So You Think You Can Multiply?

A History of Multiplication

Stephen Lucas

Department of Mathematics and Statistics
James Madison University, Harrisonburg VA

February 28 2010

Outline

- Ancient Techniques
  - Definitions
  - Squares and Triangular Numbers
  - Doubling and Halving
  - Geometry
- Positional Notation
  - Positional Definition
  - Hinge and Scratch
  - Cross
  - Lattice
  - Napier's Rods and the "Modern" method
  - Genaille's Rods
- Multiplication as Addition
  - Prosthaphaeresis
  - Logarithms
  - Powers and Pascal's Triangle
- High Precision
  - Karatsuba
  - Toom-Cook
  - Schönhage-Strassen

Definitions

(a) If a and b are natural numbers, $a \times b$ equals a added to itself b times, or b added to itself a times, $= b \times a$.

Definitions

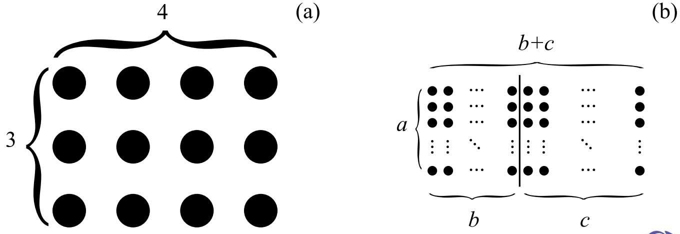
(a) If a and b are natural numbers, $a \times b$ equals a added to itself b times, or b added to itself a times, $= b \times a$.

(b) If a, b and c are natural numbers, $a(b + c) = ab + ac$.

Definitions

(a) If a and b are natural numbers, $a \times b$ equals a added to itself b times, or b added to itself a times, $= b \times a$.

(b) If a, b and c are natural numbers, $a(b + c) = ab + ac$.



Using Squares & Triangular Numbers

Ancient Babylon:

$(a+b)^2 = a^2 + 2ab + b^2$ and $(a-b)^2 = a^2 - 2ab + b^2$. Subtract:

$$ab = \frac{(a+b)^2 - (a-b)^2}{4}.$$

Using Squares & Triangular Numbers

Ancient Babylon:

$(a+b)^2 = a^2 + 2ab + b^2$ and $(a-b)^2 = a^2 - 2ab + b^2$. Subtract:

$$ab = \frac{(a+b)^2 - (a-b)^2}{4}.$$

Needs a table of squares, which can be built by adding successive odd integers: $(n+1)^2 = n^2 + (2n+1)$.

Using Squares & Triangular Numbers

Ancient Babylon:

$(a+b)^2 = a^2 + 2ab + b^2$ and $(a-b)^2 = a^2 - 2ab + b^2$. Subtract:

$$ab = \frac{(a+b)^2 - (a-b)^2}{4}.$$

Needs a table of squares, which can be built by adding successive odd integers: $(n+1)^2 = n^2 + (2n+1)$.

Also: $ab = \left((a+b)^2 - a^2 - b^2\right)/\,2$ or $(A+d)(A-d) = A^2 - d^2$.

Using Squares & Triangular Numbers

Ancient Babylon:

$(a+b)^2 = a^2 + 2ab + b^2$ and $(a-b)^2 = a^2 - 2ab + b^2$. Subtract:

$$ab = \frac{(a+b)^2 - (a-b)^2}{4}.$$

Needs a table of squares, which can be built by adding successive odd integers: $(n+1)^2 = n^2 + (2n+1)$.

Also: $ab = \left((a+b)^2 - a^2 - b^2\right)/\,2$ or $(A+d)(A-d) = A^2 - d^2$.

Teacher Resources on Line: If $T_n = 1 + 2 + \cdots + n = n(n+1)/2$, then $ab = T_a + T_{b-1} - T_{a-b}$.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

41×59

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59$

.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59$

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59 = 10 \times 236 + 59$

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59 = 10 \times 236 + 59 = 5 \times 472 + 59$

.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59 = 10 \times 236 + 59 = 5 \times 472 + 59 = 4 \times 472 + 472 + 59$.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59 = 10 \times 236 + 59 = 5 \times 472 + 59 = 4 \times 472 + 472 + 59 = 2 \times 944 + 531$.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59 = 10 \times 236 + 59 = 5 \times 472 + 59 = 4 \times 472 + 472 + 59 = 2 \times 944 + 531 = 1 \times 1888 + 531$.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59 = 10 \times 236 + 59 = 5 \times 472 + 59 = 4 \times 472 + 472 + 59 = 2 \times 944 + 531 = 1 \times 1888 + 531 = 2419$.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59 = 10 \times 236 + 59 = 5 \times 472 + 59 = 4 \times 472 + 472 + 59 = 2 \times 944 + 531 = 1 \times 1888 + 531 = 2419$.

Traditional way: list halvings of first number (round down) and doublings of second, add second numbers with odd first number.

Russian(?) Peasant

Doubling and Halving: If a is even, $a \times b = (a/2) \times (2b)$, and if a is odd, $a \times b = (a - 1 + 1) \times b = (a - 1) \times b + b$.

$41 \times 59 = 40 \times 59 + 59 = 20 \times 118 + 59 = 10 \times 236 + 59 = 5 \times 472 + 59 = 4 \times 472 + 472 + 59 = 2 \times 944 + 531 = 1 \times 1888 + 531 = 2419.$

Traditional way: list halvings of first number (round down) and doublings of second, add second numbers with odd first number. For example

$\surd$	41	59
	20	118
	10	236
$\surd$	5	472
	2	944
$\surd$	1	1888

$59 + 472 + 1888 = 2419.$

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two:

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$.

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

41	59

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

	41	59
1		59

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

	41	59
1		59
2		118

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

	41	59
1		59
2		118
4		236

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

	41	59
1		59
2		118
4		236
8		472

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

	41	59
1		59
2		118
4		236
8		472
16		944

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

	41	59
1		59
2		118
4		236
8		472
16		944
32		1888

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

	41	59
1		59
2		118
4		236
8		472
16		944
32	$41 - 32 = 9$	1888

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

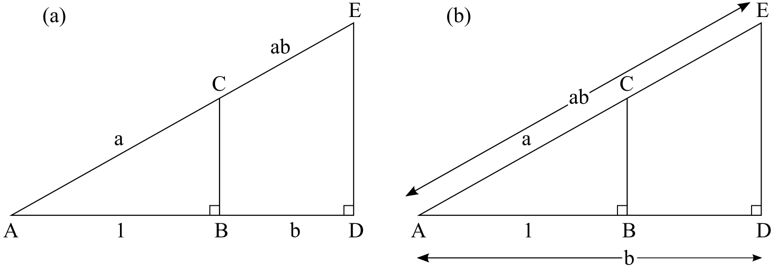
	41	59
1		59
2		118
4		236
8	$9 - 8 = 1$	472
16		944
32	$41 - 32 = 9$	1888

Egyptian Doubling

Doubling and halving is equivalent to converting from base ten to base two: $41_{10} = 101001_2$, so $41 \times 59 = (2^5 + 2^3 + 2^0) \times 59$. But you can convert to base two by subtracting powers of two.

	41	59
1	$1 - 1 = 0$	59
2		118
4		236
8	$9 - 8 = 1$	472
16		944
32	$41 - 32 = 9$	1888

Geometry



Positional Definition Example

By the definition,

$$243 \times 596$$
$$= \left(2 \times 10^2 + 4 \times 10^1 + 3 \times 10^0\right) \times \left(5 \times 10^2 + 9 \times 10^1 + 6 \times 10^0\right)$$

Positional Definition Example

By the definition,

$$
\begin{aligned}
&243 \times 596 \\
&= \left(2 \times 10^2 + 4 \times 10^1 + 3 \times 10^0\right) \times \left(5 \times 10^2 + 9 \times 10^1 + 6 \times 10^0\right) \\
&= (2 \times 5) \times 10^4 + (2 \times 9) \times 10^3 + (2 \times 6) \times 10^2 + (4 \times 5) \times 10^3 \\
&\quad +(4 \times 9) \times 10^2 + (4 \times 6) \times 10^1 + (3 \times 5) \times 10^2 + (3 \times 9) \times 10^1 \\
&\quad +(3 \times 6) \times 10^0
\end{aligned}
$$

Positional Definition Example

By the definition,

$$
\begin{aligned}
&243 \times 596 \\
&= \left(2 \times 10^2 + 4 \times 10^1 + 3 \times 10^0\right) \times \left(5 \times 10^2 + 9 \times 10^1 + 6 \times 10^0\right) \\
&= (2 \times 5) \times 10^4 + (2 \times 9) \times 10^3 + (2 \times 6) \times 10^2 + (4 \times 5) \times 10^3 \\
&\quad + (4 \times 9) \times 10^2 + (4 \times 6) \times 10^1 + (3 \times 5) \times 10^2 + (3 \times 9) \times 10^1 \\
&\quad + (3 \times 6) \times 10^0 \\
&= 10 \times 10^4 + (18 + 20) \times 10^3 + (12 + 36 + 15) \times 10^2 \\
&\quad + (24 + 27) \times 10^1 + 18 \times 10^0
\end{aligned}
$$

Positional Definition Example

By the definition,

$$
\begin{aligned}
&243 \times 596 \\
&= (2 \times 10^2 + 4 \times 10^1 + 3 \times 10^0) \times (5 \times 10^2 + 9 \times 10^1 + 6 \times 10^0) \\
&= (2 \times 5) \times 10^4 + (2 \times 9) \times 10^3 + (2 \times 6) \times 10^2 + (4 \times 5) \times 10^3 \\
&\quad + (4 \times 9) \times 10^2 + (4 \times 6) \times 10^1 + (3 \times 5) \times 10^2 + (3 \times 9) \times 10^1 \\
&\quad + (3 \times 6) \times 10^0 \\
&= 10 \times 10^4 + (18 + 20) \times 10^3 + (12 + 36 + 15) \times 10^2 \\
&\quad + (24 + 27) \times 10^1 + 18 \times 10^0 \\
&= 10 \times 10^4 + 38 \times 10^3 + 63 \times 10^2 + 51 \times 10^1 + 18 \times 10^0
\end{aligned}
$$

Positional Definition Example

By the definition,

$$
\begin{aligned}
&243 \times 596 \\
&= (2 \times 10^2 + 4 \times 10^1 + 3 \times 10^0) \times (5 \times 10^2 + 9 \times 10^1 + 6 \times 10^0) \\
&= (2 \times 5) \times 10^4 + (2 \times 9) \times 10^3 + (2 \times 6) \times 10^2 + (4 \times 5) \times 10^3 \\
&\quad + (4 \times 9) \times 10^2 + (4 \times 6) \times 10^1 + (3 \times 5) \times 10^2 + (3 \times 9) \times 10^1 \\
&\quad + (3 \times 6) \times 10^0 \\
&= 10 \times 10^4 + (18 + 20) \times 10^3 + (12 + 36 + 15) \times 10^2 \\
&\quad + (24 + 27) \times 10^1 + 18 \times 10^0 \\
&= 10 \times 10^4 + 38 \times 10^3 + 63 \times 10^2 + 51 \times 10^1 + 18 \times 10^0 \\
&= 1 \times 10^5 + 4 \times 10^4 + 4 \times 10^3 + 8 \times 10^2 + 2 \times 10^1 + 8 \times 10^0 \\
&= 144\,228.
\end{aligned}
$$

Positional Example Continued

Laying out the digit products:

			2	4	3
		×	5	9	6
1	0				
	1	8			
		1	2		
	2	0			
		3	6		
			2	4	
		1	5		
			2	7	
	$_1$	$_1$	$_1$	1	8
1	4	4	8	2	8

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

		2	4	3
5	9	6		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

1	0				
			2	4	3
	~~5~~	9	6		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

	1				
1	0	8			
			2	4	3
	~~5~~	~~9~~	6		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

	1	1			
1	0	8	2		
			~~2~~	4	3
	~~5~~	~~9~~	~~6~~		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

	1	1			
1	0	8	2		
			~~2~~	4	3
	~~5~~	~~9~~	~~6~~	6	
		5	9		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

	2	0			
	1	1			
1	0	8	2		
			~~2~~	4	3
	~~5~~	~~9~~	~~6~~	6	
		~~5~~	9		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

		3			
	2	0			
	1	1	6		
1	0	8	2		
			~~2~~	4	3
	~~5~~	~~9~~	~~6~~	6	
		~~5~~	~~9~~		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

		3			
	2	0	2		
	1	1	6		
1	0	8	2	4	
			~~2~~	~~4~~	3
	~~5~~	~~9~~	~~6~~	~~6~~	
		~~5~~	~~9~~		

JAMES MADISON UNIVERSITY

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

		3			
	2	0	2		
	1	1	6		
1	0	8	2	4	
			~~2~~	~~4~~	3
	~~5~~	~~9~~	~~6~~	~~6~~	6
		~~5~~	~~9~~	9	
			5		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

		1			
		3	5		
	2	0	2		
	1	1	6		
1	0	8	2	4	
			~~2~~	~~4~~	3
	~~5~~	~~9~~	~~6~~	~~6~~	6
		~~5~~	~~9~~	9	
			~~5~~		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

		1	2		
		3	5		
	2	0	2		
	1	1	6	7	
1	0	8	2	4	
			~~2~~	~~4~~	3
	~~5~~	~~9~~	~~6~~	~~6~~	6
		~~5~~	~~9~~	~~9~~	
			~~5~~		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

		1	2		
		3	5		
	2	0	2	1	
	1	1	6	7	
1	0	8	2	4	8
			~~2~~	~~4~~	~~3~~
	~~5~~	~~9~~	~~6~~	~~6~~	~~6~~
		~~5~~	~~9~~	~~9~~	
			~~5~~		

Hinge Multiplication

Lay out the digit multiples, the entire second number times the digits of the first, then add. (Early Hindu texts, Medieval English)

1	4_1	4_1	8_1	2	8
		1	2		
		3	5		
	2	0	2	1	
	1	1	6	7	
1	0	8	2	4	8
			~~2~~	~~4~~	~~3~~
	~~5~~	~~9~~	~~6~~	~~6~~	~~6~~
		~~5~~	~~9~~	~~9~~	
			~~5~~		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

		2	4	3
5	9	6		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

1	0				
			2	4	3
	~~5~~	9	6		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

$$\begin{array}{cccccc} & 1 & & & & \\ 1 & \not{0} & 8 & & & \\ \hline & & & 2 & 4 & 3 \\ & \not{5} & \not{9} & 6 & & \end{array}$$

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

	1	9			
1	~~0~~	~~8~~	2		
			~~2~~	4	3
	~~5~~	~~9~~	~~6~~		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

	1	9			
1	~~0~~	~~8~~	2		
			~~2~~	4	3
	~~5~~	~~9~~	~~6~~	6	
		5	9		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

	3				
	~~1~~	9			
1	~~0~~	~~8~~	2		
			~~2~~	4	3
	~~5~~	~~9~~	~~6~~	6	
		~~5~~	9		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

	4				
	~~3~~	2			
	~~1~~	~~9~~	8		
1	~~0~~	~~8~~	~~2~~		
			~~2~~	4	3
	~~5~~	~~9~~	~~6~~	6	
		~~5~~	~~9~~		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

	4	3			
	~~3~~	~~2~~	0		
	~~1~~	~~9~~	~~8~~		
1	~~0~~	~~8~~	~~2~~	4	
			~~2~~	~~4~~	3
	~~5~~	~~9~~	~~6~~	~~6~~	
		~~5~~	~~9~~		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

	4	3			
	~~3~~	~~2~~	0		
	~~1~~	~~9~~	~~8~~		
1	~~0~~	~~8~~	~~2~~	4	
			~~2~~	~~4~~	3
	~~5~~	~~9~~	~~6~~	~~6~~	6
		~~5~~	~~9~~	9	
			5		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

		4			
	4	~~3~~	5		
	~~3~~	~~2~~	~~0~~		
	~~1~~	~~9~~	~~8~~		
1	~~0~~	~~8~~	~~2~~	4	
			~~2~~	~~4~~	3
	~~5~~	~~9~~	~~6~~	~~6~~	6
		~~5~~	~~9~~	9	
			~~5~~		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

		4	8		
	4	~~3~~	~~5~~		
	~~3~~	~~2~~	~~0~~		
	~~1~~	~~9~~	~~8~~	1	
1	~~0~~	~~8~~	~~2~~	~~4~~	
			~~2~~	~~4~~	3
	~~5~~	~~9~~	~~6~~	~~6~~	6
		~~5~~	~~9~~	~~9~~	
			~~5~~		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

		4	8		
	4	~~3~~	~~5~~		
	~~3~~	~~2~~	~~0~~	2	
	~~1~~	~~9~~	~~8~~	~~1~~	
1	~~0~~	~~8~~	~~2~~	~~4~~	8
			~~2~~	~~4~~	~~3~~
	~~5~~	~~9~~	~~6~~	~~6~~	~~6~~
		~~5~~	~~9~~	~~9~~	
			~~5~~		

Scratch Multiplication

As for hinge, but add new products above the line. Very popular in Medieval Europe.

		4	8		
	4	~~3~~	~~5~~		
	~~3~~	~~2~~	~~0~~	2	
	~~1~~	~~9~~	~~8~~	~~1~~	
1	~~0~~	~~8~~	~~2~~	~~4~~	8
—	—	—	—	—	—
			~~2~~	~~4~~	~~3~~
	~~5~~	~~9~~	~~6~~	~~6~~	~~6~~
		~~5~~	~~9~~	~~9~~	
			~~5~~		

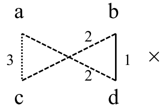
$$243 \times 596 = 144\,828$$

Cross Multiplication

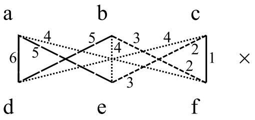
In terms of digits, $abc \times def = ad \times 10^4 + (ae + bd) \times 10^3 + (af + be + cd) \times 10^2 + (bf + ce) \times 10^1 + cf \times 10^0$.

Cross Multiplication

In terms of digits, $abc \times def = ad \times 10^4 + (ae + bd) \times 10^3 + (af + be + cd) \times 10^2 + (bf + ce) \times 10^1 + cf \times 10^0$.



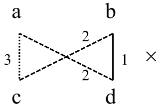
ac	ad	bd
	bc	



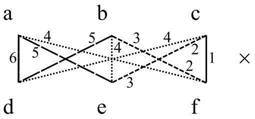
ad	bd	cd	ce	cf
	ae	be	bf	
		af		

Cross Multiplication

In terms of digits, $abc \times def = ad \times 10^4 + (ae + bd) \times 10^3 + (af + be + cd) \times 10^2 + (bf + ce) \times 10^1 + cf \times 10^0$.



ac	ad	bd
	bc	



ad	bd	cd	ce	cf
	ae	be	bf	
		af		

Same effort as hinge, different order of digits. Recommended for mental arithmetic.

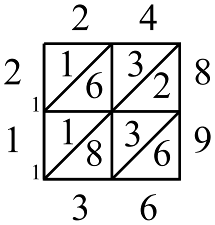
Lattice

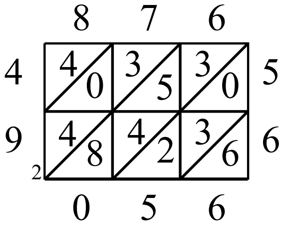
Hinge separates digit multiples from carries, scratch and cross don't. Lattice is like hinge, but easier.

Lattice

Hinge separates digit multiples from carries, scratch and cross don't. Lattice is like hinge, but easier.

For example, $24 \times 89 = 2136$ and $876 \times 56 = 49\,056$.





Napier's Rods

To make digit products easier, in 1617 John Napier built rods engraved with the digit multiplication table.

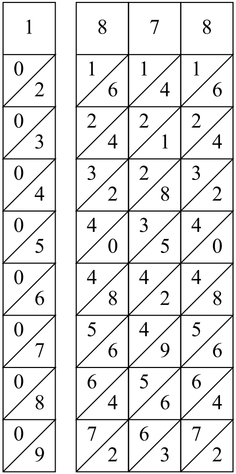
0	1	2	3	4	5	6	7	8	9
0/0	0/2	0/4	0/6	0/8	1/0	1/2	1/4	1/6	1/8
0/0	0/3	0/6	0/9	1/2	1/5	1/8	2/1	2/4	2/7
0/0	0/4	0/8	1/2	1/6	2/0	2/4	2/8	3/2	3/6
0/0	0/5	1/0	1/5	2/0	2/5	3/0	3/5	4/0	4/5
0/0	0/6	1/2	1/8	2/4	3/0	3/6	4/2	4/8	5/4
0/0	0/7	1/4	2/1	2/8	3/5	4/2	4/9	5/6	6/3
0/0	0/8	1/6	2/4	3/2	4/0	4/8	5/6	6/4	7/2
0/0	0/9	1/8	2/7	3/6	4/5	5/4	6/3	7/2	8/1

Napier's Rods Example

Consider 878×944.

Napier's Rods Example

Consider 878×944.



3512

7902

Napier's Rods Example

Consider 878×944.

1	8	7	8	
0/2	1/6	1/4	1/6	
0/3	2/4	2/1	2/4	
0/4	3/2	2/8	3/2	3512
0/5	4/0	3/5	4/0	
0/6	4/8	4/2	4/8	
0/7	5/6	4/9	5/6	
0/8	6/4	5/6	6/4	
0/9	7/2	6/3	7/2	7902

$$
\begin{array}{cccccc}
 & & & 8 & 7 & 8 \\
 & & \times & 9 & 4 & 4 \\
\hline
 & & 3 & 5 & 1 & 2 \\
 & 3 & 5 & 1 & 2 & \\
7 & 9 & 0 & 2 & & \\
\hline
8_1 & 2 & 8 & 8 & 3 & 2
\end{array}
$$

or

$$
\begin{array}{cccccc}
 & & & 8 & 7 & 8 \\
 & & \times & 9 & 4 & 4 \\
\hline
7 & 9 & 0 & 2 & & \\
 & 3 & 5 & 1 & 2 & \\
 & & 3 & 5 & 1 & 2 \\
\hline
8_1 & 2 & 8 & 8 & 3 & 2
\end{array}
$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself.

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$\begin{array}{rccc} & 8 & 7 & 8 \\ \times & 9 & 4 & 4 \\ \hline \end{array}$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$\begin{array}{rrrr} & & {\scriptstyle 3} & \\ & 8 & 7 & 8 \\ \times & 9 & 4 & 4 \\ \hline & & & 2 \end{array}$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$\begin{array}{rrrr} & {\scriptstyle 3} & {\scriptstyle 3} & \\ & 8 & 7 & 8 \\ \times & 9 & 4 & 4 \\ \hline & & 1 & 2 \end{array}$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$\begin{array}{rrrr} & {\scriptstyle 3} & {\scriptstyle 3} & \\ & 8 & 7 & 8 \\ \times & 9 & 4 & 4 \\ \hline 3 & 5 & 1 & 2 \end{array}$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$\begin{array}{cccc} & 3 & & \\ & \not{3} & 3 & \\ & 8 & 7 & 8 \\ \times & 9 & 4 & 4 \\ \hline 3 & 5 & 1 & 2 \\ & & 2 & \end{array}$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$\begin{array}{cccc}
 & {\scriptstyle 3} & & \\
{\scriptstyle 3} & {\scriptstyle \cancel{3}} & {\scriptstyle 3} & \\
 & 8 & 7 & 8 \\
\times & 9 & 4 & 4 \\
\hline
3 & 5 & 1 & 2 \\
 & 1 & 2 &
\end{array}$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$
\begin{array}{ccccc}
 & & 3 & & \\
 & 3 & \not{3} & 3 & \\
 & & 8 & 7 & 8 \\
 & \times & 9 & 4 & 4 \\
\hline
 & 3 & 5 & 1 & 2 \\
3 & 5 & 1 & 2 &
\end{array}
$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$
\begin{array}{ccccc}
 & 7 & 3 & & \\
 & \not{3} & \not{3} & 3 & \\
 & & 8 & 7 & 8 \\
 & \times & 9 & 4 & 4 \\
\hline
 & 3 & 5 & 1 & 2 \\
3 & 5 & 1 & 2 & \\
 & & 2 & &
\end{array}
$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$
\begin{array}{ccccc}
 & 7 & 3 & & \\
7 & \cancel{3} & \cancel{3} & 3 & \\
 & & 8 & 7 & 8 \\
 & \times & 9 & 4 & 4 \\
\hline
 & 3 & 5 & 1 & 2 \\
3 & 5 & 1 & 2 & \\
 & 0 & 2 & &
\end{array}
$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$
\begin{array}{cccccc}
 & & 7 & 3 & & \\
 & 7 & \cancel{3} & \cancel{3} & 3 & \\
 & & & 8 & 7 & 8 \\
 & & \times & 9 & 4 & 4 \\
\hline
 & & 3 & 5 & 1 & 2 \\
 & 3 & 5 & 1 & 2 & \\
7 & 9 & 0 & 2 & & \\
\hline
\end{array}
$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

		7	3		
	7	~~3~~	~~3~~	3	
			8	7	8
		×	9	4	4
		3	5	1	2
	3	5	1	2	
7	9	0	2		
					2

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

		7	3		
	7	~~3~~	~~3~~	3	
			8	7	8
		×	9	4	4
		3	5	1	2
	3	5	1	2	
7	9	0	2		
				3	2

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$
\begin{array}{cccccc}
 & & 7 & 3 & & \\
 & 7 & \not{3} & \not{3} & 3 & \\
 & & & 8 & 7 & 8 \\
 & & \times & 9 & 4 & 4 \\
\hline
 & & 3 & 5 & 1 & 2 \\
 & 3 & 5 & 1 & 2 & \\
7 & 9 & 0 & 2 & & \\
\hline
 & & & 8 & 3 & 2
\end{array}
$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$
\begin{array}{cccccc}
 & & 7 & 3 & & \\
 & 7 & \not{3} & \not{3} & 3 & \\
 & & & 8 & 7 & 8 \\
 & & \times & 9 & 4 & 4 \\
\hline
 & & 3 & 5 & 1 & 2 \\
 & 3 & 5 & 1 & 2 & \\
7 & 9 & 0 & 2 & & \\
\hline
 & & 8 & 8 & 3 & 2
\end{array}
$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$
\begin{array}{cccccc}
 & & \scriptstyle 7 & \scriptstyle 3 & & \\
\scriptstyle 1 & \scriptstyle 7 & \scriptstyle \cancel{3} & \scriptstyle \cancel{3} & \scriptstyle 3 & \\
 & & & 8 & 7 & 8 \\
 & & \times & 9 & 4 & 4 \\
\hline
 & & 3 & 5 & 1 & 2 \\
 & 3 & 5 & 1 & 2 & \\
7 & 9 & 0 & 2 & & \\
\hline
 & 2 & 8 & 8 & 3 & 2
\end{array}
$$

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

		7	3		
1	7	~~3~~	~~3~~	3	
			8	7	8
		×	9	4	4
		3	5	1	2
	3	5	1	2	
7	9	0	2		
8	2	8	8	3	2

The Modern Method

Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$
\begin{array}{cccccc}
 & & 7 & 3 & & \\
1 & 7 & \not{3} & \not{3} & 3 & \\
 & & & 8 & 7 & 8 \\
 & & \times & 9 & 4 & 4 \\
\hline
 & & 3 & 5 & 1 & 2 \\
 & 3 & 5 & 1 & 2 & \\
7 & 9 & 0 & 2 & & \\
\hline
8 & 2 & 8 & 8 & 3 & 2
\end{array}
\qquad
\begin{array}{cccccc}
 & & & 8 & 7 & 8 \\
 & & \times & 9 & 4 & 4 \\
\hline
 & & 3 & 5_3 & 1_3 & 2 \\
 & 3 & 5_3 & 1_3 & 2 & \\
7 & 9_7 & 0_7 & 2 & & \\
\hline
8_1 & 2 & 8 & 8 & 3 & 2
\end{array}
$$

The Modern Method

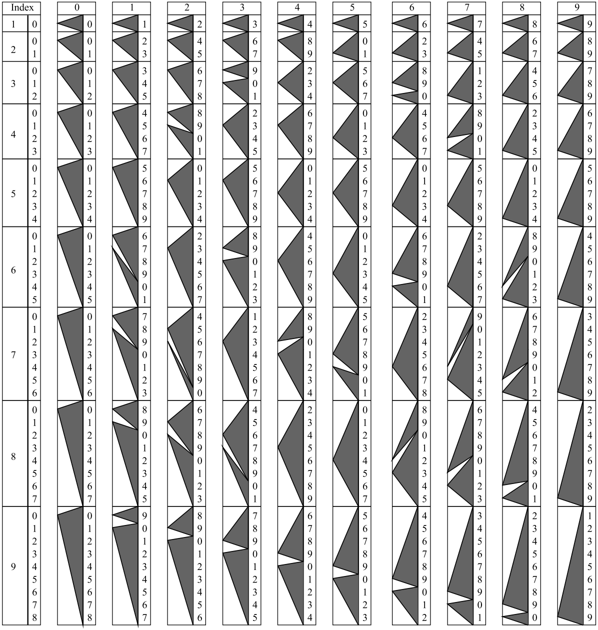
Just like Napier's Rods, but you have to do digit multiplications and intermediate carries yourself. For example

$$\begin{array}{cccccc} 1 & 7 & \overset{7}{\not{3}} & \overset{3}{\not{3}} & 3 & \\ & & & 8 & 7 & 8 \\ & & \times & 9 & 4 & 4 \\ \hline & & 3 & 5 & 1 & 2 \\ & 3 & 5 & 1 & 2 & \\ 7 & 9 & 0 & 2 & & \\ \hline 8 & 2 & 8 & 8 & 3 & 2 \end{array}$$

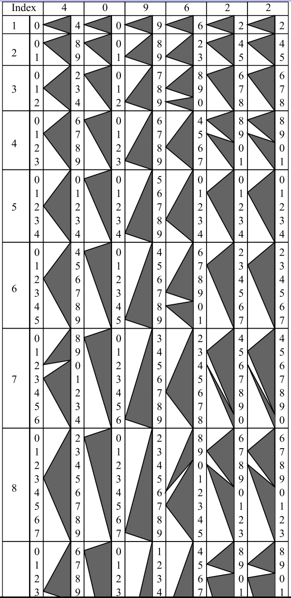
$$\begin{array}{cccccc} & & & 8 & 7 & 8 \\ & & \times & 9 & 4 & 4 \\ \hline & & 3 & 5_3 & 1_3 & 2 \\ & 3 & 5_3 & 1_3 & 2 & \\ 7 & 9_7 & 0_7 & 2 & & \\ \hline 8_1 & 2 & 8 & 8 & 3 & 2 \end{array}$$

I prefer the second: product and sum carries are with the associated numbers.

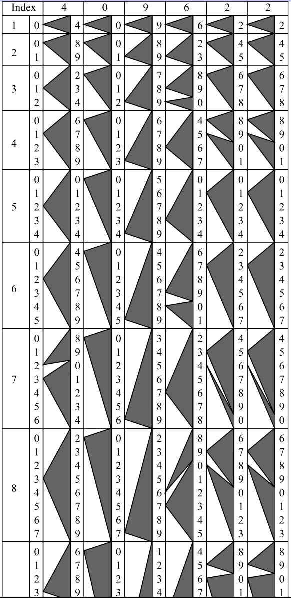
Genaille's Rods 1891, Napier's rods without carries



Genaille's Rods Example



Genaille's Rods Example



$$
\begin{array}{ccccccccc}
 & & & 4 & 0 & 9 & 6 & 2 & 2 \\
 & & \times & & & & 3 & 8 & 8 \\
\hline
 & & 3 & 2 & 7 & 6 & 9 & 7 & 6 \\
 & 3 & 2 & 7 & 6 & 9 & 7 & 6 & \\
1 & 2 & 2 & 8 & 8 & 6 & 6 & & \\
\hline
1 & 5 & 8_1 & 9_2 & 3_2 & 3_2 & 3_1 & 3 & 6
\end{array}
$$

Prosthaphaeresis

$$\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b)).$$

Prosthaphaeresis

$\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b))$.
Scale numbers to between zero and one, so $x = \cos a$, $y = \cos b$, or $a = \cos^{-1} x$, $b = \cos^{-1} y$.

Prosthaphaeresis

$\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b))$.
Scale numbers to between zero and one, so $x = \cos a$, $y = \cos b$, or $a = \cos^{-1} x$, $b = \cos^{-1} y$. Then
$xy = \frac{1}{2}(\cos(\cos^{-1} x + \cos^{-1} y) + \cos(\cos^{-1} x - \cos^{-1} y))$.

Prosthaphaeresis

$\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b))$.
Scale numbers to between zero and one, so $x = \cos a$, $y = \cos b$, or $a = \cos^{-1} x$, $b = \cos^{-1} y$. Then
$xy = \frac{1}{2}(\cos(\cos^{-1} x + \cos^{-1} y) + \cos(\cos^{-1} x - \cos^{-1} y))$.
Particularly promoted by Tycho Brahe (1580 on).

Prosthaphaeresis

$\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b))$.
Scale numbers to between zero and one, so $x = \cos a$, $y = \cos b$, or $a = \cos^{-1} x$, $b = \cos^{-1} y$. Then
$xy = \frac{1}{2}(\cos(\cos^{-1} x + \cos^{-1} y) + \cos(\cos^{-1} x - \cos^{-1} y))$.
Particularly promoted by Tycho Brahe (1580 on).
For example: $43.287 \times 1.1033 = 0.43287 \times 10^2 \times 0.11033 \times 10^1$.

Prosthaphaeresis

$\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b))$.
Scale numbers to between zero and one, so $x = \cos a$, $y = \cos b$, or $a = \cos^{-1} x$, $b = \cos^{-1} y$. Then
$xy = \frac{1}{2}(\cos(\cos^{-1} x + \cos^{-1} y) + \cos(\cos^{-1} x - \cos^{-1} y))$.
Particularly promoted by Tycho Brahe (1580 on).
For example: $43.287 \times 1.1033 = 0.43287 \times 10^2 \times 0.11033 \times 10^1$.
From tables, the best we have is $\cos(64^\circ 21' 1'') \approx 0.43287$ and $\cos(83^\circ 39' 56'') \approx 0.11033$.

Prosthaphaeresis

$\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b))$.
Scale numbers to between zero and one, so $x = \cos a$, $y = \cos b$, or $a = \cos^{-1} x$, $b = \cos^{-1} y$. Then
$xy = \frac{1}{2}(\cos(\cos^{-1} x + \cos^{-1} y) + \cos(\cos^{-1} x - \cos^{-1} y))$.
Particularly promoted by Tycho Brahe (1580 on).
For example: $43.287 \times 1.1033 = 0.43287 \times 10^2 \times 0.11033 \times 10^1$.
From tables, the best we have is $\cos(64^\circ 21' 1'') \approx 0.43287$ and $\cos(83^\circ 39' 56'') \approx 0.11033$. So
$xy = \frac{1}{2}(\cos(148^\circ 0' 57'') + \cos(-19^\circ 18' 55'')) \times 10^3 = \frac{1}{2}(-0.848194503 + 0.943712787) \times 10^3 = 0.047759142 \times 10^3 = 47.759142$.

Prosthaphaeresis

$\cos a \cos b = \frac{1}{2}(\cos(a+b) + \cos(a-b))$.

Scale numbers to between zero and one, so $x = \cos a$, $y = \cos b$, or $a = \cos^{-1} x$, $b = \cos^{-1} y$. Then

$xy = \frac{1}{2}(\cos(\cos^{-1} x + \cos^{-1} y) + \cos(\cos^{-1} x - \cos^{-1} y))$.

Particularly promoted by Tycho Brahe (1580 on).

For example: $43.287 \times 1.1033 = 0.43287 \times 10^2 \times 0.11033 \times 10^1$.

From tables, the best we have is $\cos(64^\circ 21' 1'') \approx 0.43287$ and $\cos(83^\circ 39' 56'') \approx 0.11033$. So

$xy = \frac{1}{2}(\cos(148^\circ 0' 57'') + \cos(-19^\circ 18' 55'')) \times 10^3 = \frac{1}{2}(-0.848194503 + 0.943712787) \times 10^3 = 0.047759142 \times 10^3 = 47.759142$. The true value is 47.7585471, five digits of accuracy.

Logarithms

Napier (1614): if $y = \log x$ then $x/10^7 = (1 - 10^7)^y$. Then $\log 10^7 = 0$, logs increase as the number decreases, and $\log xy = \log x + \log y$.

Logarithms

Napier (1614): if $y = \log x$ then $x/10^7 = (1 - 10^7)^y$. Then $\log 10^7 = 0$, logs increase as the number decreases, and $\log xy = \log x + \log y$.

Briggs (1617): Common logarithms: $\log 1 = 0$ and $\log 10 = 1$, so if $y = \log x$ then $x = 10^y$.

Logarithms

Napier (1614): if $y = \log x$ then $x/10^7 = (1 - 10^7)^y$. Then $\log 10^7 = 0$, logs increase as the number decreases, and $\log xy = \log x + \log y$.

Briggs (1617): Common logarithms: $\log 1 = 0$ and $\log 10 = 1$, so if $y = \log x$ then $x = 10^y$.

Mercator (1666): Area under the hyperbola $y = 1/x$ from $x = 1$ to $x = a$ is called $\ln a$. Geometrically satisfies $\ln ab = \ln a + \ln b$ and the base is e.

Logarithms

Napier (1614): if $y = \log x$ then $x/10^7 = (1 - 10^7)^y$. Then $\log 10^7 = 0$, logs increase as the number decreases, and $\log xy = \log x + \log y$.

Briggs (1617): Common logarithms: $\log 1 = 0$ and $\log 10 = 1$, so if $y = \log x$ then $x = 10^y$.

Mercator (1666): Area under the hyperbola $y = 1/x$ from $x = 1$ to $x = a$ is called $\ln a$. Geometrically satisfies $\ln ab = \ln a + \ln b$ and the base is e.

Slide Rule (Oughtred 1622): Rulers with logarithmic scales add lengths to multiply numbers.

Pascal's Triangle and Powers of Eleven

						1						
					1		1					
				1		2		1				
			1		3		3		1			
		1		4		6		4		1		
	1		5		10		10		5		1	
1		6		15		20		15		6		1

Pascal's Triangle and Powers of Eleven

						1						
					1		1					
				1		2		1				
			1		3		3		1			
		1		4		6		4		1		
	1		5		10		10		5		1	
1		6		15		20		15		6		1

$$11^0 = 1$$
$$11^1 = 11$$
$$11^2 = 121$$
$$11^3 = 1331$$
$$11^4 = 14\,641$$
$$11^5 = 161\,051$$
$$11^6 = 1\,771\,561$$

Pascal's Triangle and Powers of Eleven

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	

$$
\begin{aligned}
11^0 &= 1\\
11^1 &= 11\\
11^2 &= 121\\
11^3 &= 1331\\
11^4 &= 14\,641\\
11^5 &= 161\,051\\
11^6 &= 1\,771\,561
\end{aligned}
$$

Using carries, Pascal's triangle rows give powers of eleven.

Explanation

	a	b	c	d	
			1	1	$\times$
	a	b	c	d	
a	b	c	d		
a	$a+b$	$b+c$	$c+d$	d	

so

	a		b		c		d	
a		$a+b$		$b+c$		$c+d$		d

Explanation

	a	b	c	d	$\times$
			1	1	
	a	b	c	d	
a	b	c	d		
a	$a+b$	$b+c$	$c+d$	d	

each number is the sum of the pair diagonally above.

so

$$\begin{array}{ccccccccc} & a & & b & & c & & d & \\ a & & a+b & & b+c & & c+d & & d \end{array}$$

Generalization

Start with one, then if each digit is b times upper left plus a times upper right, each row is a power of $a \times 10 + b$.

Generalization

Start with one, then if each digit is b times upper left plus a times upper right, each row is a power of $a \times 10 + b$. For example 27:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 2 & & 7 & & & & \\
 & & & 4 & & 28 & & 49 & & & \\
 & & 8 & & 84 & & 294 & & 343 & & \\
 & 16 & & 224 & & 1176 & & 2744 & & 2401 & \\
32 & & 560 & & 3920 & & 13\,720 & & 24\,010 & & 16\,807
\end{array}
$$

Generalization

Start with one, then if each digit is b times upper left plus a times upper right, each row is a power of $a \times 10 + b$. For example 27:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 2 & & 7 & & & & \\
 & & & 4 & & 28 & & 49 & & & \\
 & & 8 & & 84 & & 294 & & 343 & & \\
 & 16 & & 224 & & 1176 & & 2744 & & 2401 & \\
32 & & 560 & & 3920 & & 13\,720 & & 24\,010 & & 16\,807
\end{array}
$$

$$27^0 = 1,\ 27^1 = 27,\ 27^2 = 729,\ 27^3 = 19\,683,\ 27^4 = 531\,441,$$
$$27^5 = 14\,348\,907.$$

Karatsuba

Multiplying a pair of n digit number requires n^2 digit multiplies.
Large numbers lead to life-of-universe timings.

Karatsuba

Multiplying a pair of n digit number requires n^2 digit multiplies. Large numbers lead to life-of-universe timings.

Karatsuba (1962): Given base B and $m \approx n/2$, let $x = x_1 B^m + x_0$ and $y = y_1 B^m + y_0$.

Karatsuba

Multiplying a pair of n digit number requires n^2 digit multiplies.
Large numbers lead to life-of-universe timings.

Karatsuba (1962): Given base B and $m \approx n/2$, let $x = x_1 B^m + x_0$ and $y = y_1 B^m + y_0$. Then

$$xy = (x_1 B^m + x_0)(y_1 B^m + y_0) = x_1 y_1 B^{2m} + (x_1 y_0 + x_0 y_1) B^m + x_0 y_0.$$

Four $(n/2)$ digit multiplications means n^2 digit multiples.

Karatsuba

Multiplying a pair of n digit number requires n^2 digit multiplies. Large numbers lead to life-of-universe timings.

Karatsuba (1962): Given base B and $m \approx n/2$, let $x = x_1 B^m + x_0$ and $y = y_1 B^m + y_0$. Then

$$xy = (x_1 B^m + x_0)(y_1 B^m + y_0) = x_1 y_1 B^{2m} + (x_1 y_0 + x_0 y_1) B^m + x_0 y_0.$$

Four $(n/2)$ digit multiplications means n^2 digit multiples. But

$$\begin{aligned} x_1 y_0 + x_0 y_1 &= (x_1 y_1 + x_1 y_0 + x_0 y_1 + x_0 y_0) - (x_1 y_1 + x_0 y_0) \\ &= (x_1 + x_0)(y_1 + y_0) - x_1 y_1 - x_0 y_0, \end{aligned}$$

reduces us to three multiplications: $3n^2/4$ digit multiples.

Karatsuba

Multiplying a pair of n digit number requires n^2 digit multiplies. Large numbers lead to life-of-universe timings.

Karatsuba (1962): Given base B and $m \approx n/2$, let $x = x_1 B^m + x_0$ and $y = y_1 B^m + y_0$. Then

$$xy = (x_1 B^m + x_0)(y_1 B^m + y_0) = x_1 y_1 B^{2m} + (x_1 y_0 + x_0 y_1) B^m + x_0 y_0.$$

Four $(n/2)$ digit multiplications means n^2 digit multiples. But

$$\begin{aligned} x_1 y_0 + x_0 y_1 &= (x_1 y_1 + x_1 y_0 + x_0 y_1 + x_0 y_0) - (x_1 y_1 + x_0 y_0) \\ &= (x_1 + x_0)(y_1 + y_0) - x_1 y_1 - x_0 y_0, \end{aligned}$$

reduces us to three multiplications: $3n^2/4$ digit multiples.

Applied recursively, reduces to $O(3n^{\log_2 3}) \approx O(3n^{1.585})$.

Karatsuba

Multiplying a pair of n digit number requires n^2 digit multiplies. Large numbers lead to life-of-universe timings.

Karatsuba (1962): Given base B and $m \approx n/2$, let $x = x_1 B^m + x_0$ and $y = y_1 B^m + y_0$. Then

$$xy = (x_1 B^m + x_0)(y_1 B^m + y_0) = x_1 y_1 B^{2m} + (x_1 y_0 + x_0 y_1) B^m + x_0 y_0.$$

Four $(n/2)$ digit multiplications means n^2 digit multiples. But

$$\begin{aligned} x_1 y_0 + x_0 y_1 &= (x_1 y_1 + x_1 y_0 + x_0 y_1 + x_0 y_0) - (x_1 y_1 + x_0 y_0) \\ &= (x_1 + x_0)(y_1 + y_0) - x_1 y_1 - x_0 y_0, \end{aligned}$$

reduces us to three multiplications: $3n^2/4$ digit multiples.

Applied recursively, reduces to $O(3n^{\log_2 3}) \approx O(3n^{1.585})$.

Practically better than traditional method with more than ~ 400 (decimal) digits.

Toom-Cook

Andrei Toom (1963) and Stephen Cook (1966), splits large integers into k smaller parts.

Toom-Cook

Andrei Toom (1963) and Stephen Cook (1966), splits large integers into k smaller parts.

For example (GNU MP), with $k = 3$, let $X(t) = x_2 t^2 + x_1 t + x_0$ and $Y(t) = y_2 t^2 + y_1 t + y_0$ with $X(b) = x$, $Y(b) = y$.

Toom-Cook

Andrei Toom (1963) and Stephen Cook (1966), splits large integers into k smaller parts.

For example (GNU MP), with $k = 3$, let $X(t) = x_2 t^2 + x_1 t + x_0$ and $Y(t) = y_2 t^2 + y_1 t + y_0$ with $X(b) = x$, $Y(b) = y$.

Let $W(t) = X(t)Y(t) = w_4 t^4 + w_3 t^3 + w_2 t^2 + w_1 t + w_0$, so $xy = W(b)$.

Toom-Cook

Andrei Toom (1963) and Stephen Cook (1966), splits large integers into k smaller parts.

For example (GNU MP), with $k = 3$, let $X(t) = x_2 t^2 + x_1 t + x_0$ and $Y(t) = y_2 t^2 + y_1 t + y_0$ with $X(b) = x$, $Y(b) = y$.

Let $W(t) = X(t)Y(t) = w_4 t^4 + w_3 t^3 + w_2 t^2 + w_1 t + w_0$, so $xy = W(b)$. To find the w_i's, evaluate $X(t)$ and $Y(t)$ at five points, giving $W(t)$ at those points.

Toom-Cook

Andrei Toom (1963) and Stephen Cook (1966), splits large integers into k smaller parts.

For example (GNU MP), with $k = 3$, let $X(t) = x_2t^2 + x_1t + x_0$ and $Y(t) = y_2t^2 + y_1t + y_0$ with $X(b) = x$, $Y(b) = y$.

Let $W(t) = X(t)Y(t) = w_4t^4 + w_3t^3 + w_2t^2 + w_1t + w_0$, so $xy = W(b)$. To find the w_i's, evaluate $X(t)$ and $Y(t)$ at five points, giving $W(t)$ at those points. Then interpolate! Choosing the t's carefully leads to easy Gaussian elimination.

Toom-Cook

Andrei Toom (1963) and Stephen Cook (1966), splits large integers into k smaller parts.

For example (GNU MP), with $k = 3$, let $X(t) = x_2t^2 + x_1t + x_0$ and $Y(t) = y_2t^2 + y_1t + y_0$ with $X(b) = x$, $Y(b) = y$.

Let $W(t) = X(t)Y(t) = w_4t^4 + w_3t^3 + w_2t^2 + w_1t + w_0$, so $xy = W(b)$. To find the w_i's, evaluate $X(t)$ and $Y(t)$ at five points, giving $W(t)$ at those points. Then interpolate! Choosing the t's carefully leads to easy Gaussian elimination. Finally, recombine.

Toom-Cook

Andrei Toom (1963) and Stephen Cook (1966), splits large integers into k smaller parts.

For example (GNU MP), with $k = 3$, let $X(t) = x_2t^2 + x_1t + x_0$ and $Y(t) = y_2t^2 + y_1t + y_0$ with $X(b) = x$, $Y(b) = y$.

Let $W(t) = X(t)Y(t) = w_4t^4 + w_3t^3 + w_2t^2 + w_1t + w_0$, so $xy = W(b)$. To find the w_i's, evaluate $X(t)$ and $Y(t)$ at five points, giving $W(t)$ at those points. Then interpolate! Choosing the t's carefully leads to easy Gaussian elimination. Finally, recombine.

This version is $O(n^{\log_3 5}) \approx O(n^{1.465})$, but has a larger constant than Karatsuba. Better with more than 700 digits.

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

Then $xy = \sum_{i=0}^{m} \sum_{j=0}^{m} 2^{w(i+j)} a_i b_j$

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

Then $xy = \sum_{i=0}^{m} \sum_{j=0}^{m} 2^{w(i+j)} a_i b_j = \sum_{k=0}^{2m} 2^{wk} \sum_{i=0}^{k} a_i b_{k-i}$

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

Then $xy = \sum_{i=0}^{m} \sum_{j=0}^{m} 2^{w(i+j)} a_i b_j = \sum_{k=0}^{2m} 2^{wk} \sum_{i=0}^{k} a_i b_{k-i} = \sum_{k=0}^{2m} 2^{wk} c_k$ where $a_i, b_j = 0$ for $i, j > m$ and $\{c_k\}$ is the convolution of $\{a_i\}$ and $\{b_j\}$.

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

Then $$xy = \sum_{i=0}^{m} \sum_{j=0}^{m} 2^{w(i+j)} a_i b_j = \sum_{k=0}^{2m} 2^{wk} \sum_{i=0}^{k} a_i b_{k-i} = \sum_{k=0}^{2m} 2^{wk} c_k$$
where $a_i, b_j = 0$ for $i, j > m$ and $\{c_k\}$ is the convolution of $\{a_i\}$ and $\{b_j\}$.

The convolution can be found by (i) computing the Fast Fourier Transform of $\{a_i\}$ and $\{b_j\}$,

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

Then $xy = \sum_{i=0}^{m} \sum_{j=0}^{m} 2^{w(i+j)} a_i b_j = \sum_{k=0}^{2m} 2^{wk} \sum_{i=0}^{k} a_i b_{k-i} = \sum_{k=0}^{2m} 2^{wk} c_k$ where $a_i, b_j = 0$ for $i, j > m$ and $\{c_k\}$ is the convolution of $\{a_i\}$ and $\{b_j\}$.

The convolution can be found by (i) computing the Fast Fourier Transform of $\{a_i\}$ and $\{b_j\}$, (ii) multiplying the elements term by term,

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

$$\text{Then } xy = \sum_{i=0}^{m} \sum_{j=0}^{m} 2^{w(i+j)} a_i b_j = \sum_{k=0}^{2m} 2^{wk} \sum_{i=0}^{k} a_i b_{k-i} = \sum_{k=0}^{2m} 2^{wk} c_k$$

where $a_i, b_j = 0$ for $i, j > m$ and $\{c_k\}$ is the convolution of $\{a_i\}$ and $\{b_j\}$.

The convolution can be found by (i) computing the Fast Fourier Transform of $\{a_i\}$ and $\{b_j\}$, (ii) multiplying the elements term by term, (iii) computing the inverse Fourier transform,

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

Then $xy = \sum_{i=0}^{m} \sum_{j=0}^{m} 2^{w(i+j)} a_i b_j = \sum_{k=0}^{2m} 2^{wk} \sum_{i=0}^{k} a_i b_{k-i} = \sum_{k=0}^{2m} 2^{wk} c_k$ where $a_i, b_j = 0$ for $i, j > m$ and $\{c_k\}$ is the convolution of $\{a_i\}$ and $\{b_j\}$.

The convolution can be found by (i) computing the Fast Fourier Transform of $\{a_i\}$ and $\{b_j\}$, (ii) multiplying the elements term by term, (iii) computing the inverse Fourier transform, and (iv) add the part of $c_k > 2^w$ to c_{k+1}: dealing with carries.

Schönhage-Strassen (1971)

Split the numbers into $m+1$ groups, each of which is small enough to fit in a computer variable: $x = \sum_{i=0}^{m} 2^{w_i} x_i$ and $y = \sum_{j=0}^{m} 2^{w_j} y_j$.

Then $xy = \sum_{i=0}^{m} \sum_{j=0}^{m} 2^{w(i+j)} a_i b_j = \sum_{k=0}^{2m} 2^{wk} \sum_{i=0}^{k} a_i b_{k-i} = \sum_{k=0}^{2m} 2^{wk} c_k$ where $a_i, b_j = 0$ for $i, j > m$ and $\{c_k\}$ is the convolution of $\{a_i\}$ and $\{b_j\}$.

The convolution can be found by (i) computing the Fast Fourier Transform of $\{a_i\}$ and $\{b_j\}$, (ii) multiplying the elements term by term, (iii) computing the inverse Fourier transform, and (iv) add the part of $c_k > 2^w$ to c_{k+1}: dealing with carries.

Best with more than about ten to forty thousand digits.

Conclusion

So, just how would you like to multiply now?