第二讲　同余的表示

同余的定义

设 a、b 是两个整数，如果 a 和 b 除以正整数 m 所得的**余数相同**，则称 a 与 b 对于**模 m 同余**，记作 $a\equiv b\pmod m$，否则称 a 与 b 对于模 m 不同余，记作 $a\not\equiv b\pmod m$.

显然 $a\equiv b\pmod m\Leftrightarrow m\mid(a-b)\Leftrightarrow a=km+b\,(k\in\mathbb{Z})$.

同余关系和等式关系十分类似，它们都具备如下基本性质：

反身性：对任意整数 a，有 $a\equiv a\pmod m$

对称性：若整数 a、b 满足 $a\equiv b\pmod m$，则 $b\equiv a\pmod m$

传递性：若整数 a、b、c 满足 $a\equiv b\pmod m$，$b\equiv c\pmod m$，则 $a\equiv c\pmod m$

同余的性质

在进行同余分析时，我们往往会用到以下几条性质：

性质 1：若 $a_1\equiv b_1\pmod m$，$a_2\equiv b_2\pmod m$，则 $a_1\pm a_2\equiv b_1\pm b_2\pmod m$.

性质 2：若 $a_1\equiv b_1\pmod m$，$a_2\equiv b_2\pmod m$，则 $a_1a_2\equiv b_1b_2\pmod m$.

特别的，若 $a\equiv b\pmod m$，则 $a^k\equiv b^k\pmod m$.

性质 3：若 $ac\equiv bc\pmod m$，$(m,c)=d$，则 $a\equiv b\left(\bmod \dfrac{m}{d}\right)$.

特别的，若 $ac\equiv bc\pmod{mc}$，则 $a\equiv b\pmod m$.

性质 4：若 $a\equiv b\pmod m$，$a\equiv b\pmod n$，则 $a\equiv b\pmod{[m,n]}$.

性质 5：若 $a\equiv b\pmod m$，$n\mid m$，则 $a\equiv b\pmod n$.

【例题】

例1. （1）计算 3^{300} 的个位数字.

（2）求 $2001\times2002+2003\times2004+2005\times2006$ 除以 45 的余数.

（1）$3^{100}\equiv9^{50}\equiv(-1)^{50}\equiv1\pmod{10}$，故个位数字为 1.

（2）$2001\times2002+2003\times2004+2005\times2006\equiv21\times22+23\times24+25\times26$

$\equiv462+552+650\equiv12+12+20\equiv44\pmod{45}$

例2. 求证：对于任何正整数 k，均有 $7\mid2^{3k+1}+3^{6k}+5^{6k}+3$.

因为 $2^{3k+1}\equiv2\cdot8^k\equiv2\cdot1^k\equiv2\pmod7$，$3^{6k}\equiv729^k\equiv1\pmod7$，$5^{6k}\equiv25^{3k}\equiv4^{3k}\equiv64^k\equiv1\pmod7$.

所以 $2^{3k+1}+3^{6k}+5^{6k}+3\equiv2+1+1+3\equiv0\pmod7$，从而 $7\mid2^{3k+1}+3^{6k}+5^{6k}+3$.

例3. （1）求所有整数 x，使得 $5x\equiv 4\pmod{11}$.

（2）求所有整数 x，使得 $6x\equiv 1\pmod 8$.

（3）求所有整数 x，使得 $75x\equiv 30\pmod{51}$.

（1）$5x\equiv 4\equiv 15\pmod{11}$，故 $x\equiv 3\pmod{11}$．所以 $x=11k+3$（$k\in\mathbb{Z}$），检验其满足要求.

（2）由 $6x\equiv 1\pmod 8$ 可得 $6x\equiv 1\pmod 2$，但 $6x\equiv 2\cdot(3x)\equiv 0\pmod 2$，矛盾．故这样的 x 不存在

（3）由 $75x\equiv 30\pmod{51}$ 可得 $5x\equiv 2\pmod{17}$，于是 $5x\equiv 2\equiv -15\pmod{17}$

故 $x\equiv -3\pmod{17}$．所以 $x=17k-3$（$k\in\mathbb{Z}$），检验其满足要求.

中国剩余定理

中国剩余定理：设 $n\geq 2$，$m_1,m_2,\cdots,m_n$ 是 n 个两两互质的正整数．则对任意 $c_1,c_2,\cdots,c_n\in\mathbb{Z}$，同余方程组

$$\begin{cases}x\equiv c_1\pmod{m_1}\\x\equiv c_2\pmod{m_2}\\\cdots\\x\equiv c_n\pmod{m_n}\end{cases}$$

在 $1\sim m_1m_2\cdots m_n$ 中**存在唯一解**.

例4. 求整数 n，使得 $n\equiv 2\pmod 7$，$n\equiv 7\pmod{11}$，$n\equiv 4\pmod{13}$.

思路一：从模 13 余 4 的数中找出模 11 余 7 的，最小为 95.

从模 143 余 95 的数中找出模 7 余 2 的，最小为 667.

这样的 n 可以写为 $1001k+667$（$k\in\mathbb{Z}$）的形式.

思路二：注意到 $3n+1\equiv 0\pmod 7$，$3n+1\equiv 0\pmod{11}$，$3n+1\equiv 0\pmod{13}$，从而 $1001\mid 3n+1$.

解得 $n\equiv 667\pmod{1001}$．故 $n=1001k+667$（$k\in\mathbb{Z}$）.

例5. （1）已知正整数 $n\leq 100$，使得 $1+2+3+\cdots+n$ 的结果为 8 的倍数，求满足要求的 n 的个数；

（2）试求最小的正整数 n，使得 $1+2+3+\cdots+n$ 的结果末三位数字组成的三位数恰好是 256.

（1）$16\mid n(n+1)$，则 n 为 16 的倍数或模 16 余 15，共 12 个.

（2）由已知有 $\dfrac{n(n+1)}{2}\equiv 256\pmod{1000}$，从而有 $\dfrac{n(n+1)}{2}\equiv 0\pmod 8$ 及 $\dfrac{n(n+1)}{2}\equiv 6\pmod{125}$，

等价于 $8\mid\dfrac{n(n+1)}{2}$、$125\mid\dfrac{n(n+1)}{2}-6$，由 $(2,125)=1$ 及 $\dfrac{n(n+1)}{2}\in\mathbb{Z}$ 可知，

等价于 $16\mid n(n+1)$、$125\mid n(n+1)-12$.

由 $(n,n+1)=1$ 可知，n 模 16 余 0 或 15.

由 $n(n+1)-12=(n-3)(n+4)$，以及 $(n-3,n+4)=(n-3,7)=1$ 或 7 可知，n 模 125 余 3 或 121.

当n模 125 余 3 时，满足模 16 余 0 或 15 的n最小为 128.

当n模 125 余 121 时，128 以内只有 121 满足条件，而 121 模 16 余 9.

综上所述，满足条件的最小正整数$n=128$.

例6. 求最小的正整数 n，使得2^n-n是 3 的倍数，3^n-n是 5 的倍数，5^n-n是 2 的倍数.

由2^n-n是 3 的倍数可得：$n\equiv 4,5\pmod 6$；

由3^n-n是 5 的倍数可得：$n\equiv 7,13,14,16\pmod{20}$；

由5^n-n是 2 的倍数可得：$n\equiv 1\pmod 2$.

综上可得$n\equiv 47,53\pmod{60}$，故 n 最小为 47.