欧拉定理

主讲人：邓哲也

欧拉函数

设 n 是一个正整数。欧拉函数 $\Phi(n)$ 定义为不超过 n 且与 n 互素的正整数的个数。

n	1	2	3	4	5	6	7	8	9	10	11	12
$\Phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

模 n 的既约剩余系

模 n 的既约剩余系是由 $\Phi(n)$ 个整数构成的集合，集合中的每个元素均与 n 互素，且任何两个元素模 n 不同余。

如 {1，3，5，7} 就是模 8 的一个既约剩余系。

欧拉定理

设 m 是一个正整数，a 是一个整数且 (a, m) = 1，那么

$a^{\phi(m)} \equiv 1 \pmod{m}$

比如 a = 3, m = 8

3 * 1， 3 * 3， 3 * 5， 3 * 7 是模 8 的既约剩余系

(3 * 1) * (3 * 3) * (3 * 5) * (3 * 7) ≡ 1 * 3 * 5 * 7 (mod 8)

因为 (1 * 3 * 5 * 7, 8) = 1，故 $3^4 \equiv 1 \pmod{8}$

欧拉定理

设 m 是一个正整数，a 是一个整数且 (a, m) = 1，那么

$a^{\phi(m)} \equiv 1 \pmod{m}$

由此可以得到求 a 模 m 的逆的方法。

$a^{\phi(m)} \equiv 1 \pmod{m}$

$a * a^{\phi(m)-1} \equiv 1 \pmod{m}$

$a^{\phi(m)-1}$ 就是 a 模 m 的逆。

欧拉定理求同余方程

对于同余方程　　$ax \equiv b \pmod m$

两边同乘 a 的逆　　$a^{\phi(m)-1} ax \equiv a^{\phi(m)-1} b \pmod m$

就可以得到　　$x \equiv a^{\phi(m)-1} b \pmod m$

比如：由 $\phi(10) = 4$，对于同余方程 $3x \equiv 7 \pmod{10}$

解为 $x \equiv a^{\phi(m)-1} b \equiv 3^3 * 7 \equiv 9 \pmod{10}$

欧拉函数的性质

【定理1】如果 p 是素数，那么 φ(p) = p - 1。反之，如果 p 是一个正整数且满足 φ(p) = p - 1，那么 p 是素数。

证明显然。如果 p 不是素数，那肯定存在一个大于 1 小于 p 的因子。

欧拉函数的性质

【定理2】如果 p 是素数，a 是一个正整数，那么 $\Phi(p^a) = p^a - p^{a-1}$.

证明：所有不超过 p^a，且和 p 不互素的正整数就是那些不超过 p^a，且能够被 p 整除的所有整数，即 kp (1 <= k <= p^{a-1})

因为恰有 p^{a-1}个这样的整数，所以 $\Phi(p^a) = p^a - p^{a-1}$.

欧拉函数的性质

【定理3】设 m 和 n 是互素的正整数，那么

$$\phi(mn) = \phi(m)\phi(n)$$

第二行和第四行，每个元素都不和 4 互素。

剩下的两行，每个元素都和 4 互素，但各有 6 个数和 9 互素。

(1)	(5)	9	(13)	(17)	21	(25)	(29)	33
2	6	10	14	18	22	26	30	34
3	(7)	(11)	15	(19)	(23)	27	(31)	(35)
4	8	12	16	20	24	28	32	36

欧拉函数的性质

【定理4】设 $n = p_1^{a_1}\ p_2^{a_2} \dots\ p_k^{a_k}$ 为正整数 n 的素数幂分解，

那么：

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

证明只要对每个质因子单独考虑。

欧拉函数的性质

【定理5】设 n 为一个正整数，那么 $\sum_{d|n}\phi(d)=n$

证明：我们将从1到n的整数构成的集合分类。整数m如果与n的最大公因子为d，则m属于C_d类。就是说，如果m属于C_d，那么(m, n)=d，当且仅当(m/d, n/d)=1。所以，C_d类中所含整数的个数是所有不超过n/d且和n/d互素的正整数的个数。从上面的分析，我们可以看到C_d类中存在 Φ (n/d)个整数。因为我们将1到n的所有整数分成互不相交的类，且每个整数只属于其中一个类。那么这些不同的类所含的所有整数的个数之和就是n，所以 $\sum_{d|n}\phi(d)=n$

下节课再见