PROBABILITY AND PELL'S EQUATION

By

John E. Sasser, Ph.D.

This article involves the probability of determining the number of objects in a set containing two different types in order to obtain all possible solutions for a given probability when randomly selecting two like objects. It's solution has important application in the sciences. One example in the biological sciences would be those questions concerned with the mechanism of inheritance.

For brevity we will state this problem in terms of a box containing two types objects, red and black, and call it the "Two-Objects Problem".

Statement of the Problem

A box contains red (x) and black (y) objects. When two objects are drawn at random, the probability that both are red is p. What are all possible solutions?

Our problem of determining all possible numbers of objects in a set containing two different types for a given probability (p) when randomly selecting two like objects, can be answered by finding all solutions to the following equation:

$$\frac{x}{x+y} \bullet \frac{x-1}{x+y-1} = p \qquad (1)$$

(x = number of reds & y = number of blacks)

Let a = x and t = x + y (total objects in set)

Our equation is: $\frac{a}{t} \bullet \frac{a-1}{t-1} = p$. This implies $p(t^2 - t) = a(a-1)$. Let $k = a(a-1)$. So,

$$p(t^2 - t) - k = 0$$

$$t^2 - t - \frac{k}{p} = 0 \qquad (2)$$

$$\Rightarrow \quad \mathbf{t = \frac{1}{2} + \frac{1}{2}\sqrt{1+\frac{4k}{p}}}$$

For the total (t) to be an integer:

$$\mathbf{\frac{1}{2}\sqrt{1+\frac{4k}{p}} \in \left\{\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \ldots\right\}}$$

$$\Rightarrow \mathbf{\sqrt{1+\frac{4k}{p}} \in \{1,3,5,\ldots\} = m} \qquad \mathbf{(3)}$$

From Equation (3) let the smallest m that works be m_1.

$\mathbf{m \geq m_1}$. So,

$$\mathbf{\sqrt{1+\frac{4k}{p}} = m_1} \qquad \mathbf{(4)}$$

We have let $\mathbf{k = a(a-1)}$, so: $\mathbf{k = a^2 - a} \;\Rightarrow\; \mathbf{a^2 - a - k = 0}$ **(5)**

$$\Rightarrow \mathbf{\frac{1}{2}a^2 - \frac{1}{2}a - \frac{k}{2} = 0} \qquad \mathbf{(6)}$$

We know, $\mathbf{\sqrt{1+\frac{4k}{p}} = m_1}$

$$\Rightarrow \mathbf{k = \frac{p(m_1^2 - 1)}{4}}$$

Divide k by 2: $\mathbf{\frac{k}{2} = \frac{p(m_1^2 - 1)}{8}}$

So, Equation (6) gives:

$$\mathbf{\frac{1}{2}a^2 - \frac{1}{2}a - \frac{p(m_1^2 - 1)}{8} = 0}$$

$$\mathbf{4a^2 - 4a - pm_1^2 + p = 0}$$

$$\mathbf{(2a-1)^2 - 1 - pm_1^2 + p = 0}$$

$$\mathbf{(2a-1)^2 - pm_1^2 = 1 - p}$$

Let y = 2a - 1

$$\boxed{pm_1^2 - y^2 = p - 1} \qquad \textbf{(7)}$$

We will call equation (7) the ***general equation for the two-objects problem*** .

Now in our example, p=.5:

$$\frac{1}{2}m_1^2 - y^2 = \frac{1}{2} - 1$$

$$\Rightarrow m^2 - 2y^2 = -1 \qquad \textbf{(8)}$$

Whatever the value of p, we will always get the general equation:

$$m^2 - Ny^2 = C \qquad \textbf{(9)}$$

Our example of determining all possible numbers of objects in a set containing two different types for a given probability of 0.5, when randomly selecting two like objects, can be answered by substituting the value of p in the general equation for the two-objects problem and solving the resulting equation (8).

Theorem: (m,y) is a solution for:

$$m^2 - 2y^2 = -1 \text{ with } y > 0 \text{ iff } m + y\sqrt{2} = (1+\sqrt{2})^n,\ n \in N$$

Moreover, y is odd ⇔ n is odd. In general: To make y odd ⇔ $Z = Z_i^n$, n is odd.

Proof:

$F = Q(\sqrt{2})$

Let $Z = m + y\sqrt{2}$

then $Z \in F$ and $\overline{Z} = m - y\sqrt{2}$

$(m - \sqrt{2}y)(m + \sqrt{2}y) = -1$, becomes $Z \bullet \bar{Z} = -1$

If $Z = m + y\sqrt{2}$ satisfies $Z \bullet \overline{Z} = -1$, then Z must be a power of

$Z_1 = -1 + \sqrt{2}$ times ± 1.

$$m^2 - 2y^2 = -1$$
$$\left(m - y\sqrt{2}\right)\left(m + y\sqrt{2}\right) = -1$$

$$
\begin{aligned}
Z_1 &= Z^1 = \left(1+\sqrt{2}\right)^1 &&= 1 + 1\sqrt{2}\\
Z_2 &= Z^2 = \left(1+\sqrt{2}\right)^2 &&= 3 + 2\sqrt{2}\\
Z_3 &= Z^3 = \left(3+2\sqrt{2}\right)\left(1+\sqrt{2}\right) &&= 7 + 5\sqrt{2}\\
Z_4 &= Z^4 = \left(7+5\sqrt{2}\right)\left(1+\sqrt{2}\right) &&= 17 + 12\sqrt{2}\\
Z_5 &= Z^5 = \left(17+12\sqrt{2}\right)\left(1+\sqrt{2}\right) &&= 41 + 29\sqrt{2}\\
Z_7 &= Z^7 = Z^5 \bullet Z^2 &&= 239 + 169\sqrt{2}\\
Z_9 &= Z^9 = Z^5 \bullet Z^4 &&= 1393 + 985\sqrt{2}\\
Z_{11} &= Z^{11} = Z^9 \bullet Z^2 &&= 8119 + 5741\sqrt{2}\\
&\quad . &&\qquad\qquad .\\
Z_i &= &&= \alpha + \beta\sqrt{2}
\end{aligned}
$$

In general, (m,y) is a solution for $m^2 - 2y^2 = -1$ **with** $y > 0$

iff, $m+y\sqrt{2}=\left(1+\sqrt{2}\right)^n$, **n an integer**. Moreover, y is odd ⇔ n is odd.

This represents ALL solutions to our equation, as illustrated below:

In our equation **(7)**: $y = 2a-1$, so:

- For, $Z_1 = Z^1 = (1+1\sqrt{2})^1 = 1+1\sqrt{2}$

$\Rightarrow m = 1, y = 1 \Rightarrow 2a-1=1 \Rightarrow \boxed{a=1}$

From equation (1), when p = .5, we get:

$$x^2 - x - y^2 + y - 2xy = 0 \tag{10}$$

so,

$$(1)^2 - (1) - y^2 + y - 2(1)y = 0$$
$$y^2 + y = 0$$
$$\Rightarrow y(y+1) = 0$$
$$\Rightarrow \boxed{y=-1}$$

and a negative will not work. Reds must be at least two, and blacks at least one.)

- For, $\mathbf{Z_3 = Z^3 = \left(3+2\sqrt{2}\right)\left(1+\sqrt{2}\right) = 7+5\sqrt{2}}$

y = 2a -1 = 5 ⇒ **a = 3**

so, using equation (10): $(3)^2 - (3) - y^2 + y - 2(3)y = 0$

⇒ $y^2 + 5y - 6 = 0$

⇒ **y =1** **So, (3 red, 1 black) = 4 is the smallest possible number of objects we can have.**

- For, $\mathbf{Z_5 = Z^5 = \left(17+12\sqrt{2}\right)\left(1+\sqrt{2}\right) = 41+29\sqrt{2}}$

y = 2a-1 - 29 ⇒ **a=15**

so, $(15)^2 - (15) - y^2 + y - 2(15)y = 0$

⇒ $y^2 + 29y - 210 = 0$

⇒ **y=6** **So, (15 red, 6 black)**

- For, $\mathbf{Z_7 = Z^7 = \qquad = 239+169\sqrt{2}}$

y = 2a - 1 = 169 ⇒ **a=85**

so, $(85)^2 - (85) - y^2 + y - 2(85)y = 0$

⇒ $y^2 = 169y - 7140 = 0$

⇒ **y=35** **Thus, we have (85,35).**

- For, $\mathbf{Z_9 = Z^9 = \qquad = 1393+985\sqrt{2}}$

y = 2a - 1 = 985 ⇒ **a=493**

$(493)^2 - (493) - y^2 + y - 2(493)y = 0$

⇒ $y^2 + 985y - 242556 = 0$

$(y-204)(y+1189) = 0$

⇒ **y=204** **Thus, the next solution (493,204).**

Since the coefficients in the quadratic equation solving for y become increasingly larger, we find an easy way to calculate y:

Z_i						$a=x$	y
Z_3	=	Z^3	=	$(3+2\sqrt{2})(1+\sqrt{2})$	=	$7+5\sqrt{2}$	3	1
Z_5	=	Z^5	=	$(3+2\sqrt{2})(1+\sqrt{2})$	=	$41+29$	15	6
Z_7	=	Z^7	=		=	$239+169\sqrt{2}$	85	35
Z_9	=	Z^9	=		=	$1393+985\sqrt{2}$	493	204
Z_{11}	=	Z^{11}	=	$Z^9 \bullet Z^2$		$8119+5741\sqrt{2}$		
						$2a-1 \Rightarrow 5741 \Rightarrow a =$	2871	
•							•	
$Z_i=Z^i$		$Z^{i-2} \bullet Z^2$	=		=	$\alpha + \beta\sqrt{2}$	a_i	$\frac{(a_i - a_{i-1})}{2}$
Z_{11}		For example,	=		=	$\frac{(2871-493)}{2}$		1189

Equation (7) is a diophantine equation. There are few theorems that apply to a wide class of these equations. Special equations are attacked with special methods, and what works for one will generally not work for another.

Notice that for certain equations there are no solutions. For example, the Two-Objects problem for **p= 1/4** results in the equation:

$$4y^2 - m^2 = 3$$

$$\Rightarrow \quad y^2 = \sqrt{\frac{m^2+3}{4}}$$

$$\Rightarrow \quad y = \frac{1}{4}(m^2+3))$$

where y must equal some positive integer squared, say n:

$$y = \frac{1}{4}(m^2+3) = n^2$$

$$\Rightarrow m^2 + 3 = 4n^2 = (2n)^2$$

$$\Rightarrow \ (2n)^2 - (m)^2 = 3$$

which is impossible for n,m э J.