18.783 Elliptic Curves **Spring 2019**
Problem Set #3

Description

These problems are related to the material covered in Lectures 5-7.

Instructions: First do Problems 1 and 2, then pick one of Problems 3–5 to solve; finally, complete Problem 6, which is a short survey. Your solutions are to be written up in latex and submitted as a pdf-file with a filename of the form `SurnamePset3.pdf`.

Collaboration is permitted/encouraged, but you must identify your collaborators, and any references not listed in the course syllabus. The first to spot each non-trivial typo/error in the problem sets or lecture notes will receive 1-5 points of extra credit.

Problem 1. The discriminant of an elliptic curve (9 points)

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$ with $A, B \in \mathbb{Z}$. For each prime p, we can reduce the coefficients of E modulo p to get an equation that defines a curve E_p over the finite field $\mathbb{F}_p$. Prove that E_p defines a smooth projective curve (and therefore an elliptic curve with a distinguished rational point $(0 : 1 : 0)$ at infinity) if and only if p does not divide the *discriminant*

$$\Delta(E) := -16(4A^3 + 27B^2).$$

(You may wonder why we use the leading coefficient -16 rather than 2, which would yield an integer with the same property; this will be made clear in later lectures). Next, show that one can have $\mathbb{Q}$-isomorphic elliptic curves E and E' defined by short Weierstrass equations with integer coefficients such that $\Delta(E)$ is divisible by primes that do not divide $\Delta(E')$ (thus $\Delta(E)$ is not an isomorphism class invariant, and the set of primes for which E_p is an elliptic curve depends on the model one chooses).

Problem 2. Vélus formulas (9 points)

Let $E_1/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 21x + 47$. Show that E_1 admits a rational isogeny $\phi\colon E_1 \to E_2$ of degree 3 whose kernel is generated by the point $(1, 3\sqrt{3})$ and use Vélu's formulas to compute an explicit equation for $E_2/\mathbb{Q}$ and an explicit rational map for the isogeny $\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ in standard form. Then compute $\phi(P)$, where P is the rational point $(-2, 9)$ on E_1 and verify that $\phi(P)$ is a rational point on E_2.

Problem 3. The torsion subgroup of $E(\mathbb{Q})$ (79 points)

Let E be an elliptic curve over $\mathbb{Q}$. The problem of determining the rational points on E is a famously hard problem that is still unsolved. However, determining the rational points of finite order is easy. In this problem you will design (but need not implement) an efficient algorithm for doing so.

We shall assume that E is defined by a Weierstrass equation $y^2 = x^3 + Ax + B$, where A and B are *integers*. This assumption is not restrictive: we can always pick $u \in \mathbb{Z}$ so that the isomorphic curve $y^2 = x^3 + u^4Ax + u^6B$ has integer coefficients.

Let $P = (x_1, y_1)$ be a point of finite order $m > 0$ in $E(\mathbb{Q})$. Our first goal is to prove that P must have integer coordinates. This was proved independently first by Nagell [4] and then by Lutz [3] in the 1930's and is the first half of the Nagell-Lutz Theorem. The standard proof [5, §8.1] relies on a p-adic filtration, but in this problem you will give a shorter and simpler proof that relies only on properties of the division polynomials. As shown in lecture, for any integer n not divisible by m, the x-coordinate x_n of the point $nP = (x_n, y_n)$ is given by $x_n = \phi_n(x_1)/\psi_n^2(x_1)$ where

$$\phi_n(x) = x^{n^2} + \cdots,$$
$$\psi_n^2(x) = n^2x^{n^2-1} + \cdots,$$

with each ellipsis denoting lower order terms; see Problem 4 for the full definition of ϕ_n and ψ_n, which depend on the curve coefficients A and B.

(a) Prove that for any positive integer $n < m$, if x_n is an integer, then x_1 must be an integer. Use this to reduce to the case that m is prime.

(b) Prove that if $m = 2$ then P has integer coordinates.

(c) If m is an odd prime then x_1 is a root of $\psi_m(x) = mx^{(m^2-1)/2} + \cdots \in \mathbb{Z}[x]$. Using this, prove that x_1 is an integer, and then show that y_1 must also be an integer (thus P has integer coordinates as claimed).

We now need a few facts about the image of the torsion subgroup under reduction modulo a prime p of good reduction for E. So let $\Delta(E) := -16(4A^3 + 27B^2)$ be the discriminant of E, and let p be a prime that does not divide Δ. Reducing the coefficients A and B modulo p then gives an elliptic curve $E_p/\mathbb{F}_p$. Since we know that torsion points in $E(\mathbb{Q})$ have integer coordinates, we can always reduce the coordinates of such a point modulo p to get the coordinates of a point in $E_p(\mathbb{F}_p)$.

(d) Prove that if $P \in E(\mathbb{Q})$ has order m, then its reduction in $E_p(\mathbb{F}_p)$ has order m. Deduce that the reduction map from $E(\mathbb{Q})$ to $E_p(\mathbb{F}_p)$ is injective at torsion points.

We now recall Mazur's theorem from Lecture 1, which tells us that the order of a torsion point in $E(\mathbb{Q})$ can be at most 12 (and cannot be 11). Our strategy is to pick a prime $p \geq 11$ of good reduction for E, find all the points of order less than or equal to 12 in $E_p(\mathbb{F}_p)$, and then use the algorithm from Problem 5 of Problem Set 2 to try and lift these points to $E(\mathbb{Q})$. As proved in part (d) of that problem, given a polynomial $f \in \mathbb{Z}[x]$ and root x_0 of f modulo p that is not also a root of f' modulo p, we can use Hensel's method to find a root $r \in \mathbb{Z}$ satisfying $r \equiv x_0 \bmod p$ or prove that no such r exists in $O(d\mathsf{M}(\log B))$ time; here $d = \deg f$ and B is a bound on the absolute values of its coefficients.

The first step is to find a prime p that does not divide the discriminant Δ. Doing this by trial division is not fast enough to give a quasi-linear running time, so we need to be a bit more clever. We will instead use an algorithm for fast simultaneous modular reduction [2, Alg. 10.16]. to compute $\Delta \bmod p_i$ for the first several primes $p_1, \cdots, p_k$ greater than 11, where k is chosen so that $M = p_1 \cdots p_k > \Delta$ (so we know that $\Delta \bmod p_i$ is nonzero for some p_i, we'll just pick the least one).

This is accomplished using a *product tree*, a binary tree of integers whose bottom level (the leaves of the tree) consists of the primes p_i; for the sake of simplicity let us assume we round k up to a power of 2 so that we have a complete binary tree. Working our way up from the leaves, we set the value of each internal node to the product of its children; eventually we reach the root of the tree, which then has the value $M = p_1 \cdots p_k$. We then replace the root M with $d = |\Delta| \bmod M$, and for each of its children m_1 and m_2 we replace m_i with $d_i = d \bmod m_i$ (which is $|\Delta| \bmod m_i$). Recursively working our way down the tree, we eventually get $|\Delta| \bmod p_i$ in the leaves.

In order to bound the complexity of our algorithm, we define

$$n := \lg|A| + \lg|B|,$$

which represents the bit-size of the input, the elliptic curve $E/\mathbb{Q}$ given as $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Note that we then also have $\log|\Delta| = O(n)$.

(e) Prove that we can determine the least prime $p \geq 11$ that does not divide Δ in time $O(\mathsf{M}(n)\log n)$, and use the Prime Number Theorem to show that $p = O(n)$. Feel free to use our usual assumption that $M(n)$ grows super-linearly ($a\mathsf{M}(b) \leq \mathsf{M}(ab)$).

For each integer $m > 1$, define the polynomial $f_m \in \mathbb{Z}[x]$ as follows:

$$f_m(x) = \begin{cases} x^3 + Ax + B & \text{if } m = 2, \\ \psi_m/\psi_2 & \text{if } m > 2 \text{ is even}, \\ \psi_m & \text{if } m \text{ is odd}, \end{cases}$$

where ψ_m denotes the mth division polynomial of the elliptic curve $E\colon y^2 = x^3 + Ax + B$.

(f) Prove that if $P = (x_1, y_1) \in E(\mathbb{Q})$ has finite order m not divisible by p then we have $f_m(x_1) = 0 \bmod p$ and $f_m'(x_1) \neq 0 \bmod p$.

It follows that their exist suitable starting values x_0 and z_0 to which we can apply the root-finding algorithm from Problem Set 2 (see Problem 5) to obtain an integer root of $f_m(x)$ that is congruent to x_0 modulo p. By part (c), this root must be equal to x_1. This still leaves the question of how to find such an x_0. We know it must appear as the x-coordinate of some point in $E_p(\mathbb{F}_p)$ of order m, so it suffices to find all such points for all the values of $m \leq 12$ permitted by Mazur's theorem.

(g) Give an algorithm to enumerate all the points $(x_0, y_0) \in E_p(\mathbb{F}_p)$ in time $O(n\mathsf{M}(\log n))$.

(h) Give an algorithm to construct the set S consisting of all points in $E_p(\mathbb{F}_p)$ of order at most 12 in time $O(n\mathsf{M}(\log n))$, and prove that the cardinality of S is $O(1)$ (meaning it is bounded by a constant that does not depend on n).

(i) Prove that there is a bound $H > 0$ with $\log H = O(n)$ such that the coefficients of f_m all have absolute value bounded by H, for $2 \leq m \leq 12$. You don't need to give an explicit value for H, just show that it exists and can be effectively computed.

(j) Using the $O(d\mathsf{M}(\log H))$ complexity bound of the root-finding algorithm (proved in part (d) of Problem 5 on Problem Set 2), show that for any point $Q \in S$ of order m you can either find a point $P \in E(\mathbb{Q})$ of order m that reduces to Q modulo p, or prove that no such P exists[1] in time $O(\mathsf{M}(n))$.

[1] Note that not every point $Q \in S$ is necessarily the reduction of a point $P \in E(\mathbb{Q})$.

(k) Conclude that you can enumerate the torsion points in $E(\mathbb{Q})$ in $O(\mathsf{M}(n)\log n)$ time.

It is worth noting that the algorithm you have just designed is asymptotically faster than both of the algorithms given in [5]: one is based on the the Lutz–Nagell Theorem [5, Thm. 8.7], which requires factoring Δ and is not polynomial time, and the other uses Doud's algorithm [1] which is quasi-quadratic but not quasi-linear.[2]

(l) Now suppose we would like an algorithm that does not depend on Mazur's result. Explain how to modify the algorithm above to replace 12 with an alternative bound (which may depend on E), and analyze the complexity of the resulting algorithm.

Problem 4. Computing division polynomials (79 points)

For integers $n \geq 0$, define $\psi_n \in \mathbb{Z}[x,y,A,B]$ by

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
\psi_{2m} &= \frac{1}{2y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \qquad (m \geq 3),\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad (m \geq 2).
\end{aligned}$$

Let $\phi_1 = x$ and $\omega_1 = y$, and for integers $n > 1$ define

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
\omega_m &= \frac{1}{4y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

It is a straight-forward exercise (which you are not required to do) to show that these polynomials have the form

$$\begin{aligned}
\phi_n(x) &= x^{n^2} + \cdots,\\
\omega_n(x,y) &= \begin{cases} y(x^{3(n^2-1)/2} + \cdots) & n \text{ odd},\\ x^{3n^2/2} + \cdots & n \text{ even},\end{cases}\\
\psi_n(x,y) &= \begin{cases} nx^{(n^2-1)/2} + \cdots & n \text{ odd},\\ y(nx^{(n^2-4)/2} + \cdots) & n \text{ even},\end{cases}
\end{aligned}$$

where each ellipsis denotes terms of lower degree in x.

In practical applications it is more convenient to work with the univariate polynomials

$$f_n(x) = \begin{cases} \psi_n & n \text{ odd},\\ \psi_n/\psi_2 & n \text{ even}.\end{cases}$$

[2] Doud gives a quasi-cubic complexity bound in [1] but with fast arithmetic it is quasi-quadratic.

Note that $\psi_2 = 2y$, and it follows from the formulas above that f_n does not depend on y. If $P = (x_0, y_0)$ is a point on the elliptic curve $y^2 = x^3 + Ax + B$ with $y_0 \neq 0$ (so P is not a 2-torsion point), then $f_n(x_0) = 0$ if and only if $nP = 0$. In this problem you will develop an efficient algorithm to compute f_n.

(a) Let $F(x) = 4(x^3+Ax+B)$. Using the recursion formulas for ψ_{2m} and ψ_{2m+1}, derive recursion formulas for f_{2m} and f_{2m+1} that involve $f_{m-2}, \ldots, f_{m+2}$ and F. Note that for f_{2m+1} you will need to distinguish the cases where m is odd and even.

(b) Show that for any $k \geq 3$, if you are given the polynomials $f_{k-3}, \ldots, f_{k+5}$ and F, you can compute the polynomials $f_{2k-3}, \ldots, f_{2k+5}$ (call this *doubling*), and you can also compute the polynomials $f_{2k+1-3}, \ldots, f_{2k+1+5}$ (call this *doubling-and-adding*).

(c) Implement an algorithm that, given a positive integer n, a prime p, and coefficients A and B, computes the division polynomial $f_n \in \mathbb{F}_p[x]$ for the elliptic curve $E/\mathbb{F}_p$ defined by $y^2 = x^3 + Ax + B$, using a left-to-right binary exponentiation approach. Here are a few tips, but you are free to use any design you like.

- Work in the polynomial ring $\mathbb{F}_p[x]$, which you can create in Sage by typing `R.<x>=PolynomialRing(GF(p))`. Note that A and B are now scalars in $\mathbb{F}_p$, not variables. Precompute $F = 4(x^3 + Ax + B) \in \mathbb{F}_p[x]$.
- You need an initial vector of division polynomials $v = [f_{k-3}, \ldots, f_{k+5}]$ to get started. If the leading two bits of n are "11", then let $v = [f_0, \ldots, f_8]$ and $k = 3$. Otherwise, let $[f_1, \ldots, f_9]$ and $k = 4$ if the top three bits of n are "100", and let $v = [f_2, \ldots, f_{10}]$ and $k = 5$ if the top three bits of n are "101".
- Implement a function that, given k, $v = [f_{k-3}, \ldots, f_{k+5}]$, F, and a bit b, computes $k' = 2k + b$ and $v = [f_{k'-3}, \ldots, f_{k'+5}]$. To perform left-to-right binary exponentiation, call this function repeatedly, passing in the bits of n starting from either 2 or 3 bits from in the top and working down to the low order bit.
- To test your code, you can compare results with Sage, which already knows how to compute f_n, via

```
FF=GF(p); R.<x>=PolynomialRing(FF)
E=EllipticCurve([FF(A),FF(B)])
E.division_polynomial(n,x,0)
```

- Your program should be quite fast, but be careful not to test it with values of n that are too large — the degree of f_n is quadratic in n, so if n is, say, a million, you would need several terabytes of memory to store f_n.

(d) Analyze the asymptotic complexity (in terms of time and space) of your program as a function of $\log p$ and n. Use $\mathsf{M}(b)$ to denote the time to multiply two b-bit integers.

(e) Modify your program so that it performs its computations modulo x^7 (to compute $f(x) \bmod x^7$ in Sage use `f.mod(x^7)`). Now let A be the least prime greater than the last two digits of your student ID, let B be the least prime greater than the first two digits of your student ID, and let $p = 65537$. Let $E/\mathbb{F}_p$ be the elliptic curve defined by $y^2 = x^3 + Ax + B$, and let $n = N^{100} + 1$, where N is the integer formed by adding the last three digits of your student ID to 9000.

(i) Use your modified program to compute $f_n \bmod x^7$ and record the result in your problem set. Be sure to first test your program with smaller values of n and verify the results with Sage (your answer to this question will be heavily weighted when grading this problem, so please be careful).

(ii) Time your program using the `timeit` function in Sage.

Problem 5. Galois actions and ℓ-isogenies (79 points)

Let k be a perfect field (so every extension of k is separable; this holds when $\operatorname{char}(k) = 0$ or k is a finite field, for example), fix an algebraic closure $\bar{k}$, and let E/k be an elliptic curve. For each $n \geq 0$ the field $k(E[n])$ obtained by adjoining the coordinates of every point in the n-torsion subgroup $E[n] := \{P \in E(\bar{k}) : nP = 0\}$ is the *n-torsion field* of E. For any point $P = (x : y : z) \in E(\bar{k})$ and automorphism $\sigma \in \operatorname{Gal}(\bar{k}/k)$ let $\sigma(P) := (\sigma(x) : \sigma(y) : \sigma(z))$.

(a) Show that for any $P \in E(\bar{k})$ and $\sigma \in \operatorname{Gal}(\bar{k}/k)$ we have $\sigma(P) \in E(\bar{k})$, and that for all $P, Q \in E(\bar{k})$ we have $\sigma(P+Q) = \sigma(P)+\sigma(Q)$. Conclude that the map $P \mapsto \sigma(P)$ defines a group action of $\operatorname{Gal}(\bar{k}/k)$ on $E(\bar{k})$ that commutes with addition, and that each $\sigma \in \operatorname{Gal}(\bar{k}/k)$ thus induces an automorphism of the group $E(\bar{k})$.

(b) Show that the action of $\operatorname{Gal}(\bar{k}/k)$ on $E(\bar{k})$ restricts to an action on $E[n]$. Conclude that $k(E[n])$ is a Galois extension of k.

(c) Give an explicit example of an elliptic curve E/k and a finite subgroup $G \subseteq E(\bar{k})$ for which the action of $\operatorname{Gal}(\bar{k}/k)$ in $E(\bar{k})$ does *not* restrict to an action on G; that is, exhibit a point $P \in G$ and an automorphism $\sigma \in \operatorname{Gal}(\bar{k}/k)$ for which $\sigma(P) \notin G$. Now give an example (possibly the same one) where the field extension of k obtained by adjoining the coordinates of every point $P \in G$ is not even a Galois extension.

(d) Show that for any finite subgroup G of $E(\bar{k})$ there is a separable isogeny $\phi\colon E \to E'$ defined over k with kernel G if and only if G is *Galois stable*, meaning that $\sigma(P) \in G$ for all $P \in G$ and $\sigma \in \operatorname{Gal}(\bar{k}/k)$, and that in this case the field $k(\ker \phi)$ obtained by adjoining the coordinates of every point $P \in \ker \phi$ to k is a Galois extension of k.

Let ℓ be an odd prime different from the characteristic of k.

(e) Show that $\operatorname{Aut}(E[\ell]) \simeq \operatorname{GL}_2(\mathbb{F}_\ell)$, and that the action of $\operatorname{Gal}(\bar{k}/k)$ on $E[\ell]$ induces an injective group homomorphism $\rho_\ell\colon \operatorname{Gal}(k(E[\ell])/k) \to \operatorname{GL}_2(\mathbb{F}_\ell)$. Use this to show that the degree of the field extension $k(E[\ell])/k$ is less than ℓ^4.

(f) Show that when k is a finite field the degree of $k(E[\ell])/k$ is actually less than ℓ^2.

The isomorphism you proved in (e) is not unique; for the sake of concreteness, let us view $\operatorname{GL}_2(\mathbb{F}_\ell)$ as acting on column vectors by multiplication on the left.

(g) The ℓ-division $\psi_\ell(x)$ of E has degree $(\ell^2-1)/2$ (see Problem 4). Its splitting field L is necessarily a subfield of the ℓ-torsion field $k(E[\ell])$. Show that $[k(E[\ell])\colon L] \leq 2$.

(h) Show that $[k(E[\ell])\colon L] = 2$ if and only if the image of ρ_ℓ contains $-I \in \operatorname{GL}_2(\mathbb{F}_\ell)$.

We say that E *admits a rational ℓ-isogeny* if there exists an isogeny $\phi\colon E \to E'$ of degree ℓ that is defined over k.

(i) Show that whenever E admits a rational ℓ-isogeny the ℓ-division polynomial $\psi_\ell(x)$ has a factor of degree $(\ell-1)/2$. Does the converse hold? Show that if $\phi\colon E \to E'$ is a rational ℓ-isogeny then the field extension $k(\ker\phi)/k$ has degree less than ℓ.

(j) Show that E admits a rational ℓ-isogeny if and only if the image G_ℓ of $\mathrm{Gal}(k(E[\ell])/k)$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$ fixes a linear subspace of $\mathbb{F}_\ell^2$, in which case G_ℓ is conjugate to a subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$ and the degree of $k(E[\ell])/k$ is less than ℓ^3.

(k) Show that E has a rational point of order ℓ if and only if G_ℓ is conjugate to a subgroup of matrices $\left(\begin{smallmatrix}1&*\\0&*\end{smallmatrix}\right)$, in which case the degree of $k(E[\ell])/k$ is less than ℓ^2.

(l) Let m be the number of rational ℓ-isogenies admitted by E that have distinct kernels. Show that $m \in \{0,1,2,\ell+1\}$, with $m \ge 2$ if and only if G_ℓ is conjugate to a subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$, and $m = \ell+1$ if and only if G_ℓ is conjugate to a subgroup of scalar matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Problem 6. Survey (3 points)

Complete the following survey by rating each of the problems you attempted on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			
Problem 4			
Problem 5			

Also, please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast"), and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
2/25	Isogenies and division polynomials				
2/27	Isogenies and endomorphisms				

Feel free to record any additional comments you have on the problem sets or lectures.

References

[1] D. Doud, *A procedure to calculate torsion of elliptic curves over $\mathbb{Q}$*, Manuscripta Mathematica **95** (1998), 463–469.

[2] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, third edition, Cambridge University Press, 2013.

[3] E. Lutz, *Sur l'equation $y^2 = x^3 - ax - b$ dans les corps p-adic*, J. Reine Angew. Math. **177** (1937), 237–247.

[4] T. Nagell, *Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre*, Wid. Akad. Skrifter Oslo I **1** (1935).

[5] L. Washington, *Elliptic curves: Number theory and cryptography*, second edtion, CRC press, 2008.

18.783 Elliptic Curves
Spring 2019