

1.12 生产全体素数

随便拿出一个自然数,问我们是不是素数,一般是无言以对的,但却有一个公式,以自然数对为双亲,从理论上说,能生育出所有的素数:

$$f(m, n) = \frac{n-1}{2} (|[m(n+1) - (n! + 1)]^2 - 1| - \{[m(n+1) - (n! + 1)]^2 - 1\}) + 2$$

是素数,其中 m, n 是自然数,且 $f(m, n)$ 的值域是全体素数。

这个公式的证明很容易。事实上,若 $[m(n+1) - (n! + 1)]^2 \geq 1$,

则 $f(m, n) = 2$, 得到素数。若 $[m(n+1) - (n! + 1)]^2 = 0$, 则 $f(m, n) = n + 1$, 又 $m(n+1) - (n! + 1) = 0$, $m(n+1) = n! + 1$ 。即 $n + 1$ 可整除 $n! + 1$, 由威尔逊定理, $n + 1$ 是素数, 即 $f(m, n)$ 也算出素数, 至此知 $f(m, n)$ 只能是素数。

下证 $f(m, n)$ 的值域是全体素数集合。

任取定一素数 p , 由威尔逊定理, $(p-1)! + 1$ 被 p 整除, 取

$$n = p - 1, m = \frac{1}{p} [(p-1)! + 1]$$

则

$$mp = (p-1)! + 1, n + 1 = p$$

$$m(n+1) = mp = (p-1)! + 1 = n! + 1$$

于是 $m(n+1) - (n! + 1) = 0$, $f(m, n) = n + 1 = p$, 由 p 的任意性知 $f(m, n)$ 的值域是全体素数的集合。

还可以证明, 每个奇素数, $f(m, n)$ 恰取到一次。

事实上

$$f(m, n) = \begin{cases} 2, [m(n+1) - (n! + 1)]^2 \geq 1 \\ n + 1, m(n+1) = n! + 1 \end{cases}$$

$f(m, n)$ 取到的奇素数中形如 $p = n + 1$, 在使 $f(m, n) = n + 1$ 的数组 (m, n) 中, 只有 $n = p - 1$, 这时 $m(n+1) = n! + 1$, $m = \frac{n! + 1}{n + 1}$,

于是 $(m, n) = \left(\frac{n! + 1}{n + 1}, n \right) = \left(\frac{(p-1)! + 1}{p}, p - 1 \right)$ 是唯一的使 $f(m, n) = p = n + 1$ 的一对自然数 m, n 。

公式 $f(m, n)$ 给出了产生全体素数的一个算法, 只可惜它其实是个坏算法, 为计算出奇素数 p , 要计算 $(p-1)!$, p 很大时, $(p-1)!$ 实际上是算不出来的, 空间和时间都不够用; 而且这个公式还有一个讨厌的地方, 就是大多数情形, 算出的都是 2 这个最小素数。

看起来, 如何产生素数, 如何鉴别素数, 仍然是困扰数学家的严重课题。