Expressing integers in the form $a^2 - b^2$

Dr Richard Kenderdine
Kenderdine Maths Tutoring

One of the problems given in `*Teaching Problem-solving in Undergraduate Mathematics*` [A] is the following:

Which numbers can be written as the difference of two perfect squares, e.g. $6^2 - 2^2 = 32$*?*

I interpret `*number*` to mean integer (whole number).

An initial investigation of the values of $a^2 - b^2$ for $2 \le a \le 12$ and $1 \le b \le a$-1 yielded the output:

	b=a-1	a-2	a-3	a-4	a-5	a-6	a-7	a-8	a-9	a-10	a-11
a=2	3										
3	5	8									
4	7	12	15								
5	9	16	21	24							
6	11	20	27	32	35						
7	13	24	33	40	45	48					
8	15	28	39	48	55	60	63				
9	17	32	45	56	65	72	77	80			
10	19	36	51	64	75	84	91	96	99		
11	21	40	57	72	85	96	105	112	117	120	
12	23	44	63	80	95	108	119	128	135	140	143

For example, the entries in the third row, where $a = 4$, are obtained from $4^2 - 3^2 = 7$, $4^2 - 2^2 = 12$ and $4^2 - 1^2 = 15$.

The first column consists of all the odd numbers greater than 1. Hence the numbers differ by 2. The numbers in the second column differ by 4, those in the third column by 6 and so on. Note that some numbers can be represented in more than one way eg $24 = 5^2 - 1^2 = 7^2 - 5^2$.

We can see from the table that all the odd numbers greater then 1 and all even numbers greater than 4 that are multiples of 4 can be expressed as the difference of two squares.

This leaves us with the question: why cannot even numbers that are not multiples of 4 be expressed as the difference of two squares?

Consider these points:

(1) even numbers can be expressed as $2n$ and odd numbers as $2n + 1$, for integer $n \ge 0$.

(2) multiples of 4 can be expressed as $4n$, even numbers that are not multiples of 4 can be expressed as $4n + 2$ and odd numbers as one of $4n + 1$ or $4n - 1$, for integer $n \ge 0$. Note that numbers of the form $4n - 1$ have a remainder of 3 when divided by 4 (in the language of modulus arithmetic they are said to be congruent to 3 *mod* 4).

Now consider the forms that $a^2 - b^2$ can take for the possible combinations of parity of a and b:

(1) both a and b even. Let $a = 2n$ and $b = 2m$ then $a^2 - b^2 = 4(n^2 - m^2)$

(2) a even and b odd. Let $a = 2n$ and $b = 2m + 1$ then $a^2 - b^2 = 4(n^2 - m - m^2) - 1$

(3) a odd and b even. Let $a = 2n + 1$ and $b = 2m$ then $a^2 - b^2 = 4(n^2 + n - m^2) + 1$

(4) both a and b odd. Let $a = 2n + 1$ and $b = 2m + 1$ then $a^2 - b^2 = 4(n - m)(n + m + 1)$

We see that when both a and b have the same parity $a^2 - b^2$ is a multiple of 4 greater than 4, whereas when they are of different parity $a^2 - b^2$ is an odd number. None of the expressions were of the form $4n + 2$.

Note that the first even number that can be expressed in the form $a^2 - b^2$ is 8, using combination (4) with $n = 1$ and $m = 0$, giving $4(1 - 0)(1 + 0 + 1) = 4(1)(2) = 8$.

Hence we agree with the conclusion given above:

All odd numbers greater than 1 and multiples of 4 greater than 4 can be expressed in the form $a^2 - b^2$.

Reference

A. **Teaching Problem-solving in Undergraduate Mathematics**, MS Badger, CJ Sangwin, TO Hawkes with RP Burns, J Mason and S Pope. Downloaded from http://mellbreak.lboro.ac.uk/problemsolving/sites/default/files/guide/Guide.pdf on 17/11/2014