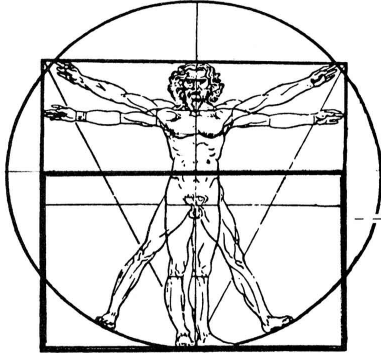


# Mathematics

Office: Ground Floor  
163 Ditchling Rise  
Brighton BN1 4QR  
UK

---



---

Saturday 10<sup>th</sup> October 2009

by: Jim Adams

Version M 4.2B

## **SUPEREXPONENTIATION** **(developed from Exponentiation,** **second edition)**

- Original Version M 2.2.** 6<sup>th</sup> February 2008.  
**Version M 2.5.** 29<sup>th</sup> February 2008. (Section 7).  
**Version M 2.8.** 28<sup>th</sup> April 2008. (Sections 8 & 9).  
**Version M 2.9.** 27<sup>th</sup> May 2008.  
**Version M 3.1.** 14<sup>th</sup> July 2008. (Extended Sections 5 & 8).  
**Version M 3.4.** 15<sup>th</sup> August 2008. (First Edition complete).

NOTE: Sections 9 on ramification and complex exponentiation and 11 on intricate representations of  $\text{Mat}(2^n, \mathbf{R})$  were removed from Version M 3.4, with the intention that these topics would reappear in future versions.

---

- Version M 3.6.** 21<sup>st</sup> December 2008. (Extended Section 8).  
**Version M 3.7.** 25<sup>th</sup> January 2009. (Extended Section 12).  
**Version M 3.8.** 15<sup>th</sup> June 2009. (Extended Sections 1 & 5, reorganisation incorporating Section 6 and a reinsert of part of Section 11).

Updates are in progress.

# Superexponentiation

JIM ADAMS

<http://www.jimhadams.com>

## 1. *Introduction.*

This conceptual work-in-progress describes explorations of the mathematical landscape mainly concerning global theorems for higher-order exponential operations, the generic term for which is superexponentiation. These operations are in general non-associative.

The context in which this is developed is in terms of *intricate* and *hyperintricate* numbers, being a particular representation of  $GL(2^n)$ . This is especially convenient in that complex numbers are a subalgebra of intricate numbers, so that our results naturally incorporate results involving complex numbers.

We present this subject as a room in which the wallpaper is stripped off and on the floor, the skirting board is half-painted in undercoat, one strip of wallpaper is affixed to the wall and the total outline of the décor has yet to be fully determined!

In Section 2, we introduce an exponential notation, which is developed later in the Section on superexponentiation.

Section 3 discusses binary quadratic forms, the complex binomial theorem and its ramification.

We then proceed, in Section 4, to discuss global class field theory.

Section 5 then introduces *intricate numbers*, a particular representation of  $GL(2)$ , and develops various aspects of these, including *Taylor series*, *intricate Argand diagrams* and then continues with *hyperintricate numbers* – a representation of  $GL(2^n)$ . We relate these ideas to exponentiation and to *L-series*.

In Section 6 we discuss *Mihăilescu's theorem*, obtaining from previous results prime number constraints on  $\gamma^t - \delta^v$ , for  $t, v \in \mathbf{N}$ .

Section 7 discusses *Fermat's Last Theorem* and *Beal's conjecture*.

In Section 8 we discuss the non-associative *permutrix product*.

We end with Section 9 on *superexponentiation*, a higher-order generalisation of iterative operations like addition, multiplication and exponentiation. A symbolic notation for these usually non-associative operations is developed. We discuss *metagraphs* in this context.

I would like to thank especially Doly García for discussions.

## 2. Notations. [4]

We use sparingly a special symbolism to obtain our results and think a supplementary notation “ $\uparrow$ ” for  $a \uparrow b = a^b$  is suggestive and appropriate. “ $a \uparrow b$ ” must coexist with the current convention, so we would still use e.g.  $\sin^2 \theta$ . This has the advantages of being more compact than  $\exp\{b\}$ , complicated expressions become more visible and simpler to notate, long sequences of exponents of exponents become easy to write and friendly on line spacing, the choice between  $(a \uparrow b) \uparrow c$  and  $a \uparrow (bc)$  for real  $a, b, c$  allows flexibility and nuance, and because usually  $a \uparrow (b \uparrow c) \neq (a \uparrow b) \uparrow c$ , the non-associative nature of exponentiation becomes easy to specify.

Let  $a, b, \dots$  to  $h, \alpha, \beta, \gamma, \delta \in \mathbf{R}^+$  be non-negative real numbers and  $j, k, \dots$  to  $z \in \mathbf{N}$  be natural numbers.  $\mathbf{N}$  starts from 1, unless 0 is otherwise indicated. Multiplication will take precedence over exponentiation in implicit bracketing.

Factorisation of real numbers, or of complex numbers  $a + ib$ , is not unique. Natural numbers factorise uniquely, and there is a type of unique factorisation for Heegner numbers, given by  $p + q\sqrt{-1}$ ,  $p + q\sqrt{-2}$  or  $\frac{1}{2}(p + q\sqrt{-r})$ , where  $-r$  is one of  $-3, -7, -11, -19, -43, -67$  or  $-163$ .

We adopt the convention  $0! = 1$ , writing linearly put  $a \times q = \Sigma(r = 0, q - 1) a$ , where the sum is 0 if  $q = 0$ , and put  $a \uparrow q = \Pi(r = 0, q - 1) a$ , where the product is 1 if  $q = 0$ .

## 3. Binary quadratic forms and the complex binomial theorem.

For  $n = 2m + 1$  odd

$$z^n + z^{n-1}x + z^{n-2}x^2 + \dots + x^n$$

factorises, since

$$z^{n+1} - x^{n+1} = (z - x)(z + x)(z^{2m} + z^{2m-2}x^2 + z^{2m-4}x^4 + \dots + x^{2m}),$$

and  $(z^{n+1} - x^{n+1})/(z - x)$  is a whole number.

A similar situation arises with the above argument under the transformation  $x \rightarrow -x$ .

For  $n$  even

$$z^n + z^{n-1}x + z^{n-2}x^2 + \dots + x^n = \Pi(k = 1, \dots, n)(z + (\omega_{n+1})^k x),$$

and similarly under the transformation  $x \rightarrow -x$ . ■

We can compare this with a previous result, that if  $z \not\equiv x \pmod{3}$  then

$$z^2 + zx + x^2 \equiv 1 \pmod{3}. \quad \blacksquare$$

## 4. Global class field theory.

### 5. Intricate and hyperintricate numbers.

We investigate *intricate numbers*, denoted by  $\mathbf{H}$  – particular representations of  $2 \times 2$  real matrices [13] – an extension of the idea of complex numbers, and extend these ideas to *hyperintricate numbers*,  $\mathbf{H}_n$ , the corresponding representations for real  $2^n \times 2^n$  matrices.

Let  $a, b, c, d$  be real numbers and

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \phi = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then

$$a1 + bi + c\alpha + d\phi$$

is an *intricate number*, in which we define  $a1$  as the *real* part,  $bi$  as the *imaginary* part,  $c\alpha$  as the *actual* part and  $d\phi$  as the *phantom* part.

It is clear that

$$a1 + bi$$

acts as a complex number in the traditional sense.

We have the following relationships

$$1^2 = -i^2 = \alpha^2 = \phi^2 = 1,$$

$$1i = i1 = i, \quad 1\alpha = \alpha1 = \alpha, \quad 1\phi = \phi1 = \phi$$

and

$$-i\alpha = \alpha i = \phi, \quad i\phi = -\phi i = \alpha, \quad \alpha\phi = -\phi\alpha = i. \quad \square \blacksquare$$

If the  $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$  matrix is a real  $2 \times 2$  matrix, then its intricate representation is uniquely

$$\frac{1}{2}(e + h)1 + \frac{1}{2}(f - g)i + \frac{1}{2}(e - h)\alpha + \frac{1}{2}(f + g)\phi. \quad \square \blacksquare$$

A matrix is invertible if and only if its determinant is non-zero. So under this invertibility

$$eh - gf \neq 0,$$

or to put it another way

$$\mathcal{Y} = a^2 + b^2 - c^2 - d^2 \neq 0.$$

Thus the intricate inverse of

$$a1 + bi + c\alpha + d\phi,$$

where it exists, is

$$\mathcal{R}^{-1}(a_1 - b_1i - c\alpha - d\phi). \blacksquare$$

We can represent intricate numbers in a four-dimensional hyperplane, in a similar way to complex numbers in the Argand plane.

By a Taylor series expansion, the Euler relation

$$e^{i\theta} = \cos\theta + i\sin\theta$$

becomes, for intricate numbers  $\alpha$  and  $\phi$ ,

$$e^{\alpha\theta} = \cosh\theta + \alpha\sinh\theta$$

and

$$e^{\phi\theta} = \cosh\theta + \phi\sinh\theta.$$

Thus

$$\begin{aligned} re^{i\mu + \alpha\nu + \phi\lambda} &= re^{i\mu} e^{\alpha\nu} e^{\phi\lambda} \\ &= r\{ [\cos\mu\cosh\nu\cosh\lambda - \sin\mu\sinh\nu\sinh\lambda]1 \\ &\quad + [\sin\mu\cosh\nu\cosh\lambda + \cos\mu\sinh\nu\sinh\lambda]i \\ &\quad + [\sinh\nu\cos\mu\cosh\lambda + \cosh\nu\sin\mu\sinh\lambda]\alpha \\ &\quad + [\sinh\lambda\cos\mu\cosh\nu - \cosh\lambda\sin\mu\sinh\nu]\phi \}. \blacksquare \end{aligned}$$

We point out that by multiplicative non-commutativity

$$e^{(\alpha + \phi)\theta} = e^{\alpha\theta} e^{\phi\theta} \neq e^{\phi\theta} e^{\alpha\theta} = e^{(\phi + \alpha)\theta}.$$

Rather than retain commutativity for exponentiated addition by other means, we adopt the non-standard procedure of considering adding intricate exponents relative to the *ordered basis*

$$\{1, i, \alpha, \phi\}$$

since here additive order now affects multiplication.

For matrices A, B and X, the solution of

$$AX = XB$$

is given by the familiar

$$B = X^{-1}AX,$$

but under what conditions is the above independent of X? For intricate expressions

$$x = x_1 1 + x_2 i + x_3 \alpha + x_4 \phi$$

$$a = a_1 1 + a_2 i + a_3 \alpha + a_4 \phi$$

$$b = b_1 1 + b_2 i + b_3 \alpha + b_4 \phi$$

commutativity holds under the transformation  $\alpha \rightarrow \phi, \phi \rightarrow \alpha, a_1 \rightarrow b_1, a_2 \rightarrow b_2, a_3 \rightarrow b_3, a_4 \rightarrow b_4$ . Hence to be independent of x,  $x_3 = x_4$ .

In general,  $xa = ax$  if and only if

$$xa = [x_1 1 + x_2 i + x_3 \alpha + x_4 \phi][a_1 1 + a_2 i + (x_3 a_2 / x_2) \alpha + (x_4 a_2 / x_2) \phi]$$

with  $x_2 \neq 0$ , or  $x_2 = 0$  and

$$xa = [x_1 1 + x_3 \alpha + x_4 \phi][a_1 1 + a_3 \alpha + (x_4 a_3 / x_3) \phi]$$

with  $x_3 \neq 0$ , or  $x_2 = 0, x_3 = 0$  and

$$xa = x_1 1 [a_1 1 + a_2 i + a_3 \alpha]$$

or

$$xa = [x_1 1 + x_4 \phi] a_1 1.$$

We define *hyperintricate numbers*,  $I_n$ , as follows. For  $GL(2)$ , ‘+’ is defined as the intricate number

$$a_1 1 + b_1 i + c_1 \alpha + d_1 \phi$$

and ‘-’ as the intricate number

$$-a_1 1 - b_1 i - c_1 \alpha - d_1 \phi.$$

Recursively for  $GL(2^n)$ , we define 0 as the zero  $GL(2^{n-1})$  matrix, ‘+’ as a general  $GL(2^{n-1})$  matrix and ‘-’ as the  $GL(2^{n-1})$  matrix with entries minus those of ‘+’.

Then if  $a_n, b_n, c_n$  and  $d_n$  are real numbers, starting with the following notation for the hyperintricate basis of  $I_n$ ,

$$I_{n-1} 1 = \begin{pmatrix} + & \mathbf{0} \\ \mathbf{0} & + \end{pmatrix}, \quad I_{n-1} i = \begin{pmatrix} \mathbf{0} & + \\ - & \mathbf{0} \end{pmatrix},$$

$$I_{n-1} \alpha = \begin{pmatrix} + & \mathbf{0} \\ \mathbf{0} & - \end{pmatrix}, \quad I_{n-1} \phi = \begin{pmatrix} \mathbf{0} & + \\ + & \mathbf{0} \end{pmatrix},$$

we can define a hyperintricate number  $\in I_n$  as

$$a_n I_{n-1} 1 + b_n I_{n-1} i + c_n I_{n-1} \alpha + d_n I_{n-1} \phi.$$

Alternatively, if  $A_B$  and  $C_D$  are hyperintricate basis numbers for  $n = 2$ , where  $A, B, C$ , and  $D = 1, i, \alpha$  or  $\phi$

then

$$(A_B)(C_D) = (AC)_{BD}$$

and

$$A_{-B} = -(A_B) = (-A_B).$$

More generally, consider instead of stepping down a further subscript level to expand this out, introducing a comma, thus:

$$A_{B,C}$$

so that

$$(AB)_{CD,EF} = (A_{C,E})(B_{D,F}).$$

## 6. Mihăilescu's theorem.

*No representations of primes are of the form*

$$\Xi = \gamma^t - \delta^v,$$

*except possibly for the cases equivalent to  $t$  and  $v$  having no common factor other than 1, with either  $p = 1$ , or  $p$  prime and  $\gamma^t - \delta^v = 1$ .*

*Proof.* Apply the above general prime representation theorem to

$$(\gamma \uparrow t) \uparrow p - (\delta \uparrow v) \uparrow p,$$

so that either  $p = 1$ , or  $p$  is prime and

$$\gamma \uparrow t - \delta \uparrow v = 1.$$

In the latter case, if  $t$  and  $v$  have a factor  $k \neq 1$  in common, say  $t = ku$  and  $v = kw$ , then we would have a prime

$$(\gamma \uparrow u) \uparrow (kp) - (\delta \uparrow w) \uparrow (kp),$$

a contradiction by this theorem above. If  $p = 1$ , then either  $t$  and  $v$  have a prime or non-prime factor  $k \neq 1$  in common, reducing to the previous case, or  $k = 1$ . ■

The theorem above has the corollary: *No number of the form*

$$\gamma \uparrow ((tp)^u) - \delta \uparrow ((vp)^w)$$

with  $p, u, w > 1$  is prime.

*Alternative proof.* The *second FSFT* allows an  $m > 1$  factorisation. ■

There are many solutions of  $\gamma \uparrow t - \delta \uparrow v = 1$  for  $t = 1$  or  $v = 1$ , also  $1 \uparrow t - 0 \uparrow v = 1$ . Catalan's conjecture states that  $3 \uparrow 2 - 2 \uparrow 3 = 1$  is the only other example. Mihăilescu's proof of Catalan's conjecture has appeared in print [23] and is accepted as correct and valid [7], [22], [25].

Our theorem above for prime  $\Xi = \gamma \uparrow tp - \delta \uparrow vp$  has the following implication.

*If  $\Xi = \gamma \uparrow tp - \delta \uparrow vp$  is prime and  $p, t, v \neq 1$ , then  $p$  divides*

$$\Xi - 1 = 9 \uparrow p - 8 \uparrow p - 1.$$

*Proof.*  $\gamma \uparrow t - \delta \uparrow v = 1$ , so by Mihăilescu's theorem,  $\gamma = 3$ ,  $t = 2$ ,  $\delta = 2$  and  $v = 3$ . By Fermat's 'little' theorem, if  $p$  is prime (as it must if  $p \neq 1$ ) then  $p$  divides the sum of  $\gamma^p - \gamma^t$  and  $\delta^v - \delta^{vp}$ , so  $p$  divides  $3^{2p} - 2^{3p} - 3^2 + 2^3$ . ■

*Let  $\Xi = \gamma^p - \delta^{vp}$ , with  $p$  odd prime. Then for some  $s$*

$$\Xi = 4s - (x + 1)[\gamma^{2t} - (x + 1)\gamma^t + (1/3)(x - 1)(x + 3)]$$

with

$$\gamma^t - \delta^v = 1 + x.$$

$p$  divides  $\Xi - x - 1$ .

*Proof.* Put  $\gamma^t = (4r + 1 + u)$  and  $\delta^v = (4r + u - x)$  from the differences of prime powers theorem in section 5, with  $r = 0$ . The divisibility result is a direct transcription of a theorem preceding that one. ■

A corollary to one of our section 5 generalised factorisation theorems is

*Let  $p = (2 \uparrow k_0) \prod_{i=1}^n (q_i \uparrow k_i)$ , where the  $q_i$  are distinct odd primes,  $t$  and  $v$  are coprime and  $\gamma > \delta \geq 1$ . Then  $9 \uparrow p - 8 \uparrow p$  has at least  $\sum_{i=0}^n k_i$  factors. If it does not correspond to this case, then  $\gamma^p - \delta^{vp}$  has at least  $1 + \sum_{i=0}^n k_i$  factors. ■*

Consequently our interest now concentrates on where  $t$  and  $v$  have no non-trivial common factor and  $\gamma \uparrow t - \delta \uparrow v$  is prime. A more general expression may be written as  $\Omega_p = \eta(\gamma^p) + \theta(\delta^p)$ , with  $p$  odd,  $\eta = \gamma^{t-p}$  and  $\theta = \pm(\delta^{v-p})$ , so the *LCFT* provides primality constraints.

*Example.* Define the *exponential commutator* by

$$E_c = (\gamma \uparrow \delta) - (\delta \uparrow \gamma)$$

and the *exponential anticommutator* by

$$E_a = (\gamma \uparrow \delta) + (\delta \uparrow \gamma).$$

We will consider the case for  $E_a$  where  $\delta = 2^q$ , and assume  $E_a$  is odd, so  $\gamma$  is odd. A similar example holds for  $E_c$ . To apply the *LCFT*, we choose  $p = 1$ , so we write  $E_a$  as

$$E_a = [\gamma \uparrow (2^q - 1)] \cdot \gamma + [2^{q\gamma - 1}] \cdot 2.$$

For the  $p = 1$  case,  $X = Y = 1$ , leading to

$$E_a = \frac{1}{2} [[\gamma \uparrow (2^q - 1) + 2^{q\gamma - 1}](\gamma + 2) + [\gamma \uparrow (2^q - 1) - 2^{q\gamma - 1}](\gamma - 2)].$$

So if  $[\gamma \uparrow (2^q - 1) + 2^{q\gamma - 1}]$  and  $[\gamma \uparrow (2^q - 1) - 2^{q\gamma - 1}]$  have a common factor  $c$ , then both

$$mc = [\gamma \uparrow (2^q - 1) + 2^{q\gamma - 1}]$$

and

$$nc = [\gamma \uparrow (2^q - 1) - 2^{q\gamma - 1}],$$

giving

$$(m - n)c = 2^{q\gamma},$$

which is a contradiction with the statement that  $c$  is odd. This means  $[\gamma \uparrow (2^q - 1) + 2^{q\gamma - 1}]$  and  $[\gamma \uparrow (2^q - 1) - 2^{q\gamma - 1}]$  are coprime, as are similarly  $(\gamma + 2)$  and  $(\gamma - 2)$ .

Hence to search for a factorisation of  $E_a$ , e.g.  $E_a = 25 + 32$ , a good choice is to look for common factors between  $[\gamma \uparrow (2^q - 1) + 2^{q\gamma - 1}]$  and  $(\gamma - 2)$  and between  $[\gamma \uparrow (2^q - 1) - 2^{q\gamma - 1}]$  and  $(\gamma + 2)$ . If such a factor exists, then  $E_a$  is not prime.

Computationally, the representation of  $2^{q\gamma - 1}$  is simple in binary, and for large  $\gamma$  we are looking for factors of  $(\gamma - 2)$  and  $(\gamma + 2)$ . ■

We can distinguish special cases of

$$\Omega_p = \frac{1}{2} [(\gamma \uparrow (t - p) \pm (\delta \uparrow (v - p)))(\gamma + \delta)X + (\gamma \uparrow (t - p) \pm -(\delta \uparrow (v - p)))(\gamma - \delta)Y].$$

If  $p = 1$ , then  $X = Y = 1$ . On the other hand, if, say,  $t > v$ , if  $v$  is odd, we can put  $v = p$ , whereas if  $v$  is even, we can put  $v = p + 1$ . These three special cases are then  $\Omega_1$ ,  $\Omega_v$  and  $\Omega_{v-1}$ . Explicitly

$$\Omega_1 = \frac{1}{2} [(\gamma \uparrow (t - p) \pm (\delta \uparrow (v - p)))(\gamma + \delta) + (\gamma \uparrow (t - p) \pm -(\delta \uparrow (v - p)))(\gamma - \delta)],$$

$$\Omega_v = \frac{1}{2} [(\gamma \uparrow (t - p) \pm 1)(\gamma + \delta)X + (\gamma \uparrow (t - p) \pm -1)(\gamma - \delta)Y]$$

and

$$\Omega_{v-1} = \frac{1}{2} [(\gamma \uparrow (t - p) \pm \delta)(\gamma + \delta)X + (\gamma \uparrow (t - p) \pm -\delta)(\gamma - \delta)Y]. \blacksquare$$

Cyclotomically, we can write

$$\Omega_p = a[\gamma \uparrow (t/p) - (\pm \omega_p)(\delta \uparrow (v/p))]$$

$$(1/a)[\Sigma(s = 0, p - 1)[(\gamma \uparrow (ts/p))((\pm 1) \uparrow (p - 1 - s)/p)(\delta \uparrow (v(p - 1 - s)/p))],$$

where we have introduced a  $p$ th root of unity,  $\omega_p$ , which equals 1 in the real case, and a number  $a$  to indicate the factors in [ ] are not unique. ■

## 7. Fermat's Last Theorem and Beal's conjecture.

Masser's ABC conjecture states that if  $\gamma(n)$  is the largest squarefree divisor of  $n$ , then for each fixed  $\varepsilon > 0$  there are at most finitely many coprime positive integer triples  $a$ ,  $b$ ,  $c$  with

$$a + b = c, \gamma(abc) < c^{1-\epsilon}.$$

A special case that has been proved is the Fermat-Catalan conjecture, which asserts that if  $x, y$  and  $z$  are coprime and  $1/p + 1/q + 1/r < 2$  then there are finitely many  $x^p + y^q = z^r$ .

The absence of solutions for  $x, y, z$  coprime when  $p, q, r > 2$  is conjectured. ■

We make some minor remarks about Fermat's Last Theorem.

If  $x^p + y^p = z^p$  where  $x, y, z$  and  $n < p$  are positive  $\in \mathbf{N}$ , then  $x^{p-n} + y^{p-n} > z^{p-n}$ .

*Proof.*  $z > x$ , so  $z^n > x^n$  and  $z^n x^{p-n} > x^p$ , with similar statements for  $y$  instead of  $x$ . Thus  $z^n x^{p-n} + z^n y^{p-n} > z^n z^{p-n}$ . ■

*Corollary.* If  $x^p + y^p = z^p$ , then  $x + y - z$  is positive. ■

Let  $p$  and  $q$  be prime, with  $q < p$  and

$$x^p + y^p = z^p$$

as before. Then

$$x^{p-q+1} + y^{p-q+1} - z^{p-q+1} = 6q\mathbb{I}_q$$

(or =  $q\mathbb{I}_q$  for  $q = 2$  and =  $2q\mathbb{I}_q$  for  $q = 3$ ) for some natural number  $\mathbb{I}_q$ .

*Proof.* By Fermat's little theorem, write  $x^q - x = 6q\mathbb{I}_x$ ,  $y^q - y = 6q\mathbb{I}_y$  and  $z^q - z = 6q\mathbb{I}_z$  (where instead, for  $q = 2$ ,  $x^q - x = q\mathbb{I}_x$ , etc. and for  $q = 3$ ,  $x^q - x = 2q\mathbb{I}_x$ , etc.). Here  $\mathbb{I}_x, \mathbb{I}_y$  and  $\mathbb{I}_z$  are given by the 'explicit' Bernoulli formulae. Then

$$\begin{aligned} 0 &= x^{p-q}(6q\mathbb{I}_x + x) + y^{p-q}(6q\mathbb{I}_y + y) - z^{p-q}(6q\mathbb{I}_z + z) \\ &= -6q\mathbb{I}_q + (x^{p-q+1} + y^{p-q+1} - z^{p-q+1}). \quad \blacksquare \end{aligned}$$

*Corollary.* The conditions of the above converse to Fermat's Last Theorem imply

$$x^{p-1} + y^{p-1} - z^{p-1} = 2\mathbb{I}_2,$$

$$x^{p-2} + y^{p-2} - z^{p-2} = 6\mathbb{I}_3,$$

...

$$x + y - z = 6p\mathbb{I}_p. \quad \blacksquare$$

[further inserts will be made]

The following formula was used by Euler in proving Fermat's last theorem for  $n = 3$ :

$$(na^2 + b^2)(t^2 + nu^2) = n(at + bu)^2 + (nau - bt)^2.$$

The formula used in the proof of Lagrange's theorem that every natural number may be represented by a sum of four squares is related to quaternionic multiplication where

$$e^{\uparrow}(i\theta + j\phi + k\sigma) = (\cos\theta + i\sin\theta)(\cos\phi + j\sin\phi)(\cos\sigma + k\sin\sigma)$$

– the exponential addition is non-abelian – and can be extended to a formula similar to Euler's above:

$$\begin{aligned} (na^2 + b^2 + c^2 + d^2)(t^2 + nu^2 + nv^2 + nw^2) &= \\ n(at + bu + cv + dw)^2 + (nau - bt + ncw - ndv)^2 &+ \\ + (nav - ct + ndu - nbw)^2 + (naw - dt + nbv - ncu)^2. &\quad \blacksquare \end{aligned}$$

### 8. A Model for Non-Associativity.

Non-associative operations (we will denote these by  $*$ ), acting on elements  $a, b, c$  of a set – we mean this:

$$(a * b) * c \neq a * (b * c)$$

are quite prevalent in mathematics.

An example is the *octonions*, otherwise known as *Cayley numbers*, discovered by Graves in 1843 [1], [2]. Multiplication of octonions, say  $a, b, c$ , is non-associative:

$$(ab)c \neq a(bc).$$

A more obvious example is exponentiation, since in general for real numbers  $a, b, c$

$$(a^b)^c \neq a^{(b^c)}.$$

An objective of *category theory* is to mimic the behaviour of compositions of functions (i.e. mappings), which are borrowed from the ideas of addition, multiplication and exponentiation of numbers or matrices. Thus the idea of addition is able to transmute to *direct sums* – disjoint unions of sets – otherwise more generally known as *coproducts*. The idea of multiplication can become the idea of *Cartesian products* – putting pairs of elements of a set together – otherwise more generally known as *products*, and the idea of exponentiation might become *exponential mappings* – related to *adjoints*. [3]

Because category theory, or its generalisations, underpins much of mathematics (strictly speaking, however, category theory deals with *associative* mappings), it is desirable to have a model for non-associative operations.

If we look at multiplication, we know we have a model for non-commutative multiplication with *matrices*, that is, if  $A$  and  $B$  are matrices, then

$$AB \neq BA$$

in general. However, matrices *are* associative

$$(AB)C = A(BC).$$

Nevertheless, it is possible to change the multiplication algorithm so that it *is* non-associative.

It would be desirable, however, to maintain some nice properties of matrices, i.e. that a non-singular matrix has an inverse – we mean here the *determinant* of the matrix (the  $n$  dimensional hypervolume of a parallelepiped, in which those edges through the origin are given by the  $n$  vectors from the rows or columns of the matrix)  $\neq 0$ .

We proceed to swim by first putting our toe in the water.

For a matrix  $B$  we can form the *transpose*  $B^T$  by swapping rows with columns. This means we can define a new type of matrix multiplication by

$$A * B = AB^T.$$

Then in general

$$(A * B) * C = (AB^T)C^T = A(B^T C^T) \\ \neq A * (B * C) = A(BC^T)^T = A(CB^T).$$

We note that since the inverse  $B^{-1}$  of  $B$  satisfies

$$(B^{-1})^T = (B^T)^{-1}$$

we have an inverse “ $A^{-1}$ ” for  $A$  under the  $*$  operation

$$A * “A^{-1}” = A((A^T)^{-1})^T$$

so

$$“A^{-1}” = (A^T)^{-1}.$$

Instead of swapping rows and columns to form the transpose, we could also, for example, invert the *order* of the  $B$  matrix, so the last row or column becomes first and the first becomes last, and similarly invert elements in between.

Rather than proceed with this example, we dive into the deep end with a further generalisation.

Consider the elements  $(b_{11}, b_{12}, b_{21}, \dots \text{etc.})$  of the matrix  $B$ . We form a permutation  $pB$  of those elements. We now define

$$A *_p B = A(pB).$$

It is clear that the previous examples are a special case of this. Generalising what we had before – we are using the Einstein summation convention here, repeated indices are summed:

$$(pA)(pB) = (pa_{ij})(pb_{jk}) = p(a_{ij}b_{jk}) = p(AB)$$

and

$$(pB)^{-1} = p(B^{-1}),$$

so the inverse for  $A$  under the  $*_p$  operation, “ $A^{-1}$ ”, where  $p^{-1}p$  is the identity permutation, is

$$p^{-1}(A^{-1}),$$

since

$$A *_p “A^{-1}” = A(pp^{-1})A^{-1} = A(p“A^{-1}”) = Ap(p^{-1}A^{-1}).$$

Thus we have both inverses *and* non-associativity in general:

$$(A *_p B) *_p C \neq A *_p (B *_p C).$$

In passing, we note the following little result. Since  $(pA)(pB) = p(AB)$ , if

$$pA = B,$$

then

$$A = p^{-1}B,$$

so

$$B *_p B = (pA)(pB) = p((p^{-1}B)B).$$

We have not yet begun to swim in the open sea.

We now note that under permutations

$$p, q, \dots r$$

the inverses of  $A$  are

$$p^{-1}A^{-1}, q^{-1}A^{-1}, \dots r^{-1}A^{-1}.$$

Since  $A^{-1}$  is common to these, we may form linear combinations of these inverses:

$$(\alpha_p p^{-1} + \alpha_q q^{-1} + \dots + \alpha_r r^{-1})A^{-1},$$

where the sum

$$\sum_{n=p, n} \alpha_n = X,$$

with  $X$  a real number. We now claim we have a general (finite) model for non-associative multiplication.

We know in the arithmetic of real numbers

$$e^a e^b = e^{a+b},$$

so that exponentiation, multiplication and addition are related. The corresponding formula for matrices (but expressed with commutators) is the *Campbell-Baker-Hausdorff* formula, given e.g. in [4], the content of which can be simplified as follows.

The exponential map  $e^A$  of matrix  $A$  is

$$e^A =$$

## 9. Superexponentiation.

Superexponentiation involves the generalisation of addition, multiplication and exponentiation to higher-order operators.

In order to develop notions (semantics) utilising superexponentiation, we believe it is necessary to develop a suitable notation (syntax), so that meanings can be expressed by symbolic manipulations – ‘meaning’ we think of as specific instances of mappings from symbolic or other representational manifestations to the world.

To this end we introduce the superexponentiation  $\hat{\uparrow}$  symbol.

We shall adjoin a number, say  $n$ , to this operation, so that when  $n = 0$  we are dealing with addition, when  $n = 1$  with multiplication, and  $n = 2$  with exponentiation. The higher-order superexponentiation operations, for  $n > 2$ , will be described inductively by stepping down to the  $(n - 1)$  case, and so on.

Since exponentiation is, even for real numbers, not in general associative, i.e. very often  $(a \hat{\uparrow} (b \hat{\uparrow} c)) \neq ((a \hat{\uparrow} b) \hat{\uparrow} c)$ , we have decided on a representation that describes a regular nesting of brackets, so that when this regular nesting occurs, we may dispense with brackets.

In particular, we introduce  ${}_n\hat{\uparrow}$  to indicate nesting on the left, e.g.

$$(((a \hat{\uparrow} b) \hat{\uparrow} c) \dots \hat{\uparrow} d) \equiv a \hat{\uparrow} b \hat{\uparrow} c \dots \hat{\uparrow} d.$$

When there is a danger of confusing  $(a_i)_{j\hat{\uparrow}} b$  with  $a_{(ij\hat{\uparrow})} b$  we will introduce a  $<$  sign  $a_i <_{j\hat{\uparrow}} b$  or  $a <_{ij\hat{\uparrow}} b$ .

Lastly we introduce an alternative notation for the above, which we will use sparingly, for example when  $n$  is a complicated expression, for emphasis, or for calculation rather than display. This is

$$<n\hat{\uparrow} \text{ for } {}_n\hat{\uparrow}.$$

For nesting on the right, we introduce a completely analogous notation, namely

$$(a \hat{\uparrow}_n \dots (b \hat{\uparrow}_n (c \hat{\uparrow}_n d))) \equiv a \hat{\uparrow}_n b \hat{\uparrow}_n c \dots \hat{\uparrow}_n d,$$

the expression with a subscripted  $>$  sign

$$a_h \hat{\uparrow}_{ij>} b_k,$$

and the equivalent non-subscript notation

$$a_h \hat{\uparrow} ij> b_k.$$

For comprehensibility, when non-associativity involves mixtures of  ${}_n\hat{\uparrow}$  and  $\hat{\uparrow}_n$ , we find it advisable to use the full panoply of distinguishable brackets,  $( )$ ,  $[ ]$  and  $\{ \}$ , the order of preference from inner to outer nestings being in the order given.

Since  $p$  terms of  $m$  added together give  $mp$ , we are at liberty to define  $\hat{\uparrow}_{-1}$  alternatively  $_{-1}\hat{\uparrow}$  as the operation on  $m$  which iterated for  $p$  terms gives  $m \hat{\uparrow}_{-1} p = m + p$ . Thus  $m \hat{\uparrow}_{-1} p = m(p^{-1}) + 1$ , and  $m \hat{\uparrow}_{-n} p = m(p^{-n}) + p^{-n+1}$ .

## References.

1. J.H. Adams, *Exponentiation*, <http://www.jimhadams.com/math/ExponentialFactorisationTheorems.pdf>, (October 15 2009).
2. Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, (1966).
3. D.M. Burton, *Elementary Number Theory*, Wm.C. Brown, (1989).
4. J.H. Conway and R.K. Guy, *The Book of Numbers*, Copernicus Books, (2006).
5. J.H. Conway and D.A. Smith, *On Quaternions and Octonions*, A.K. Peters, (2003).
6. G. Cornell, J.H. Silverman and G. Stevens eds, *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, (1997).
7. J. Daems, *A Cyclotomic Proof of Catalan's Conjecture*, <http://www.math.leidenuniv.nl/~jdaems/scriptie/Catalan.pdf>, (September 29 2003).
8. P.G.L. Dirichlet, *Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré*, Mathematische Werke, vol. 1, 21-46.
9. Ebbinghaus et al., *Numbers*, Springer (1991).
10. H.M. Edwards, *Fermat's Last Theorem*, Springer (1977).
11. R.K. Guy, *Unsolved Problems in Number Theory*, Springer (1994).
12. W.R. Hamilton, *Elements of Quaternions*, Vol I, page 275, reprint Chelsea, (1969).
13. H. Jacquet and R.P. Langlands, *Automorphic Forms on  $GL(2)$* , Springer-Verlag, (1970).
14. E.E. Kummer, *Collected Papers*, ed. André Weil, vol. 1, *Contributions to Number Theory*, Springer-Verlag, (1975).
15. E.E. Kummer, *De numeris complexis, qui radicibus unitatis et numeris integris redibus constant*, *ibid.* 165-192.
16. E.E. Kummer, *Beweis des Fermat'schen Satzes der Unmöglichkeit von  $x^\lambda + y^\lambda = z^\lambda$ , für eine unendliche Anzahl Primzahlen  $\lambda$* , *ibid.* 274-297.
17. F.W. Lawvere and R. Rosebrugh, *Sets for Mathematics*, Cambridge University Press, (2003).
18. S. Mac Lane, *Categories for the Working Mathematician*, Second Edition, Springer (1997).
19. Yu.I. Manin and A.A. Panchiskin, *Introduction to Modern Number Theory*, Springer, (2005, 2007).
20. B. Mazur, *Modular Curves and the Eisenstein Ideal*, *IHES Publ. Math* **47**, 33-186, (1977).
21. B. Mazur, *Rational Isogenies of Prime Degree*, *Invent. Math.* **44**, 129-162, (1978).
22. T. Metsänkylä, *Catalan's Conjecture: Another Old Diophantine Problem Solved*, *Bull. Amer. Math Soc.* **41**, 43-57, (2003).
23. P. Mihăilescu, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, *J. reine angew. Math* **572**, 167-195, (2004).
24. J. Rotman, *Galois Theory*, Second Edition, Springer (1998).
25. R. Schoof, *Catalan's Conjecture*, Springer-Verlag, (2008).
26. J.H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, (1992).
27. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, (1986).
28. R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, *Ann. Math., II. Ser.* 141, No. 3, 553-572, (1995).

29. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math., II. Ser. 141, No. 3, 443-551, (1995).
30. L.C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, (1982).
31. H. Weyl, *Algebraic Theory of Numbers*, Princeton University Press, (1940).

JIM ADAMS