Math 116

Extra problem on elliptic curves, due April 7

Let E be the elliptic curve considered in class on March 19, i.e., the curve with equation $y^2 = x^3 + x - 1$. Let P be the point $(1, 1)$. Using `gp`, I calculated P, $2P = P + P$, $3P \ldots$, $7P$ and wrote down some of the data on the board during my lecture on March 19. How did I do this? I entered the command

```
E = ellinit([0,0,0,1,-1]) ;
```

the three 0s are basically placeholders; 1 and -1 are the trailing coefficients of the cubic $x^3 + x - 1$. I then entered

```
P=[1,1]
```

and defined `f(n) = ellpow(E,P,n)`. Then `f(5)`, for example, gives the coordinates of $5 \cdot P$, which are $685/121$ and $-18157/1331$. Type in "`factor(1331)`" and you'll see that it's 11^3.

Now I want to start "reducing" E mod p; this means that I want to consider E over $\mathbf{F}_p$ for different primes p. When you type in the "`ellinit`" command, you get back a huge amount of data about E. The -496 early on in the string tells you that you have the right to reduce E mod p for all primes p that do not divide 496. We can take any $p \neq 2, 31$. For each such p, the group $E(\mathbf{F}_p)$ is finite, and its order is traditionally written $p + 1 - a_p$. As I mentioned on March 19, a theorem of Hasse tells you that $|a_p| \leq 2\sqrt{p}$. The values of a_p are found by the command "`ellap(E,p)`"; using it, we find that E has 5 points mod 9, 18 points mod 17, and so on and so forth. For instance $a_{17} = 0$, which gives the value 18 for the number of points of E mod 17. (Because $a_p = 0$ here, E is said to have *supersingular* reduction mod 17.

The group $E(\mathbf{F}_{17})$ has 18 elements; how does the point $(1, 1)$ fit in?

"`Q = [Mod(1,17),Mod(1,17)]`"

introduces the point $(1, 1)$ on E mod 17. The command "`ellisoncurve(E,Q)`" confirms that Q is a point on E. Type in "`ellpow(E,Q,2)`" and you see that $2Q = (2, 14)$, where the entries are regarded mod 17. Similarly $9Q = (6, 0)$ is a point of order 2 (because the y-coordinate is 0) but not the identity. Thus Q has order 18 on E mod 17. In other words, $(1, 1)$ generates $E(\mathbf{F}_1 7)$, which we knew a priori to be cyclic. (All abelian groups of order 18 are cyclic!)

Now we turn to the problem, which is basically to perform calculations like mine for the elliptic curve $E' : y^2 = x^3 + 2x - 2$ and the point $P := (1, 1)$. Note that $P \in E'(\mathbf{Q})$; that's how I chose the equation!

Specifically:

a. Calculate $-P$, $2P$, $3P$ and $4P$ on this curve.

b. Find the order of $E'(\mathbf{F}_p)$ for $p = 11, 13, 17, 19, 23, 29$. (The primes of "bad reduction" for this curve are 2, 5 and 7.)

c. For $p = 19$ and $p = 23$, find the order of the point $(1, 1)$ in the group $E'(\mathbf{F}_p)$.