2.9.2 Problems

P10 Try small prime numbers first.

p	p^2+2
2	6
3	11
5	27
7	51
11	123

Among the primes in this table, only the prime 3 has the property that (p^2+2) is also a prime. We try to prove that no other primes has this property. The only thing we have learnt about primes in this section is Theorem 20. We have checked the primes 2 and 3 in the table, so we can assume $p \geq 5$, and we only have to consider the two cases of congruence mod 6 in the theorem.

Case 1: $p \equiv 1 \pmod 6$. Raising both sides to 2 gives

$$p^2 \equiv 1 \pmod 6$$

Adding 2 to both sides gives

$$p^2+2 \equiv 3 \pmod 6$$

so p^2+2 must be divisible by 3, and hence it is not a prime.

Case 2: $p \equiv 5 \pmod 6$. Exactly the same argument shows that (p^2+2) is again divisible by 3, so it is not a prime.

Hence 3 is the only prime such that (p^2+2) is also prime.

P11 Just as in the case treated in the text, we can write

$$n = \sum_{j=0}^{k} a_j \cdot 10^j$$

The alternating digit sum is

$$\sum_{j=0}^{k} (-1)^j a_j = a_0 - a_1 + a_2 - \ldots$$

If j is even, then

$$a_j \equiv a_j \cdot 10^j \pmod{11}$$

and if n is odd, we have

$$-a_j \equiv a_j \cdot 10^j \pmod{11}$$

Adding these congruences for all j shows that n is congruent to its alternating digit sum, mod 11.

P12 We use Theorem 20.
Case 1: p gives remainder 1 when divided by 6.
In this case we have

$$p = 6q + 1$$

where q is the quotient on division by 6. This implies

$$p^2 - 1 = 36q^2 + 12q = 12q(3q + 1)$$

If q is even, then clearly $12q$ is divisible by 24, so $(p^2 - 1)$ is also divisible by 24. If q is odd, then $(3q + 1)$ is even, so $12(3q + 1)$ is divisible by 24. Hence $(p^2 - 1)$ is divisible by 24 also in this case.
Case 2: p gives remainder 5 when divided by 6.
Now we can write

$$p = 6q + 5$$

and use a similar argument as in Case 1.
P13 Since we always have the congruence

$$38x \equiv 4x \pmod{17}$$

the Problem is the same as finding a solution to

$$4x \equiv 5 \pmod{17}$$

The positive integers congruent to 5 mod 17 are:

$$5, 22, 39, 56 \ldots$$

Since $56 = 4 \cdot 14$, we can take $x = 14$.
P14 Suppose there exists such a positive integer n. Let

$$m = n^2 - n$$

The condition in the problem is the same as saying that every prime number p divides m. This can happen only if $m = 0$, that is, only if $n = 1$. Hence $n = 1$ is the only positive integer with the given property.
P15 We try to find a pattern.

$$\begin{aligned} 1 &= 1 \\ 1+3 &= 4 \\ 1+3+5 &= 9 \\ 1+3+5+7 &= 16 \\ 1+3+5+7+9 &= 25 \end{aligned}$$

It seems like the sum of the first n odd numbers is equal to n^2, and we guess that this is always true. The kth odd number is $(2k - 1)$, so our guess says that

$$\sum_{k=1}^{n} (2k - 1) = n^2$$

We could prove it by induction, as before, but here we give an alternative solution, using Theorem 22, which we have already proved.
We compute, using basic properties of summation:

$$\begin{aligned}\sum_{k=1}^{n}(2k-1) &= 2\cdot\sum_{k=1}^{n}k-\sum_{k=1}^{n}1 \\ &= 2\cdot\frac{n(n+1)}{2}-n \\ &= n^2+n-n \\ &= n^2\end{aligned}$$

which proves our guess.
P16 We let $S(n)$ be the statement

"F_{3n} is even"

Base step: Since $F_3 = 2$, the statement $S(1)$ is true.
Induction step: We assume that $S(n)$ is true, in other words that F_{3n} is even. We have

$$\begin{aligned}F_{3n+1} &= F_{3n}+F_{3n-1} \\ F_{3n+2} &= F_{3n+1}+F_{3n}=2F_{3n}+F_{3n-1} \\ F_{3n+3} &= F_{3n+2}+F_{3n+1}=3F_{3n}+2F_{3n-1}\end{aligned}$$

(The second line is obtained using the definition of F_{3n+1}, and the last equality is obtained by adding the first two equations.) Beacuse F_{3n} is even, and $2F_{3n-1}$ is even, we can conclude that

$$3F_{3n}+2F_{3n-1}$$

also is even. In other words, $S(n+1)$ is true. This completes the induction proof.
P17 We let $S(n)$ be the formula to be proved.
Base step: Since $F_1 = 1$, $F_2 = 1$, and $F_3 = 2$, the statement $S(1)$ is true.
Induction step: We assume that $S(n)$ is true, in other words that

$$F_nF_{n+2}+(-1)^n=F_{n+1}^2$$

We add $[(-1)^{n+1}+F_{n+1}F_{n+2}]$ to both sides. This gives

$$F_nF_{n+2}+F_{n+1}F_{n+2}=F_{n+1}^2+F_{n+1}F_{n+2}+(-1)^{n+1}$$

(Here we have used that $(-1)^n+(-1)^{n+1}=0$.)
This equation can be rewritten as

$$(F_n+F_{n+1})\cdot F_{n+2}=F_{n+1}(F_{n+1}+F_{n+2})+(-1)^{n+1}$$

and this implies

$$F_{n+2}^2 = F_{n+1}F_{n+3} + (-1)^{n+1}$$

which means that we have proved the statement $S(n+1)$. This completes the induction proof.

P18 By Fermat's theorem, we have

$$a^p \equiv a \pmod{p}$$

and

$$b^p \equiv b \pmod{p}$$

Adding these two congruences gives

$$a^p + b^p \equiv a + b \pmod{p}$$

But Fermat's theorem also says

$$(a+b)^p \equiv a + b \pmod{p}$$

which proves the desired congruence.

P19 We let

$$m = 1^p + 2^p + \ldots + (p-1)^p$$

By Fermat's last theorem

$$\begin{aligned} 1 &\equiv 1^p \pmod{p} \\ 2 &\equiv 2^p \pmod{p} \\ 3 &\equiv 3^p \pmod{p} \end{aligned}$$

and so on. Adding all these congruences shows that

$$1 + 2 + \ldots + (p-1) \equiv m \pmod{p}$$

By Theorem 22, we know that

$$1 + 2 + \ldots + (p-1) = \frac{p-1}{2} \cdot p$$

Since p is odd, the number $\frac{p-1}{2}$ is an integer, so the above equation shows that the sum

$$1 + 2 + \ldots + (p-1)$$

is a congruent to 0 mod p. Hence m is also congruent to 0 mod p.

P20 We compute all values of f and collect them in a table:

x	$f(x)$
0	0
1	4
2	3
3	2
4	1

From the table, it is clear that f is injective and surjective. Hence it is also bijective.

P21 We compute all values of g and collect them in a table:

x	$f(x)$
0	0
1	4
2	8
3	2
4	6
5	0
6	4
7	8
8	2
9	6

Now it is clear that g is NOT injective (for example, $g(0) = g(5)$). It is also clear that g is NOT surjective (for example, 1 is not in the image). Therefore, g is also not bijective.