = \sum a_i 10^i.$$

where $a_1, a_2, \dots, a_n$ are digits, so that a_i are integers between 0 and 9. Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n.$$

Then

$$a = f(10).$$

If we work modulo 9 we get we have

$$10 \equiv 1 \mod 9,$$

so that

$$\begin{aligned} a &\equiv f(1) \mod 10 \\ &= a_0 + a_1 + \dots + a_n. \end{aligned}$$

So throwing out nines just means that if we work modulo 9, we are just adding the digits and working modulo 9 respects addition and multiplication.
3.1.7. As r and s are odd we can find a and b such that $r = 2a + 1$ and $s = 2b + 1$.

(a) We have

$$\begin{aligned}
\frac{rs-1}{2} &= \frac{(2a+1)(2b+1)-1}{2} \\
&= \frac{4ab+2a+2b+1-1}{2} \\
&= 2ab+a+b \\
&\equiv a+b \mod 2 \\
&= \frac{r-1}{2}+\frac{s-1}{2}.
\end{aligned}$$

Thus

$$\frac{rs-1}{2} \equiv \frac{r-1}{2}+\frac{s-1}{2} \mod 2.$$

(b) Now one of a or $a+1$ is even, so that $a(a+1)$ is always divisible by 2 and $4a(a+1)$ is always divisible by 8. Thus, we have

$$\begin{aligned}
r^2 &= (2a+1)^2 \\
&= 4a^2+4a+1 \\
&= 4a(a+1)+1 \\
&\equiv 1 \mod 8.
\end{aligned}$$

(c) As a^2+a is always divisible by 2 it follows that $2(a^2+a)(b^2+b)$ is divisible by 8. Thus

$$\begin{aligned}
\frac{(rs)^2-1}{8} &= \frac{(2a+1)^2(2b+1)^2-1}{8} \\
&= \frac{(4a^2+4a+1)(4b^2+4b+1)-1}{8} \\
&= \frac{4a^2+4a}{8}+\frac{4b^2+4b}{8}+2(a^2+a)(b^2+b) \\
&\equiv \frac{r^2-1}{8}+\frac{s^2-1}{8} \mod 8.
\end{aligned}$$

3.1.8. Let n be an integer. Suppose that n is even and n is prime. Then $n=\pm 2$. If $n=-2$ then $n=0$ which is not prime. If $n=2$ then $n+2=4$ which is not prime. Thus if n and $n+2$ are both prime then n is odd.
Suppose that n is odd. As $[0]$, $[2]$ and $[4]=[1]$ are distinct equivalence classes, modulo 3, it follows that one of n, $n+2$ and $n+4$ is congruent to zero modulo three, so that one of them is divisible by 3. Thus if all three of n, $n+2$ and $n+4$ are prime, then one of n, $n+2$, $n+4$ is equal to ± 3. Since this gives only finitely many possible values for n,

it follows that the set

$$\{ n \in \mathbb{Z} \,|\, n,\ n+2 \text{ and } n+4 \text{ are all prime} \}$$

is finite.

3.1.10. First note that

$$k + 3 \equiv k \mod 3.$$

On the other hand, working modulo three, we have

$$[0]^3 = [0^3] = 0 \qquad [1]^3 = [1^3] = [1] \qquad \text{and} \qquad [2]^3 = [2^3] = [8] = [2].$$

Thus

$$[0]^6 = 0 \qquad [1]^6 = [1] \qquad \text{and} \qquad [2]^6 = ([2]^3)^2 = [2]^2 = [4] = [1].$$

Thus

$$\begin{aligned} (k+6)^{k+6} &\equiv k^{k+6} \mod 3 \\ &= k^6 \cdot k^k \\ &\equiv k^k \mod 3. \end{aligned}$$

Thus the sequence $k^k \mod 3$ repeats itself every sixth integer. Therefore the period is a divisor of six. Consider the first few terms

$$0^0 = 0 \qquad 1^1 = 1 \qquad 2^2 = 4 \equiv 1 \mod 3 \qquad \text{and} \qquad 3^3 = 27 \equiv 0 \mod 3.$$

This sequence does not repeat itself every second term but the third term is a repeat. Therefore the period is either 3 or 6. But

$$\begin{aligned} 5^5 &\equiv 2^5 \mod 3 \\ &= 2^3 \cdot 2^2 \\ &\equiv 2 \cdot 2^2 \mod 3 \\ &\equiv 2 \mod 3. \end{aligned}$$

Thus the period is six.