1.

(a) $x^2 \equiv 11 \pmod{511}$

$511 = 7 \cdot 73$，且 $\gcd(11, 511) = 1$。
在模 511 下有解 $\Longleftrightarrow$ 在模 7 和模 73 下分别都有解。

- **模 7：**

$$x^2 \equiv 11 \equiv 4 \pmod{7}$$

$2^2 \equiv 4 \pmod{7}$，故模 7 下有解：$x \equiv \pm 2 \pmod{7}$。

- **模 73：**

看勒让德符号 $\left(\frac{11}{73}\right)$。

由二次互反律：

$$\left(\frac{11}{73}\right) = \left(\frac{73}{11}\right) = (-1)^{\frac{11-1}{2} \cdot \frac{73-1}{2}} \left(\frac{11}{73}\right) = \left(\frac{7}{11}\right)$$

（因为 $5 \cdot 36$ 为偶数）。

模 11 的二次剩余集合是

$$1^2, 2^2, 3^2, 4^2, 5^2 \equiv 1, 4, 9, 5, 3 \pmod{11},$$

里面没有 7，所以

$$\left(\frac{7}{11}\right) = -1, \quad \Rightarrow \quad \left(\frac{11}{73}\right) = -1.$$

因此 11 不是模 73 的二次剩余，方程 $x^2 \equiv 11 \pmod{73}$ 无解。

所以模 511 下同余方程 **无解**。

(b)

$91 = 7 \cdot 13$，且 $\gcd(11, 91) = 1$。
在模 91 下有解 $\iff$ 在模 7 与模 13 下都可解。

模 7

$$11x^2 \equiv -6 \pmod 7 \iff 4x^2 \equiv 1 \pmod 7$$

$4^{-1} \equiv 2 \pmod 7$，所以

$$x^2 \equiv 2 \pmod 7.$$

枚举平方：

$$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 2,\ 4^2 \equiv 2 \pmod 7,$$

2 是二次剩余，解为 $x \equiv 3, 4 \pmod 7$。

模 13

$$11x^2 \equiv -6 \equiv 7 \pmod{13}.$$

$11^{-1} \equiv 6 \pmod{13}$（因为 $11 \cdot 6 = 66 \equiv 1 \pmod{13}$），

$$x^2 \equiv 7 \cdot 6 \equiv 42 \equiv 3 \pmod{13}.$$

枚举平方：

$$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 9,\ 4^2 \equiv 3,\ 5^2 \equiv 12,\ 6^2 \equiv 10, \ldots$$

有 $4^2 \equiv 9^2 \equiv 3 \pmod{13}$，故解为 $x \equiv 4, 9 \pmod{13}$。

模 7 有 2 个解，模 13 有 2 个解，由中国剩余定理，模 91 下共有 $2 \cdot 2 = 4$ 个解。

所以 $11x^2 \equiv -6 \pmod{91}$ **有解（4 个）**。

2.

方程：

$$2x^3 - x^2 + 3x + 11 \equiv 0 \pmod 5.$$

先化简（在 $\mathbb{Z}_5$ 上）：

$$11 \equiv 1, \quad -x^2 \equiv 4x^2,$$

于是

$$f(x) = 2x^3 + 4x^2 + 3x + 1 \in \mathbb{Z}_5[x].$$

把 $x = 0, 1, 2, 3, 4$ 逐一代入（下面等号都理解为模 5）：

- $x = 0$: $f(0) = 1 \not\equiv 0$;
- $x = 1$: $f(1) = 2 + 4 + 3 + 1 = 10 \equiv 0$;
- $x = 2$: $f(2) = 2 \cdot 8 + 4 \cdot 4 + 3 \cdot 2 + 1 = 16 + 16 + 6 + 1 = 39 \equiv 4 \not\equiv 0$;
- $x = 3$: $f(3) = 2 \cdot 27 + 4 \cdot 9 + 3 \cdot 3 + 1 = 54 + 36 + 9 + 1 = 100 \equiv 0$;
- $x = 4$: $f(4) = 2 \cdot 64 + 4 \cdot 16 + 3 \cdot 4 + 1 = 128 + 64 + 12 + 1 = 205 \equiv 0$。

所以模 5 的解为

$$x \equiv 1, 3, 4 \pmod 5,$$

共 3 个解。

所以该同余方程在模 5 下的解数为 **3**。

3.

记 $\delta_m(a)$ 为模 m 下 a 的阶：最小正整数 h 使 $a^h \equiv 1 \pmod m$。

(1) $\delta_{91}(11)$

$91 = 7 \cdot 13$,
$\varphi(91) = (7-1)(13-1) = 6 \cdot 12 = 72$。
所以 $\delta_{91}(11) \mid 72$。

计算若干幂（都模 91）：

- $11^2 = 121 \equiv 30$;

- $11^3 \equiv 11 \cdot 30 = 330 \equiv 57$;
- $11^4 \equiv 30^2 = 900 \equiv 81$;
- $11^6 = (11^3)^2 \equiv 57^2 = 3249 \equiv 64$;
- $11^8 = (11^4)^2 \equiv 81^2 = 6561 \equiv 9$;
- $11^{12} = 11^8 \cdot 11^4 \equiv 9 \cdot 81 = 729 \equiv 1$。

所以 $11^{12} \equiv 1 \pmod{91}$，故 $\delta_{91}(11) \mid 12$。

再查 12 的真因数 $1, 2, 3, 4, 6$：

- $11^1 \equiv 11 \not\equiv 1$;
- $11^2 \equiv 30 \not\equiv 1$;
- $11^3 \equiv 57 \not\equiv 1$;
- $11^4 \equiv 81 \not\equiv 1$;
- $11^6 \equiv 64 \not\equiv 1$。

没有更小的指数组成 1。

因此 $\delta_{91}(11) = 12$。

(2)

$231 = 3 \cdot 7 \cdot 11$,

$$\varphi(231) = (3-1)(7-1)(11-1) = 2 \cdot 6 \cdot 10 = 120.$$

利用阶在互素模数下的性质：若 $\gcd(m, n) = 1$，$\gcd(a, mn) = 1$，则

$$\delta_{mn}(a) = \operatorname{lcm}\big(\delta_m(a), \delta_n(a)\big).$$

于是

$$\delta_{231}(5) = \operatorname{lcm}\big(\delta_3(5), \delta_7(5), \delta_{11}(5)\big).$$

分别计算三个素模下的阶。

模 3：

$5 \equiv 2 \pmod{3}$,

$$2^1 \equiv 2 \not\equiv 1, \quad 2^2 \equiv 4 \equiv 1 \pmod{3},$$

故 $\delta_3(5) = 2$。

模 7：

逐步算：

$$5^1 \equiv 5, \quad 5^2 \equiv 25 \equiv 4, \quad 5^3 \equiv 4 \cdot 5 = 20 \equiv 6,$$

再平方 6：

$$5^6 \equiv 6^2 = 36 \equiv 1 \pmod 7.$$

且 $5, 5^2, 5^3$ 均不为 1，故 $\delta_7(5) = 6$。

模 11：

$$5^2 \equiv 25 \equiv 3, \quad 5^4 \equiv 3^2 = 9, \quad 5^5 \equiv 9 \cdot 5 = 45 \equiv 1 \pmod{11}.$$

前面各幂不为 1，所以 $\delta_{11}(5) = 5$。

于是

$$\delta_{231}(5) = \operatorname{lcm}(2, 6, 5) = 30.$$

$\delta_{231}(5) = 30$

4. 设 p 为素数，$\delta_p(a) = h$，证明：

1. 若 $2 \mid h$，则 $a^{h/2} \equiv -1 \pmod p$；
2. 若 $4 \mid h$，则 $\delta_p(-a) = h$；
3. 若 $2 \mid h$，$4 \nmid h$，则 $\delta_p(-a) = h/2$。

(a)

设 $h = 2k$。因为 $\delta_p(a) = h$，有

$$a^{2k} \equiv 1 \pmod p.$$

记 $b = a^k$，则

$$b^2 \equiv 1 \pmod{p}.$$

在域 $\mathbb{F}_p$ 中，方程 $x^2 \equiv 1 \pmod{p}$ 的解只有 $x \equiv \pm 1$。

- 若 $b \equiv 1$，则 $a^k \equiv 1$，与 $h = 2k$ 为最小阶矛盾；
- 故只能是 $b \equiv -1$。

即

$$a^{h/2} = a^k \equiv -1 \pmod{p}.$$

(b)

设 $h = 4m$。
由 (a) 知

$$a^{h/2} = a^{2m} \equiv -1 \pmod{p}.$$

先看 $(-a)^h$：

$$(-a)^h = (-a)^{4m} = \left((-a)^2\right)^{2m} = (a^2)^{2m} = a^{4m} \equiv 1 \pmod{p}.$$

故 $\delta_p(-a) \mid h$。

再算

$$(-a)^{h/2} = (-a)^{2m} = \left(a^2\right)^m = a^{2m} \equiv -1 \not\equiv 1 \pmod{p},$$

所以 $\delta_p(-a) \nmid h/2$，即 $\delta_p(-a) > h/2 = 2m$。

$\delta_p(-a)$ 是 $h = 4m$ 的因数，又大于 $2m$。
只有一种可能：$\delta_p(-a) = 4m = h$。

因而 $\delta_p(-a) = h$。

(c)

此时可写 $h = 2m$，其中 m 是奇数。

由 $a^{2m} \equiv 1$ 得

$$(a^m)^2 \equiv 1 \pmod{p}.$$

所以 $a^m \equiv \pm 1$。

- 若 $a^m \equiv 1$，则阶 $\delta_p(a) \mid m$，与 $\delta_p(a) = 2m$ 矛盾；
- 因此必有 $a^m \equiv -1$。

于是

$$(-a)^m = (-1)^m a^m \equiv (-1) \cdot (-1) = 1 \pmod{p}$$

（因为 m 为奇数），所以

$$\delta_p(-a) \mid m = h/2.$$

再证没有更小的正因数 $d < m$ 使 $(-a)^d \equiv 1$：

- 若 d 为偶数，$d = 2k$，则

  $$1 \equiv (-a)^{2k} = a^{2k} \pmod{p},$$

  于是 $h = 2m \mid 2k \Rightarrow m \mid k$，但 $k = d/2 < m/2 < m$，矛盾。
- 若 d 为奇数，$d = 2k + 1$，则

  $$1 \equiv (-a)^d \Rightarrow 1 \equiv \left((-a)^d\right)^2 = a^{2d} \pmod{p},$$

  所以 $h = 2m \mid 2d \Rightarrow m \mid d$，但 $d < m$，也是矛盾。

因此不存在 $0 < d < m$ 满足 $(-a)^d \equiv 1 \pmod{p}$，从而

$$\delta_p(-a) = m = h/2.$$

5.

(a)

设

$$\delta_m(a) = h, \quad \delta_m(b) = k, \quad \lambda = (h,k).$$

由引理，

$$\delta_m(a^\lambda) = \frac{h}{(h,\lambda)} = \frac{h}{\lambda}, \qquad \delta_m(b^\lambda) = \frac{k}{(k,\lambda)} = \frac{k}{\lambda}.$$

所以

$$\big(\delta_m(a^\lambda), \delta_m(b^\lambda)\big) = \left(\frac{h}{\lambda}, \frac{k}{\lambda}\right) = \frac{(h,k)}{\lambda} = 1.$$

在模 m 的乘法群，若元素 x, y 的阶分别为 r, s，且 $(r,s) = 1$，则

$$\delta(xy) = rs.$$

应用到 $x = a^\lambda,\ y = b^\lambda$，得

$$\delta_m(a^\lambda b^\lambda) = \delta_m(a^\lambda), \delta_m(b^\lambda) = \frac{h}{\lambda} \cdot \frac{k}{\lambda} = \frac{hk}{\lambda^2}.$$

又因为

$$a^\lambda b^\lambda \equiv (ab)^\lambda \pmod{m},$$

故

$$\delta_m((ab)^\lambda) = \frac{\delta_m(a)\delta_m(b)}{\lambda^2},$$

等价于

$$\lambda^2 \delta_m((ab)^\lambda) = \delta_m(a)\delta_m(b).$$

(b)

对 $x = ab,\ r = \lambda$ 应用引理：

$$\delta_m((ab)^\lambda) = \frac{\delta_m(ab)}{(\delta_m(ab), \lambda)}.$$

而由 (a) 已知

$$\delta_m((ab)^\lambda) = \frac{\delta_m(a)\delta_m(b)}{\lambda^2}.$$

两式相等，得

$$\frac{\delta_m(ab)}{(\delta_m(ab), \lambda)} = \frac{\delta_m(a)\delta_m(b)}{\lambda^2}.$$

两边同乘 $\lambda^2(\delta_m(ab), \lambda)$，得到

$$\lambda^2\delta_m(ab) = (\delta_m(ab), \lambda), \delta_m(a)\delta_m(b).$$