31.1-6

$$p \mid \binom{p}{k} = p \mid \frac{p!}{k!(p-k)!}$$

$p \mid p!$ we can use unique factorization for both $p!$ and $k!(p-k)!$

we already know $p!$ is a multiple of p.

If we show $k!(p-k)!$ is not a multiple of p, we can be sure ~~that~~ in unique multiplicaeion form, p will not be canceled out and $\frac{p!}{k!(p-k)!}$ is an integer. Because $k < p$ and $p-k < p$. and p is prime. the uniqee factorization form of $k!(p-k)!$ will have p^0 and ~~there~~fore $\frac{p!}{k!(p-k)!}$ is a multiple of p and $p \mid \frac{p!}{k!(p-k)!}$

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b^1 \cdots \binom{p}{k} a^{p-k} b^k \cdots \binom{p}{p-1} a^1 b^{p-1} + b^p$$

Because $p \mid \frac{p!}{k!(p-k)!}$ all $\binom{p}{k} a^{p-k} b^k \bmod p$ is 0 so $(a+b)^p \bmod p$ is $a^p + b^p$

so $(a+b)^p \equiv a^p + b^p \mod p$

31.1.7

$a \mid b \Rightarrow b = ka$ let $x \bmod b = r$

$x = qb + r$ (1) for some quotient q

$q = \lfloor x/b \rfloor$ put $b = ka$ into (1)

$x = qka + r$ qka is a multiple of a so

$x \bmod a = r$ $r = x \bmod b$

So $x \bmod a = x \bmod b$ $r < a$

$\Rightarrow (x \bmod b) \bmod a = x \bmod a$

$x \equiv y \bmod b \Rightarrow x - y = qb$

$q = \lfloor y/b \rfloor$ $b = ka$

$x - y = qka \Rightarrow a \mid x - y$

$\Rightarrow x \equiv y \bmod a$ so

$x \equiv y \bmod a$ if $y \equiv y \bmod b$

31.1-8

Unique factorization will be a good approach. First we write β in form $\beta = p_1^{k_1} \cdot p_2^{k_2} \cdots\cdots$

Then we do the above operation recursively on each $p_n^{k_n}$ until there is only 1 $p_n^{k_n}$ exist or all the remaining p cannot be further factorized.

In this recursion, there will be $n!$ cases and running time would be $O(n!)$

31.2-3

Because $\gcd(a,n)$ divides a and n,

$\gcd(a,n)$ divides kn $\Rightarrow$

$\gcd(a,n)$ divides $a+kn$

By corollary 31.3 $\Rightarrow$

$\gcd(a,n)$ divides $\gcd(a+kn, n)$

Also because $\gcd(a,n) \mid a+kn$

$$\gcd(a,n) = \gcd(a+kn, n)$$

31.2-4

```
Euclid (a, b):
    if b > a:
        a, b = b, a

    while b > 0:
        q = a / b
        r = a % b    (% is mod)

        return b if r == 0

        a, b = b, r
```

31.2-6

According to Theorem 31.11

$$\gcd(F_{k+1}, F_k) = \gcd(F_k, F_{k-1})$$

And extended Euclid return d, x, y

where $d = \gcd(F_k, F_{k-1}) = ax + by$

d is therefore 1.

$$|aF_k - byF_{k-1}| = 1$$

so $a = (-1)^{k-2} F_{k-3}$

$b = (-1)^{k-1} F_{k-2}$

result of extended Euclid is:

$$\left(1, (-1)^{k-2} F_{k-3}, (-1)^{k-1} F_{k-2}\right)$$

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

$(\mathbb{Z}_5^*, \cdot_5)$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

To Prove they are isomorphic,

we need that $a+b \equiv c \mod$ if and

only if $\alpha(a) \cdot \alpha(b) \equiv \alpha(c) \mod 5$

let $\alpha(x) = x+1$

31.3-2

the number of subgroup is the number of divisor. 9 has 3 diviser, 1, 3, 9

subgroup by 1 and 9 are just the trivial sub group $\{0\}$ and $\{0, 1, \ldots, 9\} = Z_9$

subgroup generated by 3 is $\{0, 3, 6\}$

For Z^{13}, Because 13 i prime. we can use 12 for it. divides of 12 are

$\{1, 2, 3, 4, 6, 12\}$ So 6 subgroups for Z^{13}

$\langle a \rangle = \{a^k = a^{12} \bmod 13 : k \geq 1\}$

$\langle 1 \rangle = \{1\}$ $\langle 3 \rangle = \{1, 3, 9\}$

$\langle 2 \rangle = \{1, 2, 3, 4 \cdots 12\}$ $\langle 4 \rangle = \{1, 3, 4, 9, 10, 12\}$

$\langle 6 \rangle = \{1, 5, 8, 12\}$

$\langle 12 \rangle = \{1, 12\}$

31.3-3

To prove theorem 31.14, we need to prove 4 properties. closure, Identity, Associativity and inversity.

Closure; Because $a \oplus b \in S'$ for all $a, b \in S'$ are in the subset, It is closed.

Identity: suppose there is $a \in S'$. Because it is closed there must be $a^p = a^q$

$a^p a^{(-q)} = 1$. So It has Identity.

Assocläutivity: Be cuse S is assotiative,

For the same binary operation, S' is assotiative too.

Inversity: As said above, there is $a^k = 1$

$$a^{k-1} \cdot a = 1$$

so there is an inverse of a

So proved theorem 31.14.

31.3-4

$$\phi(p^e) = p^{e-1}(p-1)$$