The Hunt for ABC Triples

Frank Rubin
www.contestcen.com

Marist College
January 28, 2019

Frank Rubin has an MS in Mathematics and a PhD in Computer Science.

He has been hunting for ABC Triples since 2007.

What is an ABC Triple?

An ABC Triple is a set of 3 positive integers A+B=C, where A, B and C have no common factors, and Rad(ABC) < C.

Rad(N) denotes the **radical** of the integer N, which is the product of its distinct prime factors. For example, if p, q and r are primes, then $Rad(p^x) = p$, $Rad(p^xq^y) = pq$, $Rad(p^xq^yr^z) = pqr$, and so forth. In other words, Rad(N) strips off the exponents.

.

The ratio between ln(N) and ln(Rad(N)), called the **fractional exponent**, is a measure of how much N is like a power. If $N = p^x$, then ln(N) / ln(Rad(N)) is x.

Consider the numbers $72 = 2^3 3^2$ and $108 = 2^2 3^3$. Since they have the same prime factors their radicals are the same. Rad(72) = Rad(108) = 6.

ln(72)/ln(Rad(72)) = 2.387 is smaller than ln(108)/ln(Rad(108)) = 2.613. This is because $2^3 3^2$ has the larger exponent, 3, on the smaller prime factor, 2, while $2^2 3^3$ has the larger exponent, 3, on the larger prime factor, 3.

The fractional exponent of 72 is closer to 2, and the fractional exponent of 108 is closer to 3, so 72 more like a square, while 108 is more like a cube.

What is a good Triple?

The goodness of an ABC Triple can be measured three ways: quality, merit and being unbeaten.
Let R = Rad (ABC).

Quality. Q = ln(C) / ln(R). An ABC Triple is called **Good** if Q > 1.4.

Merit. $M = (Q-1)^2 \ln(R) \ln(\ln(R))$. An ABC Triple is called **High Merit** if M > 24. It is conjectured that M is always < 48.

Unbeaten. Triple A,B,C beats triple D,E,F if C > F and the quality of A,B,C is greater than the quality of D,E,F. If no triple beats A,B,C then it is **unbeaten**.

ABC Conjecture

The ABC Conjecture was proposed independently by David Masser in 1985 and Joseph Oesterlé in 1988:

For any real number R > 1 there are only finitely many ABC Triples with quality Q > R.

The conjecture has been investigated not only for integers, but for Gaussian integers, quaternions, polynomials, linear forms, matrices, etc.

Despite massive effort, there is no accepted proof of the conjecture. It is considered the most important unsolved problem in number theory.

Greatest open question in Number Theory

David Masser (British)

Joseph Oesterlé (French)

Catalan Conjecture

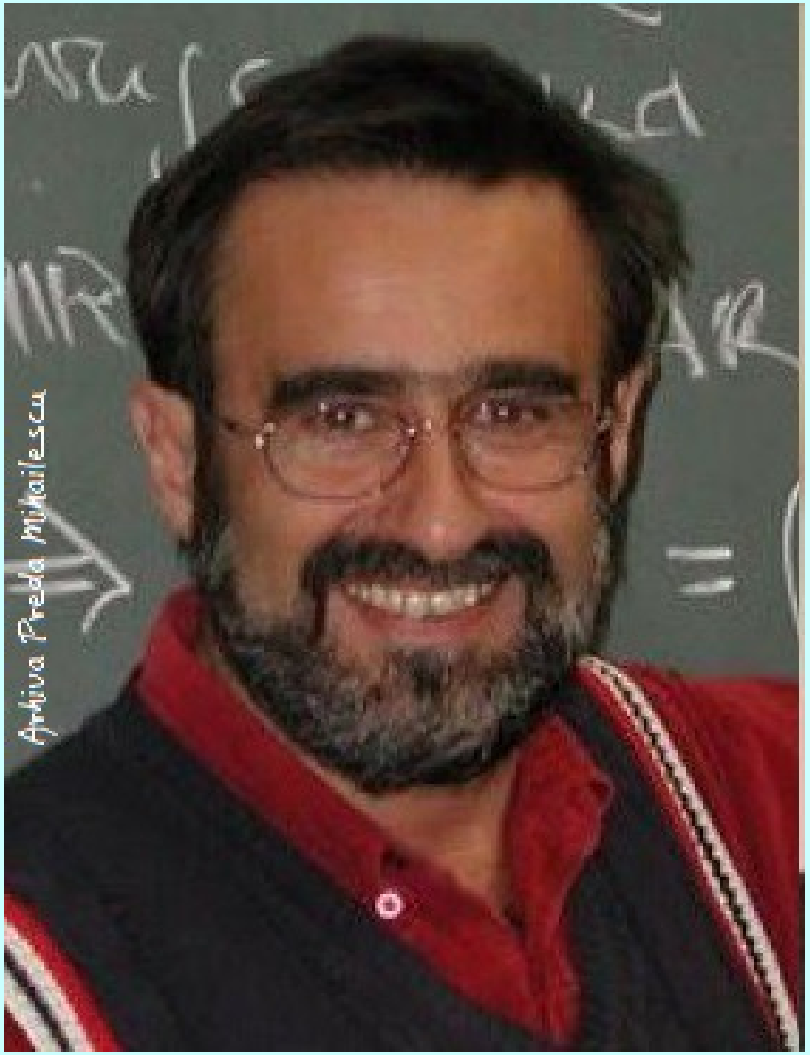
Proposed by Eugène Charles Catalan in 1844:

The only non-trivial integer solution to $x^a - y^b = 1$ is $3^2-2^3 = 1$.

Proved in 2002 by Preda Mihăilescu. (158 years!)

Eugène Charles Catalan (Belgian)

Preda Mihăilescu (Romanian)



Fermat's Theorem

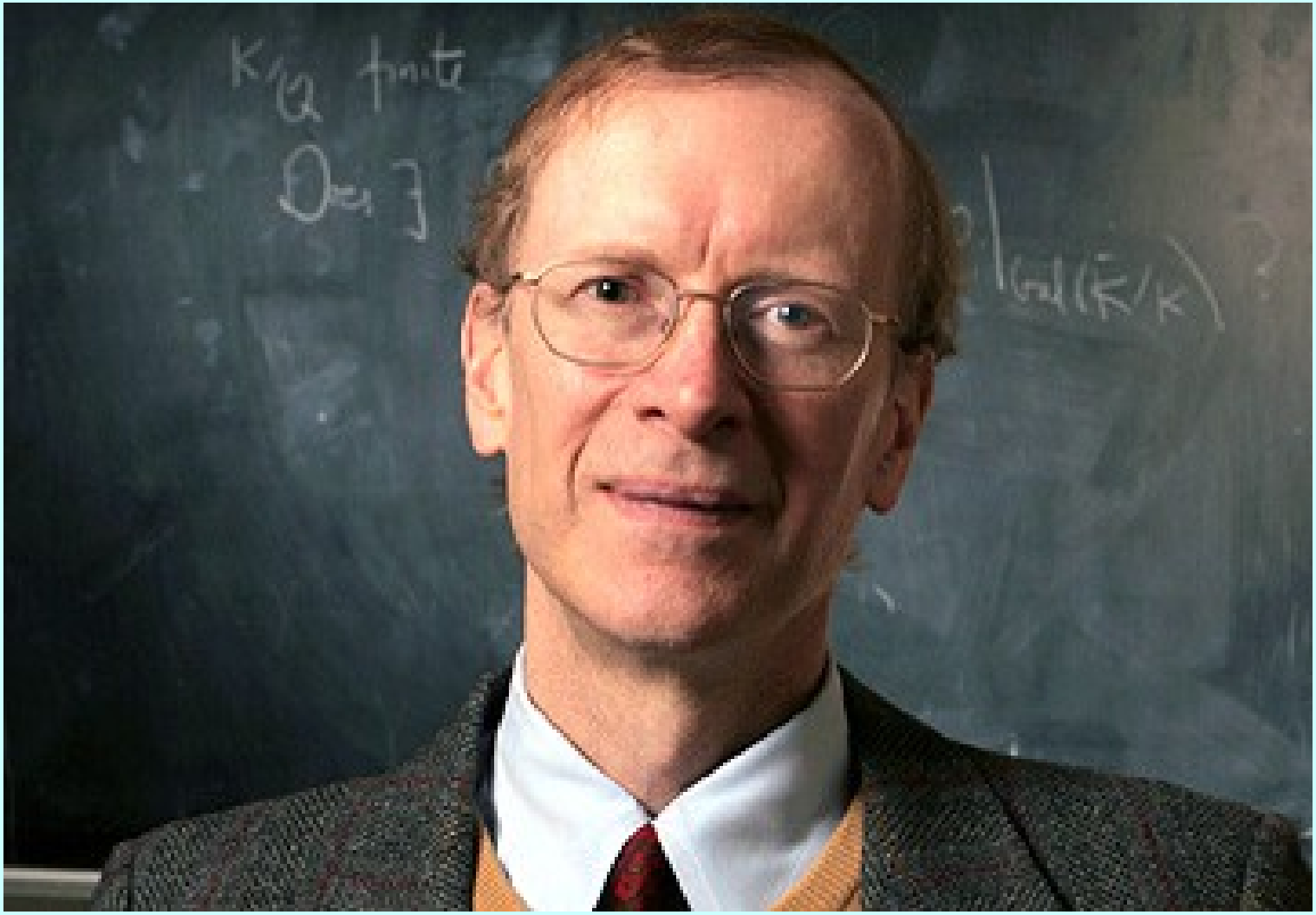
Famously described in the margin of Fermat's copy of Diophantus in 1637.

There is no non-trivial integer solution to $x^n + y^n = z^n$ for $n > 2$.

Proved in 1994 by Andrew Wiles. (357 years!!)

Pierre de Fermat (French)

Andrew Wiles (British)



gcd(A,B,C)=1, so Rad(ABC)=Rad(A)Rad(B)Rad(C). How is it possible to have Rad(ABC) < C ? This implies Rad(C) < C. C must be divisible by one or more powers.

There are two ways to make Rad(ABC) < C.

(1) A, B and C are all divisible by prime powers, for example $\mathbf{2^2+11^2=5^3}$.

(2) B and C are divisible by powers, and A is much smaller than B or C, for example $\mathbf{3+5^3=2^7}$.

This gives us two avenues of attack.

(1) Find or construct numbers divisible by powers whose difference is divisible by a power.

(2) Find or construct numbers divisible by powers whose difference is small.

Methods

Make or find A divisible by power(s)

1. Using a formula (identity)
2. Residue list method
3. Constructing powers

Make or find A small

4. Folding method
5. Heap method

Formulas and Identities

There are many mathematical identities, such as the Brahmagupta–Fibonacci identity

$$(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2)$$

Many identities were discovered by Edouard Lucas just before he died in 1892 from a tragic soup accident.

If a formula can be found that yields triples with quality $Q>1+\varepsilon$, for some $\varepsilon>0$, then the ABC Conjecture would be proved false.

For the sake of time only one formula will be considered tonight.

Pythagorean Triples

Pythagorean Triples are triples a,b,c satisfying $a^2+b^2=c^2$. Euclid gave an explicit formula for finding Pythagorean Triples.

Euclid's Formula	ABC Triple
$a = (x^2-y^2)k$	$A + B = C$
$b = 2xyk$	$a^2 + b^2 = c^2$
$c = (x^2+y^2)k$	

Since ABC Triples require gcd(A,B,C)=1, k will be fixed at 1, and x and y must be coprime and have opposite parity. These triples are called **primitive** Pythagorean Triples.

If x^2-y^2, $2xy$ and x^2+y^2 are not divisible by powers and about the same size, then $Q = \ln(C)/\ln(\text{Rad}(ABC))$ will be roughly $\ln(c^2) / \ln(c^3) = 2/3$, so the Pythagorean Triple will not be an ABC Triple.

There are several way to improve Q.

1. Make a small, that is make $x \approx y$.

2. Let x and y be powers so that $b=2xy$ is divisible by powers.

3. Iterate Euclid's formula. In the expression $c=x^2+y^2$ set $x=w^2-v^2$ and $y=2wv$. Then c will be a square and $C=c^2$ will be a fourth power.

It is possible to make $a=x^2-y^2$ both small and a power simultaneously.

Example: Set $x=122$ and $y=121=11^2$. This gives $x^2-y^2=243=3^5$, yielding the triple

$A = a^2 = 243^2 = 3^{10}$,

$B = b^2 = [2(122)(11^2)]^2 = 2^4 61^2 11^4$,

$C = c^2 = (122^2+121^2)^2 = 29525^2 = 5^4 1181^2$,

or $\mathbf{3^{10} + 2^4 61^2 11^4 = 5^4 1181^2}$

with quality $Q = \ln(5^4 1181^2) / \ln(2\cdot 3\cdot 5\cdot 11\cdot 61\cdot 1181) = 1.212$ – mediocre.

Bottom line: using formulas has not produced any good or high merit ABC Triples … so far.

One Algorithm of Each Kind

FIND triples where A is divisible by a power	FIND triples where A << C
CONSTRUCT triples where A is divisible by a power	CONSTRUCT triples where A << C

Residue List Method

Imagine a list of candidates x_1, x_2, … that is, a list of powers and products of powers. If the difference between two numbers on the list is divisible by one or more powers, then you have a potential ABC Triple.

How can this be detected? If the list is long, taking all pairs and factoring their differences would not be feasible. [Side note: the ABC@Home project did exactly this using a network of 7300 computers to find all triples up to 2^{63}.]

The list method cuts this problem down to size, by considering each possible prime factor separately.

For each small prime p, choose a convenient power p^n of p. Bigger powers mean less work, but will find fewer triples. I chose p^n around 5,000,000. Form p^n lists using chained list techniques. Place each product x_i into the list corresponding to its residue modulo p^n.

If x_i and x_j are both on list k, then $x_i=ap^n+k$ and $x_j=bp^n+k$ for some a and b. Then $x_i-x_j=(a-b)p^n$, so only (a-b) needs to be factored.

The number of pairs whose differences need to be factored has been reduced by a factor of p^n, and the size of the numbers to be factored has also been reduced by a factor of p^n.

Using this technique I was able to find 30 previously unknown good triples, including the only good triples with 30 or more digits.

$$3^{13}37^{5}44939^{2} + 5^{5}7^{23}19\cdot463\cdot863 = 2^{20}53^{8}61\cdot113^{4}$$

$$2^{14}3^{6}42487^{3} + 5^{14}29^{12}83 = 7^{8}11^{3}47^{7}46109111$$

$$2^{37}3^{12}9109^{3} + 5^{13}13^{15}2939 = 7^{23}11\cdot793345871$$

BTW, entries from 2 lists with residues x and y can be added if $x+y=p^{n}$ (complementary lists). This yields a few more triples, roughly 20% to 25% more.

Constructing Powers

Instead of finding pairs of numbers whose difference is divisible by some power, another approach is to construct such pairs of numbers.

Suppose there is a list of pairs x_1/y_1, x_2/y_2, x_3/y_3, … where all of the differences x_1-y_1, x_2-y_2, x_3-y_3, … are divisible by p^n, but not by p^{n+1}. These pairs can be combined to make new pairs whose differences are divisible by p^{n+1}.

Here is how. Let x/y and v/w be two such pairs. Then $x=ap^n+r$, $y=bp^n+r$, $v=cp^n+s$, and $w=dp^n+s$.

These two pairs can be combined to form a new pair by either multiplying or dividing them. Consider division.

$(x/y)/(v/w) = xw/yv.$

$xw = (ap^n+r)(dp^n+s) = adp^{2n} + (as+dr)p^n + rs.$

$yv = (bp^n+r)(cp^n+s) = bcp^{2n} + (bs+cr)p^n + rs.$

$xw\text{-}yv = (?)p^{2n} + [(as+dr)\text{-}(bs+cr)]\ p^n.$

So xw-yv will be a multiple of p^{n+1} if (as+dr) - (bs+cr) is a multiple of p. That is, if $as+dr \equiv bs+cr \pmod{p}$.

How can such pairs be found? Brute force?

Now here's the trick: Separate the terms in this congruence that came from x/y from the terms that came from v/w. Begin by factoring

$$as-bs \equiv cr-dr \pmod{p},$$

$$(a-b)s \equiv (c-d)r \pmod{p}.$$

Since p is a prime, and neither r nor s can be 0, both r and s have multiplicative inverses (mod p), namely r' and s'. Multiply by r's' to get

$$(a-b)r' \equiv (c-d)s' \pmod{p}.$$

Here the term (a-b)r' comes from the x/y pair, and (c-d)s' comes from the v/w pair. This means that for each pair in the list (a-b)r' (mod p) can be computed separately in a single linear-time pass.

Sort the list by (a-b)r' (mod p). There are only p-1 different values for (a-b)r' (mod p), so the sort takes only linear time.

For any two pairs in the list, if these values are equal, then those two pairs can be combined to get a new pair xw/yv with xw-yv divisible by p^{n+1}.

Pairs can also be combined as (x/y)*(v/w), $(x/y)/(v/w)^2$, and so forth to get additional new pairs.

Algorithm: For each n in the desired range, build a table of empty lists, one for each residue mod p^n.

Generate a large number of products of powers. Form the initial pairs x/y from these products. If x-y is divisible by p^n, and not by p^{n+1}, place it in list n.

Search the lists one at a time, combining pairs whose values of (a-b)r' are equal.

For each new pair, determine the greatest m for which x-y is divisible by p^m and place it in list m.

When there are more entries than the list can hold keep the smallest ones.

To save space, make the table circular. For instance, powers n, n+20, n+40, … could occupy the same slot.

Folding Method

The other approach to making Rad(ABC) smaller than C is to make A small, so that it contributes less to Rad(ABC). One such method is **folding**.

Suppose that a list of products of powers has been formed. If that list is sorted by size, then consecutive terms will have values that are close in value.

To illustrate, consider the powers of 2 and 3.

Powers of 2 and 3

2^2	4		
2^3	8		
3^2	9	9/8 = 1.125	$1+2^3=3^2$
2^4	16	16/9 = 1.778	$7+3^2=2^4$
3^3	27	27/16 = 1.688	$11+2^4=3^3$
2^5	32	32/27 = 1.185	$5+3^3=2^5$
2^6	64		
3^4	81	81/64 = 1.266	$17+2^6=3^4$
2^7	128	128/81 = 1.580	$47+3^4=2^7$
3^5	243	243/128 = 1.898	$115+2^7=3^5$
2^8	256	256/243 = 1.053	$13+3^5=2^8$
2^9	512		
3^6	729	729/512 = 1.424	$217+2^9=3^6$

$2^8/3^5 = 1.053$

$3^2/2^3 = 1.125$

$2^2/3^1 = 1.333$

$2^5/3^3 = 1.185$

$3^4/2^6 = 1.266$

$3^6/2^9 = 1.424$

$3^1/2^1 = 1.500$

$2^7/3^4 = 1.580$

$3^3/2^4 = 1.688$

$2^4/3^2 = 1.778$

$3^5/2^7 = 1.898$

$(3^2/2^3)/(2^8/3^5) = 1.125/1.053$

$3^7/2^{11} = 1.068$

$139+2^{11} = 3^7$

Continue to divide adjacent (and nearby) pairs to make the ratio C/B ever smaller.

Other ratios like P/Q^2 and P^3/Q^2, etc. can be used. Also, more than 2 pairs can be combined at each step, say P_1P_4/P_2P_3.

The more base primes that are used, the closer the ratio between C and B can be achieved.

After many iterations, the ratios C/B become very close, and very **high precision logarithms** are needed to sort them into proper order, 50, 100, even 150 decimal places.

Logarithms

150-place logarithms take up a lot of space. A better way was needed.

Recall that $\ln(1+x) = x - x^2/2 + x^3/3 - \ldots$ If x is small enough $\ln(1+x) = x$ is a decent approximation.

Since $C/B = (A+B)/B = 1+A/B$, and $A \ll C$, a first order approximation for $\ln(C/B)$ is A/B.

A/B proved to be too large, and A/C was too small, but $2A/(B+C)$ was an excellent approximation. Simply convert $(B+C)/A$ to a real value V and compute $2/V$ using floating point arithmetic.

Heap Method

A method for **finding** triples where A=C-B is small is to generate the products of powers in size order, for example $2^4 3$, 7^2, $2 \cdot 5^2$, $2 \cdot 3^3$, $2^3 7$, …

Start with several sets of base primes, for example all sets whose product is less than 1000. This would include single primes up to 1000, pairs of primes from (2,3) through (29,31), and threesomes, from (2,3,5) to (5,11,17). A few foursomes are possible.

Using these base prime sets, the goal is to generate the products of powers in size order. That part is easy. **The problem is to avoid duplicates.**

Suppose $N=2^7 5^3 11^2$ has been generated. Its successors are 2N, 5N and 11N, namely $2^8 5^3 11^2$, $2^7 5^4 11^2$ and $2^7 5^3 11^3$.

The successors of $2^8 5^3 11^2$ include $2^8 5^4 11^2$. Likewise the successors of $2^7 5^4 11^2$ include $2^8 5^4 11^2$. If all the successors were used, then $2^8 5^4 11^2$ would be generated twice.

The trick is to go left to right. Label each successor with the position of the exponent that was increased. The successors of $2^7 5^3 11^2$ become **(1)**$2^8 5^3 11^2$, **(2)**$2^7 5^4 11^2$ and **(3)**$2^7 5^3 11^3$.

When the successors of **(n)**xxxx are generated, only exponents n, n+1, … are increased.

For example, the successors of **(2)**$2^7 5^4 11^2$ would be **(2)**$2^7 5^5 11^2$ and **(3)**$2^7 5^4 11^3$, but not **(1)**$2^8 5^4 11^2$.

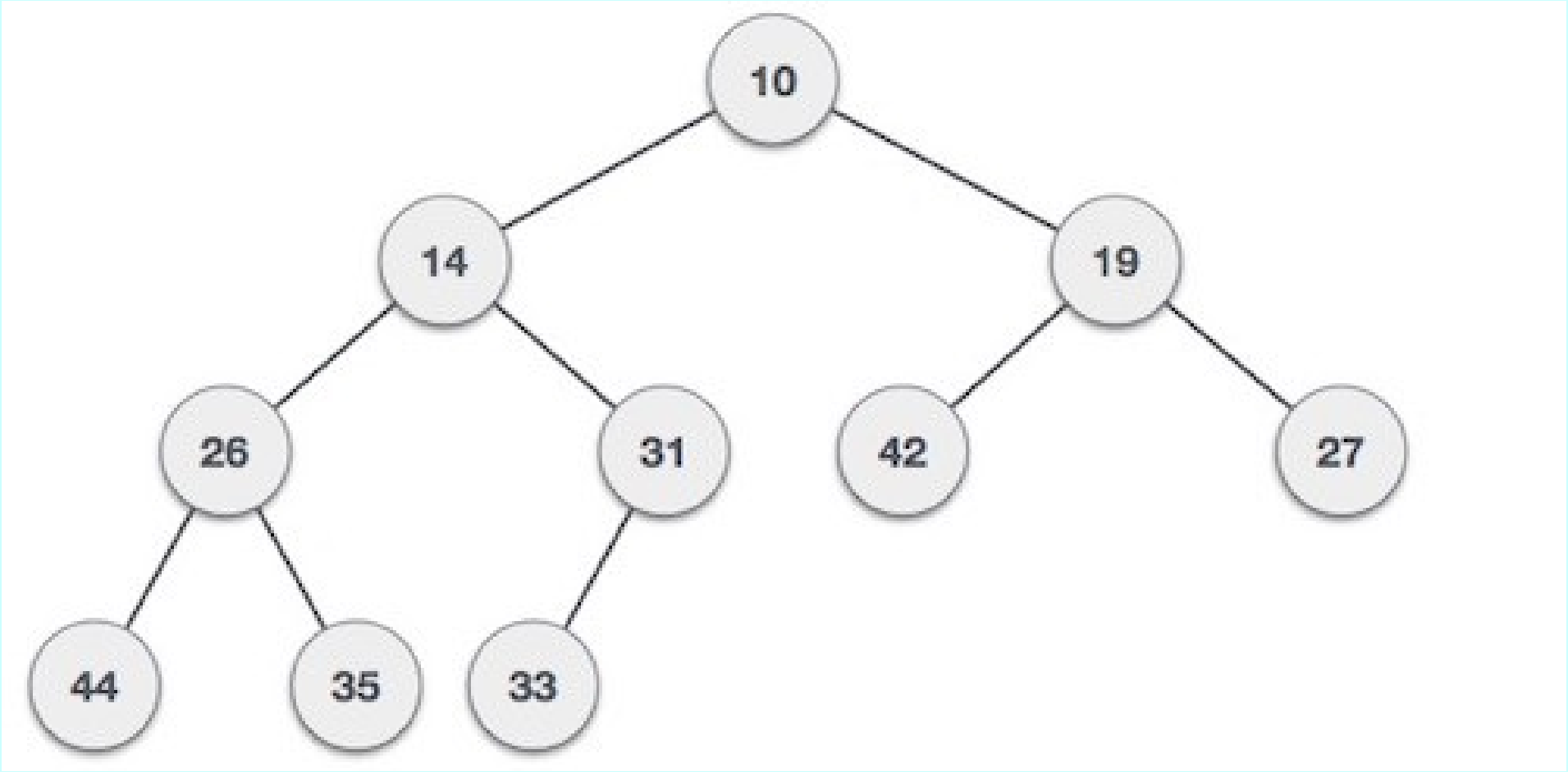
A heap is used to select the products in order. A heap is a binary tree in which the element at each node is smaller than the two elements immediately below it (its daughter nodes). Thus the top element is the smallest.

An element can added to the tree from either the top or the bottom and sifted up or down to the correct position using about $\log_2(n)$ moves.

The heap algorithm repeatedly takes the top (smallest) product from the heap and generates its successors. The first successor replaces the top element and gets sifted down. Any other successors are added to the bottom of the heap and sifted up.

This way, the products are taken from the heap in size order.

Heap



Since each product can several successors, the size of the heap grows.

After the heap has filled the allocated space, only one successor is generated for each product.

Alternatively, the successors can be kept in a set of disk files, say file n for products in the range 2^n to 2^{n+1}. When the heap gets near empty, new products are taken from the next file.

Since these files themselves become large, they are continually split into smaller and smaller ranges to fit into the heap.

Results

Good Triples: There are 240 known good triples. I have found 30 of them, including 7 of the 10 largest.

High Merit: There are 178 known high-merit triples. I have found 68 of these, including 8 of the 22 known triples with merit greater than 30.

Unbeaten: There are 164 known unbeaten triples. I have found 77 of them, including all 62 of the known triples with more than 3000 decimal digits. The largest has 13794 digits.