MODEL ANSWERS TO THE NINTH HOMEWORK

5.3.1 Note that both 503 and 773 are prime. Thus we may apply quadratic reciprocity. 773 is congruent to 1 modulo 4 and so there is no change in sign:

$$\begin{aligned}
\left(\frac{503}{773}\right) &= \left(\frac{773}{503}\right) \\
&= \left(\frac{270}{503}\right) \\
&= \left(\frac{2\cdot 3^3\cdot 5}{503}\right) \\
&= \left(\frac{2}{503}\right)\left(\frac{3}{503}\right)\left(\frac{3^2}{503}\right)\left(\frac{5}{503}\right) \\
&= -\left(\frac{503}{3}\right)\left(\frac{503}{5}\right) \\
&= -\left(\frac{2}{3}\right)\left(\frac{3}{5}\right) \\
&= -\left(\frac{2}{3}\right)\left(\frac{5}{3}\right) \\
&= -\left(\frac{2}{3}\right)\left(\frac{2}{3}\right) \\
&= -1.
\end{aligned}$$

Note that 501 is not prime; its prime factorisation is $3 \cdot 167$. Therefore

$$\begin{aligned}
\left(\frac{501}{773}\right) &= \left(\frac{3 \cdot 167}{773}\right) \\
&= \left(\frac{3}{773}\right)\left(\frac{167}{773}\right) \\
&= \left(\frac{733}{3}\right)\left(\frac{733}{167}\right) \\
&= \left(\frac{1}{3}\right)\left(\frac{65}{167}\right) \\
&= \left(\frac{5}{167}\right)\left(\frac{13}{167}\right) \\
&= \left(\frac{167}{5}\right)\left(\frac{167}{13}\right) \\
&= \left(\frac{2}{5}\right)\left(\frac{11}{13}\right) \\
&= -\left(\frac{13}{11}\right) \\
&= -\left(\frac{2}{11}\right) \\
&= -1 \cdot -1 \\
&= 1.
\end{aligned}$$

5.3.2 Since 5 is congruent to 1 modulo 4 by quadratic reciprocity we have

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Now the squares modulo 5 are 1 and 4. Thus 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1$ modulo 5.
We have

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right).$$

This is equal to one if and only if both terms on the right are one or both of them are minus one. The first is equal to one if and only if $p \equiv \pm 1 \mod 8$ and the second is equal to one if and only if $p \equiv \pm 1 \mod 5$. Thus 10 is a quadratic residue modulo p if and only if both $p \equiv \pm 1 \mod 8$ and $p \equiv \pm 1 \mod 5$, or neither $p \equiv \pm 1 \mod 8$ nor $p \equiv \pm 1 \mod 5$.

5.3.3 It is enough to show this result if q is a prime divisor of m, since d is a product of prime divisors. As q divides m there is an integer l such that $m = ql$. It follows that

$$\begin{aligned} p &= 4m + 1 \\ &= 4ql + 1 \end{aligned}$$

If $q = 2$ then

$$\left(\frac{2}{p}\right) = 1,$$

as $p \equiv 1 \mod 8$.

Otherwise, we may assume that q is odd. As $p \equiv 1 \mod 4$ if we apply quadratic reciprocity we get

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{p}{q}\right) \\ &= \left(\frac{1}{q}\right) \\ &= 1. \end{aligned}$$

5.3.4 Suppose that we may find integers r and s such that $r^2 - as^2 = n$. If $p|n$ then we have

$$r^2 \equiv as^2 \mod p.$$

There are two cases. If $p|s$ then $p|r$. Otherwise s is a unit modulo p and the equation

$$x^2 \equiv a \mod p,$$

has a solution. But then a is a quadratic residue and

$$\left(\frac{a}{p}\right) = 1.$$

5.3.5 (a) We want know if 2455 is a quadratic residue modulo 4993. We have to compute a Legendre symbol. First note that 4993 is prime, congruent to 1 modulo 4. On the other hand 2455 is not prime, its prime factorisation is $2455 = 5 \cdot 491$. We have

$$\begin{aligned}
\left(\frac{2455}{4993}\right) &= \left(\frac{5}{4993}\right)\left(\frac{491}{4993}\right)\\
&= \left(\frac{4993}{5}\right)\left(\frac{4993}{491}\right)\\
&= \left(\frac{3}{5}\right)\left(\frac{83}{491}\right)\\
&= \left(\frac{491}{83}\right)\\
&= \left(\frac{76}{83}\right)\\
&= \left(\frac{-7}{83}\right)\\
&= \left(\frac{-1}{83}\right)\left(\frac{7}{83}\right)\\
&= \left(\frac{83}{7}\right)\\
&= \left(\frac{6}{7}\right)\\
&= \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\\
&= -\left(\frac{7}{3}\right)\\
&= -\left(\frac{1}{3}\right)\\
&= -1.
\end{aligned}$$

Thus we cannot solve the equation

$$x^2 \equiv 2455 \mod 4993.$$

(b) Let a be the inverse of 1709 modulo 4993. Then a solution of the equation

$$1709x^2 \equiv 2455 \mod 4993$$

is the same as solution of the equation

$$x^2 \equiv 2455a \mod 4993$$

But

$$\begin{aligned}\left(\frac{2455a}{4993}\right) &= \left(\frac{2455}{4993}\right)\left(\frac{a}{4993}\right)\\ &= -\left(\frac{a}{4993}\right).\end{aligned}$$

On the other hand,

$$\begin{aligned}1 &= \left(\frac{1}{4993}\right)\\ &= \left(\frac{1709a}{4993}\right)\\ &= \left(\frac{1709}{4993}\right)\left(\frac{a}{4993}\right).\end{aligned}$$

Thus

$$\left(\frac{a}{4993}\right) = \left(\frac{1709}{4993}\right).$$

Note that 1709 is prime. Therefore

$$\begin{aligned}\left(\frac{1709}{4993}\right) &= \left(\frac{4993}{1709}\right)\\ &= \left(\frac{1575}{1709}\right)\\ &= \left(\frac{3^2\cdot 5^2\cdot 7}{1709}\right)\\ &= \left(\frac{7}{1709}\right)\\ &= \left(\frac{1709}{7}\right)\\ &= \left(\frac{1}{7}\right)\\ &= 1.\end{aligned}$$

Thus we cannot solve the equation

$$1709x^2 \equiv 2455 \mod 4993.$$

(c) Note that $27496 = 2^3 \cdot 7 \cdot 491$ is the prime factorisation of 27496. By the Chinese remainder theorem, we can solve this equation, if we can solve it modulo 8, 7 and 491. 245 modulo 8 is equal to 5. Thus we cannot solve

$$x^2 \equiv 245 \mod 27496$$

as we cannot solve the same equation modulo 8.
(d) $5473 \equiv 1 \mod 8$, thus we can solve this equation modulo 8. Modulo 7 we have

$$\left(\frac{5473}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Thus we cannot solve

$$x^2 \equiv 5473 \mod 27496$$

5.4.1 We check that
$x^{2^k} - 2^{2^{k-1}} = (x^2-2)(x^2+2)((x-1)^2+1)((x+1)^2+1)(x^{2^3}+2^{2^2})\dots(x^{2^{k-1}}+2^{2^{k-1}})$.

We proceed by induction on k. The induction starts with $k = 3$. In this case

$$\begin{aligned} x^{2^k} - 2^{2^{k-1}} &= x^{2^3} - 2^{2^2} \\ &= (x^4 - 4)(x^4 + 4) \\ &= (x^2 - 2)(x^2 + 2)(x^2 - 2x + 2)(x^2 + 2x + 2) \\ &= (x^2 - 2)(x^2 + 2)((x - 1)^2 + 1)((x + 1)^2 + 1). \end{aligned}$$

Now suppose that we know the result for k. In this case

$$\begin{aligned} x^{2^{k+1}} - 2^{2^k} &= x^{2\cdot 2^k} - 2^{2\cdot 2^{k-1}} \\ &= (x^{2^k} - 2^{2^{k-1}})(x^{2^k} + 2^{2^{k-1}}) \\ &= (x^2 - 2)(x^2 + 2)((x - 1)^2 + 1)((x + 1)^2 + 1)(x^{2^3} + 2^{2^2})\dots(x^{2^k} + 2^{2^{k-1}}), \end{aligned}$$

which is the correct formula for $k + 1$.
Let p be a prime. If $p = 2$ then we may take $x = 2$. Otherwise p is odd. Note that

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right).$$

Therefore at least one of -2, -1 and -1 is a quadratic residue modulo p. But then we may find a value a for x such that at least one of a^2+2, $a^2 - 2$ and $(a - 1)^2 + 1$ is divisible by p. In this case $a^{2^k} - 2^{2^{k-1}}$ is divisible by p so that

$$x^{2^k} - 2^{2^{k-1}} \equiv 0 \mod p,$$

has a solution.
5.4.2 Suppose that $n = m_1 m_2$ where m_1 and m_2 are coprime. Consider the equation

$$x^{m_1} = a.$$

Since we can solve the equation

$$x^n \equiv a \mod p^e$$

for all primes p and natural numbers e we can solve the equation

$$x^{m_1} \equiv a \mod p^e$$

since if b is a solution of the first equation then $c = b^{m_2}$ is a solution of the second equation.
On the other hand, if c is a solution of

$$x^{m_1} = a$$

and b is a solution of

$$x^{m_2} = c^{m_1}$$

then b is also a solution of the equation

$$x^n = a.$$

Thus we may assume that n is a prime. If n is even then $n = 2$ and this result is proved in the lectures. If n is odd then

$$(-1)^n = -1,$$

and so there is no harm in assuming a is positive.
Let p be a prime dividing a and let e be the largest natural number such that p^e divides a. Then we may write $a = p^e b$, where b is coprime to p. Consider the congruence

$$x^n \equiv a \mod p^{e+1}.$$

By assumption we may find a solution c to this equation. Suppose that $c = p^f d$, where c is coprime to d. Then

$$p^{nf} d^n \equiv p^e b \mod p^{e+1}.$$

It follows that there is an integer k such that

$$p^{nf} d^n = p^e b + p^{e+1} k.$$

Since the RHS is divisible by p^e it follows that $nf \geq e$. Suppose that $nf > e$. It would follow that p^{e+1} divides $p^e b$ so that p divides b, a contradiction. Therefore $e = nf$.
It follows if we write down the prime factorisation of a,

$$a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

then there are integers f_i such that $e_i = nf_i$. Therefore

$$\begin{aligned} a &= p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \\ &= p_1^{nf_1} p_2^{nf_2} \dots p_r^{nf_r} \\ &= (p_1^{f_1} p_2^{f_2} \dots p_r^{f_r})^n \\ &= b^n, \end{aligned}$$

where $b = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$. Hence b is a solution of

$$x^n = a.$$

5.4.3 Note that both 751 and 919 are prime. Thus we may apply quadratic reciprocity. Both of these numbers are congruent to 3 modulo 4 and so

$$\begin{aligned}
\left(\frac{751}{919}\right) &= -\left(\frac{919}{751}\right)\\
&= -\left(\frac{168}{751}\right)\\
&= -\left(\frac{2^3 \cdot 3 \cdot 7}{751}\right)\\
&= -\left(\frac{2}{751}\right)\left(\frac{2^2}{751}\right)\left(\frac{3}{751}\right)\left(\frac{7}{751}\right)\\
&= -\left(\frac{2}{751}\right)\left(\frac{751}{3}\right)\left(\frac{751}{7}\right)\\
&= -\left(\frac{1}{3}\right)\left(\frac{2}{7}\right)\\
&= -1 \cdot 1 \cdot 1\\
&= -1.
\end{aligned}$$

Now we use the Jacobi symbol.

$$\begin{aligned}
\left(\frac{751}{919}\right) &= -\left(\frac{919}{751}\right)\\
&= -\left(\frac{168}{751}\right)\\
&= -\left(\frac{2^3 \cdot 21}{751}\right)\\
&= -\left(\frac{2^3}{751}\right)\left(\frac{21}{751}\right)\\
&= -\left(\frac{2}{751}\right)\left(\frac{751}{21}\right)\\
&= -\left(\frac{16}{21}\right)\\
&= -1
\end{aligned}$$