为什么n^2-n+41的前40项是素数？

杨文颜

2024 年 12 月 14 日

1 Euler的素数生成多项式

观察多项式n^2-n+41的前几项.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
n^2-n+41	41	43	47	53	61	71	83	97	113	131	151	173	197	213

注意到这些数字都是素数. 事实上，对于$1 \le n \le 40$，这能给出40个不同的素数. Euler（1772）最早注意到了这一点. 这似乎是一个巧合，对于其他的数字，这样的魔法便不再出现. 其实，并不总是这样，魔法有的时候还是会有的，比如把41换成17之后，也会有类似的事情发生.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
n^2-n+17	17	19	23	29	37	47	59	73	89	107	127	149	173	199

然而这不全然是运气使然，实际上，我们可以尝试做一些因式分解.

$$n^2-n+41=(n-\tau)(n-\bar{\tau}),\quad \tau=\frac{1+i\sqrt{163}}{2}.$$

这似乎暗示我们应当考虑环$\mathbb{Z}[\tau]$上的分解. Rabinovich（1913）证明了多项式n^2-n+m对于$1 \le n \le m-1$给出素数的充要条件是$\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$是一个唯一分解整环. 其中$D=1-4m$是这个多项式的判别式，而对于$m=41$来说，这个数字是$D=-163$. 好消息是，$\mathbb{Z}[\frac{1+i\sqrt{163}}{2}]$确实是一个唯一分解整环.

这个条件的充分性是自然的，我们在这里来尝试证明它.

定理 1.1. *整数$m>1$，$R=\mathbb{Z}[\tau]$是唯一分解整环是多项式n^2-n+m对于整数$1 \le n \le m-1$均给出素数的充分条件. 其中$\tau=\frac{1+\sqrt{D}}{2}, D=1-4m$.*

我们先证如下命题.

命题 1.2. *已知$R=\mathbb{Z}[\tau]$是唯一分解整环. 那么对所有$1 \le n \le m-1$, 我们有$n-\tau$是R中素元.*

证明. 唯一分解整环中素元和不可约元等价. 假设$n-\tau$并非一个素元，那么它可约，不妨设$(a+b\tau)(c+d\tau)=(ac-mbd)+(bd+bc+ad)\tau$等于它，并且$bd \neq 0$. 故

$$bd+bc+ad=-1, 1 \le ac-mbd \le m-1.$$

我们作简单的分类讨论.

- 假设$bd>0$，那么$ac \ge mbd+1>mbd$. 因此

$$bd+1=bc+ad \ge 2\sqrt{acbd}>2\sqrt{m}bd. \implies bd<\frac{1}{2\sqrt{m}-1}<1.$$

而bd是一个整数，矛盾.

- 假设$bd < -1$，我们不妨假设$b < 0, d > 0$. 那么$bc + ad = -1 - bd < 0, ac \leq m(bd + 1) < 0$. 那么必须有$a < 0, c > 0$. 通过改变符号我们可以类似地重复第一种情况的讨论.
- 最后我们得到$bd = -1$，不妨假设$b = 1, d = -1$，那么不难得到$c = a$. 故$1 \leq a^2 + m \leq m - 1$，也矛盾.

□

之后我们注意到一个自然数中的素数，它在$\mathbb{Z}[\tau]$要么还是一个素元，要么是一个素元的平方，要么是两个不同素元的乘积. 你可能会问为什么不会分解成更多的素元之乘积，这是因为你可以注意到$\mathbb{Z}[\tau]$上天然带有一个范数（norm），即

$$N(x + y\tau) = (x + y\tau)(x + y\bar{\tau}) = x^2 - xy + my^2.$$

这里，N的实际意义是将$x + y\tau$看成一个$\mathbb{Q}$上的二维线性空间$\mathbb{Q}[\tau]$的线性变换的行列式，即乘法映射$t \mapsto (x + y\tau)t$. 如果一个素元真能写成多于三个环中元素的乘积，那么必有一个的范数为1. 这是因为范数具有完全积性：$N(ab) = N(a)N(b)$，并且只有单位的范数为1.

这似乎暗示我们应当研究二次型. 更确切地来说，我们要去研究用二次型来表示数的问题.

2 二次型的研究

Gauss被认为是第一个系统研究有理二元二次型的分解的人. 尽管Euler已经在上面花了很多气力. 自然地，对于一个实二元二次型来说，非退化本质上只有两种，分别是椭圆的（elliptic）和双曲的（hyperbolic）. 它们分别形如$x^2 + y^2$和$x^2 - y^2$. 然而对于有理数和整数来说情况大不相同. 我们考虑如下二次型 $Q(x, y) = ax^2 + bxy + cy^2$，$a, b, c \in \mathbb{Z}$，判别式$D = b^2 - 4ac$，根据经验我们知道此时有三种情况. $D > 0$时，$Q(x, y)$是一个双曲的或者说不定的二次型；$D = 0$时$Q(x, y)$是（差一个正负号）一个有理式的平方，这是退化的情形；$D < 0$时通过适当的乘以± 1可以得到$Q(x, y)$应当是一个正定的二次型.

有的时候我们可以通过变量替换将一个二次型变为另一个，比如说做替换$(x, y) \mapsto (ax + by, cx + dy)$，其中$ad - bc = 1, a, b, c, d \in \mathbb{Z}$. 或者说，群$\mathrm{SL}_2(\mathbb{Z})$作用在二次型上. 我们想把替换前后的二次型看成等价的，然后（多或少地）分类等价的有理二次型. 显然可以看出判别式D是一个在作用下不变的量. 那么D是否能作为分类的唯一依据呢？答案是否定的. 比如说我们可以看下面两个二次型.

$$Q_1(x, y) = x^2 + 5y^2, Q_2(x, y) = 2x^2 + 2xy + 3y^2.$$

如何看出来这两个二次型不同呢？我们可以这么看，假设Q_1和Q_2是等价的，那么假如整数n能被表达成$Q_1(x, y)$的形式，那么也能表达成某个$Q_2(x', y')$的形式，且两种表达方式应当一一对应. 若取$n = 5$，那么$Q_1(x, y) = 5$有2个解$(x, y) = (0, \pm 1)$. 而$Q_2(x, y) = 5$没有任何整数解，所以Q_1和Q_2不等价.

好消息是，对于特定的D，二次型等价类的数目是有限的. 等价类的数目被称为类数（class number），更准确地说，如果$D < 0$的话，这个等价类的数目是环$\mathbb{Z}[\sqrt{D}]$或者$\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$的理想类群的大小. $D > 0$的情况大体与之相同. 理想类群是一个交换群，所以事实上这些等价类作为群有加法结构，这一点Gauss已经知道. 如果类数是1并且D没有平方因子的话，这个环就是主理想整环.

让我们暂时忽略掉类数和理想类群. 至少从上面的例子中我们可以看出，n能否用这个二次型表出，以及表示方式的数目，是一个它的等价类的“身份证”.

3 用二次型表示数

用二次型表示数也是一个古老的问题. 早在17世纪，Fermat（1640）就提出了如下定理.

定理 3.1. *任何一个奇素数能表为两平方数之和的充要条件是这个素数模4余1.*

奇素数	3	5	7	11	13	17	19	23	29	31	37	41	43	47
两平方数之和？	否	1^2+2^2	否	否	2^2+3^2	1^2+4^2	否	否	2^2+5^2	否	1^2+6^2	4^2+5^2	否	否

观察一下前几个奇素数可以看到这是正确的.

证明. Fermat自己独创的无穷递降法恰好适用于这个证明. 必要性显然，下面证明充分性，设p是一个模4余1的素数.

首先，根据二次剩余性质，我们知道-1是模p二次剩余，故$\exists x$满足$x^2+1\equiv 0 \pmod 4$，故存在A,B，满足

$$A^2+B^2=Mp, \text{且} M<p.$$

如果$M=1$证明已经完成，不妨设$M\geq 2$

Fermat的想法是，用A,B,M来造出新的整数a,b,m使得

$$a^2+b^2=mp, \text{且} m\leq M-1$$

如果$m=1$那么证明又完成了，不然又可以继续做下去. 不断重复这一过程，我们便可以得到p自身可以表示为两平方数之和. 这一过程被Fermat称为递降.

递降过程如下，选取$u\equiv A, v\equiv B \pmod M$，并且$-M/2\leq u,v\leq M/2$. 那么$u^2+v^2=Mr$，且$r<M$. 如果$r=0$，那么$A,B$可以被$M$整除，那么$A^2+B^2=Mp$可以被$M^2$整除，故$M$必整除素数$p$，由于$M<p$故$M=1$，故不妨设$r\geq 1$.

接下来注意到$(uA+vB)^2+(vA-uB)^2=(u^2+v^2)(A^2+B^2)=M^2rp$. 两边同时除以$M^2$便可以得到

$$\left(\frac{uA+vB}{M}\right)^2+\left(\frac{vA-uB}{M}\right)^2=rp.$$

$vA-uB$可以被M整除，这是因为$vA-uB\equiv BA-AB\equiv 0 \pmod M$. $uA+vB\equiv A^2+B^2\equiv Mp\equiv 0 \pmod M$.

最后我们说明递降程序有效性，注意到$r=\frac{u^2+v^2}{M}\leq\frac{(M/2)^2+(M/2)^2}{M}=\frac{M}{2}<M$，所以实际上每使用递降程序一次，$p$的倍数至少减半.

□

Fermat类似地对于形如x^2+2y^2, x^2+3y^2之类的素数也建立了类似的定理，使用的也是他引以为傲的递降法. 我们使用$\mathbb{Z}[\sqrt{-1}]$和$\mathbb{Z}[\sqrt{-2}]$这些环唯一分解的性质可以更容易地证明它们. 现在让我们来尝试重新证明定理3.1.

证明. 取一个素数p模4余1. 与第一个证明相同，我们至少可以找到整数A,B使得$A^2+B^2=(A+Bi)(A-Bi)=Mp$，且A,B不是p的倍数，这说明p不是素元，由$\mathbb{Z}[\sqrt{-1}]$唯一分解性，我们知道p可约，从而可以进一步分解，故$p=(a+bi)(a-bi)$必然对某些a,b成立. □

然而对于形如x^2+5y^2的素数，Fermat只能给出一个猜想. Lagrange识别出Fermat的困难在于判别式为-20的二次型有两类，也就是之前我们在举D相同时类数大于1的反例时举出的例子.

4 类数公式1：理论性的版本

为了解决这个困难，我们真正注意到给出类数公式的重要性，接下来让我们来给出二次数域的类数公式.

我们回顾在第2节末尾我们提到，统计一个数n用二次型表示方式的数目是有用的. 我们用$r_Q(n)$来表示这个数目. 并且用$r_Q^*(n)$表示n的不等价的本原表示（primitive）的数目，也就是$n=Q(x,y)$且x与y互素的情形. 我们有如下计数公式：

$$\sum_{[Q]} r_Q^*(n)=\#\{b \pmod{2n} : b^2\equiv D \pmod{4n}\}$$

其中$[Q]$表示取遍判别式为D的二次型Q的等价类.

证明. 对于这个公式我们需要一些群论基础. 这个公式背后的哲学是，假如你有一个群G，作用在集合X和Y上，并且$S \subset X \times Y$是一个在G的对角线作用下不变的子集，那么

$$\sum_{X/G} \#S_x/G_x = \sum_{Y/G} \#S_y/G_y.$$

其中，X/G和Y/G为X和Y在G作用下的轨道. $S_x = \{y \in Y : (x,y) \in S\}$，$G_x = \{g \in G : gx = x\}$，对于$S_y$和$G_y$也是类似的. 这个公式的证明只是用两种不同方式计算G作用在S上的轨道.

现在我们取$G = \mathrm{SL}_2(\mathbb{Z})$，$X$为判别式为$D$的二次型$Q$的等价类，$Y$为互素的整数对$(x,y)$集合，$S$为满足$Q(x,y) = n$的对子$(Q,(x,y)) \in X \times Y$. 左边即为欲证式左边. 右边则为欲证式右边. □

这个等式的证明并不是最关键的，关键在于承认这个等式后，我们注意到等式右边是一个关于n的积性函数. 如果D是模p的二次剩余，或者$p = 2, D \equiv 1 \mod 8$，那么这个数对所有的$n = p^\nu > 1$都是2；如果D是模p的非二次剩余，或者$p = 2, D \equiv 5 \mod 8$，那么这个数对所有的$n = p^\nu > 1$都是0；并且如果p整除D，那么这个数对于$n = p$就是1，对于$n = p^\nu, \nu > 1$来说是0. 并且注意到$r_Q(n) = \sum_{e^2|n} r_Q^*(n/e^2)$. 因此我们可以得到等式

$$\sum_{[Q]} r_Q(n) = \sum_{d|n} \chi_D(d).$$

χ_D为一个完全积性函数，并且在p处取值为Legendre符号$(\frac{D}{p})$. 根据二次互反律我们知道χ_D是周期的并且平均值为0，因此我们可以构造一个L-函数

$$L(1,\chi_D) = \sum_{n=1}^{\infty} \frac{\chi_D(n)}{n}.$$

这个级数是收敛的. 取平均后我们得到

$$\sum_{[Q]} \langle r_Q \rangle = L(1,\chi_D), \langle r_Q \rangle = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} r_Q(n).$$

但是我们可以看到$\langle r_Q \rangle$对于所有的Q都是一样的！这是因为它们具有相同的判别式D，似乎$\sum_{n=1}^{N} r_Q(n)$是在数$Q(x,y) \le n$内的整点个数. 对于$D < 0$来说，这个图形是一个椭圆. 而椭圆内的整点个数大致是椭圆的面积，而$Q(x,y) \le n$的面积大致为$\frac{2\pi n}{\sqrt{-D}}$，所以右边似乎是$\frac{2\pi}{\sqrt{-D}}$. 但是！在这里有必要警告，$Q(x,y) = n$，那么$Q(y,x) = n$也是可行的，所以你应当除以2. 对于$D = -4$来说，唯一的等价类是$Q(x,y) = x^2 + y^2$，这个时候你还可以互换(x,y)的位置，这个时候你应当除以4. 类似$D = -3$时，你应当除以6. 仔细观察，$2,4,6$实际上是$\mathbb{Z}[\frac{\sqrt{D}}{2}]$或者$\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$的单位群的大小. 因此我们就得到了传说中的类数公式

$$h(D)\frac{2\pi}{w(D)\sqrt{-D}} = L(1,\chi_D).$$

其中的$h(D)$表示类数，$w(D)$是此时单位群的大小.

对于$D = -4$时我们不妨来看一下此时的L-函数.

$$L(1,\chi_{-4}) = 1 - \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots + \frac{1}{4k+1} - \frac{1}{4k+3} + \cdots = \frac{\pi}{4}.$$

这便是著名的Leibniz的π的交错级数，实际上我们换成$D = -3$也可以得到一个类似的公式

$$L(1,\chi_{-3}) = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \cdots + \frac{1}{3k+1} - \frac{1}{3k+2} + \cdots = \frac{\pi}{3\sqrt{3}}.$$

$D > 0$的情形其实类似，但是这时情况比较复杂，因为实际上这个时候环有着无限的单位群，比如说$\mathbb{Z}[\sqrt{2}]$，不难看出$\sqrt{2}+1$是一个单位，但它是无限阶的. 我们简单给出这个时候类数公式的一个例子.

$$L(1,\chi_4) = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} + \frac{1}{15} + \frac{1}{17} - \frac{1}{19} - \frac{1}{21} + \cdots = \frac{\log(1+\sqrt{2})}{\sqrt{2}}$$

目前这个方法只是一个指导性的，因为我们仍然不好计算L-函数特殊值，所以这个方法实效性并没有那么高. 但通过这个方法我们可以迅速得到类数的有限性. L-函数一般有一个函数方程，这使得它的解析性质比较好，也具有某种对称性[1]. 现代数论的核心问题之一是通过L-函数来研究数论中的问题.

既然直接这么做可计算性不太高，有没有具体的做法呢？

5 类数公式2：可计算的版本

答案是肯定的，首先我们注意到$\mathrm{SL}_2(\mathbb{Z})$是由 $S=\begin{pmatrix}1&1\\0&1\end{pmatrix}, T=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$这两个矩阵生成的，我们可以看它们在二次型上的作用，把它化成某种标准型. 我们设$D<0$，通过一些初等变换可以假设标准型形如

$$ax^2+bxy+cy^2, |b|\le a\le c, D=b^2-4ac.$$

这被称为所谓的既约二次型（reduced quadratic forms）的个数.

现在我们可以数出符合条件的(a,b,c)的数目了.

如果我们考察这个多项式的根$\tau=\frac{b+\sqrt{-D}i}{2a}$，用$\Re(\tau)$和$\Im(\tau)$分别表示$\tau$的实部和虚部. 那么注意到这个条件等价于

$$|\tau|\ge 1, |\Re(\tau)|\le 1/2.$$

我们也可以这么看，$\mathrm{SL}_2(\mathbb{Z})$可以作用在复平面的上半平面$\mathbb{H}=\{\tau\in\mathbb{C}:\Im(\tau)>0\}$上，作用方式就是所谓的Möbius变换.

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot z=\frac{az+b}{cz+d}.$$

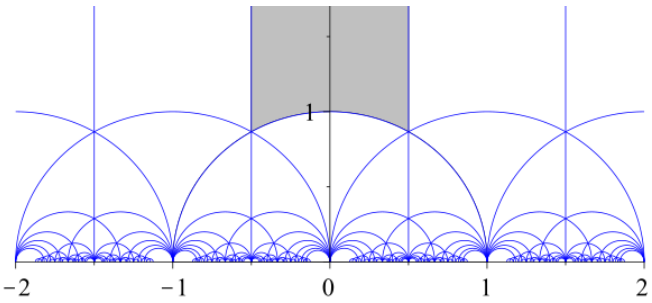

图 1: 上半平面在$\mathrm{SL}_2(\mathbb{Z})$作用下的图像

那么其实上述条件对应于什么呢？其实它对应于这个点落在所谓的$\mathrm{SL}_2(\mathbb{Z})$基本区域内（图1中灰色区域）. 所以也可以说，类数是$\mathrm{SL}_2(\mathbb{Z})$基本区域内的对应判别式为$D$的点的个数.

复数的上半平面其实是一个双曲几何模型，这是最早由Poincaré引入的. 把二次型看作这个几何模型中的点的几何的看法有时候非常有用，我们这里不过多讨论.

6 Rabinovich的证明

最后我们再回到最开始那个问题上去，简述一下Rabinovich的证明.

定理 6.1. *定理1.1中的充分性也是必要的, 即: 整数$m>1$, $R=\mathbb{Z}[\tau]$是唯一分解整环是多项式n^2-n+m对于整数$1\le n\le m-1$均给出素数的充要条件. 其中$\tau=\frac{1+\sqrt{D}}{2}, D=1-4m$.*

[1] 一类典型的例子是所谓的模性，这是一个重要的现代数学中的概念.

Rabinovich那个时代已经知道，R在取范数下一般不能构成一个Euclid整环. 然而我们可以给出类似Euclid整环的构造. 因此，他给出了这样一条引理.

引理 6.2. *对于R中任意互相不整除的非零元$s,t\in R$，$\exists a,b\in R$，使得$0<N(as+bt)<N(m)$. 那么R是一个唯一分解整环或者说类数是1.*

我们这里给出（被我们修改过的）Rabinovich论文中的不用理想语言对唯一分解性的证明. [2]

证明. 唯一因子分解整环需要两条性质：第一条是分解终止条件，这是因为若分解不终止，那么必然存在元素n使得$N(n)\in\mathbb{Z}_{\geq 0}$最小，且$n$分解不终止. 设$n=n_1\cdot n_2$且$n_1,n_2$不是单位，那么$N(n_1)>1,N(n_2)>1$，故$N(n_1)<N(n)$，于是$n_1$分解终止，类似$n_2$分解终止，于是$n$分解终止，这就得到了矛盾.[3]

第二条是分解唯一性，假设不是这样，同样必然存在元素n使得n是最小的分解不唯一的数. 我们不妨设n被非单位c整除，但$n=ab$，a和b都不能被c整除. 那么它们都不能整除c，不然可以约去c得到更小的n. 那么$\exists p,q\in R$使得$d=pa+qc$满足$0<N(d)<N(a),0<N(d)<N(c)$（用第三个条件两次并选取N较小的）. $db=pab+qc=pn+qc$可以被c整除，但d也不能被c整除（因为$N(d)<N(c)$），但是$N(db)<N(ab)=N(n)$，这就给出了矛盾.

接下来回到必要性证明. 因此假如R不唯一分解，那么必然$\exists\alpha,\beta\in R-\{0\}$使得$0<N(a\alpha+b\beta)<N(\beta)$对于$\forall a,b\in R$均不成立. 两边除以$N(\beta)$得到$0<N(\frac{\alpha}{\beta}\cdot a+b)<1$对于$a,b\in R$均不成立. 这样的数$\frac{\alpha}{\beta}$被称为干涉的（störend）. 不难知道如果$\frac{\alpha}{\beta}$是干涉的，那么$\frac{\alpha}{\beta}+p,\frac{\alpha}{\beta}\cdot p,p\in R-\{0\}$都是干涉的.

现在假如有一个数$\frac{\alpha}{\beta}$是干涉的，通过分子分母同乘$\bar{\beta}$，可以假设$\frac{\alpha}{\beta}=\frac{p+q\tau}{t}$且$t,p,q\in\mathbb{Z}$且互质. 而

$$\frac{p+q\tau}{t}\cdot\tau=\frac{-qm+(p+q)\tau}{t}.$$

通过适当的$\frac{p+q\tau}{t}\cdot\tau$和$\frac{p+q\tau}{t}$的整系数线性组合，我们可以得到一个仍然干涉的数$\frac{p'+q'\tau}{t}$，其中$q'=(p,q)$，根据互质条件，$(q',t)=1$，故再通过适当乘以一个整数并加上一个整数，可以得到一个干涉的数，形如

$$\frac{u-\tau}{v},1\leq u\leq v,v\neq 1.$$

我们断言$v\leq m$，这是因为$N(\frac{u-\tau}{v})\geq 1$必然成立，即

$$v^2-v+m\geq N(u-\tau)=u^2-u+m\geq N(v)=v^2.$$

接下来用反证法，假设所有的u^2-u+m都是素数，如果$1\leq u\leq m-1$. 若$1<v\leq m$，那么u^2-u+m与v互质，因此$\exists x,y$使得$(u^2-u+m)x-vy=1$. 或者可以写成这样的形式：

$$\frac{u-\tau}{v}(u-\bar{\tau})-v=\frac{1}{v}$$

这与$\frac{u-\tau}{v}$是干涉的矛盾，因为$N(\frac{1}{v})=\frac{1}{v^2}$. □

7 163：玄妙之数

似乎故事还没有写完. 类数为1的数字有哪些呢？Gauss在做了大量的计算之后在他的名著《算术研究》（*Disquisitiones Arithmeticae*，1798）中猜测，对于$D>0$来说有无限多这样的数字，而对于$D<0$来说似乎只有

$$-3,-4,-7,-8,-11,-19,-43,-67,-163.$$

Heegner（1952）最早尝试证明$D<0$时Gauss的猜测是正确的，因此这些数被称为Heegner数. 但他最初的证明稍有瑕疵，Stark（1967）改进了他的证明. Baker（1966）也独立发表了他的证明，最后这个定理以他们三个人的名字命名.

[2] Rabinovich避免使用理想的语言，但对于熟悉理想的读者来说，可以不困难地直接证明这是主理想整环.

[3] 对于熟悉交换代数的读者，分解终止条件可以由R是Noether环直接推出.

所以163是最后一个实现Euler多项式上的魔法的数字了. 但163能够施展的魔法远远不止于此，我们还可以看到

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999250072597\cdots$$

这非常接近于一个整数. 但这也并不是巧合，这是因为我们有一个具有魔法的函数

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots, q = e^{2\pi i\tau}.$$

如果τ就取成我们之前所说的$\tau = \frac{1+\sqrt{-D}i}{2}$，那么这个数字将给出一个代数整数. 特别地，当$D$是Heegner数时，它恰好是一个整数！也许你觉得这很神奇，但神奇不止于此，如果取$\tau = \frac{1+\sqrt{163}i}{2}$，那么我们注意到

$$j(\tau) = -262537412640768000 = -2^{18}\cdot 2^3\cdot 5^3\cdot 23^3\cdot 29^3 = -(2^6\cdot 3\cdot 5\cdot 23\cdot 29)^3$$

这是一个立方数，而且它的因子都非常的小！这并没有结束，如果再稍加思考我们会注意到这些数字似乎还有规律，可能初看起来并不明显，我们更换一下我们的视角.

$$j(\tau) - 1728 = -262537412640769728 = -2^6\cdot 3^6\cdot 7^2\cdot 11^2\cdot 19^2\cdot 127^2\cdot 163 = -163\cdot(2^3\cdot 3^3\cdot 7^2\cdot 11\cdot 19\cdot 127)^2$$

我们又看到了熟悉的数字163，同时还跟着一个平方数！类似地，它的因子也非常的小. 有观察力的读者也许能看到用163减去偶数的平方后做分解可以得到

$$\begin{aligned}
163 - 4 &= 159 = 3\cdot 53\\
163 - 16 &= 147 = 3\cdot 7^2\\
163 - 36 &= 127 = 127\\
163 - 64 &= 99 = 3^2\cdot 11\\
163 - 100 &= 63 = 3^2\cdot 7\\
163 - 144 &= 19 = 19
\end{aligned}$$

这囊括了所有出现在$j(\tau) - 1728$中出现的奇素数！对于$j(\tau)$来说答案是否如此呢，答案是，是！不过我们需要稍微调整一下. 我们使用$3\cdot 163$减去一个奇数的平方除以4之后再来做分解.

$$\begin{aligned}
(3\cdot 163 - 1)/4 &= 122 = 2\cdot 61\\
(3\cdot 163 - 9)/4 &= 120 = 2^2\cdot 3\cdot 5\\
(3\cdot 163 - 25)/4 &= 116 = 2^2\cdot 29\\
(3\cdot 163 - 49)/4 &= 110 = 2\cdot 5\cdot 11\\
(3\cdot 163 - 81)/4 &= 102 = 2\cdot 3\cdot 17\\
(3\cdot 163 - 121)/4 &= 92 = 2^2\cdot 23\\
(3\cdot 163 - 169)/4 &= 80 = 2^4\cdot 5\\
(3\cdot 163 - 225)/4 &= 66 = 2\cdot 3\cdot 11\\
(3\cdot 163 - 289)/4 &= 50 = 2\cdot 5^2\\
(3\cdot 163 - 361)/4 &= 32 = 2^5\\
(3\cdot 163 - 441)/4 &= 12 = 2^2\cdot 3
\end{aligned}$$

这也囊括了所有出现在$j(\tau)$中出现的素数. 这看似是一个巧合，实际上也并不是！Gross和Zagier（1986）证明了这样的分解的正确性. 通常分解大数是困难的，这可能是已知的整数中除了阶乘这样定义为一些数的乘积的数字之外，我们唯一可以很容易精确写出分解的大整数的例子.

这件事情的证明，本身又可以回到最初的问题上去，那就是关于类数的计算. 通过对上述j函数值[4]的分解的研究，我们可以证明Hurwitz-Kronecker类数关系

$$\sigma_1^+(m) = \sum_{D<0} \frac{h(D)}{w(D)} r_D(m) = \sum_{t^2<4m} h^*(t^2-4m) \quad (m\text{不为完全平方数}).$$

这里我们使用记号$h^*(m) = \sum_{r^2|D} h'(D/r^2), h'(D) = h(D)/\frac{1}{2}w(D), \sigma_1^+(m) = \sum_{d|m} \max(d, m/d)$. $h^*(-4m)$现在可以被表示为$h^*(D)$的表达式. 当然，现在我们还不能直接归纳计算，因为只有一半的判别式是4的倍数，但是也可以用类似的手法证明一个公式是

$$\sigma_3^-(m) = \sum_{t^2\le 4m} (m-t^2) h^*(t^2-4m).$$

我们约定$h^*(0) = \zeta(-1) = \frac{-1}{12}, \sigma_3^-(m) = \sum_{d|m} \min(d, m/d)^3$，那么我们此时就可以真正地用这两个等式来对所有的$D$归纳计算$h^*(D)$！[5]如果你想要做一个表格给出$h^*(D)$，且$D$取遍$-X < D < 0$之间所有可能的数字的话，那么你用这个方法的算法复杂度大致是$O(X^{1.5})$，看起来和之前直接使用既约二次型的计算量差不了多少，但你也许已经从这个新方法中嗅到了一丝新鲜的味道.

Pythagoras曾经说过，“万物皆数”. 但这数的方寸之间，却有着一些熠熠生辉的宝藏. 这篇文章也许只是浮光掠影地观赏了一下163这个数字的神奇，但每个数字背后，也许都有不为我们所知的秘密.

参考文献

[1] Rabinovitch, Georg (1913)*"Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern."* Proc. Fifth Internat. Congress Math. (Cambridge) 1, 418–421

[2] Heegner, Kurt (1952), *"Diophantische Analysis und Modulfunktionen"* [Diophantine Analysis and Modular Functions], Mathematische Zeitschrift (in German), 56 (3), 227–253

[3] Gross, Benedict H.; Zagier, Don B. (1984), *"On Singular Moduli"*, Journal für die reine und angewandte Mathematik (Crelles Journal), 1985, 191-220

[4] Zagier, D. (1991). *The Birch-Swinnerton-Dyer Conjecture from a Naive Point of View.* In: van der Geer, G., Oort, F., Steenbrink, J. (eds) Arithmetic Algebraic Geometry. Progress in Mathematics, vol 89. Birkhäuser, Boston, MA.

[5] Cox, David A., *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons Inc.

[4]这些虚二次数的$j(\tau)$的值也被称为singular moduli.

[5]对于这个$\zeta(-1) = -1/12$有一个玩笑说它是所有自然数的和.