PROBLEM SOLVING SEMINAR

DIOPHANTINE EQUATIONS

A DIOPHANTINE EQUATION IS A POLYNOMIAL EQUATION IN TWO OR MORE VARIABLES FOR WHICH ONE SEEKS ONLY THOSE SOLUTIONS FOR WHICH ALL OF THE VARIABLES TAKE INTEGER VALUES. SOME OBVIOUSLY HAVE NO SOLUTIONS, E.G.,

$$2x + 6y = 17$$

(IF x AND y ARE INTEGERS, THE LEFT-HAND SIDE IS EVEN, BUT THE RIGHT-HAND SIDE IS ODD). SOME HAVE NO SOLUTIONS, BUT THIS IS FAR FROM BEING OBVIOUS, E.G., FERMAT'S LAST THEOREM (CONJECTURED BY FERMAT IN 1637, BUT PROVED BY WILES ONLY IN 1995) STATES THAT, FOR $n \geq 3$, THE ONLY SOLUTIONS TO

$$x^n + y^n = z^n$$

WITH x, y AND z INTEGERS ARE THE TRIVIAL ONES ($x = 0$ OR $y = 0$). ON THE OTHER HAND,

$$x^2 + y^2 = z^2$$

HAS INFINITELY MANY INTEGER SOLUTIONS (CALLED PYTHAGOREAN TRIPLES), E.G., $x = 3, y = 4, z = 5$, OR $x = 5, y = 12, z = 13$, OR ANY INTEGER MULTIPLE OF ONE OF THESE. IN FACT,

$$x = 2mn$$
$$y = m^2 - n^2$$
$$z = m^2 + n^2$$

IS A SOLUTION FOR ANY CHOICE OF THE INTEGERS m AND n.

DECIDING WHETHER OR NOT A GIVEN DIOPHANTINE EQUATION HAS SOLUTIONS AND FINDING THEM WHEN IT DOES IS A HUGE AND VERY DIFFICULT SUBJECT. WE WILL LOOK AT JUST A FEW OF THE MORE ELEMENTARY TECHNIQUES.

<u>EXAMPLE</u> 1 : FIND ALL OF THE INTEGER SOLUTIONS TO

$$6x + 6y = xy$$

FOR THIS ONE SOME SIMPLE ALGEBRA WILL DO THE TRICK. NOTICE THAT IF $x=0$, THEN $y=0$ AND, IF $y=0$, THEN $x=0$ SO $(x,y)=(0,0)$ IS THE ONLY SOLUTION FOR WHICH EITHER IS ZERO. NOW ASSUME $x \neq 0$ AND $y \neq 0$. WRITE THE EQUATION AS

$$xy - 6x = 6y$$

$$x(y-6) = 6y$$

SINCE $y \neq 0$ WE CONCLUDE THAT $y-6$ CANNOT BE ZERO SO WE MAY WRITE

$$x = \frac{6y}{y-6}$$

$$(*) \qquad x = 6 + \frac{36}{y-6}$$

SINCE x AND 6 ARE BOTH INTEGERS, $\frac{36}{y-6}$ MUST BE AN INTEGER. THUS, $y-6$ MUST DIVIDE 36. THERE ARE 18 DIVISORS OF 36 :

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36$$

$y-6$ MUST BE ONE OF THESE, BUT IT CANNOT BE -6 SINCE THIS GIVES $y-6=-6$, OR $y=0$ AND WE HAVE ASSUMED THAT $y \neq 0$. THUS, THE SOLUTIONS OTHER THAN $(0,0)$ ARE OBTAINED BY SETTING $y-6$ EQUAL TO ONE OF $\pm 1, \pm 2, \pm 3, \pm 4, 6, \pm 9, \pm 12, \pm 18, \pm 36$, SOLVING FOR y AND PLUGGING IN $(*)$ TO GET x, E.G., $y-6=1$ GIVES $y=7$ AND $x = 6 + \frac{36}{1} = 42$. THUS, THERE ARE 18 SOLUTIONS,

EXAMPLE 2 : FIND ALL POSITIVE INTEGERS n FOR WHICH $n^2 - 19n + 99$ IS A PERFECT SQUARE.

WE ARE ASKED TO FIND THOSE POSITIVE INTEGERS n FOR WHICH

$$n^2 - 19n + 99 = k^2$$

FOR SOME INTEGER k (WE CAN CLEARLY ASSUME THAT $k \geq 0$).

AGAIN, SOME ALGEBRA WILL DO THIS.

$$k^2 - (n^2 - 19n) = 99$$

$$k^2 - \left(n^2 - 19n + \frac{361}{4}\right) = 99 - \frac{361}{4}$$

(COMPLETE THE SQUARE)

$$4k^2 - (4n^2 - 76n + 361) = 396 - 361$$

$$(2k)^2 - (2n - 19)^2 = 35$$

$$(2k - 2n + 19)(2k + 2n - 19) = 35$$

SINCE THEIR PRODUCT IS POSITIVE THESE TWO FACTORS ARE EITHER BOTH POSITIVE OR BOTH NEGATIVE. BUT THEIR SUM IS $4k \geq 0$ SO THEY ARE BOTH POSITIVE. THUS, THE ONLY POSSIBILITIES ARE

$$\begin{array}{lcllll} 2k - 2n + 19 & = & 1, & 5, & 7, & 35 \\ 2k + 2n - 19 & = & 35, & 7, & 5, & 1 \end{array}$$

SOLVING THESE FOUR SYSTEMS OF LINEAR EQUATIONS GIVES

$$(k, n) = (9, 18), (3, 10), (3, 9), (9, 1)$$

SO THE ONLY POSITIVE INTEGERS n FOR WHICH $n^2 - 19n + 99$ IS A SQUARE ARE 1, 9, 10 AND 18.

IN CONTRAST TO $x^2+y^2=z^2$ WE HAVE

EXAMPLE 3 : THE DIOPHANTINE EQUATION $x^2+y^2=3z^2$ HAS ONLY THE TRIVIAL SOLUTION $x=y=z=0$.

THE PROCEDURE WE INTEND TO EMPLOY WAS DEVISED BY FERMAT (ALTHOUGH HE PHRASED IT SOMEWHAT DIFFERENTLY) AND IS CALLED THE METHOD OF INFINITE DESCENT. WE ASSUME THAT $x^2+y^2=3z^2$ DOES HAVE A NONTRIVIAL SOLUTION. WE CAN CLEARLY ASSUME THAT $x \geq 0$, $y \geq 0$ AND $z \geq 0$. IN FACT, SINCE $z=0 \Rightarrow x=y=0$, WE CAN ASSUME THAT z IS POSITIVE, I.E., A NATURAL NUMBER. THUS, BY THE WELL-ORDERING PRINCIPLE, THERE IS SUCH A SOLUTION (x_0, y_0, z_0) WITH SMALLEST POSITIVE z_0. WE DERIVE A CONTRADICTION AS FOLLOWS:

$$x_0^2+y_0^2=3z_0^2 \Rightarrow x_0^2+y_0^2 \equiv 0 \bmod 3$$

BUT EVERY SQUARE IS $\equiv \bmod 3$ TO 0 OR 1 SO WE MUST HAVE $x_0^2 \equiv 0 \bmod 3$ AND $y_0^2 \equiv 0 \bmod 3$, I.E., x_0^2 AND y_0^2 ARE BOTH DIVISIBLE BY 3. BUT 3 IS PRIME SO BOTH x_0 AND y_0 ARE DIVISIBLE BY 3. WRITE

$$x_0 = 3x_1 \quad \text{AND} \quad y_0 = 3y_1$$

FOR NON-NEGATIVE INTEGERS x_1 AND y_1. THEN

$$9x_1^2+9y_1^2=3z_0^2$$

SO

$$x_1^2+y_1^2=3\left(\frac{z_0}{3}\right)^2$$

THUS, $(x_1, y_1, \frac{z_0}{3})$ IS A SOLUTION WITH $x_1 \geq 0$, $y_1 \geq 0$, $\frac{z_0}{3} > 0$, BUT $\frac{z_0}{3} < z_0$ AND THIS CONTRADICTS THE MINIMALITY OF z_0.

<u>NOTE</u>: FERMAT WOULD HAVE SAID THIS IN THE FOLLOWING WAY. ASSUMING THAT (x_0, y, z_0) IS ANY SOLUTION WITH $z_0 > 0$ THE PROCEDURE JUST DESCRIBED PRODUCES ANOTHER SOLUTION (x_1, y_1, z_1) WITH $0 < z_1 < z_0$. REPEATING THE PROCEDURE WITH (x_1, y_1, z_1) WE OBTAIN A SOLUTION (x_2, y_2, z_2) WITH $0 < z_2 < z_1 < z_0$. REPEATING THE PROCESS BY INDUCTION GIVES SOLUTIONS $(x_0, y_0, z_0), (x_1, y_1, z_1), (x_2, y_2, z_2), \ldots$ WITH $0 < \cdots < z_3 < z_2 < z_1 < z_0$ AND THIS IS IMPOSSIBLE BECAUSE EACH z_i IS A POSITIVE INTEGER.

WE HAVE ALREADY SEEN (PROBLEM SET 3, #5) THAT $x^2 - 2y^2 = 3$ HAS NO INTEGER SOLUTIONS (I.E., THE HYPERBOLA $x^2 - 2y^2 = 3$ CONTAINS NO LATTICE POINTS). BY CONTRAST WE HAVE

<u>EXAMPLE 4</u> : FIND FOUR SOLUTIONS IN POSITIVE INTEGERS TO THE EQUATION

$$x^2 - 3y^2 = 1.$$

ONE OBVIOUS SOLUTION IS $(x, y) = (2, 1)$.

$$2^2 - 3 \cdot 1^2 = 1$$

NOW WRITE THIS AS

$$(2 - 1\sqrt{3})(2 + 1\sqrt{3}) = 1.$$

NOTICE THAT IF WE COULD FIND POSITIVE INTEGERS a AND b WITH

$$(a - b\sqrt{3})(a + b\sqrt{3}) = 1$$

THEN $(x, y) = (a, b)$ WOULD ALSO BE A SOLUTION $(a^2 - 3b^2 = 1)$.

TO FIND SUCH A PAIR SQUARE BOTH SIDES OF

$$(2 - 1\sqrt{3})(2 + 1\sqrt{3}) = 1$$

$$(2 - 1\sqrt{3})^2 (2 + 1\sqrt{3})^2 = 1$$

$$(7 - 4\sqrt{3})(7 + 4\sqrt{3}) = 1.$$

THUS, $(x, y) = (7, 4)$ IS A SOLUTION. $(7^2 - 3 \cdot 4^2 = 1)$

TO GET ANOTHER SOLUTION WE COULD SQUARE BOTH SIDES OF $(7 - 4\sqrt{3})(7 + 4\sqrt{3}) = 1$, BUT INSTEAD LET'S MULTIPLY IT BY $(2 - 1\sqrt{3})(2 + 1\sqrt{3}) = 1$.

$$(7 - 4\sqrt{3})(2 - 1\sqrt{3})(7 + 4\sqrt{3})(2 + 1\sqrt{3}) = 1$$

$$(26 - 15\sqrt{3})(26 + 15\sqrt{3}) = 1.$$

THUS, $(x, y) = (26, 15)$ IS A SOLUTION. NOW MULTIPLY THIS BY $(2 - 1\sqrt{3})(2 + 1\sqrt{3}) = 1$ TO GET

$$(26-15\sqrt{3})(2-1\sqrt{3})(26+15\sqrt{3})(2+1\sqrt{3}) = 1$$

$$(97-56\sqrt{3})(97+56\sqrt{3}) = 1$$

SO $(x,y) = (97,56)$ IS A SOLUTION. THAT'S FOUR SOLUTIONS AS REQUIRED, BUT WE COULD CLEARLY CONTINUE THIS INDEFINITELY TO OBTAIN AS MANY SOLUTIONS AS WE LIKE (IN FACT, ONE CAN PROVE THAT ALL OF THE SOLUTIONS TO THE EQUATION CAN BE OBTAINED IN THIS WAY FROM $(2-1\sqrt{3})(2+1\sqrt{3}) = 1$.

NOTE: THIS IS A SPECIAL CASE OF WHAT IS CALLED PELL'S EQUATION

$$x^2 - Dy^2 = N$$

WHERE N IS AN INTEGER AND D IS AN INTEGER THAT IS NOT A PERFECT SQUARE.