课时三：考点 1 同余的概念与性质

题 1：（1）√　　　　（2）×

题 2：$9|\overline{3AA_1} \Rightarrow 9|14+2A$　　$\therefore 4+2A=18$　　$A=7$

题 3：B

题 4：$2002^{2002} \equiv 1^{2002} \equiv 1(\bmod 3)$余数为 1

题 5：$2002^{2003} \equiv 2^{2003}(\bmod 10)$

$\because 2^5 = 2(\bmod 10)$

$$\begin{aligned}\therefore 2^{2003} &= \left(2^5\right)^{400} \cdot 2^3 \equiv 2^{400} \cdot 2^3 \\ &\equiv \left(2^5\right)^{80} \cdot 2^3 \equiv 2^{80} \cdot 2^3 \\ &\equiv \left(2^5\right)^{16} \cdot 2^3 \equiv 2^{16} \cdot 2^3 \equiv 2^{19} \\ &\equiv \left(2^5\right)^3 \cdot 2^4 \equiv 2^3 \cdot 2^4 \equiv 2^7 \equiv 2^5 \cdot 2^2 \\ &\equiv 2^3 \equiv 8(\bmod 10)\end{aligned}$$

$2^1 \equiv 2$，$2^2 \equiv 4$，$2^3 \equiv 8$，$2^4 \equiv 6$，$2^5 \equiv 2$

$2003 \equiv 3(\bmod 4)$　　$\therefore 2002^{2001} \equiv 8(\bmod 10)$

末位数字为 8

题 6：证明：$2^{2^5}+1 \equiv 0(\bmod 641)$

$2^4 \equiv 16$，$2^8 \equiv 256$

$2^{16} \equiv 154$，$2^{32} \equiv 640 \equiv -1(\bmod 641)$

to $641|2^{32}+1$

考点 2　完全剩余系

题 1：0,1,2,3,4,5

题 2：√

题 3：×

考点 3　欧拉函数

（1）$\varphi(1000)=\varphi\left(2^3\times 5^3\right)=1000\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=400$

（2）$\varphi(1)+\varphi(p)+\cdots+\varphi\left(p^n\right)$

$=1+p-1+p^2-p+\cdots+p^n-p^{n-1}$

$=p^n$

考点 4　简化剩余系

题 1：×

题 2：$\varphi(18)=\varphi\left(2\times 3^2\right)=18\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=18\times\frac{1}{2}\times\frac{2}{3}=6$　　　选 C

题 3：B

题 4：5.25

考点 5　欧拉定理和费马定理

题 1：1，质数

题 2：B

题 3：$17408=2^{10}\times 17$　　　不循环的位数为 10

题 4：$3.\dot{2}=3+\frac{2}{9}=\frac{29}{9}$　　　$\therefore 0.3\dot{2}=\frac{29}{90}$

题 5：$8^{4965}(\bmod 13)$

$\because 8^{12} \equiv 1(\bmod 13)$

$\therefore 8^{4965} = \left(8^{12}\right)^{413} \cdot 8^{9} \equiv 2^{27} \equiv \left(2^{12}\right)^{2} \cdot 2^{3} \equiv 8(\bmod 13)$

题 6：欧拉定理：$m>1$，$(a,m)=1$，则 $a^{\varphi(m)} \equiv 1(\bmod m)$

证明：设 $r_1, r_2, r_{\varphi(m)}$ 为 m 的简化剩余数：

$\because (a,m)=1$，$\therefore ar_1, ar_2, \cdots, ar_{\varphi(m)}$ 为 m 的简化余数；

$\therefore (ar_1)(ar_2)\cdots\left(ar_{\varphi(m)}\right) \equiv r_1 r_2 \cdots r_{\varphi(m)} (\bmod m)$

即 $a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} (\bmod m)$

又 $(r_i, m)=1$　　$\therefore \left(r_1 r_2 \cdots r_{\varphi(m)}, m\right)=1$　　$\therefore a^{\varphi(m)} \equiv 1(\bmod m)$

课时四：一次同余式

考点 1

题 1：$(a,m)/6$

题 2：$(28,35)=7/21$　　$\therefore$ 有 7 个解　选 B

题 3：检验　　选 C

题 4：（1）$73x \equiv 1(\bmod 13)$ 等价于 $8x \equiv 1(\bmod 13)$

$(8,13)=1$ 同余式有 1 个解

即 $8x-13y=1$　　$x=5$　　$y=3$ 为解

同余式的解为　　$x \equiv 5(\bmod 13)$

（2）$20x \equiv 44(\bmod 72)$　　$(20,72)=4 \mid 44$

$\therefore$ 同余式有 4 个解

考察：$20x-72y=44$　即 $5x-18y=11$

$x=13$， $y=3$为一个解

$\therefore$ 同余式的解为 $x=12+18t \pmod{72}$　　$t=0,1,2,3$

即 $x=13,31,49,67 \pmod{72}$

题 5： $m_1=4$， $m_2=5$， $m_3=7$， $m=m_1m_2m_3=140$

$M_1=35$， $M_2=28$， $M_3=20$

$M_1M_1' \equiv 1 \pmod{m_1}$即 $35M_1' \equiv 1 \pmod 4$取 $M_1'=-1$

$M_2M_2' \equiv 1 \pmod{m_2}$即 $28M_2' \equiv 1 \pmod 5$取 $M_2'=2$

$M_3M_3' \equiv 1 \pmod{m_3}$即 $20M_3' \equiv 1 \pmod 7$取 $M_3'=-1$

$\therefore x \equiv 35\times(-1)\times 3+28\times 2\times 2+20\times(-1)\times 6$

$\quad \equiv -105+112-120 \equiv -113 \equiv 27 \pmod{140}$

题 6： $\begin{cases} x \equiv -2 \pmod 3 \\ x \equiv -2 \pmod 4 \\ x \equiv 0 \pmod 2 \\ x \equiv 6 \pmod 5 \\ x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases}$　　等价于 $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 1 \pmod 5 \end{cases}$

$m_1=3$， $m_2=4$， $m_3=5$

$M_1=20$， $M_2=15$， $M_3=12$

$M_1M_1' \equiv 1 \pmod{m_1}$　　$20M_1' \equiv 1 \pmod 3$　　$M_1'=-1$

$M_2M_2' \equiv 1 \pmod{m_2}$　　$15M_2' \equiv 1 \pmod 4$，取 $M_2'=-1$

$M_3M_3' \equiv 1 \pmod{m_3}$　　$12M_3' \equiv 1 \pmod 5$　取 $M_3'=3$

$\therefore x \equiv 20\times(-1)\times 1+15\times(-1)\times 2+12\times 3\times 1$

$\quad \equiv -20-30+36 \pmod{60}$

$\equiv -14 \equiv 46$

考点 3，威尔逊定理

题 7：证明：$p|(p-1)!q^p + a$，即 $(p-1)!q^p + a \equiv 0(\bmod p)$

$(p-1)!a^p + a \equiv 0(\bmod p)$　　　$(p-1)!a^p + a \equiv -1 \cdot a^p + a$

$\equiv -1 \cdot a + a$

$\equiv 0(\bmod p)$

题 8：$2p+1$为素数

$\therefore (2p)! \equiv -1(\bmod 2p+1)$

又 $-1 \equiv (2p)! = 1 \times 2 \times 3 \times \cdots \times p(p+1)(p+2)(2p)$

$\equiv 1 \times 2 \times 3 \times \cdots \times p \times (-p) \times (-p+1) \cdots (-1)$

$\equiv 1 \times 2 \times 3 \times p(-1)^p \cdot p(p-1) \cdots 1$

$\equiv (-1)^p (p!)^2 (\bmod 2p+1)$

$\therefore (-1)^p (p!) + 1 \equiv 0(\bmod 2p+1)$　　　$\therefore (p!)^2 + (-1)^p \equiv 0(\bmod 2p+1)$

课时 5，考点 1 平方剩余和平方非剩余

题 1：模 7 的平方判余

$x^2 \equiv a(\bmod 7)$　　　$x = \pm 1, \pm 2, \pm 3$ 代入得 $a \equiv 1, 4, 2(\bmod 7)$

选 C

题 2：模 11 的平方非剩余

$x^2 \equiv a(\bmod 11)$　　　$x = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5$ 代入得

$a = 1, 4, 9, 5, 3(\bmod 11)$为平方剩余

2，6，7，8，10为平方非剩余

选 D

考点 2 欧拉判别条件

题 3：选 B

题 4：$\frac{17-1}{2}=8$个

在 1-16 中，$x^2\equiv a(\bmod 17)$，$x=\pm1,\pm2,\pm3,\pm4,\pm5,\pm6,\pm7,\pm8$代入得

$$\equiv 1,4,9,16,8,2,15,13$$

故 1，2，4，8，9，13，15，16 为平方剩余

$\pm1,\pm2,\pm4,\pm8$

题 5：× ，√

勒让德符号

题 6：$\left(\frac{18}{11}\right)=\left(\frac{-4}{11}\right)=\left(\frac{-1}{11}\right)$ A 正确

$\left(\frac{12}{5}\right)=\left(\frac{-3}{5}\right)=\left(\frac{-1}{5}\right)\cdot\left(\frac{3}{5}\right)=\left(\frac{3}{5}\right)$ ×

$\left(\frac{7}{11}\right)=\left(\frac{-4}{11}\right)=\left(\frac{-1}{11}\right)\left(\frac{4}{11}\right)=-\left(\frac{4}{11}\right)$ ×

题 7：p，q为不同的奇偶数，则

$$\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

题 8：（1）$\left(\frac{3}{83}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{83-1}{2}}\left(\frac{83}{3}\right)=-\left(\frac{2}{3}\right)=1$

$\therefore$ 同等式有解，且有两个解

（2）$\left(\frac{q}{p}\right)=(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\cdot\left(\frac{p}{q}\right)$

$\because p\equiv 1(\bmod 4)$ $\therefore \frac{p-1}{2}$ 为偶数

$\therefore (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}$ 为偶数 $\therefore \frac{q}{(p)}=\frac{p}{(q)}$

题 9：$\left(\frac{1742}{769}\right)=\left(\frac{2\times 871}{769}\right)=\left(\frac{2}{769}\right)\left(\frac{871}{769}\right)$

$\because 769\equiv 1 \quad (\bmod 8)$

$\therefore \left(\frac{2}{796}\right)=1$

$\left(\frac{871}{769}\right)=\left(\frac{102}{769}\right)=\left(\frac{2}{769}\right)\left(\frac{5}{769}\right)=\left(\frac{51}{769}\right)$

$=-1^{\frac{51-1}{2}\cdot\frac{769-1}{2}}\left(\frac{769}{51}\right)=\left(\frac{4}{51}\right)=1$

$\therefore \left(\frac{1742}{769}\right)=1$

所以同余方程有解

扫码观看
视频讲解更清晰