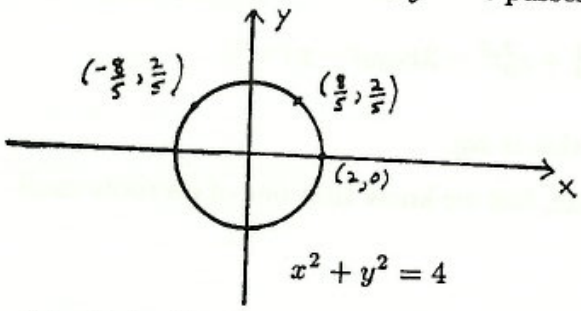
RATIONAL POINTS ON A CIRCLE

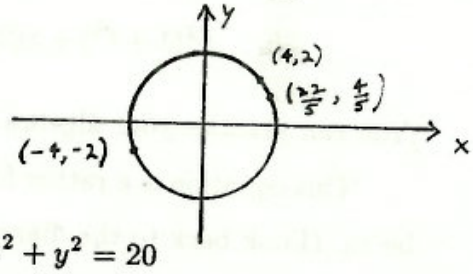
Peter Brown

Given a circle $x^2+y^2=p$, centre (0,0) radius $\sqrt{p}$, does the circle always pass through points whose co-ordinates are rational numbers?

Clearly the circle $x^2+y^2=4$ passes through rational points so does $x^2+y^2=20$.



$x^2+y^2=4$

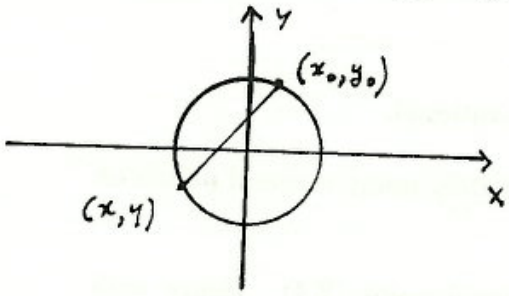


$x^2+y^2=20$

The circle $x^2+y^2=7$ however does not pass through **any** points with rational co-ordinates, as we shall see later.

A point with rational co-ordinates will be called a **rational point**. We begin with a rather surprising theorem.

Theorem 1. *If $x^2+y^2=p$ has one rational point then it has infinitely many of them.*



$x^2+y^2=p$

Proof: Suppose we have a rational point (x_0,y_0) on $x^2+y^2=p$. Draw any line (other than a tangent) from (x_0,y_0) which meets the circle at (x,y).

I claim that (x,y) is a rational point if and only if the gradient of the line is rational.

Clearly if the line meets the circle at (x,y) which is a rational point, then the gradient t is given by $t=\dfrac{y_0-y}{x_0-x}$ which is rational since x,y,x_0,y_0 are rational numbers by assumption.

Conversely, suppose t is rational, then the equation of the line is

$$y-y_0=t(x-x_0) \tag{1}$$

we solve this with

$$x^2+y^2=p \tag{2}$$

to find the intersection point in terms of x_0, y_0 and t.

From (1) $y = y_0 + t(x - x_0)$ and substituting into (2) we have

$$x^2 + [y_0 + t(x - x_0)]^2 = p$$

which 'reduces' to

$$x^2(1 + t^2) + x(2y_0t - 2x_0t^2) + (y_0^2 + x_0^2t^2 - 2x_0y_0t - p) = 0$$

[You can practise your algebra by showing that this is so].

This equation is a rather formidable quadratic, but we know that one of its roots must be x_0. (Look back to the diagram to see why).

Let the other root be x, then

$$xx_0 = \frac{y_0^2 + x_0^2t^2 - 2x_0y_0t - p}{1 + t^2} \qquad \text{(product of the roots)}$$

and so, noting that $x_0^2 + y_0^2 = p$, we have

$$x = \frac{x_0t^2 - 2y_0t - x_0}{1 + t^2} \qquad \text{which is rational.}$$

and using (1),

$$y = \frac{y_0 - y_0t^2 - 2x_0t}{1 + t^2} \qquad \text{which is also rational.}$$

Since t can be chosen as **any** rational number, there are infinitely many rational points on the circle.

Example: On the circle $x^2 + y^2 = 20$, we have the rational point (2,4). Hence with $x_0 = 2, y_0 = 4$ and choosing t as $\frac{1}{2}$ say, then

$$x = -\frac{22}{5}, \; y = \frac{4}{5}.$$

[Check that $x^2 + y^2 = 20$].

Exercise: Find one rational point on $x^2 + y^2 = 29$. Using the formulae above, find at least 3 other rational points on the circle.

Perhaps it is the case that every circle $x^2 + y^2 = p$ has rational points on it. This is not true as we shall shortly see. Firstly some 'new' ideas. You may already be acquainted

with the concept of congruence modulo n in which case you can skip to the next theorem, if not ...

Take any whole number n (e.g. 7), divide it by 4 and look at the remainder.

For example $7 \div 4 = 1$ rem 3. We will say that 7 is congruent to 3 modulo 4, which simply means that we get a remainder of 3 when 7 is divided by 4, and write

$$7 \equiv 3 \bmod 4.$$

Using (if necessary) a calculator, convince yourself of the following congruences

$$16 \equiv 2 \bmod 7$$

$$128 \equiv 3 \bmod 5$$

$$10256 \equiv 50 \bmod 63.$$

Theorem 2. *The circle $x^2 + y^2 = 7$ has no rational points.*

Proof. Suppose $x^2 + y^2 = 7$ has rational points X, Y. We are aiming to get some sort of contradiction, which will then prove the theorem.

Since X, Y are fractions we write them as $X = \frac{r}{s}$, $y = \frac{t}{s}$ where r, s, t are integers **with no factor common to all three.** * (Note that any two fractions can be made to have the same denominator).

Hence

$$r^2 + t^2 = 7s^2$$

Now we read the equation modulo 4, so

$$r^2 + t^2 \equiv 3s^2 \pmod 4$$

Every integer is congruent to 0,1,2 or 3 modulo 4, and so we can write down a table of squares mod 4, for any integers

r	t	s	r^2	s^2	t^2
0	0	0	0	0	0
1	1	1	1	1	1
2	2	2	0	0	0
3	3	3	1	1	1

} mod 4

look now at the different possible values of s.

$s \equiv 0 \mod 4$: In this case $r^2 + t^2 \equiv 0 \mod 4$, so r, t must be congruent to 0 or 2 mod 4.

This will mean that r, s, t are all even. This contradict condition *

$s \equiv 2 \mod 4$: Once again r, s, t will all be even.

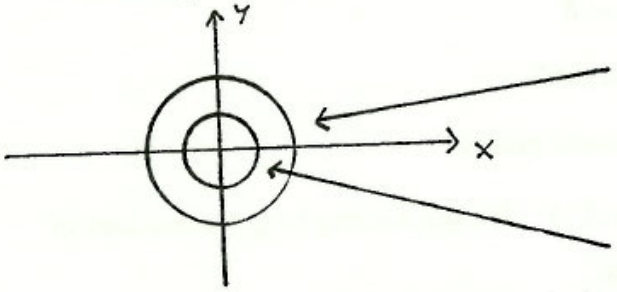
$s \equiv 1 \mod 4$: Hence $r^2 + t^2 \equiv 3 \mod 4$

But this is impossible since from the table above $r^2 + t^2 \equiv 0$, 1 or 2 mod 4

$s \equiv 3 \mod 4$: Once again $r^2 + t^2 \equiv 3 \mod 4$

Each of the possible values of s yields a contradiction and so the theorem is proved.

This result is rather remarkable since for example $x^2 + y^2 = 8$ has **infinitely many rational points**, while $x^2 + y^2 = 7$ has **none.**



$x^2 + y^2 = 8$ has infinitely many rational points

$x^2 + y^2 = 7$ has no rational points

There are in fact many other circles with no rational points. The following theorem completely analyses the problem. Its proof however is rather difficult but is similar to the proof of theorem 2.

Theorem 3. *Suppose n is a natural number. Write n as $n_1^2 p_1 p_2 \cdots p_k$ where n_1 is an integer (possibly 1) and $p_1, p_2 \cdots p_k$ are primes. Then $x^2 + y^2 = n$ has rational points if and only if n can be written in the above form, with* **none** *of the primes $p_1, p_2 \cdots p_k$ are congruent to 3 mod 4.*

Examples:

1) $n = 12 = 2^2.3$, so $x^2 + y^2 = n$ has no rational points.
2) $n = 5150 = 5^2 \times 2 \times 103$ and 103 in prime $\equiv 3 \mod 4$. so $x^2 + y^2 = 5150$ has no rational points.
3) $n = 36 = 3^2.2.2$, since $2 \not\equiv 3 \mod 4$, $x^2 + y^2 = 36$ has (infinitely many) rational points.