Elliptic Curves. Solutions to Sheet 0.

1.
(a). There is an identity element $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, but the matrix $\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$, for example, does not have an inverse, since there does not exist a matrix A such that $A\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)A = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$; so, not a group.
(b). This is group, with identity $\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$. Closure and associativity are easy to show. The inverse of $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ is $\left(\begin{smallmatrix}-a&-b\\-c&-d\end{smallmatrix}\right)$.

2.
(a). Not a homomorphism since, for example, $\phi(1+3) = \phi(4) = 17$, but $\phi(1) \times \phi(3) = 2 \times 10 = 20$.
(b). This is a homomorphism since, for all $v, w \in \mathbb{Q}$, we have $\phi(v+w) = \sqrt{2}(v+w) = \sqrt{2}\,v + \sqrt{2}\,w = \phi(v) + \phi(w)$. The map is injective since, for all $v, w \in \mathbb{Q}$, if $\phi(v) = \phi(w)$, then $\sqrt{2}\,v = \sqrt{2}\,w$, and so $v = w$. The map is not surjective since, for example, 2 is not in the image of ϕ (since there is no $v \in \mathbb{Q}$ such that $\sqrt{2}\,v = 2$). Hence the map is not bijective. Finally, $v \in \ker\phi \iff \sqrt{2}\,v = 0 \iff v = 0$, and so $\ker\phi = \{0\}$.
(c). This is a homomorphism since, for all $v, w \in \mathbb{Z}$, we have $\phi(v+w) = 2(v+w) = 2v + 2w = \phi(v) + \phi(w)$. The map is not injective since, for example, the elements 0 and 3 (which are distinct in $\mathbb{Z}$) both map to 0 in $\mathbb{Z}/3\mathbb{Z}$; therefore the map is also not bijective. The map is surjective since $0 \mapsto 0$, $1 \mapsto 2$ and $2 \mapsto 1$ so that all three elements of $\mathbb{Z}/3\mathbb{Z}$ are in the image of ϕ. Finally, $v \in \ker\phi \iff 2v = 0$ in $\mathbb{Z}/3\mathbb{Z} \iff 3|2v \iff 3|v$ in $\mathbb{Z}$. Hence the kernel of ϕ is $\{\ldots -3, 0, 3 \ldots\} = 3\mathbb{Z}$.

3.
(a). $3 = (1/27) \times 81$ and $81 = 9^2 \in (\mathbb{Q}^*)^2$, so $3 = 1/27$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. $-4 = 4 \times (-1)$ and $-1 \notin (\mathbb{Q}^*)^2$, so $-4 \neq 4$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Finally, $3 = (5/6) \times (18/5)$, and $18/5 \notin (\mathbb{Q}^*)^2$, so $3 \neq 5/6$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.
(b). In $\mathbb{Q}^*/(\mathbb{Q}^*)^2$: $-2/27 = (-2/27) \times 9^2 = -6$, $16 = 16 \times (1/4)^2 = 1$, $12 = 12 \times (1/2)^2 = 3$, and $1/3 = (1/3) \times 3^2 = 3$.
(c). In $\mathbb{Q}^*/(\mathbb{Q}^*)^2$: $6 \times 10 = 60 = 60 \times (1/2)^2 = 15$, $10/21 = (10/21) \times 21^2 = 210$, $15^{101} = 15 \times (15^{50})^2 = 15$, and $3^{-1} = 3^{-1} \times 3^2 = 3$.
(d). Whenever p_1, p_2 are distinct primes, we have that $p_1 = p_2 \times (p_1/p_2)$, where $p_1/p_2 \notin (\mathbb{Q}^*)^2$. Hence, $p_1 \neq p_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. This means that the primes are all distinct in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, and so $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is infinite (note that this does not describe all elements in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, but the above argument is sufficient to show that the size of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is infinite). In $\mathbb{R}^*/(\mathbb{R}^*)^2$, every $r > 0$ is equal to 1 (since such an r is a member of $(\mathbb{R}^*)^2$), and similarly any $r < 0$ is equal to -1. But $1 \neq -1$ in $\mathbb{R}^*/(\mathbb{R}^*)^2$, since $-1 \notin (\mathbb{R}^*)^2$. Hence, $\mathbb{R}^*/(\mathbb{R}^*)^2$ has exactly 2 distinct elements: 1 and -1. Finally, everything in $\mathbb{C}^*$ is in $(\mathbb{C}^*)^2$ (since every complex number is a square of some complex number), and so $\mathbb{C}^*/(\mathbb{C}^*)^2$ has exactly 1 element.

4.
(a). A singular point (x, y) must satisfy the three equations: $f(x,y) = x^4 + y^3 - 3x^2y = 0$, $g(x,y) = (\partial f/\partial X)(x,y) = 4x^3 - 6xy = 0$ and $h(x,y) = (\partial f/\partial Y)(x,y) = 3y^2 - 3x^2 = 0$.

From $h(x,y)=0$, we get $(y+x)(y-x)=0$ and so $y=x$ or $y=-x$, which we now consider as separate cases.

Case 1. $y=x$. In this case, $f(x,y)=0$ becomes $x^3(x-2)=0$ (with solutions $x=0,2$) and $g(x,y)=0$ becomes $2x^2(2x-3)=0$ (with solutions $x=0,3/2$), and so the only simultaneous solution for x is $x=0$. Substituting $x=0$ into $f(x,y)=0$ gives $y^3=0$ and so $y=0$. Hence, $(0,0)$ is the only possibility within case 1.

Case 2. $y=-x$. In this case, $f(x,y)=0$ becomes $x^3(x+2)=0$ (with solutions $x=0,-2$) and $g(x,y)=0$ becomes $2x^2(2x+3)=0$ (with solutions $x=0,-3/2$), and so the only simultaneous solution for x is $x=0$. As before, substituting $x=0$ into $f(x,y)=0$ gives $y^3=0$ and so $y=0$.

In either case, $(0,0)$ is the only possible point which could be singular.

[*Alternative Method (harder than the above, but guaranteed to work for any curve): Let* $\alpha(x)=Res(f,g)$ *with respect to* y, *and* $\beta(x)=Res(g,h)$ *with respect to* y, *and finally use resultants with respect to* x *to show that* $x=0$ *is the only common root of* $\alpha(x)$ *and* $\beta(x)$].

Finally, note that $(0,0)$ does indeed satisfy $f(x,y)=g(x,y)=h(x,y)=0$ and so is a singular point. Conclusion: $(0,0)$ is the only singular point.

$f(X+0,Y+0)=R_3(X,Y)+R_4(X,Y)$, where $R_3(X,Y)=Y^3-3X^2Y=Y(Y-\sqrt{3}\,X)(Y+\sqrt{3}\,X)$. So the three tangents at $(0,0)$ are $Y=0$, $Y=\sqrt{3}\,X$ and $Y=-\sqrt{3}\,X$.

(b). A singular point (x,y) must satisfy the three equations: $f(x,y)=y^2-x(x^2-1)^2=0$, $g(x,y)=(\partial f/\partial X)(x,y)=-(x^2-1)(5x^2-1)=0$ and $h(x,y)=(\partial f/\partial Y)(x,y)=2y=0$. From $h(x,y)=0$ we have $y=0$ and, on substituting this into $f(x,y)=0$ we have $-x(x^2-1)^2=0$, and so the only possible values for x are $x=0,1-1$. But from $g(x,y)=0$ we see that x must also satisfy $x=1-1,\sqrt{1/5},-\sqrt{1/5}$. The only common solutions are: $x=1,-1$. Substituting $x=1$ or $x=-1$ into $f(x,y)=0$ gives that $y=0$, and so the only possible points which could be singular are: $(1,0)$ and $(-1,0)$. Finally, note that $x=1,y=0$ does indeed satisfy $f(x,y)=g(x,y)=h(x,y)=0$ as does $x=-1,y=0$. Conclusion: $(1,0)$ and $(-1,0)$ are the only singular points.

At $(0,0)$, we have $f(X+0,Y+0)=-X+$ terms of degree at least 2, and so there is a unique tangent at the point $(0,0)$, namely the line $X=0$. At $(1,0)$, we note that $f(X+1,Y+0)=(Y^2-4X^2)+$ terms of degree at least 3. Here, $(Y^2-4X^2)=L_1(X,Y)L_2(X,Y)$, where $L_1(X,Y)=Y-2X$ amd $L_2(X,Y)=Y+2X$. Finally, the two tangents to $\mathcal{C}$ at $(1,0)$ are therefore $L_1(X-1,Y-0)=Y-2(X-1)=0$ and $L_2(X-1,Y-0)=Y+2(X-1)=0$.

5. If (x,y) is singular on $Y^2=X^3+AX+B$, then (x,y) satisfies the three equations: $f(x,y)=y^2-(x^3+Ax+B)=0$, $g(x,y)=(\partial f/\partial X)(x,y)=-(3x^2+A)=0$ and $h(x,y)=(\partial f/\partial Y)(x,y)=2y=0$. From $h(x,y)=0$, we have $y=0$; substituting $y=0$ into $f(x,y)=0$, we deduce $x^3+Ax+B=0$. From $g(x,y)=0$, we see that x also satisfies $3x^2+A=0$; that is, x is a common root of $p_1(x)=x^3+Ax+B$ and its derivative $p_2(x)=3x^2+A$; that is, x satisfies: $p_1(x)=x^3+Ax+B=0$ and $p_2(x)=3x^2+A=0$. Then x would satisfy: $p_3(x)=3p_1(x)-xp_2(x)=2Ax+3B=0$, and so: $p_4(x)=2Ap_2(x)-3xp_3(x)=-9Bx+2A^2$, and so: $p_5(x)=9Bp_3(x)+2Ap_4(x)=4A^3+27B^2=0$. But we are told that $4A^3+27B^2\neq 0$ and so no such x can exist; therefore there are no singular points. [The above is from first principles. An easier alternative method is to compute: Disc(x^3+Ax+B) is $4A^3+27B^2$; if this is nonzero, no such x can exist, and so no singular point can exist.]

6.

(a). Let $f(X,Y) = Y^2 - X^5$. Imagine that $f(X,Y) = g(X,Y)h(X,Y)$, where g, h are non-constant polynomials defined over $\mathbb{C}$. Since $f(X,Y)$ has degree 2 in Y, there are three possibilities: g has degree 0 in Y and h has degree 2 in Y; g has degree 1 in Y and h has degree 1 in Y; g has degree 2 in Y and h has degree 0 in Y.

Case 1. g has degree 0 in Y and h has degree 2 in Y. Then we can write: $g(X,Y) = \phi_0(X)$, where $\phi_0(X)$ is a polynomial in X, and $h(X,Y) = \theta_2(X)Y^2 + \theta_1(X)Y + \theta_0(X)$, where each $\theta_i(X)$ is a polynomial in X. Then, equating the coefficients of Y^2 in the equation $f(X,Y) = g(X,Y)h(X,Y)$ gives that $1 = \phi_0(X)\theta_2(X)$, and so both $\phi_0(X)$ and $\theta_2(X)$ must be constants. But then $g(X,Y)$ would be constant, contradicting out initial assumption that g, h are non-constant.

Case 2. g has degree 1 in Y and h has degree 1 in Y. Then we can write: $g(X,Y) = \phi_1(X)Y + \phi_0(X)$, where each $\phi_i(X)$ is a polynomial in X, and $h(X,Y) = \theta_1(X)Y + \theta_0(X)$, where each $\theta_i(X)$ is a polynomial in X. Then, equating the coefficients of Y^2 in the equation $f(X,Y) = g(X,Y)h(X,Y)$ gives that $1 = \phi_1(X)\theta_1(X)$, and so both $\phi_1(X)$ and $\theta_1(X)$ must be constants (and multiplicative inverses); say $\phi_1(X) = r$ and $\theta_1(X) = 1/r$, where $r \in \mathbb{C}$ is a nonzero constant. Then the equation $f(X,Y) = g(X,Y)h(X,Y)$ becomes: $Y^2 - X^5 = Y^2 + \big(r\theta_0(X) + (1/r)\phi_0(X)\big)Y + \theta_0(X)\phi_0(X)$. Equating coefficients of Y gives that $r\theta_0(X) + (1/r)\phi_0(X) = 0$ and so $\phi_0(X) = -r^2\theta_0(X)$. Hence the equation becomes: $Y^2 - X^5 = Y^2 - r^2\big(\theta_0(X)\big)^2$. But, $r^2\big(\theta_0(X)\big)^2$ is a polynomial of even degree in X, whereas X^5 is of odd degree, a contradiction.

Case 3. g has degree 2 in Y and h has degree 0 in Y. This gives the same contradiction as in Case 1, but with g, h interchanged.

In summary, our initial assumption, that $f(X,Y) = g(X,Y)h(X,Y)$, where g, h are non-constant polynomials defined over $\mathbb{C}$, lead to a contradiction in all cases. Hence, it is not possible to write $f(X,Y)$ as such a product, and so $f(X,Y)$ is irreducible over $\mathbb{C}$. Of course, this means that $f(X,Y)$ is irreducible over $\mathbb{Q}$, also.

(b). Let $f(X,Y) = Y^3 - X^3 = (X-Y)(X^2+XY+Y^2) = (X-Y)(X-\omega Y)(X-\omega^2 Y)$, where $\omega = e^{2\pi/3} = (1+\sqrt{-3})/2$. So, the irreducible components over $\mathbb{C}$ are: $X-Y$, $X-\omega Y$ and $X+\omega Y$, whereas the irreducible components over $\mathbb{Q}$ are $X-Y$ and X^2+XY+Y^2 (since t^2+t+1 cannot be factorised over $\mathbb{Q}$).

(c). This is irreducible over $\mathbb{C}$ (and so irreducible over $\mathbb{Q}$) by the same argument as in (a). Note that this argument applies to any curve of the form $Y^2 - Q(X) = 0$, where $Q(X)$ is not the square of a polynomial.

7.

(a). Trying simple substitutions of the form where X, Y are replaced by $aX + bY$ and $cX + dY$ in $2X^2 - Y^2 = 1$ gives: $(2a^2 - c^2)X^2 + (2b^2 - d^2)Y^2 + (4ab - 2cd)XY = 1$; we can now notice that the coefficients on the LHS can be made to be $1, 1, -6$ by taking (for example) $a = 1, b = -1, c = 1, d = 1$. Be careful to note that $(X,Y) \mapsto (X-Y, X+Y)$ is then a birational transformation from $\mathcal{D} : X^2 + Y^2 - 6XY = 1$ to $\mathcal{C} : 2X^2 - Y^2 = 1$ [since $X^2 + Y^2 - 6XY = 1$ can be rewritten as $2(X-Y)^2 - (X+Y)^2 = 1$, and so a point (X,Y) on $\mathcal{D}$ maps to a point $(X-Y, X+Y)$ in $\mathcal{C}$]. The inverse map from $\mathcal{C}$ to $\mathcal{D}$ is $(X,Y) \mapsto \big((X+Y)/2, (Y-X)/2\big)$.

(b). Let $\mathcal{C} : Y^2 = (X+2)^6(X^3+1)$ and $\mathcal{D} : Y^2 = X^3 + 1$. Then $\mathcal{C}$ can be rewritten

as $\big(Y/(X+2)^3\big)^2 = X^3+1$ and so there is a birational map $(X,Y) \mapsto \big(X, Y/(X+2)^3\big)$ from $\mathcal{C}$ to $\mathcal{D}$. This is a birational transformation, since there is the inverse map $(X,Y) \mapsto \big(X, Y(X+2)^3\big)$.

(c). The map $(X,Y) \mapsto (\sqrt{2}\,X, Y)$ give a birational transformation over $\mathbb{C}$ from $Y^2 = 2X^2$ to $Y^2 = X^2$, with inverse map $(X,Y) \mapsto (X/\sqrt{2}, Y)$. There is no birational transformation over $\mathbb{Q}$, since $Y^2 = X^2$ has infinitely many $\mathbb{Q}$-rational points of the form $(a/b, \pm a/b)$, where $a, b \in \mathbb{Z}$, whereas $Y^2 = 2X^2$ has $(0,0)$ as its only $\mathbb{Q}$-rational point (since $\sqrt{2}$ is irrational).

8.

(a). The discriminant of X^4-2 is the same as $\mathrm{Res}(X^4-2, 4X^3)$, which is the determinant of the matrix:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & -2 & 0 \\ 1 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The determinant is $\mathrm{Disc}(X^4-2) = 2^{11}$.

(b). The resultant of $X^3 - a$ and $X^2 - b$ is the determinant of the matrix:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & -a \\ 1 & 0 & 0 & -a & 0 \\ 0 & 0 & 1 & 0 & -b \\ 0 & 1 & 0 & -b & 0 \\ 1 & 0 & -b & 0 & 0 \end{pmatrix}.$$

The determinant is $\mathrm{Res}(X^3 - a, X^2 - b) = a^2 - b^3$.

9. First note that, if there is an intersection point of $X^3 + Y^3 = Z^3$ and $X^2 + Y^2 = Z^2$ with $Z = 0$, then $X^3 = -Y^3$ and $X^2 = -Y^2$; squaring both sides of the first equation, and cubing both sides of the second equation one deduces: $X^6 = Y^6$ and $X^6 = -Y^6$; adding these gives $2X^6 = 0$, and so $X = 0$, and so $Y = 0$. But the point $(0,0,0)$ is not allowed in projective coordinates, so we conclude that there are no points of intersection with $Z = 0$. We can therefore consider only points with $Z \neq 0$.

Given that $Z \neq 0$, we can therefore use the affine models $x^3 + y^3 = 1$ and $x^2 + y^2 = 1$. [Each point (x,y) of intersection on $x^3+y^3 = 1$ and $x^2+y^2 = 1$ will give the point $(x,y,1)$ of intersection on $X^3 + Y^3 = Z^3$ and $X^2 + Y^2 = Z^2$; conversely, each point (X,Y,Z) of intersection on $X^3 + Y^3 = Z^3$ and $X^2 + Y^2 = Z^2$ with $Z \neq 0$ (which we have established must be the case) will give the point $(X/Z, Y/Z)$ of intersection on $x^3 + y^3 = 1$ and $x^2 + y^2 = 1$].

Let (x,y) be a point of intersection on $x^3+y^3 = 1$ and $x^2+y^2 = 1$. Then $x^6 = (1-y^3)^2$ and $x^6 = (1-y^2)^3$, and so y must satisfy: $(1-y^3)^2 = (1-y^2)^3$, which can be rewritten as:

$$y^2(y-1)^2(2y^2+4y+3) = 0 \qquad (*)$$

[Note that $(*)$ can also be derived as $\mathrm{Res}(x^2+y^2-1, x^3+y^3-1)$ with respect to the variable x].

The solutions in y are: $0, 1, -1+\sqrt{-1/2}, -1-\sqrt{-1/2}$. When $y=0$, then x simultaneously satisfies $x^3 = 1-0^3$ and $x^2 = 1-0^2$ so $x=1$, giving rise to the point of intersection: $P_1 = (1,0)$. When $y=1$, then x simultaneously satisfies $x^3 = 1-1^3$ and $x^2 = 1-1^2$ so $x=0$, giving rise to the point of intersection: $P_2 = (0,1)$. When $y = -1+\sqrt{-1/2}$, then x simultaneously satisfies $x^3 = 1-(-1+\sqrt{-1/2})^3$ and $x^2 = 1-(-1+\sqrt{-1/2})^2$, and so $x = x^3/x^2 = \big(1-(-1+\sqrt{-1/2})^3\big)/\big(1-(-1+\sqrt{-1/2})^2\big) = -1-\sqrt{-1/2}$; this gives rise to the point of intersection: $P_3 = (-1-\sqrt{-1/2}, -1+\sqrt{-1/2})$. Similarly, the final possibility for y, namely $y = -1-\sqrt{-1/2}$ gives rise to the point $P_4 = (-1+\sqrt{-1/2}, -1-\sqrt{-1/2})$. We have shown that P_1, P_2, P_3, P_4 are the only possible points of intersection, and substitution into $x^3+y^3=1$ and $x^2+y^2=1$ shows that they are all indeed points of intersection, so we have a complete list. Bézout's Theorem tells us that there should be 6 points of intersection, so some of the multiplicities must be greater than 1. At $P_1 = (1,0)$, we see that $\mathrm{d}x/\mathrm{d}y = 0$ on both curves, but that $\mathrm{d}^2x/\mathrm{d}y^2$ differ (since $\mathrm{d}^2x/\mathrm{d}y^2 = 0$ on $x^3+y^3=1$ but is nonzero on $x^2+y^2=1$). We conclude that $P_1 = (1,0)$ is a point of intersection of multiplicity exactly 2. Similarly (but using $\mathrm{d}y/\mathrm{d}x$ and $\mathrm{d}^2y/\mathrm{d}x^2$), we see (by symmetry) that $P_2 = (0,1)$ is a point of intersection of multiplicity exactly 2. We can now apply Bézout's Theorem to see that P_3, P_4 must each be points of intersection of multiplicity only 1 (since the total of all multiplicities must be 6); or one can check directly that the value of $\mathrm{d}y/\mathrm{d}x$ on $x^3+y^3=1$ at P_3 is distinct from the value of $\mathrm{d}y/\mathrm{d}x$ on $x^2+y^2=1$ at P_3 (and similarly for P_4).

On the original projective curves, $X^3+Y^3=Z^3$ and $X^2+Y^2=Z^2$, the six points of intersection are therefore:

$(1,0,1)$, with multiplicity 2.
$(0,1,1)$, with multiplicity 2.
$(-1-\sqrt{-1/2}, -1+\sqrt{-1/2}, 1)$, with multiplicity 1.
$(-1+\sqrt{-1/2}, -1-\sqrt{-1/2}, 1)$, with multiplicity 1.

10. (a). From the rule that 2 is a quadratic residue residue mod p ($p \neq 2$) iff $p \equiv \pm 1$ modulo 8, we have that 2 is a quadratic residue modulo 1009 (since 1009 is prime and $1009 \equiv 1$ modulo 8).

By quadratic reciprocity, since 3 and 1009 are both odd primes, and since at least one of them is congruent to 1 modulo 4, we have $(\frac{3}{1009}) = (\frac{1009}{3}) = (\frac{1}{3}) = 1$, since $1 \equiv 1^2$ mod 5. Hence, 3 is a quadratic residue modulo 1009.

Again applying quadratic reciprocity, $(\frac{5}{1009}) = (\frac{1009}{5}) = (\frac{4}{5}) = 1$, since $4 \equiv 2^2$ mod 5. Hence, 5 is a quadratic residue modulo 1009.

$(\frac{10}{1009}) = (\frac{2}{1009})(\frac{5}{1009}) = 1 \cdot 1 = 1$. Hence, 10 is a quadratic residue modulo 1009.
$(\frac{15}{1009}) = (\frac{3}{1009})(\frac{5}{1009}) = 1 \cdot 1 = 1$. Hence, 15 is a quadratic residue modulo 1009.

(b). When $p \equiv 1$ mod 4, we have by quadratic reciprocity that $(\frac{3}{p}) = (\frac{p}{3})$, which is 1 when $p \equiv 1$ mod 3, and is -1 when $p \equiv 2$ mod 3. When $p \equiv 3$ mod 4, we have $(\frac{3}{p}) = -(\frac{p}{3})$, which is -1 when $p \equiv 1$ mod 3, and is 1 when $p \equiv 2$ mod 3. In summary:
$(\frac{3}{p}) = 1$ when p satisfies both $p \equiv 1$ mod 4 and $p \equiv 1$ mod 3, that is, when $p \equiv 1$ mod 12.
$(\frac{3}{p}) = -1$ when p satisfies both $p \equiv 1$ mod 4 and $p \equiv 2$ mod 3, that is, when $p \equiv 5$ mod 12.

$(\frac{3}{p}) = -1$ when p satisfies both $p \equiv 3 \bmod 4$ and $p \equiv 1 \bmod 3$, that is, when $p \equiv 7 \bmod 12$.
$(\frac{3}{p}) = 1$ when p satisfies both $p \equiv 3 \bmod 4$ and $p \equiv 2 \bmod 3$, that is, when $p \equiv 11 \bmod 12$.

Hence, 3 is a quadratic residue mod p when $p \equiv 1$ or $11 \bmod 12$, and 3 is not a quadratic residue mod p when $p \equiv 5$ or $7 \bmod 12$. This describes what happens for all primes apart from $p = 2, 3$ (since any prime $p \neq 2, 3$ must be congruent to one of $1, 5, 7, 11 \bmod 12$). Finally, when $p = 2$ or 3 we have that 3 is a quadratic residue mod p.

It is always true by quadratic reciprocity that, for any prime $p \neq 2$, $(\frac{5}{p}) = (\frac{p}{5})$, since $5 \equiv 1 \bmod 4$; that is 5 is a quadratic residue mod p iff p is a quadratic residue mod 5. But then $(\frac{p}{5}) = 1$ when $p \equiv 1, 4 \bmod 5$ (since $1 \equiv 1^2$ and $4 = 2^2 \bmod 5$) and $(\frac{p}{5}) = -1$ when $p \equiv 2, 3 \bmod 5$ (since none of $0^2, 1^2, 2^2, 3^2, 4^2$ are congruent to either of 2 or 3 mod 5). In summary, 5 is a quadratic residue mod p when $p \equiv 1, 4 \bmod 5$, and 5 is not a quadratic residue mod p when $p \equiv 2, 3 \bmod 5$. This describes what happens for all primes apart from $p = 2, 5$ (since any prime $p \neq 5$ must be congruent to one of $1, 2, 3, 4 \bmod 5$). Finally, when $p = 2$ or 5 we have that 5 is a quadratic residue mod p (since it is congruent mod p to 1^2 and 0^2, respectively).

We know $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p})$. For $p \neq 2, 5$ we can use the standard rules that $(\frac{2}{p}) = 1$ when $p \equiv 1, 7 \bmod 8$, that $(\frac{2}{p}) = -1$ when $p \equiv 3, 5 \bmod 8$; also, $(\frac{5}{p}) = 1$ when $p \equiv 1, 4 \bmod 5$, and $(\frac{5}{p}) = -1$ when $p \equiv 2, 3 \bmod 5$ (done above). Note that $(\frac{10}{p}) = 1$ when $(\frac{2}{p}) = (\frac{5}{p}) = 1$ or $(\frac{2}{p}) = (\frac{5}{p}) = -1$ and $(\frac{10}{p}) = -1$ when $(\frac{2}{p})$ and $(\frac{5}{p})$ have opposite sign.

In a similar manner to the first example, we therefore have that (for any $p \neq 2, 5$), $(\frac{10}{p}) = 1$ when $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \bmod 40$, and $(\frac{10}{p}) = -1$ when $p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \bmod 40$. This describes what happens for all primes apart from $p = 2, 5$ (since any prime $p \neq 5$ must be congruent to one of $1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39 \bmod 40$). Finally, when $p = 2$ or 5 we have that 10 is a quadratic residue mod p (since it is congruent mod p to 0^2).

11. Suppose there were integers a, b, c, not all 0 such that $2a^2 + 5b^2 = c^2$. Without loss of generality, we can divide through by the square of any common factor of a, b, c, and assume that $\gcd(a, b, c) = 1$. Reducing the equation modulo 5 gives: $2a^2 \equiv c^2 \pmod 5$.

Imagine that 5 does not divide a; then there would exist $\lambda \in \mathbb{Z}$ such that $\lambda a \equiv 1 \pmod 5$; multiplying both sides by λ^2 would then give $2 \equiv (\lambda c)^2 \pmod 5$; but this is a contradiction, since 2 is not a quadratic residue mod 5 [to see this, check that: $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 4$, $4^2 \equiv 1 \pmod 5$]. This contradiction shows that our assumption '5 does not divide a' must be false, and so we conclude that: $5|a$.

Since $5|a$ and $2a^2 + 5b^2 = c^2$, we can deduce that $5|c^2$ and so $5|c$. Therefore $5^2|a^2$ and $5^2|c^2$ and so $5|5b^2$; but only 5^1 divides into 5, and so $5|b^2$, giving $5|b$. We now have that 5 divides all of a, b, c, contradicting the fact that $\gcd(a, b, c) = 1$. This proves that no such a, b, c exist.

12. Define $S(n) = \{x \in \mathbb{N} : 1 \leqslant x \leqslant n \text{ and } \gcd(x, n) = 1\}$, so that $\phi(n) = \#S(n)$.

For any p, to get $S(p^r)$ we remove all multiples of p from the set $\{1, \ldots, p^r\}$, and so $\phi(p^r) = \#S(p^r)$ is $p^r - \frac{1}{p}p^r$; that is: $p^r - p^{r-1}$.

For two distinct primes p_1, p_2, note that $S(p_1p_2)$ can be obtained by removing from the set $\{1, \ldots p_1p_2\}$ all multiples of p_1 (of which there are $\frac{1}{p_1}p_1p_2 = p_2$) and all multiples of

p_2 (of which there are $\frac{1}{p_2}p_1p_2 = p_1$). But note that the element p_1p_2, which is a multiple of both p_1 and p_2, should only be counted once. Hence the total number of elements removed is: $p_2 + p_1 - 1$, so $\phi(p_1p_2) = p_1p_2 - (p_2 + p_1 - 1) = (p_1 - 1)(p_2 - 1)$.

Applying Euler's Theorem, that $a^{\phi(n)} \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$, gives as follows.

$2^{12} \equiv 2^{\phi(13)} \equiv 1 \pmod{13}$, since $\gcd(2, 13) = 1$. $3^{12} \equiv 3^{\phi(13)} \equiv 1 \pmod{13}$, since $\gcd(3, 13) = 1$. Hence, $3^{24} \equiv (3^{12})^2 \equiv 1^2 \equiv 1 \pmod{13}$. Similarly, $3^{12000} \equiv (3^{12})^{1000} \equiv 1^{1000} \equiv 1 \pmod{13}$, and $3^{12002} \equiv (3^{12})^{1000} \cdot 3^2 \equiv 1^{1000} \cdot 9 \equiv 9 \pmod{13}$.

Since $(4, 35) = 1$ and $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$, we have $4^{24} \equiv 1 \pmod{35}$. So, $4^{48} \equiv (4^{24})^2 \equiv 1^2 \equiv 1 \pmod{35}$, also. Similarly, $4^{48000001} \equiv 4^{48000000} \cdot 4 \equiv (4^{24})^{2000000} \cdot 4 \equiv 1^{2000000} \cdot 4 \equiv 4 \pmod{35}$.

We cannot do the same thing for 7^r, since $(7, 35) \neq 1$. Note that $7^5 \equiv 7 \pmod{35}$ [this is due to the fact that $7^5 \equiv 7$ modulo each of 5 and 7], and so $7^{24} \equiv (7^5)^4 \cdot 7^4 \equiv 7^4 \cdot 7^4 \equiv 7^5 \cdot 7^3 \equiv 7 \cdot 7^3 \equiv 21 \pmod{35}$. Similarly, $7^{48} \equiv (7^5)^9 \cdot 7^3 \equiv 7^9 \cdot 7^3 \equiv (7^5)^2 \cdot 7^2 \equiv 7^2 \cdot 7^2 \equiv 21 \pmod{35}$. Similarly, $7^{48000000} \equiv 21 \pmod{35}$, so that $7^{48000001} \equiv 21 \cdot 7 \equiv 7 \pmod{35}$.