《初等数论》

期末突击课

课时1 数的整除性

考点	重要程度	占分	题型
1. 整除的概念与性质	★★★	2~8	判断、证明
2. 带余除法	★★★	2~6	填空、证明
3. 最大公因数与最小公倍数	★★★★	4~6	选填、计算
4. 质数	★★★	2~6	填空、证明
5. 高斯函数	★★★	2	填空

考点1 整除的概念与性质

定义： 设$a,b\in Z$，$b\neq 0$，如果存在$q\in Z$，使得等式$a=bq$成立，那么称b整除a或a能被b整除，记作：$b|a$，此时称b为a的因数（约数），a为b的倍数。

性质： 设$a,b,c\in Z$，$b\neq 0$，$c\neq 0$，则

（1）如果$c|b$，$b|a$，那么$c|a$；

（2）如果$b|a$，那么$bc|ac$；反之亦真；

（3）如果$c|a$，$c|b$，那么，对于任意$m,n\in Z$，有$c|(ma+nb)$；

（4）如果$b|a$，$a\neq 0$，那么$|b|\leq|a|$；

（5）如果$b|a$，$a|b$，那么$|b|=|a|$；

（6）如果$b|a$，$c|a$，$(b,c)=1$,则$bc|a$。

扫码观看
视频讲解更清晰

【题1】判断：

（1）设a,b是整数，若a|b，则$a^2|b^2$。（ ）

（2）若a|c，b|c，则ab|c。（ ）

（3）设a,b是整数，若a|a+b，则a|b。（ ）

【题2】设n是不能被3整除的奇数，证明：$24|n^2-1$

考点2 带余除法

带余除法：

设$a,b\in Z$，$b>0$，则存在$q,r\in Z$，使得$a=bq+r$，$0\le r<b$，并且q及r是唯一的。

考点3 最大公因数与最小公倍数

定义1 设a,b是两个整数，若整数d满足d|a，d|b,则称d为a，b的一个公因数；

整数a,b的公因数中最大的一个称为最大公因数，记作：(a，b)；

若(a，b)=1，则称a,b互质（互素）。

性质2：

（1）(a，b)=(|a|,|b|)；

（2）若b是任一正整数，则(0,b)=b；

（3）设a,b,c是任意三个不全为零的整数，且a=bq+c，其中q∈Z，则(a,b)= (b,c)；

考点3 最大公因数与最小公倍数

辗转相除法(欧几里得(Euclid)算法) 设$a,b\in Z$， $b>0$ ，按下述方式反复做带余除法，有限步之后必然停止(即余数为零)

用b除a： $a=bq_0+r_0$ ， $0<r_0<b$;

用r_0除b: $b=r_0q_1+r_1$， $0<r_0<r_1$;

用r_1除r_0: $r_0=r_1q_2+r_2$， $0<r_2<r_1$;

用r_{n-1}除r_{n-2}: $r_{n-2}=r_{n-1}q_n+r_n$， $0<r_n<r_{n-1}$;

用r_n除r_{n-1}: $r_{n-1}=r_nq_{n+1}$

则$(a,b)=r_n$

事实上，由于余数满足$r_0>r_1>\ldots>r_{n-1}>\ldots\geq 0$ ，故上述带余除法有限步后余数必为零，

我们有$(a, b) = (b,r_0)= (r_0,r_1) =\ldots = (r_{n-1},r_n)=r_n$

考点3 最大公因数与最小公倍数

推论3 a,b的公因数与(a,b) 的因数相同。

定理4 设a，b是任意两个不全为0的整数，m是任一正整数，则

（1）(ma, mb) =m(a,b);

（2）若 δ是a，b的任一公因数，则 $\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{|\delta|}$

特别地，$(\frac{a}{(a,b)},\frac{b}{(a,b)})=1$。

定义5 设a,b是两个非零整数，若整数m满足a|m，b|m,则称m为a，b的一个公倍数；整数a,b的所有正的公倍数中最小的一个称为a,b的最小公倍数，记作：[a，b]。

考点3 最大公因数与最小公倍数

性质6

(1) $[a, 1] = |a|$，$[a, a] = |a|$；

(2) $[a, b] = [b, a]$；

(3) $[a, b] = [|a|, |b|]$；

(4) 若$a|b$，则$[a, b] = |b|$，$(a, b) = |a|$；

(5) 对任意的正整数a，b，有$[a, b] = \dfrac{ab}{(a,b)}$。

【题3】 （1515，600）=_____；已知（a,b）=1,则（13a+21b,34a+55b）=_____.

【题4】 正整数a,b， ab=60,[a,b]=15,则(a,b)=_____.

【题5】 求532与336的最大公因数与最小公倍数.

【题6】 求整数x,y,使得（5767，4453）=5767x+4453y.

【题7】 设n是正整数，证明：$\frac{21n+4}{14n+3}$ 是既约分数.

扫码观看
视频讲解更清晰

考点4 质数

定义1 一个大于1的整数，如果它的正因数只有1和它本身，那么称之为质数；否则称为合数。

性质2

（1）若p是一质数，a是任一整数，则p|a或（a,p)=1；

（2）设a_1，a_2，…，a_n是 n个整数，p是质数，若$p|a_1a_2 \dots a_n$，则a_1，a_2,…，a_n中至少有一个被p整除；

（3）质数有无穷多个。

考点4 质数

定理3（算术基本定理）

任一大于1的整数能表示成质数的乘积，即任一大于1的整数 $a = p_1p_2\cdots p_n$ ，

$p_1 \le p_2 \le \cdots \le p_n$，其中$p_1,p_2,..,p_n$是质数，

并且若$a = q_1q_2\cdots q_m, q_1 \le q_2 \le \cdots \le q_m$,其中$q_1,q_2,...,q_m$是质数，则$m=n$, $p_i=q_i$

$i= 1,2,... ,n$

定理4 设a是任一大于1的正整数，

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \qquad \alpha_i > 0, \qquad i = 1, 2, \cdots, k$$

是a的标准分解式，则a的正因数个数为 $T(a) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1) = \prod_{i=1}^{k}(\alpha_i + 1)$

【题8】梅森数M_n是质数，则n是_____.

【题9】480的正因数的个数是_____.

【题10】下列数中是质数的是（　）

A. 101　　B. 111　　C. 121　　D. 141

【题11】两个素数的和为31，则这两个素数为_____.

【题12】**判断：**若整数n与质数p不互质，则 p|n.（　）

【题13】**证明：**质数有无穷多个.

考点5 高斯函数

定义

函数 $[x]$与$\{x\}$是定义在实数集上的函数，

函数 $[x]$的值等于不大于x的最大整数，

函数$\{x\}$的值是 $x-[x]$

$[x]$叫做x的整数部分（也称为高斯函数），$\{x\}$叫做 x的小数部分。

考点5 高斯函数

性质

(1) $x=[x]+\{x\}$;

(2) $[x]\le x<[x]+1$, $x-1<[x]\le x$, $0\le\{x\}<1$;

(3)$[n+x]=n+[x],n\in Z$;

(4) $[x]+[y]\le[x+y]$，$\{x\}+\{y\}\ge\{x+y\}$;

(5)$[-x]=\begin{cases}-[x]-1, & \text{当 } x\notin \boldsymbol{Z} \text{ 时}\\ -[x], & \text{当 } x\in \boldsymbol{Z} \text{ 时}\end{cases}$;

(6)设a,b $\in Z^+$，则不大于 a而为b的倍数的正整数的个数为 $[\frac{a}{b}]$.

考点5 高斯函数

定理

在n! 的标准分解式中，质因数p（p≤n）的指数

$$h=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]$$

推论

$$n!=\prod_{p\le n}p^{\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$$

扫码观看
视频讲解更清晰

【题14】从1到2022的正整数中，3的倍数有_____个.

【题15】100至500的正整数中，能被17整除的有(　　)个.

A.23　B. 24　C. 25　D. 26

【题16】[x]=3,[Y]=4,[Z]=2,则[X-2Y+3Z]可能的值为_____.

【题17】 7在2022！中的最高幂指数为_____.

【题18】 设x是任意实数，证明：[x]+[x+1/2]=[2x].

扫码观看
视频讲解更清晰

《初等数论》

期末突击课

课时2 不定方程

考点	重要程度	占分	题型
1. 二元一次不定方程	★★★	2-8	选择、填空、计算
2. 多元一次不定方程	★★	2-6	选择、计算
3. 勾股数	★★	2-6	判断、计算

扫码观看
视频讲解更清晰

考点1 二元一次不定方程

定理1： 二元一次不定方程$ax+by=c\left(a,b\text{不为零}\right)$ 有整数解的充要条件是$(a,b)\mid c$ 。

定理2： 设$(a,b)=d$，$a=a_1d,b=b_1d$，如果(x_0,y_0)是方程的一组解,则它所有整数

解都可以写成$\begin{cases}x=x_0-b_1t\\y=y_0+a_1t\end{cases}$，其中$t$为任意整数。

【题1】 不定方程 $8x+6y=14$ 的全部整数解是（　）

A. $\begin{cases} x=1+6t \\ y=1+8t \end{cases}(t\in Z)$　　B. $\begin{cases} x=1-6t \\ y=1+8t \end{cases}(t\in Z)$

C. $\begin{cases} x=1-3t \\ y=1+4t \end{cases}(t\in Z)$　　D. $\begin{cases} x=1+4t \\ y=1-3t \end{cases}(t\in Z)$

【题2】 $ax+by=c$ 有整数解的充要条件是_____。

【题3】 $17x+2y=3$ 的通解为_____。

【题4】解不定方程：$4x+5y=10$

解：

考点2 多元一次不定方程

定理： 已知 $a_1, a_2, \cdots, a_n$ 是非零整数,c是整数,若 $d=(a_1, a_2, \cdots, a_n)$，则方程 $a_1x_1+a_2x_2+\cdots+a_nx_n=c$ 有整数解的充要条件是 $d \mid c$。

【题1】$ax+by+cz=N$ 有整数解的充要条件是_____。

【题2】下列多元不定方程无整数解的是（　）

A. $9x+24y-5z=1000$　　B. $15x+10y+6z=61$

C. $4x-9y+5z=8$　　D. $6x+9y+15z=2$

【题3】求方程 $15x_1+10x_2+6x_3=61$ 的全部整数解。

解：

扫码观看
视频讲解更清晰

考点3 勾股数

定理1： 不定方程$x^2+y^2=z^2$满足条件：$x>0,y>0,z>0,(x,y)=1,2|x$ 的一切正整数解可以用下列公式表示出来：$x=2ab,y=a^2-b^2,z=a^2+b^2,a>b>0,(a,b)=1,$ a,b 一奇一偶。

【题1】 判断：

（1）满足勾股方程$x^2+y^2=z^2$的x,y必是一奇一偶.（　）

（2）若$x^2+y^2=z^2$，$(x,y)=1$,则x,y必是一奇一偶.（　）

【题2】求 $x^2+y^2=65^2$ 的全部正整数解。

解：

扫码观看
视频讲解更清晰

《初等数论》

期末突击课

课时3　同余

考点	重要程度	占分	题型
1. 同余的概念与性质	★★★	2-10	选择、填空、计算、证明
2. 完全剩余系	★★	2	选择、填空
3. 欧拉函数	★★	2	选择、填空
4. 简化剩余系	★★	2	选择、填空
5. 欧拉定理和费马定理	★★★	2-6	填空、证明

考点1 同余的概念与性质

定义： 给定正整数m,如果整数a与b之差被m整除,则称a与b对于模m同余,

记作 $a \equiv b \pmod{m}$;如果整数a与b之差不能被m整除,则称a与b对于模m不同余,

记作 $a \not\equiv b \pmod{m}$ 。

定理1： 下面的三种叙述是等价的

① $a \equiv b \pmod{m}$;

② 存在整数 q, 使得$a = b + qm$;

③ 存在整数 q_1, q_2, 使得 $a = q_1 m + r$， $b = q_2 m + r (0 \le r < m)$ 。

扫码观看
视频讲解更清晰

定理2： 同余具有如下性质

① $a \equiv a \pmod{m}$

② $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

③ $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

定理3： 设 a,b,c,d 是整数，$a \equiv b \pmod{m}, c \equiv d \pmod{m}$ ，则

① $a+c \equiv b+d \pmod{m}$;

② $ac \equiv bd \pmod{m}$.

定理4： 若 $a+b \equiv c \pmod{m}$ ，则 $a \equiv c-b \pmod{m}$.

定理5： 下列结论成立

① $a \equiv b(\bmod m), d \mid m, d > 0 \Rightarrow a \equiv b(\bmod d)$ ；

② $a \equiv b(\bmod m), k > 0 \Rightarrow ak \equiv bk(\bmod mk)$ ；

③ $a \equiv b(\bmod m_i), 1 \le i \le k \Rightarrow a \equiv b(\bmod [m_1, m_2, \cdots, m_k])$ ；

④ $a \equiv b(\bmod m), \Rightarrow (a, m) = (b, m)$；

⑤ $ac \equiv bc(\bmod m), (c, m) = 1 \Rightarrow a \equiv b(\bmod m)$.

定理6： 设 $a_i, b_i (0 \le i \le n)$, x, y都是整数,并且 $x \equiv y(\bmod m), a_i \equiv b_i(\bmod m), (0 \le i \le n)$ ，

则 $\sum_{i=0}^{n} a_i x^i \equiv \sum_{i=0}^{n} b_i y^i \pmod m$

定理7： 设 $N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_n 10 + a_0$,则

$(1) 3 \mid N \Leftrightarrow 3 \mid \sum_{i=0}^{n} a_i; (2) 9 \mid N \Leftrightarrow 9 \mid \sum_{i=0}^{n} a_i; (3) 11 \mid N \Leftrightarrow 11 \mid \sum_{i=0}^{n} (-1)^i a_i.$

【题1】判断：

（1）若 $a \equiv b(\bmod m), k \in Z$，则 $ka \equiv kb(\bmod m)$. （　　）

（2）若 $ab \equiv 0(\bmod m)$ 则 $a \equiv 0(\bmod m)$ 或 $b \equiv 0(\bmod m)$. （　　）

【题2】四位数 $\overline{3AA1}$ 能被9整除，则 $A=$_____。

【题3】下列各数中，能被11整除的是（ ）

A.75523　　B.868967　　C.1095874　　D.38635

【题4】2002^{2002} 被3除后余数为_____。

【题5】 2^{2003} 的末位数是_____。

【题6】证明：$641 \mid 2^{2^5}+1$

证明：

考点2 完全剩余系

定义1： 给定正整数m,将所有整数按照除以m的余数可以分成m类，称为模m的剩余类.

定义2： 从模m的剩余类中，每一类中任取一个数，得到的m个数称为模m的一个完全剩余系.

注： (1) $0,1,2,\cdots,m-1$ 是模m的最小非负完全剩余系;

(2) m为偶数时，$-\frac{m}{2}+1,\cdots,-1,0,1,\cdots,\frac{m}{2}$ 为模m的绝对最小完全剩余系;

m为奇数时，$-\frac{m-1}{2},\cdots,-1,0,1,\cdots,\frac{m-1}{2}$ 为模m的绝对最小完全剩余系。

定理1： 模m的一个完全剩余系当且仅当m个整数对模m两两不同余.

定理2： 设 $m \geq 1, a, b$ 是整数，$(a, m) = 1$，$\{x_1, x_2, \cdots x_m\}$ 是模m的一个完全剩余系，则 $\{ax_1 + b, ax_2 + b, \cdots, ax_m + b\}$ 也是模m的一个完全剩余系.

定理3： 若 $m_1, m_2 \in N^*, (m_1, m_2) = 1$，则当 x_1 与 x_2 分别通过模 m_1 与模 m_2 的完全剩余系时，$m_2 x_1 + m_1 x_2$ 通过模 $m_1 m_2$ 的完全剩余系.

【题1】模6的绝对最小完全剩余系是_____。

【题2】判断：有些整数的完全剩余系中的数可以都是偶数；（ ）

【题3】判断：当x遍历模10的完全剩余系时，$2x+3$所取得值也遍历模10的完全剩余系。

（ ）

考点3 欧拉函数

定义： 对于正整数k,函数$\varphi(k)$的值等于序列 $0,1,2,\cdots,k-1$ 中与k互素的数的个数,称$\varphi(k)$为欧拉(Euler)函数.

注： (1) 特别地,当p是素数时, $\varphi(p)=p-1,\varphi(p^k)=p^k-p^{k-1}$

(2) $\varphi(1)=1$

定理1： 若 $m_1,m_2\in Z_+,(m_1,m_2)=1$,则 $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$ 。

定理2： $n\in Z_+$, $p_1,p_2,\cdots,p_k$ 是它的全部素因数,则 $\phi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$

【题3】计算：

(1) $\varphi(1000)=$ _____。

(2) $\varphi(1)+\varphi(P)+\cdots\varphi(P^n)=$ _____。

解：

考点4 简化剩余系

定义： 若模m的剩余类中的任一个数都与m互质，称为模m的一个简化剩余类。从模m的所有简化剩余类中各取一个数，构成了模m的一个简化剩余系。

定理1： 设a是整数，$(a,m)=1, B=\{x_1,x_2,\cdots,x_{\varphi(m)}\}$是模$m$的简化剩余系，则$A=\{ax_1,ax_2,\cdots,ax_{\varphi(m)}\}$也是模$m$的简化剩余系。

定理2： 设$m_1,m_2\in N,(m_1,m_2)=1$，又设$X=\{x_1,x_2,\cdots,x_{\varphi(m_1)}\}$与$Y=\{y_1,y_2,\cdots,y_{\varphi(m_2)}\}$分别是模$m_1,m_2$的简化剩余系，则$A=\{m_1y+m_2x\mid x\in X,y\in Y\}$是模$m_1m_2$的简化剩余系。

【题1】判断：若 x_0、x_1、$x_2 \cdots x_k$ 是模m的一个简化剩余系，则 ax_0、ax_1、$ax_2 \cdots ax_k$ 也是模m的一个简化剩余系。（ ）

【题2】模18的最小正简化剩余系有（ ）个数。

A.18　　B.7　　C.6　　D.5

【题3】从满足以下要求的整数中，能选取出模20的简化剩余系的是（ ）

A.2的倍数　　B.3的倍数　　C.4的倍数　　D.5的倍数

【题4】写出6的一个简化剩余系，要求每项都是5的倍数_____。

考点5 欧拉定理和费马定理

定理1： 欧拉(Euler)定理，设m是正整数，$(a,m)=1$，则 $a^{\varphi(m)}\equiv 1(\mathrm{mod}\, m)$.

定理2： 费马(Fermat)定理，设p是素数,则对于任意的整数a,有 $a^{p}\equiv a(\mathrm{mod}\, p)$

定理3： 有理数 $\frac{a}{b},0<a<b,(a,b)=1$，能表示成纯循环小数的充要条件是 $(b,10)=1$.

定理3： 若 $\frac{a}{b}$ 是有理数，其中 $0<a<b,(a,b)=1,b=2^{\alpha}5^{\beta}b_1,(b_1,10)=1,b_1\neq 1,\alpha,\beta$ 不全为零，则 $\frac{a}{b}$ 可以表成混循环小数，其中不循环的位数是 $\mu=\max\{\alpha,\beta\}$.

【题1】若 $(a,m)=1$，则 $a^{\varphi(m)}\equiv$ _____ $(\mathrm{mod}\, m)$；

若m是_____时，$a^m\equiv a(\mathrm{mod}\, m)$.

【题2】以下四个分数不能化为纯循环小数的是（ ）

A. $\frac{15}{37}$　　B. $\frac{139}{875}$　　C. $\frac{9}{13}$　　D. $\frac{1}{17}$

【题3】$\frac{1}{17408}$化为混循环小数，其不循环部分位数是（ ）位

A.10　　B.12　　C.14　　D.16

【题4】 $0.3\dot{2}$化为分数是_____。

【题5】 求13除 8^{4965} 的余数.

扫码观看
视频讲解更清晰

【题6】 叙述并且证明欧拉定理。

《初等数论》

期末突击课

课时4 同余式

考点	重要程度	占分	题型
1.一次同余式	★★★	2-10	选择、填空、计算
2.孙子定理	★★★	8	填空、计算
3.威尔逊定理	★★	2-6	证明

考点1 一次同余式

定理 设a，b是整数，$a \not\equiv 0 \pmod{m}$。则一次同余式

$$ax \equiv b \pmod{m}$$

有解的充要条件是$(a, m) | b$。若有解，则恰有$d = (a, m)$个解。

扫码观看
视频讲解更清晰

【题1】$ax \equiv b \pmod{m}$ 有解的充要条件是_____。

【题2】同余式$28x \equiv 21 \pmod{35}$的解的个数（　　）

A. 1　　B. 7　　C. 3　　D. 0

【题3】同余式 $8x \equiv 9 \pmod{11}$的解为（　　）

A. $x \equiv 6 (\mathrm{mod} 11)$　　B. $x \equiv 7 (\mathrm{mod} 11)$

C. $x \equiv 8 (\mathrm{mod} 11)$　　D. $x \equiv 9 (\mathrm{mod} 11)$

【题4】解下列同余式：

(1) $73x \equiv 1 (\mathrm{mod}\, 13)$

(2) $20x \equiv 44 (\mathrm{mod}\, 72)$

考点2 孙子定理

定理(孙子定理)

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \\ \cdots\cdots \\ x \equiv a_k (\mathrm{mod}\, m_k) \end{cases}$$

设$m_1, m_2, \ldots, m_k$是正整数，

$(m_i, m_j) = 1$， $1 \le i, j \le k$， $i \ne j$,

记$m = m_1 m_2 \ldots m_k$， $M_i = \frac{m}{m_i}$ ， $1 \le i \le k$,

则存在整数M_i'（$1 \le i \le k$），使得

$M_i M_i' \equiv 1 \pmod{m_i}$,

并且

$$x \equiv \sum_{i=1}^{k} a_i M_i M_i' \pmod{m}$$

是同余方程组的解.

【题5】解同余式组：

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

【题6】解同余式组：

$$\begin{cases} x \equiv -2 \pmod{12} \\ x \equiv 6 \pmod{10} \\ x \equiv 1 \pmod{15} \end{cases}$$

扫码观看
视频讲解更清晰

考点3 威尔逊定理

定理〔Wilson定理〕

p为素数，则$(p-1)! \equiv -1 (\mathrm{mod}\ p)$

【题7】证明：设P为素数，试证对任整数a，都有 $P\mid(P-1)!a^{P}+a$。

【题8】证明：设$2p+1$为素数，试证 $(p!)^2+(-1)^p\equiv 0(\mathrm{mod}\,2p+1)$

扫码观看
视频讲解更清晰

《初等数论》

期末突击课

课时5 二次同余式和平方剩余

考点	重要程度	占分	题型
1.平方剩余和平方非剩余	★★	2	选择、填空
2.欧拉判别条件	★★	2	选择、填空
3.勒让德符号	★★★	2-8	填空、选择、计算
4.雅克比符号	★★	2	选择、填空

考点1 平方剩余和平方非剩余

定义 设p是素数，a为整数，且$(a,p)=1$.

若 $x^2 \equiv a(\mathrm{mod}\, p)$ 有解，称a为模p的平方剩余；

若 $x^2 \equiv a(\mathrm{mod}\, p)$ 无解，称a为模p的平方非剩余.

扫码观看
视频讲解更清晰

【题1】模7的平方剩余为（ ）

A. 1,2,3,4,5,6　　B. 1,2,3　　C. 1,2,4　　D. 4,5,6

【题2】模11的平方非剩余为（ ）

A. 1,2,3,4,5　　B. 6,7,8,9,10　　C. 1,3,4,5,9　　D. 2,6,7,8,10

考点2 欧拉判别条件

定理1(欧拉判别条件) 若$(a, p)=1$, $x^2 \equiv a(\mathrm{mod}\ p)$.

则a是p的平方剩余的充要条件是 $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$;

a是p的平方非剩余的充要条件是 $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$;

且若a是p的平方剩余，则 $x^2 \equiv a(\mathrm{mod}\ p)$ 有两个解.

考点2 欧拉判别条件

定理2 模p的简化剩余系中平方剩余和平方非剩余各为 $\frac{p-1}{2}$，而且 $\frac{p-1}{2}$ 个平方剩余分别与序列 $1^2,2^2,\cdots,(\frac{p-1}{2})^2$ 中之一数同余，且仅与一数同余.

【题3】设p为单质数，$(a,p)=1$，则a是模p的平方剩余的充分必要条件是（　　）

A. $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

B. $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

C. $a \equiv \frac{p-1}{2} \pmod{p}$

D. $a \equiv -\frac{p-1}{2} \pmod{p}$

【题4】模17的平方剩余有_____个，在其绝对最小简化剩余系中，_____是平方剩余.

【题5】判断：

设p是奇素数，则模p的两个平方非剩余的乘积是平方非剩余；（　　）

设p是奇素数，则模p的平方剩余和平方非剩余的个数相同；（　　）

扫码观看
视频讲解更清晰

考点3 勒让德符号

定义

勒让得（Legendre）符号$(\frac{a}{p})$ (读作a对p的勒让得符号)是一个对于给定的单质数

定义p在一切整数a上的函数，它的值规定如下：

$$(\frac{a}{p})=\begin{cases}1, a\text{是模p的平方剩余}\\ -1, \text{a是模p的平方非剩余}\\ 0, p\mid \text{a}.\end{cases}$$

考点3 勒让德符号

性质

(1) $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\ p)$

(2) $a \equiv b(\mathrm{mod}\ p), \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$

(3) $(\frac{a_1 a_2 \cdots a_k}{p}) = (\frac{a_1}{p})(\frac{a_2}{p}) \cdots (\frac{a_k}{p})$

(4) $(\frac{1}{p}) = 1$

考点3 勒让德符号

性质

(5) $$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, p=4k+1\\-1, p=4k+3\end{cases}$$

(6) $$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right),\quad p\nmid b$$

(7) $$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, p=8k\pm1\\-1, p=8k\pm3\end{cases}$$

考点3 勒让德符号

定理(高斯二次互反律) 设p与q是不相同的两个奇素数，则

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

【题6】以下正确的是：

A. $\left(\frac{18}{11}\right)=\left(\frac{-1}{11}\right)$　　B. $\left(\frac{12}{5}\right)=-\left(\frac{3}{5}\right)$

C. $\left(\frac{5}{12}\right)=\left(\frac{5}{2}\right)$　　D. $\left(\frac{7}{11}\right)=\left(\frac{4}{11}\right)$

【题7】高斯互反律是_____.

扫码观看
视频讲解更清晰

【题8】 （1）判断方程 $x^2 \equiv 3 \pmod{83}$ 是否有解，若有解，则有几解。

（2）设p，q是两个不同的奇素数，且 $p \equiv 1 \pmod{4}$，证明：$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ 。

考点4 雅克比符号

定义 给定正奇数$m>1$，$m=p_1p_2\cdots p_k$，其中p_i（$1\le i\le k$）是奇素数，对于任意的整数a，定义 $\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$

其中右端的 $\left(\frac{a}{p_i}\right)$（$1\le i\le k$）是勒让德符号，称 $\left(\frac{a}{m}\right)$ 是雅克比符号.

考点4 雅克比符号

性质

(1) 若$a \equiv a_1 \pmod{m}$，则 $\left(\frac{a}{m}\right)=\left(\frac{a_1}{m}\right)$；

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

(3) 对于任意的整数$a_1, a_2, \ldots, a_t$，有 $\left(\frac{a_1 a_2 \cdots a_t}{m}\right)=\left(\frac{a_1}{m}\right)\left(\frac{a_2}{m}\right)\cdots\left(\frac{a_t}{m}\right)$

(4) 对于任意的整数a，b，(a, m) = 1，有 $\left(\frac{a^2 b}{m}\right)=\left(\frac{b}{m}\right)$

考点4 雅克比符号

性质

(5) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$

(6) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$

(7) 设m，n是大于1的奇数，则 $\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$

扫码观看
视频讲解更清晰

【题9】已知769是素数，判定下列方程是否有解：

$$x^2 \equiv 1742 \pmod{769}$$