第三讲　从费马小定理谈起

例1. 利用费马小定理，

$2730=2\times3\times5\times7\times13$．故而只需分别证明 2,3,5,7,13 分别整除 $n^{13}-n$ 即可．

对任意 $p\in\{2,3,5,7,13\}$，验证可知 $p-1|12$．

对整数 n，若 $p|n$，则 $p|n^{13}-n$；若 $(p,n)=1$，则 $p|n^{p-1}-1$，于是由 $p-1|12$ 可得 $p|n^{12}-1$，也有 $p|n^{13}-n$．

例2. （1）$10^n\div7$ 余数规律为：3,2,6,4,5,1 循环．由费马小定理可得 $10^6\equiv1(\bmod 7)$，

且 $10^{10}\equiv4(\bmod 6)$，可知 $10^{10^{10}}\equiv10^4\equiv4(\bmod 7)$，故而为星期四．

（2）$77=7\times11$，由费马小定理可得 $999^6\equiv1(\bmod 7)$，且 $999\equiv3(\bmod 6)$，

故而 $999^{999}\equiv999^3\equiv5^3\equiv6(\bmod 7)$，又因 $999^{10}\equiv1(\bmod 11)$，

$999\equiv9(\bmod 11)$，$999^{999}\equiv999^9\equiv(-2)^9\equiv5(\bmod 11)$．

再由中国剩余定理计算可得 $999^{999}\equiv27(\bmod 77)$．

例3. 由费马小定理可知，若 k 是 p 的倍数，则有 $k^{p-1}\equiv0(\bmod p)$；若 k 不是 p 的倍数，则有 $k^{p-1}\equiv1(\bmod p)$．

而 1,2,3,…,100 中 p 的倍数共有 $\left[\dfrac{100}{p}\right]$ 个，因此 $\sum\limits_{k=1}^{100}k^{p-1}\equiv100-\left[\dfrac{100}{p}\right](\bmod p)$．

设 $100=mp+r,m\ge0,0\le r<p$，则有 $p|100-m$，于是 $p|m-r$．

若 $m=r$，则 $100=r(p+1)$，由 $r<p$ 及 p 为质数可算得 $p=19$；

若 $m\ne r$，则 $m\ge p+r$，于是 $100\ge p^2$，逐一检验可知 $p=2,5$ 满足条件．

综上所述，所求数为 2,5,19．

例4. 由费马小定理可得，$a^p\equiv a(\bmod p)$，$b^p\equiv b(\bmod p)$．$p|(a^p-b^p)$ 等同于 $p|(a-b)$，

只需证 $p|\dfrac{a^p-b^p}{a-b}=a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}$，

（1）利用同余：因 $a\equiv b(\bmod p)$，则 $a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}\equiv pa^{p-1}\equiv0(\bmod p)$，

故而 $p^2|(a^p-b^p)$．

（2）利用二项式定理：设 $a-b=m$，则 $a=m+b$．则 $\dfrac{a^p-b^p}{a-b}=\dfrac{(b+m)^p-b^p}{m}=C_p^1b^{p-1}+C_p^2b^{p-2}m+\ldots+C_p^{p-1}bm^{p-2}+m^{p-1}$，因为 $p|m$，故而上式为 p 的倍数．故而 $p^2|(a^p-b^p)$．

例5. 只需证①对任意正整数 $t,tm_0\in M$，②若 $k\in M$，则 $m_0|k$．

①由 $m_0\in M$，可知 $am_0\equiv1(\bmod n)$，

于是 $a^{tm_0}\equiv(a^{m_0})^t\equiv1^t\equiv1(\bmod n)$，

故而 $tm_0\in M$．

②若 $k\in M$，则 $a^k\equiv 1\pmod n$

设 $k=tm_0+r,0\le r<m_0$（带余除法）.

则 $a^{tm_0+r}\equiv 1\pmod n$，

而 $a^{tm_0+r}\equiv a^r\left(a^{m_0}\right)^t\equiv a^r\cdot 1^t\equiv a^r\pmod n$.

因此 $a^r\equiv 1\pmod n$，由 m_0 最小可知 $r=0$，即 $m_0\mid k$.

例6. 设 $\operatorname{ord}_m(a)=x,\operatorname{ord}_m(b)=y,\operatorname{ord}_m(ab)=k$，则有 $(ab)^{xy}\equiv\left(a^x\right)^y\cdot\left(b^y\right)^x\equiv 1\pmod m$，因此由阶的结论，有 $k\mid xy$．另外，由 $(ab)^k\equiv 1\pmod m$ 可得 $(ab)^{kx}\equiv 1\pmod m$，而 $a^{kx}\equiv\left(a^x\right)^k\equiv 1\pmod m$，所以有 $b^{kx}\equiv 1\pmod m$，因此由阶的结论，有 $y\mid kx$．注意到已知条件有 $(x,y)=1$，所以 $y\mid k$．同理可得 $x\mid k$，进而有 $xy\mid k$.

综上可知，$k=xy$，命题得证.