ALGEBRAIC CURVES (MA40188): SOLUTIONS TO 2003 EXAM

1. The simplest way to describe the group law is to choose an embedding in $\mathbb{P}^2$ such that O is an inflection point and then say that three collinear points add to O. *[In hurriedly retyping the question I lost some notation. P is the point $(0:0:1)$ and the point $(-9:-18\sqrt{3}:1)$ should have another name, such as Q. The question then asks for A such that $A+A=P$, not $O=(0:1:0)$]*
To find the tangent line we could differentiate but since we are told in the question two points that it goes through, it is easiest to do the two parts together. The line through $(-9,-18\sqrt{3})$ and $(0,0)$ (in affine coordinates in $z=1$) is simply $y=2\sqrt{3}x$, i.e. the set of points $(t,2\sqrt{3}t)$ for $t\in K$ and this meets $y^2=x(x+3)(x+27)$ when

$$12t^2=t(t+3)(t+27).$$

If $t\neq 0$ that gives $12t=(t+3)(t+27)=t^2+30t+81$, so $0=t^2+18t+81=(t+9)^2$. Therefore the line meets the curve twice at $t=-9$, i.e. at $(-9,-18\sqrt{3})$, so it is tangent to the curve there.
If $A+A=P$ then the tangent line at A passes through P. So which lines through P are tangent to the curve, and where? A line through O is of the form $y=\lambda x$, so a point on it is $(t,\lambda t)$. This meets the curve when

$$\lambda^2t^2=t(t+3)(t+27))$$

and after discarding the solution $t=0$ we are left with $t^2+(30-\lambda^2)t+81=0$. To get a tangent line we want that to have repeated roots, so we want

$$(30-\lambda^2)^2-324=0$$

so $30-\lambda^2=\pm\sqrt{324}=\pm 18$, so $\lambda^2=12$ or 48, so $\lambda=\pm 2\sqrt{3}$ or $\pm 4\sqrt{3}$. Taking $\lambda^2=12$ we get $t^2+18t+81=0$ so $t=-9$ and that gives $(-9,\pm 18\sqrt{3})$; taking $\lambda^2=48$ we get $t=9$ and that gives $(9,\pm 36\sqrt{3})$ in affine coordinates.
2. The only non-bookwork part of this is the last part. But $\mathbb{Z}_{100}$ is finite so it has to be Noetherian (there aren't even infinitely many elements, so any ideal has to be finitely generated); then the Basis Theorem tells us that $\mathbb{Z}_{100}[X]$ is Noetherian too.
3. Again the last part is the only non-bookwork bit. Put $f(x,y)=(x^2+y^2+1)^3+27x^2y^2$ (we aren't asked about what happens at infinity so the affine equation is all we need). Then $f_x=6x(x^2+y^2+1)^2+54xy^2$ and $f_y=6y(x^2+y^2+1)^2+54x^2y$.

We want to know when $f_x = f_y = f = 0$. One obvious thing is $x = 0$; then $f_x = 0$ and the equation $f_y = 0$ becomes $y(y^2 + 1) = 0$, so $y = 0$ or $\pm i$. Only the last two of these also satisfy $f(x, y) = 0$. So $(0, \pm i)$ and (by symmetry) $(\pm i, 0)$ are singular points.

Are there any others? If x and y are nonzero then $f_x = 0$ gives $(x^2 + y^2 + 1)^2 = -9y^2$ and $f_y = 0$ gives $(x^2 + y^2 + 1)^2 = -9x^2$, so $x^2 = y^2$. Therefore $(2x^2 + 1)^2 + 9x^2 = 0$ and from $f(x, y) = 0$ we get $(2x^2 + 1)^3 = 27x^4$. Since $81x^4 = (-9x^2)^2 = (2x^2 + 1)^2$ that gives $3(2x^2 + 1)^3 = (2x^2 + 1)^2$, so $2x^2 + 1 = 0$ or $2x^2 + 1 = 1$, i.e. $x = \pm i/2$ or 0. The latter is already excluded; the former gives $(2x^2 + 1)^2 = 0 \neq -9x^2$. So there are no more singular points.

4. The rational map given is self-inverse: applying it twice gives $(x : y : z) \mapsto (zxxy : xyyz : yzzx) = (x : y : z)$ as long as all the coordinates are non-zero.

For the last part, apply the transformation: replace x, y and z in the first equation by yz, zx and xy, getting

$$0 = z^2x^2z - yz(yz - xy)(yz - 2xy) = z(x^3z - y^2z^2 + 3xy^2z - 2x^2y^2)$$

which is what we are asked for if $z \neq 0$.