31.1-6 Since

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$$

and neither of numbers $k, k-1, \ldots, 1$ is not divisible by p (for $k = 1, 2, \ldots, p-1$), we conclude that factor p cannot be canceled from the numerator of $\binom{p}{k}$ so, $p \mid \binom{p}{k}$.

Now using binomial theorem, one gets

$$(a+b)^p = \sum_{k=0}^{p} a^k b^{p-k} = a^p + \underbrace{\sum_{k=1}^{p-1} a^k b^{p-k}}_{\equiv_p 0} + b^p \equiv_p a^p + b^p$$

31.1-7 If $a \mid b$ then there exists positive integer k such that $b = ka$. Let $s = x \bmod b$ and $t = s \bmod a$. Then, there exist positive integers x' and s' such that $x = x'b + s$ and $s = s'a + t$. Since now

$$x = bx' + s = x'ka + s'a + t = (x'k + s')a + t$$

and $0 \le t < a$, we conclude that $(x \bmod b) \bmod a = t = x \bmod a$.

Also, if $x \equiv_b y$ then $b \mid (x - y)$ and since $a \mid b$, we conclude that $a \mid (x - y)$.

31.1-8 If $n = a^b$ then $b = \log_a n < \lg n < \beta$. Therefore, for each $b = 2, 3, \ldots, \beta$, one can check whether there exists a such that $a^b = n$. That can be done efficiently by binary search and recursive powering. The binary search check can be performed as follows:

Algorithm 1 BinarySearchCheckPower(b, n)

Require: Positive integers b and n.

$l := 1, r := n$
while $r - l > 1$ **do**
  $m := \lfloor (l + r)/2 \rfloor$
  if $m^b > n$ **then**
    $r := m$
  else
    $l := m$
  end if
end while
return $l^b = n$ or $r^b = n$

The complexity of a single multiplication of β-bit numbers is $\mathcal{O}(\beta^2)$. To find a^k, we can use repeated squaring, i.e.

$$a^k = \begin{cases} a & k = 1, \\ (a^l)^2 & k = 2l \\ (a^l)^2 \cdot a & k = 2l + 1, \quad l > 0 \end{cases}$$

It takes $\lg k$ multiplications, so the complexity of computing a^k is $\mathcal{O}(\beta^2 \lg \beta)$. To check whether there exists a such that $a^b = n$ for fixed b, requires $\mathcal{O}(\lg b)$ powering operations, which gives the complexity $\mathcal{O}(\beta^2 (\lg \beta)^2)$. Finally, that checking has to be done β times, so the total complexity is $\mathcal{O}(\beta^3 (\lg \beta)^2)$, which is polynomial in β.

31.2-3 Let x be any common divisor of a and n. Then $a = a'x$ and $n = n'x$ for some positive integers a' and n' and $a + kn = a'x + kn'x = (a' + kn')x$ so $x \mid a + kn$.

On the other hand, let x be any common divisor of $a+kn$ and n. Then $a = a'x$ and $a+kn = cx$ for some positive integers n' and c, and therefore $a = cx-kn = cx-kn'x = (c-kn')x$, implying that $x \mid a$.
This proves that the sets of common positive divisors of a and n, and $a+kn$ and n, are equal. Then so are it's maximal elements, i.e. $\gcd(a,n) = \gcd(a+kn,n)$.

31.2-4

Algorithm 2 $\textsc{Euclid}(a, b)$

Require: Positive integers a and b.

```
while b > 0 do
    r := a mod b
    a := b
    b := r
end while
return a
```

31.2-6 It returns $(1, (-1)^{k+1}F_{k-2}, (-1)^k F_{k-1})$. We will prove this by mathematical induction. If we define $F_{-1} := 1$ then $F_1 = F_0 + F_{-1} = 0 + 1 = 1$ and hence, the Fibonacci property holds. In the case $k = 1$, the tuple is $(1, 1, 0) = (1, (-1)^2 F_{-1}, (-1)^1 F_0)$, by the definition of the $b = 0$ case of $\textsc{Extended-Euclid}$. Assume that the statement is correct for $k-1$. Then since $F_{k+1} = F_k + F_{k-1}$, taking $a = F_{k+1}$ and $b = F_k$, one finds that $a \bmod b = F_{k-1}$, so the recursive call in step 3 is $\textsc{Extended-Euclid}(F_k, F_{k-1})$ and $\lfloor a/b \rfloor = \lfloor F_{k+1}/F_k \rfloor = 1$. By induction hypothesis, it returns the tuple $(d', x', y') = (1, (-1)^k F_{k-3}, (-1)^{k-1} F_{k-2})$. Then

$$\begin{aligned} d &= d' = 1 \\ x &= y' = (-1)^{k-1} F_{k-2} = (-1)^{k+1} F_{k-2} \\ y &= x' - \lfloor a/b \rfloor y' = (-1)^k F_{k-3} - \lfloor F_{k+1}/F_k \rfloor (-1)^{k-1} F_{k-2} \\ &= (-1)^k (F_{k-3} + F_{k-2}) = (-1)^k F_{k-1} \end{aligned}$$

which completes the proof by induction.

31.3-1

$(\mathbb{Z}_4, +_4)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_5^*, +_5)$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Define $\alpha(x) = 2^x \bmod 5$ for $x \in \mathbb{Z}_4$. Then

$$\alpha(x) \cdot_5 \alpha(y) = (2^x \bmod 5) \cdot (2^y \bmod 5) \bmod 5 = 2^{x+y} \bmod 5$$

Let $x + y = 4k + z$ where $z = x +_4 y = x + y \bmod 4$ and k is positive integer. Since $2^4 = 16 \bmod 5 = 1$, we have

$$\alpha(x) \cdot_5 \alpha(y) = 2^{4k+z} \bmod 5 = (2^4)^k \cdot 2^z \bmod 5 = 2^z \bmod 5 = \alpha(z) = \alpha(x +_4 y).$$

Moreover, since $\alpha(0) = 1$, $\alpha(1) = 2$, $\alpha(2) = 4$, $\alpha(3) = 3$, we conclude that $\alpha : \mathbb{Z}_4 \to \mathbb{Z}_5^*$ is required isomorphism.

31.3-2 Since $\mathbb{Z}_9$ is commutative cyclic group, according to Lagrange theorem, it's proper non-trivial subgroup must be of order 3, i.e. it's $[3] = \{0, 3, 6\}$ (equipped with $+_9$). The other two are $[0]$ and $\mathbb{Z}_9$ itself.

On the other hand, $\mathbb{Z}_{13}^*$ is of the order 12. According to the same Lagrange theorem, it's subgroups have orders $1, 2, 3, 4, 6, 12$. Therefore, the subgroups are $[1] = \{1\}$, $[3] = \{1, 3, 9\}$, $[4] = \{1, 3, 4, 9, 10, 12\}$, $[5] = \{1, 5, 8, 12\}$, $[12] = \{1, 12\}$ and $\mathbb{Z}_{13}^*$.

31.3-3 To prove that $(S', \oplus)$ is group, we only need to prove that $0 \in S'$ and that for each $a \in S'$ has it's inverse $a' \in S'$. Let $a \in S'$ be arbitrary element and define $\alpha(x) = a \oplus x$, for $x \in S'$. According to the assumption, $\alpha(S') \subseteq S'$ and hence $\alpha(x) = \alpha(y)$ implies $a \oplus x = a \oplus y$ which further implies $x = y$ (S is group). Therefore $\alpha : S' \to S'$ is bijection and hence, there exists $e \in S'$ such that $a = \alpha(e) = a \oplus e$. It implies that $e = 0 \in S'$. In the same manner, there exists $a' \in S'$ such that $0 = \alpha(a') = a \oplus a'$, i.e. an inverse element of a is in S'.

31.3-4 Since $\phi(x)$ is the number of integers $1 \leq a < x$ which are relatively prime to x. Integer a is relatively prime to p^e if and only if $p \nmid a$. Since every p-th integer is divisible by p, the total number of integers $1 \leq a < p^e$ is p^{e-1}. Therefore $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.

31.3-5 Since obviously $f_a(x) \in \mathbb{Z}_n^*$, to show that f_a is the permutation it is sufficient to show that it is $1-1$, i.e. that $f_a(x) = f_a(y)$ implies $x = y$. Since $f_a(x) = f_a(y)$ implies $ax \equiv_n ay$ which further implies $n \mid ax - ay = a(x - y)$. The fact that a and n are relatively prime implies $n \mid x - y$. If $x \neq y$ then $n \mid x - y$ leading to $|x - y| \geq n$ which is contradiction, since $x, y \in 1, 2, \ldots, n-1$. Therefore, $x = y$ and f_a is $1-1$ and hence a bijection. Since the domain and codomain of f_a are the same (i.e. $\mathbb{Z}_N^*$) we conclude that f_a is permutation of $\mathbb{Z}_n^*$.