TAKE HOME EXAM *Number Theory of Cubic Curves*

Please hand in solutions to four of the eight problems below. You are free to make your own choice which ones to pick. They should be sent to me by January 18th, 2008. This can be done in two ways:
by email, to j.top@rug.nl
by ordinary mail, to J.Top, IWI-RuG, Postbus 800, 9700AV Groningen.
If you want to receive your corrected work, put an address on it.

(1) Let p be a prime number, and take integers a, b, c such that p divides each of a, b and c, but p^2 does not divide c. Show that the cubic C, given by $y^2 = x^3 + ax^2 + bx + c$, is smooth. The reduction $\overline{C}$ of C, is the curve over $\mathbb{F}_p$ given by $y^2 = x^3$. Show that the singular point on $\overline{C}$ is *not* in the image of the reduction map

$$C(\mathbb{Q}) \longrightarrow \overline{C}(\mathbb{F}_p).$$

Now do the analog of Silverman-Tate Exc. III.3.11 with $\mathbb{Q}$ replaced by $\mathbb{F}_p$, and prove that the torsion subgroup of $C(\mathbb{Q})$ has either 1, or exactly p elements.

Given two primes $p \neq q$, what can you say about the torsion subgroup of $C(\mathbb{Q})$ with C given by $y^2 = x^3 + pqx + pq$?

(2) Do problem V.5.11 in the book by Silverman & Tate.

(3) Show that the cubic C given by $y^2 = x^3 - 4x + 64$ is smooth, and that $C(\mathbb{Q})$ contains no points $\neq O = (0 : 1 : 0)$ of finite order. Also show that the points with x-coordinate $x \in \{-4, -3, -2\}$ generate a subgroup $\cong \mathbb{Z}^3$ in $C(\mathbb{Q})$.

(4) Let p be a prime number and let C_p be given by $y^2 = x^3 + 4p^2x$. Show that the rank of $C_p(\mathbb{Q})$ is at most 2. Prove that this rank equals 1 for $p = 5$, and it equals 0 for $p = 3$.
(A somewhat more difficult challenge, which is *not* part of this exam: show that for every prime $p \equiv 5$ or 7 mod 8, the rank of $C_p(\mathbb{Q})$ is at most 1 and for $p \equiv 3$ mod 8, the rank equals 0.)

(5) Both Euler and Fermat have described a method for finding rational numbers $x \neq 0$ such that $f(x) := x^3 + ax^2 + bx + c$ is a square, provided c is a nonzero square. This works as follows. Write $c = d^2$ and then write $ax^2 + bx + c = \alpha x^2 + (\beta x + \gamma)^2$ for certain rational numbers α, β, γ. Then $x = -\alpha$ is the desired rational number.

Under what conditions on a, b, c does this method actually work?

Fermat states that in fact this method allows you to find infinitely many rational numbers x such that $f(x)$ is a square. Namely, take α as above and write $x = \xi - \alpha$. Then $g(\xi) := f(\xi - \alpha)$ is also a cubic polynomial whose constant term is a square, so the same technique will produce a value for ξ such that $f(\xi - \alpha) = g(\xi)$ is a square, et cetera.

Explain Fermat's method in terms of the point $(0, d)$ and the group law on the curve given by $y^2 = f(x)$. Give an example where indeed Fermat's method gives infinitely many such rational values.

(6) Suppose a, b, c are pairwise distinct rational numbers, and consider the cubic curve C given by $y^2 = (x-a)(x-b)(x-c)$. Define a map

$$\beta \,:\, C(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$$

by $\beta(O) = (1,1,1)$ and $\beta((a,0)) = ((a-b)(a-c), a-b, a-c)$ and $\beta((b,0) = (b-a, (b-a)(b-c), b-c)$
and $\beta((c,0)) = (c-a, c-b, (c-a)(c-b))$, and for any other $P \in C(\mathbb{Q})$ by

$$\beta(P) = (x(P) - a, x(P) - b, x(P) - c)\,.$$

Show that β is a homomorphism of groups, and that the kernel of β equals the subgroup $2C(\mathbb{Q})$. Use this to conclude that $2^r = \#\beta(C(\mathbb{Q}))/4$.

(7) In this problem you can use (without proof) the statements from the previous problem.

Under what conditions on the rational numbers a, b, c is C, given by $y^2 = (x-a)(x-b)(x-c)$ a smooth curve with the property that $C(\mathbb{Q})$ contains a rational point of order 4? Show that a smooth cubic curve over $\mathbb{Q}$ with more than four rational point of order 4 cannot exist.

Find an example of a, b, c as above such that $C(\mathbb{Q})$ contains a point of order 8.

(8) Do the problems III.3.14 and III.3.15 from the book by Silverman & Tate.