数论中的著名定理

本讲主要介绍几个数论中的著名定理，算术基本定理非常基础，这里也包括在内. 之后着重介绍欧拉定理、费马小定理与中国剩余定理. 裴蜀定理和威尔逊定理使用较少，这里稍微提及一下. 这一讲是这些定理的初步应用，更进一步的应用需要结合其它数论知识再进行详述.

算术基本定理（唯一分解定理）：

设 n 是大于 1 的整数，则 n 可写为 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 的形式，其中 $p_1,p_2,\cdots,p_k$ 是互不相同的 k 个素数，$\alpha_1,\alpha_2,\cdots,\alpha_k$ 均为正整数. 该写法在不计次序的意义下是唯一的.

欧拉函数与欧拉定理：

设 m 为正整数，在 1,2,...,m 中，与 m 互质的数的个数记为 $\varphi\ m$ ，它称为欧拉函数.

例如：$\varphi\ 1\ =1,\varphi\ 2\ =1,\varphi\ 3\ =2,\varphi\ 4\ =2,\varphi\ 5\ =4,\cdots$

欧拉函数具有性质：

(1) 如果 m 和 n 互素，则 $\varphi\ mn\ =\varphi\ m\ \varphi\ n$.

(2) 设 p 为素数，n 为正整数，则 $\varphi\ p^n\ =p^{n-1}\ p-1\ =p^n\left(1-\frac{1}{p}\right)$.

因此，对于正整数的唯一分解式 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，有：

$$\varphi\ n\ =p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

练习 1：证明 $\varphi\ n\ =\frac{1}{4}n$ 不可能成立.

欧拉定理：设整数 a 与正整数 m 互质，则 $a^{\varphi\ m}\ \equiv 1\ \mathrm{mod}\,m$.

欧拉定理的证明：取 1,2,...,m 中所有与 m 互质的数 $x_1,x_2,\cdots,x_{\varphi\ m}$ ，则 $ax_1,ax_2,\cdots,ax_{\varphi\ m}$ 都是与 m 互质的数，并且 $ax_1,ax_2,\cdots,ax_{\varphi\ m}$ 除以 m 的余数两两互不相同，因此 $ax_1,ax_2,\cdots,ax_{\varphi\ m}$ 除以

m 的余数构成的集合与 $x_1,x_2,\cdots,x_{\varphi\ m}$ 一致. 因此 $ax_1,ax_2,\cdots,ax_{\varphi\ m}$ 的乘积与 $x_1,x_2,\cdots,x_{\varphi\ m}$ 的乘积模 m 同余，即 $a^{\varphi\ m}x_1x_2,\cdots x_{\varphi\ m}\equiv x_1x_2,\cdots x_{\varphi\ m}\ \ \mathrm{mod}\,m$ ，因为 $x_1x_2,\cdots x_{\varphi\ m}$ 与 m 互素，两边约去 $x_1x_2,\cdots x_{\varphi\ m}$ 即得 $a^{\varphi\ m}\equiv 1\ \mathrm{mod}\,m$.

费马小定理：

在欧拉定理中取 m 为一个素数 p，因为 $\varphi\ \ p\ =p-1$，可得如下结论：

设整数 a 不是素数 p 的倍数，则 $a^{p-1}\equiv 1\ \mathrm{mod}\,p$. 该结论即为费马小定理.

注：这里 a 不是 p 的倍数这个条件必不可少，如果 a 是 p 的倍数，那么 $a^{p-1}\equiv 0\ \ \mathrm{mod}\,p$ ，据此也可以得到：对任意整数 a 和素数 p，有： $a^{p}\equiv a\ \ \mathrm{mod}\,p$.

中国剩余定理（孙子定理）：

设正整数 $m_1,m_2,\cdots,m_k$ 两两互质，则对于任意给定的整数 $a_1,a_2,\cdots,a_k$，同余方程组：

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

一定有解，并且它的全部解可以写成

$x=a_1b_1m_2m_3\cdots m_k+a_2b_2m_1m_3\cdots m_k+\cdots+a_kb_km_1m_2\cdots m_{k-1}+lm_1m_2\cdots m_k$ 的形式，其中 l 是任意整数，而 $b_i\ \ i=1,2,\cdots,k$ 满足： $b_i\cdot\ \ m_1m_2\cdots m_{i-1}m_{i+1}\cdots m_k\ \ \equiv 1\ \mathrm{mod}\,m_i$.

注 1：上式中出现的 $m_1m_2\cdots m_{i-1}m_{i+1}\cdots m_k$ 就是把 $m_1,m_2,\cdots,m_k$ 中除了 m_i 以外的 k-1 个数乘在一起，可以写为 $\dfrac{m_1m_2\cdots m_k}{m_i}$，或者 $m_1m_2\cdots\overline{m_i}\cdots m_k$，其中 $\overline{m_i}$ 表示在求乘积的时候，把 m_i 这一项给略去.

注 2：$b_i\cdot\ \ m_1m_2\cdots m_{i-1}m_{i+1}\cdots m_k\ \ \equiv 1\ \mathrm{mod}\,m_i$ ，也可写为 $b_i\equiv\ \ m_1m_2\cdots m_{i-1}m_{i+1}\cdots m_k\ ^{-1}\ \ \mathrm{mod}\,m_i$ ，一般来说如果 $ab\equiv 1\ \mathrm{mod}\,n\ ,n>1$，则可以写为 $a\equiv b^{-1}\ \ \mathrm{mod}\,n$ ，b^{-1} 称为 b 在模 n 下的同余逆，b^{-1} 在模 n 的意义下是唯一的.

注 3：定理中的同余方程组的解 x，在模 $m_1m_2,\cdots m_k$ 的意义下是唯一的，不难验证这个解确实满足条件.

练习 2：一个正整数除以 7 余 1，除以 8 余 2，除以 9 余 4，求这个正整数的最小可能值.

中国剩余定理不仅提供了解同余方程组的方法，而且具有极其重要的理论意义，具体来说，可以证明满足某些同余条件的数是存在的（而不必解出它），为接下来的证明作铺垫.

威尔逊定理：

设 p 为素数，则 $p-1\,!\equiv-1\ \mathrm{mod}\,p$. 反之，若大于 1 的整数 p 满足 $p-1\,!\equiv-1\ \mathrm{mod}\,p$ ，则 p 是素数.

威尔逊定理的证明可以用上述同余逆的性质. 把$1,2,\cdots,p-1$这些数作配对，每个数和它自己的同余逆配对在一起，则除了$1,p-1$以外的数可以配成$\dfrac{p-3}{2}$对（大家想想这是为什么），每一对的乘积除以 p 都余 1，因此$1,2,\cdots,p-1$这些数的乘积与$1,p-1$这两个数的乘积模 p 同余.

“反之”的这一部分的证明可以用反证法.

裴蜀(Bezout)定理：

设正整数 a,b 的最大公约数为 d，则存在整数 u 和 v，使得$ua+vb=d$.

推论：正整数 a,b 互素的充要条件是，存在整数 u 和 v，使得$ua+vb=1$.

由此可知，当正整数 a,b 互素时，形如$ua+vb\ \ u,v\in\mathbb{Z}$ 的数可以表示所有整数.

如果是任意正整数 a,b，则形如$ua+vb\ \ u,v\in\mathbb{Z}$ 的数可以表示所有 a,b 的倍数.

裴蜀定理也可以推广到任意多个正整数的最大公约数的情况，即：

对于任意的正整数$a_1,a_2,\cdots,a_n$，存在整数$k_1,k_2,\cdots,k_n$使得：

$$k_1a_1+k_2a_2+\cdots+k_na_n=\ a_1,a_2,\cdots,a_n\ .$$

例题：

1. 证明：对任意整数 x，$\dfrac{1}{5}x^5+\dfrac{1}{3}x^3+\dfrac{7}{15}x$是一个整数.

2. 求证：对任意整数 n，$2730 \mid n^{13}-n$.

3. 求所有满足 $\varphi(pq)=3p+q$ 的素数对 (p,q)，其中 $\varphi(pq)$ 是欧拉函数.

4. 求所有的素数对 (p,q)，使得 $pq \mid (5^{p}+5^{q})$.

5. 求所有的素数对 (p,q)，使得 $pq \mid (p^{p}+q^{q}+1)$.

6. 求所有的整数对 (m,n)，使得 $mn \mid (3^{m}+1)$, $mn \mid (3^{n}+1)$.

7. 证明：若 p 为奇素数，则 $\sum_{k=1}^{p-1} k^{2p-1} \equiv \frac{p(p+1)}{2} \pmod{p^{2}}$

8. 设 $m_1, m_2, \cdots, m_r$ 为两两互质的正整数，证明存在 r 个连续的自然数，使得 m_i 整除其中的第 $i\ (i=1,2,\cdots,r)$ 个.

9. 证明对任意正整数 r，存在 r 个连续正整数，它们都不是质数的幂.

10. 是否存在 1000000 个连续整数，使得每一个数都能被某个素数的平方所整除？（即每个数都有大于 1 的平方因子.）

11. (1990 年国家集训队测试题)能否找到含有 1990 个自然数的集合 S，使得
(1) S 中任意两数互素；
(2) S 中任意 $k\ (\geq 2)$ 个数的和为合数.

12. (IMO-33 预选题)是否存在具有如下性质的集合 M?

(1) 集合 M 由 1992 个自然数构成.

(2) 集合 M 中的任何元素以及其中任意个元素之和都具有 m^k 的形式(其中 $m,k\in\mathbb{N}^+,k\geq 2$).

13. 设整数 n 和 q 满足 $n\geq 5, 2\leq q\leq n$，证明： $q-1 \mid \left[\frac{n-1\ !}{q}\right]$，其中 x 表示不超过 x 的最大整数.

14. 设 n 是一个正整数，k 是一个正偶数，证明：存在整数 x,y 使得 $x,n = y,n =1$，且 $x+y\equiv k \bmod n$.

15. 证明：若 a,b,c,d 均为整数，且 $ad-bc=1$，则分数 $\frac{a^2+b^2}{ac+bd}$ 不可约.

16. (2005 年德国数学奥林匹克)在平面上的每个整点 x,y 处放一盏灯，在 $t=0$ 时刻，仅有一盏灯亮着，每过一秒，就有一些满足下列条件的灯被打开：该灯与至少一盏亮着的灯的距离为 2005. 证明：这个过程反复继续下去，每盏灯终究都能被打开.

17*. 设 n 为大于 1 的整数，证明： 2^n-1 不能被 n 整除.

18*. (IMO-40)确定所有的正整数对 n,p ，满足：p 是一个素数， $n\leq 2p$，且 $p-1^{\ n}+1$ 能够被 n^{p-1} 整除.

19* (2006 年集训队试题) 求所有的正整数对 a,n ，使得 $\frac{a+1^{\ n}-a^n}{n}$ 是整数.