2018 UCD Mathematical Enrichment Programme L1

April 14

Thomas J. Laffey.

Algebraic Techniques

(1) Leap year type problems.

Recall the rule for leap years:

Year n is a leap year if either

(1) 400 divides n

or (2) 4 divides n and 100 does not divide n.

In a consecutive period of 400 years, there are 97 leap years, so the total number of days in this period is

$N = 400 \times 365 + 97$

Note $N \equiv (1) \times (1) + 6 \equiv 0 \bmod 7$,

so there is an integer number of weeks in that period. So the calendar "repeats" every 400 years. This repetitive property is the basis of many questions. For example (Putnam) Prove that the probability that Christmas Day falls on a Sunday

is not 1/7.

Solution: In each consecutive period of 400 years, there are 400 Christmas days. Let $n_1, n_2, \ldots, n_7$ be the number of these which occur on Sunday, Monday, ..., Saturday. Then the probability that Christmas day falls on a Sunday is $\frac{n_1}{400}$ and this cannot be $\frac{1}{7}$, since 7 does not divide 400.

[In fact, there are 58 times on which Christmas Day falls on Sunday, so the probability is $\frac{58}{400} = 29/200$].

For Friday 13th, there are 4800 months in 400 years and in these the 13th is a Friday in 688 cases. It occurs on Wednesday 687 times, on Sunday also 687 times, on Monday 685 times, on Tuesday 685 times and on Thursday and on Saturday 684 times.

Problem 1. Suppose that x is a real number such that $x^3 - x$ and $x^4 - x$ are integers. Prove that x is an integer.

Solution: Let $x^3 - x = h$ and $x^4 - x = k$.

If $h = 0$, then $x(x^2 - 1) = 0$, so $x = 0, 1$ or -1, and the result holds.

Suppose then $h \neq 0$. Note that

$$\frac{k}{h} = \frac{x^4 - x}{x^3 - x} = \frac{x^2 + x + 1}{x + 1},$$ so

$$hx^2 - (k - h)x - (k - h) = 0 \quad \ldots (1)$$

Hence

$$hx^3 = (k - h)x^2 + (k - h)x, \text{ so}$$

$$h^2 x^3 = (k - h)hx^2 + (k - h)hx$$

$$= (k - h)^2 x + (k - h)^2 + (k - h)hx \quad \text{(using (1))}$$

$$= k(k - h)x + (k - h)^2.$$

Thus

$$h^2(x^3 - x) = (k(k - h) - h^2)x + (k - h)^2.$$

Since $x^3 - x = h$, this gives

$$h^3 - (k - h)^2 = (k^2 - kh - h^2)x \quad \ldots (2)$$

If $k^2 - kh - h^2 = 0$, then $h^3 - (k-h)^2 = 0$,
so $h^3 = k^2 - 2hk + h^2 = h^2 + kh - 2kh + h^2$
$= 2h^2 - kh$.
Since $h \neq 0$, this gives $h^2 = 2h - k$,
so $k = 2h - h^2$. Hence

$$0 = k^2 - kh - h^2 = 4h^2 - 4h^3 + h^4 - 2h^2 + h^3 - h^2$$
$$= h^2 - 3h^3 + h^4 = h^2(1 - 3h + h^2).$$

Since $h \neq 0$, this implies that $1 - 3h + h^2 = 0$,
so $h = \frac{3 \pm \sqrt{5}}{2}$, which is not an integer. This contradiction shows that $k^2 - kh - h^2 \neq 0$ and now (2) implies that $x = \frac{h^3 - (k-h)^2}{k^2 - kh - h^2}$. Since h and k are integers, this implies that x is a rational number. We write $x = \frac{m}{n}$, where m, n are integers with $\gcd(m,n) = 1$.
Since $\frac{m}{n} = \frac{-m}{-n}$, we may assume $n \geq 1$.
If $n = 1$, then $x = m$ is an integer as claimed.
Suppose $n > 1$. Now $h = x^3 - x = \frac{m^3}{n^3} - \frac{m}{n}$
$= \frac{m(m^2 - n^2)}{n^3}$. But $\gcd(m,n) = 1$ implies that $\gcd(m^2 - n^2, n) = 1$ and thus that $\gcd(m(m^2-n^2), n^3) = 1$. Since $n^3 > 1$, this implies $h = \frac{m(m^2-n^2)}{n^3}$ is not an integer, which is false. So $n = 1$ and x is an integer as claimed.

Problem 2. Find infinitely many pairs of integers x, y such that

$$x^2 - 19y^2 = 1.$$

Solution. Suppose we have one such pair x_0, y_0, $y_0 \neq 0$. We can assume x_0, y_0 are positive integers. Then

$$(x_0 + \sqrt{19}\, y_0)(x_0 - \sqrt{19}\, y_0) = 1 \quad \ldots (1)$$

Square

$$(x_0 + \sqrt{19}\, y_0)^2 (x_0 - \sqrt{19}\, y_0)^2 = 1,$$

that is

$$\left[(x_0^2 + 19y_0^2) + \sqrt{19}(2x_0y_0)\right]\left[(x_0^2 + 19y_0^2) - \sqrt{19}(2x_0y_0)\right] = 1$$

So $(x_1 = x_0^2 + 19y_0^2,\ y_1 = 2x_0y_0)$ gives another solution and $x_1 > x_0$, $y_1 > y_0$.

Repeating the argument in (1) with x_0, y_0 replaced by x_1, y_1, we get another solution (x_2, y_2) with $x_2 > x_1$, $y_2 > y_1$.

So if we have one non-trivial solution, this process shows that there are infinitely many. But how does one obtain one to begin with.

The Diophantine equation

$$x^2 - ny^2 = 1$$

where n is a square-free positive integer and we seek positive integer solutions x, y is called Pell's equation. Pell was a 17th century English mathematician but it was a colleague of his ~~from~~ Cork, Lord Brouncker, who was an expert on it.

Earlier it was studied in India (around 700 AD) and in France by Fermat. Euler found a complete solution.

One can try finding one solution by trial and error. However, even for fairly small n, if x_0, y_0 is a solution with $y_0 > 0$ smallest possible, y_0 can be much larger than n.

For $n = 19$, $y_0 = 39$ and $x_0 = 170$.

Euler proved that infinitely many solutions always exist and presented an algorithm to find them.

Examples. ① $x^2 - 11y^2 = 1$.

One sees that $10^2 - 11 \cdot 3^2 = 1$. One can take $x_0 = 10$, $y_0 = 3$.

② $x^2 - 17y^2 = 1$.

Observe that $4^2 - 17 \cdot 1^2 = -1$, that is

$$(4 + \sqrt{17})(4 - \sqrt{17}) = -1$$

Square:

$$(4 + \sqrt{17})^2 (4 - \sqrt{17})^2 = 1 \quad \text{that is}$$

$$(33 + 8\sqrt{17})(33 - 8\sqrt{17}) = 1, \quad \text{so}$$

$$33^2 - 17 \cdot 8^2 = 1.$$

So $(33, 8)$ is a solution.

Suppose x, y are positive integers with

$$x^2 - ny^2 = 1$$

When x, y are large, we see that

$\frac{x}{y}$ is a good approximation to $\sqrt{n}$.

This fact is the intuition behind Euler's algorithm.

A brief description of the algorithm [Alg 1]

Example 1 $x^2 - 11y^2 = 1$.

$\sqrt{11}$ is $3 + t$, where $0 < t < 1$. Write

$\sqrt{11} = \boxed{3} + (\sqrt{11} - 3)$, $\frac{1}{\sqrt{11} - 3} = \frac{\sqrt{11} + 3}{(\sqrt{11}-3)(\sqrt{11}+3)}$

$= \frac{\sqrt{11} + 3}{2}$. Now $\frac{\sqrt{11}+3}{2} = 3 + t'$ where $0 < t' < 1$.

Write $\frac{\sqrt{11}+3}{2} = \boxed{3} + \frac{\sqrt{11} - 3}{2}$. Next $\frac{2}{\sqrt{11}-3} =$

$\frac{2(\sqrt{11}+3)}{(\sqrt{11}-3)(\sqrt{11}+3)} = \sqrt{11} + 3$ and $\sqrt{11} + 3 = \boxed{6} + t''$

with $0 < t'' < 1$. Observe that $\boxed{6}$ is twice the starting number $[3]$. Stop and write down the previous boxed number as they arose. They are $\boxed{3}$, $\boxed{3}$. Form $3 + \frac{1}{3} = \frac{10}{3}$.

Observe that $10^2 - 3^2 \cdot 11 = 1$.

Example 2 $x^2 - 7y^2 = 1$

$\sqrt{7} = [2] + (\sqrt{7} - 2)$, $\frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{(\sqrt{7}-2)(\sqrt{7}+2)} = \frac{\sqrt{7}+2}{3}$,

$\frac{\sqrt{7}+2}{3} = \boxed{1} + \frac{\sqrt{7}-1}{3}$, $\frac{3}{\sqrt{7}-1} = \frac{3(\sqrt{7}+1)}{(\sqrt{7}-1)(\sqrt{7}+1)}$

$= \frac{3(\sqrt{7}+1)}{6} = \frac{\sqrt{7}+1}{2}$, $\frac{\sqrt{7}+1}{2} = \boxed{1} + \frac{\sqrt{7}-1}{2}$,

$\frac{2}{\sqrt{7}-1} = \frac{2(\sqrt{7}+1)}{(\sqrt{7}-1)(\sqrt{7}+1)} = \frac{\sqrt{7}+1}{3}$, $\frac{\sqrt{7}+1}{3} = [1] + \frac{\sqrt{7}-2}{3}$,

$\frac{3}{\sqrt{7}-2} = \frac{3(\sqrt{7}+2)}{(\sqrt{7}-2)(\sqrt{7}+2)} = \sqrt{7}+2$, $\sqrt{7}+2 = [4] + \sqrt{7}-2$

The $[4]$ is twice the initial number $[2]$.

The list of boxed numbers before [4] is

[2], [1], [1], [1] [Alg 2]

Form $[2]+\cfrac{1}{[1]+\cfrac{1}{[1]+\cfrac{1}{[1]}}}$. This fraction

equals $2+\frac{1}{3/2}=\frac{8}{3}$.

Now $8^2-3^2\cdot 7=1$.

Example 3. $x^2-37y^2=1$.

$\sqrt{37}=6+t$, with $0<t<1$. Now

$\sqrt{37}=[6]+(\sqrt{37}-6)$, $\frac{1}{\sqrt{37}-6}=\frac{\sqrt{37}+6}{(\sqrt{37}-6)(\sqrt{37}+6)}$

$=\frac{\sqrt{37}+6}{(1)}=\sqrt{37}+6=[12]+(\sqrt{37}-6)$.

Since [12] is twice [6], stop. Sequence of boxed numbers before [12] is just [6].

Now $6=\frac{6}{1}$ and $6^2-1^2\cdot 37=-1$.

Then $(6+\sqrt{37})(6-\sqrt{37})=-1$ and thus

$(6+\sqrt{37})^2(6-\sqrt{37})^2=1$. Thus

$$(73+12\sqrt{37})(73-12\sqrt{37})=1$$

and $$73^2-12^2\cdot 37=1.$$

Example 4. $x^2-19y^2=1$.

$\sqrt{19}=[4]+(\sqrt{19}-4)$, $\frac{1}{\sqrt{19}-4}=\frac{\sqrt{19}+4}{3}$, $\frac{\sqrt{19}+4}{3}=[2]+\frac{\sqrt{19}-2}{3}$,

$\frac{3}{\sqrt{19}-2}=\frac{3(\sqrt{19}+2)}{15}=\frac{\sqrt{19}+2}{5}=[1]+\frac{\sqrt{19}-3}{5}$ $\frac{5}{\sqrt{19}-3}=\frac{5(\sqrt{19}+3)}{10}=\frac{\sqrt{19}+3}{2}$,

$\frac{\sqrt{19}+3}{2}=[3]+\frac{\sqrt{19}-3}{2}$, $\frac{2}{\sqrt{19}-3}=\frac{2(\sqrt{19}+3)}{10}=\frac{\sqrt{19}+3}{5}=[1]+\frac{\sqrt{19}-2}{5}$,

$\frac{5}{\sqrt{19}-2}=\frac{5(\sqrt{19}+2)}{15}=\frac{\sqrt{19}+2}{3}=[2]+\frac{\sqrt{19}-4}{3}$ $\frac{3}{\sqrt{19}-4}=\frac{3(\sqrt{19}+4)}{3}=[8]+\cdots$

Sequence of boxed numbers: [4], [2], [1], [3], [1], [2] and fraction is $170/39$, so $170^2-39^2\cdot 19=1$.

Problem 3. Let a, b be positive integers such that $1+ab$ divides a^2+b^2. Prove that $\frac{a^2+b^2}{1+ab}$ is the square of an integer.

Solution: Suppose that the result fails and let (a,b) be a counterexample. Let $k = \frac{a^2+b^2}{1+ab}$, so k is a positive integer but k is not a perfect square. Hence $k \geq 2$.

We have $a^2+b^2 = k(1+ab)$ or equivalently

$$a^2 - kab + b^2 = k \quad \cdots (1)$$

We now fix on k and among all pairs of positive integers a, b satisfying (1), assume that b is smallest possible. Since we could swap a and b while keeping (1) true, we must have $a \geq b$. But if $a = b$, then (1) says $2b^2 = k(b^2+1)$ and this is impossible, since $k \geq 2$. Hence

$$a > b \quad \cdots (2).$$

Consider the quadratic equation

$$x^2 - kbx + b^2 - k = 0$$

We know that $x = a$ is one root

If $x = a'$ is the second root,
then (i) $a + a' = kb$ and
(ii) $aa' = b^2 - k$.

Now (i) implies that a' is an integer.

Now $a^2 + b^2 = k(1 + ab)$, so if $k > b^2$,
$a^2 > ab^2$ and $a(a - kb) = k - b^2$ implies
$a > kb$, and $k - b^2 \geq a$ and $k \geq a + b^2$.
But then $\frac{a^2 + b^2}{1 + ab} = k \geq a + b^2$ implies

$$a^2 + b^2 \geq a \cdot (1 + ab) + b^2(1 + ab)$$
$$> a^2 + b^2$$

which is impossible. Hence $k \leq b^2$
and thus $k < b^2$, since k is not a
perfect square. Hence, $b^2 - k > 0$
and $a' > 0$ by (ii) above.

Also $aa' = b^2 - k < b^2$ and $a > b$
implies $a' < b$. But a' is a positive
integer and
$$a'^2 - ka'b + b^2 = k$$
so (a', b) satisfies (i) and contradicts
the minimal property of b. This contradiction
implies the desired result.

Problem 4. A pair (x, y) is called primitive if x, y are integers with $\gcd(x, y) = 1$. Given a finite set S of primitive pairs, prove that there exists a positive integer n and integers $a_0, a_1, \cdots, a_n$ such that if

$$g(x, y) = a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \cdots + a_n y^n,$$

then $g(x_i, y_i) = 1$ for all pairs $(x_i, y_i) \in S$.

Solution. We attempt a solution based on induction on the number of elements in S, so we first consider the case where S has just one element. Say $S = \{(x_1, y_1)\}$. We are given that $\gcd(x_1, y_1) = 1$.

We need Bézout's Theorem: Suppose that a, b are integers not both zero and $d = \gcd(a, b)$, then there exist integers x, y such that $ax + by = d$.

For (x_1, y_1), this means that there exist integers a, b with

$$ax_1 + by_1 = 1$$

since $d = \gcd(x_1, y_1) = 1$.

So if we take

$$g(x, y) = ax + by,$$

(so $n = 1$, $a_0 = a$, $a_1 = b$)

the problem is solved in this case.

Suppose that S is a set with $m+1$ elements, for some positive integer m,

$$S = \{(x_1, y_1), \cdots, (x_{m+1}, y_{m+1})\}$$

and that the result holds for sets of primitive pairs containing at most m elements. Since we have proven the result for sets of one element, this is a basis for an inductive proof.

Let $S_0 = \{(x_1, y_1), \cdots, (x_m, y_m)\}$.

We know that the result holds for S_0.

So there is a polynomial

$$g_0(x,y) = b_0 x^q + b_1 x^{q-1} y + \cdots + b_q y^q$$

where q is a positive integer and

$b_0, b_1, \cdots, b_q$ are integers, such that

$$g_0(x_i, y_i) = 1, \text{ for } i = 1, 2, \cdots, m.$$

We now must try to concoct a polynomial $g(x,y)$ having the same property as $g_0(x,y)$ and, in addition, $g(x_{m+1}, y_{m+1}) = 1$.

Notice that powers of $g_0(x,y)$ also have the value 1 when (x,y) is replaced by (x_i, y_i), $i = 1, 2, \cdots, m$; $g_0(x_i, y_i)^k = 1$.

Observe also that the polynomial $x y_i - y x_i$ is zero when $(x,y) = (x_i, y_i)$.

So adding $h(x,y)(xy_1 - yx_1)(xy_2 - yx_2)\cdots(xy_m - yx_m)$ to $g_0(x,y)^k$ for any polynomial $h(x,y)$ with integer coefficients gives a polynomial in variables x, y which has the value 1 for $(x,y) = (x_i, y_i)$, $i = 1, \cdots, m$.

This suggests we try

$$g(x,y) = g_0(x,y)^k + C(ux+vy)^K \prod_{i=1}^{m}(xy_i - yx_i)$$

where $K+m = kq$, where q is the degree of $g_0(x,y)$ and u, v integers satisfying $ux_{m+1} + vy_{m+1} = 1$, k is a positive integer and C an integer to be chosen.

Observe that $g(x_i, y_i) = 1$ for $i = 1, 2, \cdots, m$.

Note that $g(x,y)$ is a homogeneous polynomial of degree kq with integer coefficients. Also $g(x_i, y_i) = 1$, for $i = 1, 2, \cdots, m$.

Substituting $x = x_{m+1}$, $y = y_{m+1}$ into $g(x,y)$ yields

$$g(x_{m+1}, y_{m+1}) = g_0(x_{m+1}, y_{m+1})^k + \cdots$$

$$+ C \prod_{i=1}^{m}(x_{m+1}y_i - x_i y_{m+1})$$

If we knew that $\prod_{i=1}^{m} (x_{m+1} y_i - y_{m+1} x_i)$ and $g_0(x_{m+1}, y_{m+1})$ are coprime (that is, their gcd $= 1$), there is at least a possibility that we could find appropriate k and C to make $g(x_{m+1}, y_{m+1}) = 1$. But unfortunately it is not clear that gcd $= 1$ is achievable. So we need a better strategy. Notice though that if $x_{m+1} = 1$ and $y_{m+1} = 0$, we can finish the proof. To see this, put $u = 1$, $v = 0$. Suppose some $x_i = -1$ and $y_i = 0$, for $1 \le i \le n$. Then $1 = g_0(x_i, y_i) = b_0 x_i^q + b_1 x_i^{q-1} y_i + \cdots + b_q y_i^q$

$$= b_0 (-1)^n.$$

So $b_0 = \pm 1$ and $b_0^2 = 1$. Also

$$g_0^2(x_j, y_j) = \left(g_0(x_j, y_j)\right)^2 = 1^2 = 1$$

for $j = 1, 2, \ldots, m$ and

$$g_0^2(x_{m+1}, y_{m+1}) = \left(g_0(1, 0)\right)^2 = b_0^2 = 1$$

so taking $k=2$, $C=0$, the result [15
holds in this case. Now if any y_j
$(1 \le j \le m)$ is 0, the corresponding
$x_j = \pm 1$, since $\gcd(x_j, y_j) = 1$ and
we are back to the case just treated.
So we can assume $y_1 \neq 0$ for $j = 1, 2, \cdots, m$.
Now with $x_{m+1} = 1, y_{m+1} = 0$, we obtain

$$g(1,0) = g_0(1,0)^k + C \prod_{i=1}^{m} y_i$$
$$= b_0^{qk} + C \prod_{i=1}^{m} y_i .$$

Suppose $\gcd\left(b_0^{qk}, \prod_{i=1}^{m} y_i\right) \neq 1$; then
there is a prime p such that p divides
b_0 and p divides y_l for some l
with $1 \le l \le m$. [This uses the property
that if a prime divides the product
of two integers, then it must divide at
least one of them.)
But now consider $g_0(x_l, y_l) =$

$$b_0 x_l^q + b_1 x_l^{q-1} y_l + \cdots + b_q y_l^q .$$

Since p divides y_l and p divides b_0,
this forces p to divide $g_0(x_l, y_l)$

Contrary to the induction hypotheses.
This contradiction forces

$$\gcd\left(b_0^{lk}, \prod_{i=1}^{m} y_i\right) = 1.$$

In particular b_0^q and $\prod_{i=1}^{m} y_i$ are coprime. We use congruences mod P where $P = \prod_{i=1}^{m} y_i$. A result called the Euler-Fermat Theorem states that if r, s are integers with $\gcd(r, s) = 1$ and $s > 0$, then $r^{\phi(s)} \equiv 1 \bmod s$, where ϕ is Euler's totient function.

$\phi(s)$ is the number of integers t with $1 \le t \le s$ such that $\gcd(s, t) = 1$.

[If $p_1, p_2, \cdots, p_c$ are the distinct primes dividing s, then $\phi(s)$ is given by the formula

$$\phi(s) = s \prod_{i=1}^{c} \left(1 - \frac{1}{p_i}\right) \Big].$$

So there

$$(b_0^q)^{\phi(P)} \equiv 1 \mod P,$$

that is

$$(b_0^q)^{\phi(P)} = 1 + PL$$

for some integer L.

Now $g(1,0) = b_0^{qk} + C\prod_{i=1}^{m} y_i$

$$= b_0^{qk} + CP,$$

so we take $k = \phi(P)$ and $C = -L$ to get $g(1,0) = 1$. Then $g(x,y)$ satisfies all the conditions

$$g(x_i, y_i) = 1 \text{ for } i = 1, 2, \cdots, m,$$

and also for $i = m+1$, since $(x_{m+1}, y_{m+1}) = (1, 0)$.

The question remaining is: How do we deal with the cases where $(x_{m+1}, y_{m+1}) \neq (1, 0)$. For this, one requires a little knowledge of matrix theory.

The idea is to [illegible] to $(1, 0)$, solve it as we have done, and then transform it back to (x_{m+1}, y_{m+1}). By 'transform' here, we mean a linear transformation using a 2×2 matrix.

By Bézout, we know that since $\gcd(x_{m+1}, y_{m+1}) = 1$, there are integers u, v with $ux_{m+1} + vy_{m+1} = 1$.

Let $M = \begin{pmatrix} u & v \\ -y_{m+1} & x_{m+1} \end{pmatrix}$. Observe that

$$M \begin{pmatrix} x_{m+1} \\ y_{m+1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

We multiply all the given (x_i, y_i) in S_0 by M as follows.

Write $M \begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} x_i' \\ y_i' \end{pmatrix} \quad (i = 1, 2, \cdots, m)$

and let S_0' be the set of all (x_i', y_i') $i = 1, 2, \cdots, m$. [We do not need to know x_i', y_i' explicitly, (but $x_i' = ux_i + vy_i$, $y_i' = -y_{m+1}x_i + x_{m+1}y_i$)]. It is clear that all the x_i' and y_i' are integers but we also need $\gcd(x_i', y_i') = 1$

in order to apply the argument used on S_0.

The key result we need is that [1]

the determinant of M is 1.

The determinant of a 2×2 matrix $N = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ is $d = a_{11}a_{22} - a_{12}a_{21}$ and, if $d \neq 0$, its inverse N^{-1} is $\begin{pmatrix} a_{22}/d & -a_{12}/d \\ -a_{21}/d & a_{11}/d \end{pmatrix}$

Notice by direct multiplication that $NN^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = N^{-1}N$ for these two matrices. Notice also that when $d = 1$, the matrix N has integer entries if and only if the matrix N^{-1} has also.

Suppose for the sake of contradiction that

$\gcd(x_i', y_i') = z > 1$ for some i

Since $ux_{m+1} + vy_{m+1} = 1$ and

$M = \begin{pmatrix} u & v \\ -y_{m+1} & x_{m+1} \end{pmatrix}$, $\det M = 1$.

Now

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = M^{-1}M \begin{pmatrix} x_i \\ y_i \end{pmatrix} = M^{-1} \begin{pmatrix} x_i' \\ y_i' \end{pmatrix}$$

$$= M^{-1} \begin{pmatrix} z x_i'' \\ z y_i'' \end{pmatrix}, \text{ where } x_i' = z x_i'', \; y_i' = z y_i''$$

and x_i'', y_i'' are integers

and $M^{-1}\begin{pmatrix} x_i'' \\ y_i'' \end{pmatrix} = \begin{pmatrix} x_i''' \\ y_i''' \end{pmatrix}$, where x_i''', y_i''' [20

are integers, since M^{-1} has integer entries. But then $\begin{pmatrix} x_i \\ y_i \end{pmatrix} = z\begin{pmatrix} x_i''' \\ y_i''' \end{pmatrix}$

and $\gcd(x_i, y_i) \neq 1$, since $z > 1$.

This contradiction shows that $\gcd(x_i', y_i') = 1$ for $i = 1, 2, \cdots, m$.

Now perform the previous argument to find $g(x,y)$ for $S' = \{(1,0)\} \cup S_0$ and then in $g(x,y)$ replace x, y by (X, Y) where $\begin{pmatrix} X \\ Y \end{pmatrix} = M^{-1}\begin{pmatrix} x \\ y \end{pmatrix}$. Let $G(x,y)$ be the function obtained.

Note that $M^{-1} = \begin{pmatrix} x_{m+1} & -v \\ y_{m+1} & u \end{pmatrix}$, so

G is also a homogeneous polynomial in x, y with integer coefficients and

$G(x_i, y_i) = 1$ for $i = 1, 2, \cdots, m+1$.

Hence the statement holds for sets with $m+1$ primitive pairs and the statement of the problem is established by induction.