18.781 practice problems A solutions

These are meant as hints about what kind of material from the last weeks could appear on the final, and as some additional practice problems about earlier material in the class. **They are not to be handed in.**

1. Can there be an elliptic curve over $\mathbb{Q}$ having exactly three points of order 2 over $\mathbb{Q}$? If you find one, write down the three rational points.

According to the end of the `curves.pdf` summary sheet, a point of order 2 of the curve $y^2 = x^3 + bx + c$ is $(x_0, 0)$ with $x_0^3 + bx_0 + c = 0$. So you are looking for b and c to make the cubic equation $x^3 + bx + c$ have exactly 3 rational roots. If the roots are to be r_1, r_2, and r_3, then the cubic must be

$$(x - r_1)(x - r_2)(x - r_3) = x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_1r_3 + r_2r_3)x - r_1r_2r_3.$$

So you can get an equation of the form we've been studying (no x^2 term) using any three distinct rational numbers adding to zero. (You also get a perfectly good curve if they *don't* add to zero.) So an easy possibility is (-1,0,1), leading to

$$\boxed{y^2 = x^3 - x}$$

with the three points of order 2 $\boxed{(-1, 0)}$, $\boxed{(0, 0)}$, $\boxed{(1, 0)}$.

2. Can there be an elliptic curve over $\mathbb{Q}$ having exactly two points of order 2 over $\mathbb{Q}$? If you find one, write down the two rational points.

This time you want a cubic equation with rational coefficients having exactly two rational roots r_1 and r_2, and a third irrational root s_3. Just as in Problem 1 we can write down the unique equation with this property, and see that the coefficient of x^2 is $-r_1 - r_2 - s_3$, which is *irrational*. So $\boxed{\text{no such curve can exist}}$.

3. This problem is about the elliptic curve $y^2 = x^3 + 2x + 1$ over $\mathbb{Z}/5\mathbb{Z}$. Find all the points of this curve over $\mathbb{Z}/5\mathbb{Z}$.

Easiest method is to list the five possible values of x. For each x, determine whether $x^3 + 2x + 1$ is a square, and if so calculate a square root y. Then we get points $(x, \pm y)$. If $x^3 + 2x + 1$ is *not* a square, then we get no points $(x, \star)$. Here is a table of the work.

x	$x^3 + 2x + 1$	square?	$\sqrt{x^3 + 2x + 1}$	points
0	1	yes	$\pm 1 = 1, 4$	$(0, 1), (0, 4)$
1	4	yes	$\pm 2 = 2, 3$	$(1, 2), (1, 3)$
2	3	no		
3	4	yes	$\pm 2 = 2, 3$	$(3, 2), (3, 3)$
4	3	no		

In addition to these six points there is also the point at infinity $[0 : 1 : 0]$: $\boxed{\text{seven points}}$ altogether.

Another way to proceed is to start with the obvious point $P = (0, 1)$ and compute its powers using the doubling and addition formulas:

$$P = (0, 1), \quad 2P = (1, 3), \quad 3P = (3, 3), \quad 4P = (3, 2).$$

Now you can notice that $4P = -3P$ (the additive inverse of (x, y) is $(x, -y)$) and deduce that P has order exactly 7:

$$5P = -2P = (1, 2), \quad 6P = -P = (0, 4), \quad 7P = 0 = [0 : 1 : 0].$$

You've now found a subgroup of seven points on the curve modulo 5. Hasse's theorem ((5.63) in the text) says that the number of points on an elliptic curve modulo p is $p+1+t$, with $|t| < 2\sqrt{p}$. For $p = 5$ this says that the number of points is between 2 and 10. Since we found a subgroup of order 7, the total number of points must be a multiple of 7; so we found all of the points.

4. For which odd primes are -1, -2, and 2 all quadratic residues? (Your answer should be something like "the remainder when p is divided by 17 must be zero or 7.")

We know that

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4. \end{cases}$$

Similarly, a formula from `euclid.pdf` says

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & p \equiv 1, 7 \pmod 8 \\ -1 & p \equiv 3, 5 \pmod 8. \end{cases}$$

So both of these Legendre symbols are 1 if and only if $\boxed{p \equiv 1 \pmod 8}$. Because the Legendre symbol is multiplicative in the numerator, in this case $-2 = -1 \cdot 2$ is also a quadratic residue. The answer is $\boxed{\text{primes congruent to 1 modulo 8}}$.

5. Prove that there must be infinitely many primes congruent to 3 modulo 4. (Hint: if there are only finitely many, you can take the product of all of them, then add 2 or 4.)

Suppose that $p_1, \ldots, p_m$ is all the primes congruent to 3 modulo 4. Define

$$N = p_1 \cdot p_2 \cdots p_m + \begin{cases} 2 & m \equiv 0 \pmod 2 \\ 4 & m \equiv 1 \pmod 2. \end{cases}$$

Because the product of the p_i is 3 (mod 4) if m is odd and 1 (mod 4) if m is even, we see that $N \equiv 3 \pmod 4$. It follows that N must have a prime factor that is 3 (mod 4); so N is divisible by some p_i. By the definition of N this forces p_i to divide 2 or 4, which is impossible. So there must have been infinitely many primes congruent to 3 modulo 4.