费马小定理、威尔逊定理和欧拉定理

小圆滚滚

1 费马小定理(Fermat's Little Theorem)

对任意质数p和整数a，如果$p \nmid a$，那么$a^{p-1} \equiv 1 \pmod{p}$.

也就是说，如果整数a不能被质数p整除，那么a^{p-1}除以p得到的余数是1，即$a^{p-1}-1$可以被p整除。

考虑整数a的前n-1个倍数$a, 2a, \cdots, (p-1)a$，其中任意两个除以p余数不同。这是因为：

假如a的第j个倍数ja和第k个倍数ka除以p有相同的余数，其中$1 \le j < k \le p-1$，那么它们的差一定可以被p整除，也就是"$p|(k-j)a$，又根据条件质数p不整除a，因此p整除k-j，但$1 \le k-j \le p-2$不可能被p整除，得到矛盾。

但任何一个整数除以p的余数只可能是$0, 1, 2, \cdots, p-1$中的一个，而$a, 2a, \cdots, (p-1)a$除以p得到的余数不为0且各不相同，因此一定是$1, 2, \cdots, p-1$每一个各取一次。

根据同余的乘法性质可得

$(a)(2a)\cdots(p-1)a \equiv (1)(2)\cdots(p-1) \pmod{p}$

也就是$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$

2 威尔逊定理(Wilson's Theorem)

对任意正整数n，$(n-1)! \equiv -1 \pmod{n}$当且仅当n是质数。

除去n=1的特殊情况（单独验证即可），我们去证明：

一、对任意质数p，$(p-1)! \equiv -1 \pmod{p}$，其中p=2的情况单独验证；

二、对任意合数n，$(n-1)! \not\equiv -1 \pmod{n}$。

2.1 对任意质数$p \neq 2$

任何整数除以p的余数有$0, 1, \cdots, p-1$，余数为0的整数正好是p的倍数，乘以任何其他整数仍然是p的倍数，余数为0。剩下p-1偶数个非零余数，我们去证明对于余数a的整数，一定可以找到余数b的整数，使得这两个整数的乘积的余数为1，也就是

对于任意$1 \le a \le p-1$，一定存在$1 \le b \le p-1$，使得$ab \equiv 1 \pmod{p}$.

我们把b称为a的逆元，逆元是唯一的。

假设还有另一个逆元b'，那么$b \equiv b(ab') \equiv (ba)b' \equiv b' \pmod{p}$，可以推出$b = b'$.

先考虑逆元是自身的余数，也就是解同余方程$x^2 \equiv 1 \pmod{p}$.

除以p余数为1等价于减掉余数1后可以被p整除，也就是$p \mid x^2-1$，分解因式得$p \mid (x+1)(x-1)$，得到$p \mid x-1$或$p \mid x+1$，对应x=1或x=p-1.

也就是逆元是自身的余数只有两个，分别是1和p-1.

再考虑剩下的p-3个余数2, 3, $\cdots$, $p-2$，对于$2 \le a \le p-2$，我们证明存在唯一的逆元$2 \le b \ne a \le p-2$，即满足$ab \equiv 1 \pmod{p}$.

利用a和p互质可得存在整数m和n使得ma+np=1，用代余除法得到m=qp+b，其中b是除以p的一个余数，代入可得

aqp+ab+np=1，也就是ab-1=-(aq+n)p是p的倍数，即$ab \equiv 1 \pmod{p}$

如果余数a不是1或p-1，得到的余数b也一定不是1或p-1.

这说明剩下的p-3的余数可以两两配对，乘积除以p得到的余数为1.

用同余的乘法性质全部乘起来可得$(p-2)! \equiv 1 \pmod{p}$.

注意到$p-1 \equiv -1 \pmod{p}$，两式相乘即可得到$(p-1)! \equiv -1 \pmod{p}$.

2.2 对于合数n

如果n是合数，一定存在质因数$p \mid n$，其中$2 \le p \le \frac{n}{2} \le n-2$.

可得$p \mid (n-1)!$，由此可推出$(n-1)! \not\equiv -1 \pmod{n}$，否则由$n \mid (n-1)!+1$可推出$p \mid (n-1)!+1$，得到矛盾$p \mid 1$.

进一步地，可以说明对于合数$n > 4$一定有$(n-1)! \equiv 0 \pmod{n}$:

如果$n = p^2$，那么$(n-1)! = (p^2-1)!$可以被p^{p-1}整除。

p=2时$n = 2^2 = 4$，$(n-1)! = 3! = 6$，$6 \equiv 2 \pmod{4}$.

$p \ne 2$时，$(p^2-1)!$可以被p^2整除，因此$(p^2-1) \equiv 0 \pmod{p^2}$.

如果n=pm，$m \ne p$，那么m和p都会在(n-1)!的乘数中出现，可以乘出因数n，因此(n-1)!可以被n整除，也就是$(n-1)! \equiv 0 \pmod{n}$.

3 欧拉定理(Euler's Theorem)和欧拉函数(Euler's function)

对于任何一个正整数n，定义$\phi(n)$为不超过n的与n互质的正整数个数，称为欧拉函数。

比如对任意质数p有$\phi(p) = p-1$，$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

不超过6的正整数中，与6互质的只有1和5两个，因此$\phi(6) = 2$.

不超过10的正整数中，与10互质的有1, 3, 7, 9，因此$\phi(10) = 4$.

不超过12的正整数中，与12互质的有1, 5, 7, 11，因此$\phi(12) = 4$.

可以看出$\phi(2) = 1$，当$m \ge 2$时，1和m-1不相等，且和m互质，一定有$\phi(m) \ge 2$.

欧拉定理：如果正整数a和m互质，那么$a^{\phi(m)} \equiv 1 \pmod{m}$.

这里互质的条件必不可少，设a和m的最大公因数是d，$d \mid a^{\phi(m)}$且$d \mid m$，

要使得$a^{\phi(m)} \equiv 1 \pmod{m}$，就一定有$m \mid a^{\phi(m)} - 1$，

由传递性得到$d \mid a^{\phi(m)} - 1$，结合$d \mid a^{\phi(m)}$可得$d \mid 1$，因此只能有d=1，也就是a和m互质。

费马小定理可以看作当m是质数p时欧拉定理的一个特殊情形。

证明方法也类似：考虑除以m得到的余数0, 1, 2, $\cdots$, $m-1$，其中与m互质的一共有$\phi(m)$个，分别记为$1 = r_1 < r_2 < \cdots < r_{\phi(m)} = m-1$.

考虑a的这些倍数：ar_1, $ar_2, \cdots, ar_{\phi(m)}$. 一方面，可知其中任何两个除以m得到的余数都不相同，这是因为$ar_j \equiv ar_k \pmod{m}$可推出$m \mid a(r_j - r_k)$，而由a和m互质，可得$m \mid r_j - r_k$，而$|r_j - r_k| \le m-2$，得到$r_j = r_k$. 另一方面，$r_j$与m互质，a也与m互质，因此$ar_j$与m互质，这些a的倍数除以m得到的余数正好就是重新排列顺序的$r_1, \cdots, r_{\phi(m)}$。利用同余的乘法性质可得

$(ar_1)(ar_1)\cdots(ar_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$

因为$r_1r_2\cdots r_{\phi(m)}$与m互质，利用同余的除法性质消去公因数可得结论

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

欧拉函数$\phi(m)$在一定意义下保持乘法，具体地，如果m和n互质，那么$\phi(mn) = \phi(m)\phi(n)$.

把从1到mn的整数排列成m行n列，

$$\begin{array}{cccc} 1 & m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & \cdots & (n-1)m+2 \\ \vdots & \vdots & & \vdots \\ m & 2m & \cdots & mn \end{array}$$

如果i与m的最大公因数是d，那么第i行第j列的整数$a_{ij} = (j-1)m + i$就可以被d整除，

从而得到d是a_{ij}和mn的公因数。如果$d \neq 1$，那么这一行整数都不和mn互质，删去这些行，只保留满足i与m互质的那些行，一共有$\phi(m)$行。

考虑其中第i行的n个整数$a_{ij} = (j-1)m + i$都与m互质。

如果$j \neq k$，那么第i行第j列$a_{ij} = (j-1)m + i$和第k列$a_{ik} = (k-1)m + i$除以n的余数不同，否则得到它们的差$a_{ij} - a_{ik} = (j-k)m$可以被n整除，由m和n互质得到$m|j-k$推出j=k矛盾。因此第i行的n个整数除以m的余数正好是打乱顺序后的0到n-1，其中与n互质的恰好有$\phi(n)$个，也就是行编号与m互质的$\phi(m)$行中每一行中的每个整数都与m互质，其中有$\phi(n)$个整数也与n互质，因此这些整数与mn互质，不超过mn的正整数中总共有$\phi(m)\phi(n)$个与mn互质。

比如$\phi(6) = \phi(2)\phi(3) = 1 \cdot 2 = 2$，

$\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$，

$\phi(12) = \phi(2^2)\phi(3) = 2 \cdot 2 = 4$.

对任意一个正整数的质因数分解$n = p_1^{e_1} \cdots p_s^{e_s}$，可以用乘法性质求出

$\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_s^{e_s}) = p_1^{e_1-1}(p_1-1) \cdots p_s^{e_s-1}(p_s-1) = n(1-1/p_1) \cdots (1-1/p_s)$.

4 同余的性质

4.1 基本性质

1. 若$p|(a-b)$，则$a \equiv b \pmod{p}$。例如 $11 \equiv 4 (mod\, 7)$， $18 \equiv 4 (mod\, 7)$.解释a-b可以被p整除。
2. $(a \,\%\, p) = (b \,\%\, p)$意味$a \equiv b \pmod{p}$
3. 对称性：$a \equiv b \pmod{p}$等价于$b \equiv a \pmod{p}$
4. 传递性：若$a \equiv b \pmod{p}$且$b \equiv c \pmod{p}$，则$a \equiv c \pmod{p}$

4.2 模运算的性质

若$(a-b)\%m == 0$,就称a,b关于m同余，或者说a,b对模数m同余。

e.g. $(100-60)\%8 == 0$,我们就说100和60对于模数8同余。

它的另一层含义就是说，100和60除以8的余数相同。

a和b对m同余，我们记作$a \equiv b \pmod{m}$

性质：

1. 如果$a \equiv b \pmod{m}, x \equiv y \pmod{m}$，则$a + x \equiv b + y \pmod{m}$//两边分别相加
2. 如果$a \equiv b \pmod{m}, x \equiv y \pmod{m}$，则$ax \equiv by \pmod{m}$//两边分别相乘
3. 如果$ac \equiv bc \pmod{m}$，且c和m互质，则$a \equiv b \pmod{m}$//c,m互质时，去掉c