1 3.1

题目2. a对模m和n的阶分别为s和t，证明：a对模$[m,n]$的阶为$[s,t]$

解答.

$$\because a^s \equiv \pmod{m}, a^t \equiv \pmod{n} \tag{1}$$

$$\therefore a^{[s,t]} \equiv 1 \pmod{[m,n]} \tag{2}$$

then using congruence property

$$a^{[s,t]} \equiv 1 \pmod{[m,n]} \tag{3}$$

let there be an positive integer k, where $a^k \equiv 1 \pmod{mod[m,n]}$，then it is $a^k \equiv 1 \pmod{m}$

$$\because m \mid [m,n], [m,n] \mid (a, k-1)$$

$$\therefore a^k \equiv 1 \pmod{n}$$

$$\therefore s \mid k, t \mid k$$

$\therefore k$ is s, t's common multiple，thus $[s,t] \mid k$

$$\therefore a\text{对模}[m,n]\text{的阶为}[s,t]$$

题目5. 若n和a均是正整数，$a \geq 2$, 证明：$n \mid \phi(a^n - 1)$

解答. Let $m = a^n - 1$

Consider the group $G = (Z/mZ)^*$ or $(Z_m)^*$, which has $\phi(m)$ elements, the order of group is $\phi(m)$

Let $\bar{a} \in Z/mZ$ be the remainder class of the integer a modulo m,

$$\because gcd(a, m) = gcd(a, a^n - 1) = 1$$

$$\therefore a \in G$$

Consider the subgroup $H = \langle \bar{a} \rangle$ that is the subgroup generated by $\bar{a}$

Now $a^n \equiv 1 \pmod{m}$ (where $m = a^n - 1$ and n is the smallest integer with this property)

but no positive integer $i < n$ satisfies $a^i \equiv 1 \pmod{m}$ (since $a^i - 1$ is a positive integer smaller than m).

This implies that order of H equals n $\therefore$ the order of a subgroup always divides the order of a group, $n \mid \phi(a^n - 1)$

题目6. 如果$n \geq 2$, 证明：$n \nmid 2^n - 1$

解答. Proof by Contradiction:

Assume that there is an integer $n \geq 2 \ni n \mid 2^n - 1$, clearly, n is odd

Take p to be the smallest prime dividing $p \mid 2^n - 1, p \mid 2^{p-1} - 1$

$$\because gcd(a^k - 1, a^l - 1) = a^{gcd(k,l)} - 1, k, l \in \mathbb{Z}^+, a > 1$$

$$\therefore p | 2^d - 1, d = gcd(n, p-1)$$

However, since p is the smallest prime divisor of n we have $d = 1$. Hence $p \mid 2^d - 1 = 1$ is a contradiction, thus $n \nmid 2^n - 1$

题目7. 设p是奇素数，$n \geq 1$,证明:

$$\sum_{k=1}^{p-1} k^n \equiv \begin{cases} -1 \pmod p, \text{如果} p-1 \mid n \\ 0 \pmod p, \text{如果} p-1 \nmid n \end{cases}. \tag{4}$$

解答. We can use the rule that every prime has a primitive root such that there is an x and considering the set

$$[x^1, x^2, \ldots, x^{p-1}] \pmod p \equiv [1, 2, \ldots, (p-1)] \pmod p$$

$$\therefore 1^k + 2^k + \cdots + (p-1)^k = x^k + x^{2k} + \cdot + x^{(p-1)k} \pmod p$$

Using the geometric sum, then

$$\Rightarrow (x^k)(1 - x^{(p-1)k})/(1 - x^k) \pmod p$$

Because of Fermats little theorem $a^{p-1} \equiv 1 \pmod p$, $(1 - x^{(p-1)k}) = 0$

$$\therefore (x^k)(0)/(1 - x^k) \pmod p = 0 \pmod p$$

If $p - 1 \mid n$, then $n = (p-1)j$ for some j

$$1^n + \cdots + (p-1)^n \equiv 1^{(p-1)j} + \cdots + (p-1)^{(p-1)j} \equiv 1 + \cdots + 1 = p - 1 \equiv -1 \pmod p$$

because If $p - 1$ divides n, then by Fermat's Theorem each term is congruent to 1 modulo p. There are $p - 1$ terms, so the sum is congruent to -1 modulo p.

题目8.

(1) 设$F_n = 2^{2^n} + 1$ (费马数), $n \geq 1$. 证明：F_n的每个素因子都有形式$2^{n+1}x + 1, x \in \mathbb{Z}$

(2) 对任意给定的整数$l \geq 1$，证明：若无穷多个素数模2^l余1

解答.

(1) Lemma: $p^2 \leftrightharpoons p \equiv \pm 1 \pmod 8$

Let p be a divisor of the Fermat Number $2^{2^n} + 1$

$$\therefore 2^{2^n} \equiv -1 \pmod p$$

$$\therefore (2^{2^n})^2 \equiv 1 \pmod p$$

$$\therefore 2^{2^{(n+1)}} \equiv 1 \pmod p$$

So $x = 2^{n+1}$ is $2^x \equiv 1 \pmod p$ smallest integer solution

$$\therefore 2 \text{ 对模 } p \text{ 的指数是 } 2^{n+1}$$

与费马小定理 $2^{p-1} \equiv 1 \pmod p$ 比较得 $2^{n+1} \mid (p-1)$

当 $n > 1$， $p \equiv 1 \pmod 8$, using the lemma, 2 is p square remainder

$$\because 2^{(p-1)/2} \equiv 1 \pmod p$$

$\therefore 2^{n+1} | \frac{p-1}{2}$, 令$(p-1)/2 = 2^{n+1} * k$ 即得 $p = 2^{n+2} * k + 1$

(2)

题目9.

(1) 设p为奇素数，$a \geq 2$. 证明：若$a^p - 1$的素因子q不整除$a-1$则必有形式$q = 2px + 1, x \in \mathbb{Z}$

(2) 设p给定的奇素数，证明：形如$2px + 1 (x \in \mathbb{Z})$的素数有无限多个

解答.

(1)

$$a^p - 1 = (a-1)[a^{p-1} + a^{p-2} + \cdots + 1]$$

由费马小定理

$$a^{p-1} \equiv 1 \pmod p$$

$$\therefore a^{p-1} = mp + 1$$

$$\Rightarrow [a^{p-2} + \cdots + 1] = [a^{p-1} - 1]/(a-1) = mp/(a-1)$$

所以 $[a^{p-2} + \cdots + 1]$ 有因数 p

$[a^{p-1} + a^{p-2} + \cdots + 1]$ 共有 p项 即奇数项

除去最后一项1 还有偶数项。无论a为奇数还是偶数

$[a^{p-1} + a^{p-2} + \cdots + a]$ 均为偶数

$\therefore [a^{p-1} + a^{p-2} + \cdots + 1] = 2px + 1$

$\therefore a^p - 1 = (a-1)(2px+1)$

如果不整除$a-1$，必须整除$2px+1$

(2)

2

题目1. 证明：m是一个素数充分必要条件是存在a,a对模m的次数为$m-1$

解答. If a has order $m-1$, then by Euler's theorem $m-1 \mid \phi(m)$

This occurs when m is prime, since $\phi(m) = m-1$. Thus, m is prime

题目2. 设g是奇素数，p的一个原根，证明：

(1) 当$p \equiv 1 \pmod 4$时,$-g$也是p的一个原根

(2) 当$p \equiv 3 \pmod 4$时,$-g$对p的次数为$\frac{p-1}{2}$

解答.

(1) Since p is odd, and we have Fermat's little theorem,

$$\because a^p \equiv a \pmod p$$

$$\therefore g \equiv g^p \equiv -(-g)^p \pmod p$$

Since $p \equiv 1 \pmod 4, x^2 \equiv -1 \pmod p$, -1 is a quadradic residual of p, (-1 is a square mod p iff $p \equiv 1 \pmod 4$)

$$\exists k \in \mathbb{Z} \ni -1 \equiv g^{2k} \equiv (-g)^{2k} \pmod p$$

Thus $g \equiv (-g)^{2k}(-g)^p \pmod p$. Since g is congruent to $-g^p$, $-g$ is also a primative root of p.

(2) Using a primative root principle, that

$$a \text{ is of order } h \pmod n\text{, then } a^k \text{ is of order } \frac{h}{gcd(h,k)} \tag{5}$$

Since g is a primitive root,

$$-1 \equiv g^{(p-1)/2} \pmod p$$

$$\therefore -g \equiv (-1)(g) \equiv g^{(p-1)/2}g \equiv g^{(p+1)/2} \pmod p$$

Now, the order of $g^{(p+1)/2} \pmod p$ according to (5) is $\frac{p-1}{gcd((p+1)/2,p-1)}$

If $p \equiv 1 \pmod 4$, then $(p+1)/2$ is odd and $gcd((p+1)/2, p-1)$ is 1, making the order of $-g$ to be $p-1$, thus it is a primative root.

Otherwise, the term $\frac{p+1}{2}$ is even and $gcd(\frac{p+1}{2}, p-1) = (p-1)/2 > 1$

Therefore, the order of $-g$ is not $p-1$. i.e. not a primitive root.