Homework

(1) Solve the diophantine equation $x^2 + 2y^2 = z^2$

(a) à la Diophantus:
Dividing through by z^2 and putting $X = x/z$, $Y = y/z$ we have to solve $X^2+2Y^2 = 1$. Substitute $X = 1-Y$; then $1-2Y+Y^2+2Y^2 = 1$, hence $Y(3Y-2) = 0$, or $Y = \frac{2}{3}$ and $X = 1-Y = \frac{1}{3}$. This gives $(1, 2, 3)$ as a solution of the original equation.
Since Diophantus did not have a symbol for more than one unknown, his problem would have been "the sum of a square and twice another square is 1"; he would have proceeded by calling the second square y (actually he would have used his own symbol for the unknown), and then saying 'let the first square be $(1 - 2y)$'.

Many of you just substituted $Y = 2X$ without explaining why. Actually, all you have done is guess a solution: the general $Y = kX$ leads to $X^2(1 + 2k^2) = Z^2$, so you have to solve $1 + 2k^2 = Z^2$, which is essentially the original equation with $x = 1$.
The substitutions of Diophantus, on the other hand, are made in such a way that they simplify the resulting equation because cancellations occur. For example, he would take $z = 4$ as an example and then write $x = 4 + ky$ e.g. with $k = -1$, because then the constant terms cancel: $4^2 = x^2 + 2y^2 = 4^2 - 8y + y^2 + 2y^2 = 4^2 - 8y + 3y^2$. Cancelling 4^2 and then y gives $y = \frac{8}{3}$ and $x = 4 - y = \frac{4}{3}$.
Another remark: square roots in the solution are, of course, not allowed, since solving diophantine equations over the reals is no problem at all. Your solutions have to be *rational*!

(b) using modern notation:
Here we can substitute $X = 1 + kY$ and get $Y[(k^2 + 2)Y + 2k] = 0$, hence $Y = -\frac{2k}{2+k^2}$ and $X = 1 + kY = \frac{2-k^2}{2+k^2}$ are solutions for every $k \in \mathbb{Q}$.

(c) using the geometric technique of sweeping lines:
Consider the ellipse $X^2 + 2Y^2 = 1$, and take the point $P(1, 0)$. The lines through this point have the form $Y = t(X - 1)$ (except for the vertical line, which intersects the curve in $(-1, 0)$). Intersecting it with the ellipse gives $X^2 - 1 + 2t^2(X - 1)^2 = 0$, and factoring out $X - 1$ shows $(X - 1)(X + 1 + 2t^2(X - 1)) = 0$. The first factor gives the known point P, the second one gives $X = \frac{2t^2-1}{2t^2+1}$ and then $Y = \frac{-2t}{2t^2+1}$.
If we substitute $k = \frac{1}{t}$, then the solution becomes $X = \frac{2-k^2}{2+k^2}$ and $Y = \frac{-2k}{2+k^2}$.
Remark: observe that you know in advance that you can factor out $(X - 1)$ since all the lines go through $(1, 0)$.

In next semester's course in algebraic geometry we will discuss this technique in detail.

(2) Solve the system of equations $x + a = u^2$, $x + b = v^2$, where a and b are given rational numbers.

Hint: subtract the two equations, find all rational points on this curve, and then determine x.

We find $a - b = u^2 - v^2 = (u - v)(u + v)$. Substitute $u - v = t$; then $u + v = \frac{a-b}{t}$, hence $2u = t + \frac{a-b}{t}$. Thus $u = \frac{t^2+a-b}{2t}$ and $v = \frac{a-b-t^2}{2t}$ gives all rational solutions.

(3) List all the element of the symmetry group of a square. Construct a multiplication table for this group. List all possible subgroups.

The group D_4 has five elements of order 2: the four reflections about symmetry axes and the rotation about 180^o. These elements generate five groups of order 2.

The groups of order 4 are either cyclic generated by one of the elements of order 4, namely the rotation R about 90^o, or they are generated by elements of order 2. There are exactly two such groups, namely $\{\text{id}, R^2, S, R^2S\}$ and $\{\text{id}, R^2, RS, R^3S\}$, where S denotes an arbitrary reflection. Note that $RS = SR^{-1}$, hence $(RS)^2 = \text{id}$.

Finally, there are the trivial subgroups $\{\text{id}\}$ and D_4.