Romanoff's theorem and elliptic curves

Artyom Radomskii

HSE University

April 4, 2025

Elliptic curves

An *elliptic curve* is given by an equation of the form

$$E: \ y^2 = x^3 + Ax + B, \tag{1}$$

with the one further requirement that the *discriminant*

$$\Delta = 4A^3 + 27B^2$$

should not vanish. The discriminant condition ensures that the cubic polynomial $P(x) = x^3 + Ax + B$ has distinct (complex) roots. For convenience, we shall generally assume that the coefficients A and B are integers.

One of the properties that make an elliptic curve E such a fascinating object is the existence of a composition law that allows us to 'add' points to one another. Let us consider the real solutions of (1) as points in the plane. Let P and Q be distinct points on E and let L be the line through P and Q. Then the fact that E is given by an equation (1) of degree 3 means that L intersects E in three points. Two of these points are P and Q. If we let R denote the third point in $L \cap E$, then the sum of P and Q is defined by

$$P + Q = (\text{the reflection of } R \text{ across the } x\text{-axis}).$$

In order to add P to itself, we let Q approach P, so L becomes the tangent line to E at P.

We define the negation of a point $P = (x, y)$ to be its reflection across the x-axis

$$-P = (x, -y).$$

The line L through P and $-P$ intersects E in only these two points, so there is no third point R to use in the addition law. To remedy these situation, we adjoin an idealized point $\mathcal{O}$ to the plane. This point $\mathcal{O}$ is called the *point at infinity*. The special rules relating to the point $\mathcal{O}$ are

$$P + (-P) = \mathcal{O} \quad \text{and} \quad P + \mathcal{O} = \mathcal{O} + P = P$$

for all points P on E.

Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points on E, $Q \neq P$, $Q \neq -P$. It can be shown that $P + Q = (x_{P+Q}, y_{P+Q})$, where

$$x_{P+Q} = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q,$$

$$y_{P+Q} = -\frac{y_Q - y_P}{x_Q - x_P}\left(\left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q\right) - \frac{y_P x_Q - y_Q x_P}{x_Q - x_P}.$$

If $Q = P$, then (*the duplication formula*)

$$x_{2P} = \frac{x_P^4 - 2Ax_P^2 - 8Bx_P + A^2}{4x_P^3 + 4Ax_P + 4B},$$

$$y_{2P} = -\frac{3x_P^2 + A}{2y_P}\left(\frac{x_P^4 - 2Ax_P^2 - 8Bx_P + A^2}{4x_P^3 + 4Ax_P + 4B}\right) - \frac{-x_P^3 + Ax_P - 2B}{2y_P}.$$

It can be shown that

$$P + Q = Q + P \quad \text{for all } P, Q \in E.$$
$$(P + Q) + R = P + (Q + R) \quad \text{for all } P, Q, R \in E.$$

Special cases of the duplication and composition law on elliptic curves, described algebraically, date back to Diophantus, but it appears that the first geometric description via secant lines is due to Newton.

Let k be a field and E be an elliptic curve given by an equation

$$y^2 = x^3 + Ax + B,$$

whose coefficients A and B are in a field k. We define

$$E(k) = \left\{(x, y) \in k^2 : y^2 = x^3 + Ax + B\right\} \cup \{\mathcal{O}\}.$$

Let p be a prime. By $\mathbb{F}_p$ we denote the field of classes of residues modulo p. Let E be an elliptic curve given by an equation

$$y^2 = x^3 + Ax + B,$$

whose coefficients A and B are integers with $\Delta = 4A^3 + 27B^2 \neq 0$. Then, by definition,

$$E(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p^2 : y^2 \equiv x^3 + Ax + B \pmod{p}\right\} \cup \{\mathcal{O}\}.$$

If A and B are in a field k (with char $k \neq 2, 3$) and if the coordinates of P and Q are in k, then the coordinates of $P \pm Q$ are also in k. We obtain

Theorem

Let k be a field with char $k \neq 2, 3$. *Let E be an elliptic curve given by an equation*

$$y^2 = x^3 + Ax + B,$$

whose coefficients A and B are in a field k with $\Delta = 4A^3 + 27B^2 \neq 0$ in k. Then the sum and difference of two points in $E(k)$ is again in $E(k)$, so $E(k)$ is a commutative group.

This theorem was first observed by Poincaré, *Jour. Math. Pures Appl.* 7 (1901).

Let us consider

$$E_1 : \ y^2 = x^3 + 7, \qquad E_2 : \ y^2 = x^3 - 43x + 166,$$
$$E_3 : \ y^2 = x^3 - 2, \qquad E_4 : \ y^2 = x^3 + 17.$$

The curve E_1 has no rational points, so $E_1(\mathbb{Q}) = \{\mathcal{O}\}$. $E_2(\mathbb{Q})$ is a finite group with 7 elements

$$E_2(\mathbb{Q}) = \{(3, \pm 8), (-5, \pm 16), (11, \pm 32), \mathcal{O}\}.$$

The group $E_3(\mathbb{Q})$ is freely generated by the single point $P = (3, 5)$, in the sense that every point in $E_3(\mathbb{Q})$ has the form nP for a unique $n \in \mathbb{Z}$. Similarly, the points $P = (-2, 3)$ and $Q = (2, 5)$ freely generate $E_4(\mathbb{Q})$ in the sense that every point in $E_4(\mathbb{Q})$ has the form $mP + nQ$ for a unique pair of integers $m, n \in \mathbb{Z}$. We note that none of these assertions concerning E_1, E_2, E_3, E_4 is obvious.

Repeated addition and negation allows us to 'multiply' points of E by an arbitrary integer m. This function from E to itself is called the *multiplication-by-m* map,

$$\phi_m : E \to E, \quad \phi_m(P) = mP = \mathsf{sign}(m)(P + \cdots + P)$$

(the sum contains $|m|$ terms). By convention, we also define $\phi_0(P) = \mathcal{O}$.

The multiplication-by-m map is defined by rational functions. Maps $E \to E$ defined by rational functions and sending $\mathcal{O}$ to $\mathcal{O}$ are called *endomorphisms* of E. Endomorphisms can be added and multiplied according to the rules

$$(\phi + \psi)(P) = \phi(P) + \psi(P) \text{ and } (\phi\psi)(P) = \phi(\psi(P)),$$

and one can show that with these operations, the set of endomorphisms $\mathrm{End}(E)$ becomes a ring.

For most elliptic curves (over the field of complex numbers $\mathbb{C}$), the only endomorphisms are the multiplication-by-m maps, so for these curves $\mathrm{End}(E) = \mathbb{Z}$. Curves that admit additional endomorphisms are said to have *complex multiplication*.

Examples of such curves include

$$E_5 : y^2 = x^3 + Ax,$$

which has the endomorphism $\phi_i(x, y) = (-x, iy)$, and

$$E_6 : y^2 = x^3 + B,$$

which has the endomorphism $\phi_\rho(x, y) = (\rho x, y)$ (here $i = \sqrt{-1}$ and $\rho = e^{(2/3)\pi i}$). These endomorphisms satisfy

$$\phi_i^2(P) = -P \quad \text{and} \quad \phi_\rho^2(P) + \phi_\rho(P) + P = \mathcal{O}.$$

One can show that $\mathrm{End}(E_5)$ is isomorphic to the ring of Gaussian integers (i.e. $a + bi$, $a, b \in \mathbb{Z}$) and that $\mathrm{End}(E_6)$ is the ring of integers in $\mathbb{Q}(\rho)$ (i.e. $a + b\rho$, $a, b \in \mathbb{Z}$).

Let $\pi(x)$ denote a number of primes not exceeding x. We prove the following result.

Theorem 1 (A. Radomskii)

Let E be an elliptic curve given by an equation

$$y^2 = x^3 + Ax + B,$$

where A and B are integers with $\Delta = 4A^3 + 27B^2 \neq 0$. Suppose that E does not have complex multiplication. Let s be a positive integer and x be a real number with $x \geq 2$. Then

$$\pi(x) \leq \sum_{p \leq x} \left(\frac{\#E(\mathbb{F}_p)}{\varphi(\#E(\mathbb{F}_p))} \right)^s \leq C(E, s)\pi(x),$$

where $C(E, s) > 0$ is a constant, depending only on an elliptic curve E and a number s.

SKETCH OF THE PROOF. We used the following result of David and Wu, *Canad. J. Math.* 64 (2012).

Theorem 2 (David and Wu)

Suppose that E does not have complex multiplication. Then for integers a and $t \geq 1$ we have

$$\#\{p \leq x : \#E(\mathbb{F}_p) \equiv a \pmod{t}\} \leq$$
$$\leq C(E)\left(\frac{\pi(x)}{\varphi(t)} + x \cdot \exp(-ct^{-2}\sqrt{\ln x})\right),$$

if $\ln x \geq t^{12} \ln t$. Here $c > 0$ is an absolute constant, $C(E) > 0$ is a constant depending only on an elliptic curve E.

And applied the following

Theorem 3 (A. Radomskii)

Let α be a real number with $0 < \alpha < 1$. Then there is a constant $C(\alpha) > 0$, depending only on α, such that the following holds. Let M be a real number, $a_1, \dots, a_N$ be positive integers (not necessarily distinct) with $a_n \leq M$ for all $1 \leq n \leq N$. We define

$$\omega(d) = \#\{1 \leq n \leq N : a_n \equiv 0 \pmod{d}\}$$

for any positive integer d. Let s be a positive integer. Then

$$\sum_{n=1}^{N} \left(\frac{a_n}{\varphi(a_n)} \right)^s \leq \left(C(\alpha)\right)^s \left(N + \sum_{p \leq (\ln M)^\alpha} \frac{\omega(p)(\ln p)^s}{p} \right).$$

2. On Romanoff's theorem

Let a be an integer with $a \geq 2$. We will focus on the representation of positive integers n in the form

$$n = p + a^j,$$

where p is a prime and j is a non-negative integer.

We have

$$\#\{p \leq x\} \sim \frac{x}{\ln x} \quad \text{and} \quad \#\{j \geq 0 : a^j \leq x\} \sim \frac{\ln x}{\ln a}.$$

If we restrict ourselves to prime numbers p not exceeding $x/2$ and non-negative integers j such that $a^j \leq x/2$, then it is clear that the number of solutions of the inequality

$$p + a^j \leq x$$

is at least cx. If "on average" not too many of the numbers $p + a^j$ represent equal numbers, then we can expect that at least cx of numbers n not exceeding x can be represented in the form $p + a^j$. This statement was proven by N. P. Romanov in 1934.

Theorem (N. P. Romanoff)

Let $a \geq 2$ be an integer. Then there is a constant $c(a) > 0$ depending only on a such that

$$\#\{1 \leq n \leq x : \ n = p + a^j \text{ for some } p \in \mathbb{P} \text{ and } j \in \mathbb{Z}_{\geq 0}\} \geq c(a)x$$

for any real number $x \geq 3$.

We recall that a set $A \subset \mathbb{N}$ has *positive density* if there exist a constant $\alpha > 0$ such that

$$\#(A \cap [1, x]) \geq \alpha x$$

for all $x \geq 1$.

It follows from Romanoff's theorem that the set

$$A = \{n : n = p + a^j \text{ for some } p \in \mathbb{P} \text{ and } j \in \mathbb{Z}_{\geq 0}\} \cup \{1\}$$

has positive density.

Consider the case $a = 2$. Let

$$\mathcal{R} = \{n \in \mathbb{N} : n = p + 2^j \text{ for some } p \in \mathbb{P} \text{ and } j \in \mathbb{Z}_{\geq 0}\}.$$

It follows from Romanoff's theorem that

$$\theta := \liminf_{x \to \infty} \frac{\#(\mathcal{R} \cap [1, x])}{x} > 0.$$

The constant θ is called *the Romanoff constant*. The Romanoff constant has been studied by many mathematicians and the best result $\theta > 0.09368$ is due to Pintz, *Acta Math. Hungar.*, 112 (2006).

Friedlander and Iwaniec showed that there are infinitely many integers $n \in \mathcal{R}$ having at most two prime factors.

Lu obtained a quantitative version of this result, *J. Number Theory* 204 (2019).

Sketch of proof of Romanoff's theorem. Let $r(n)$ denote the number of solutions of $n = p + a^j$. It is easy to see that the number of solutions of a system

$$p + a^j = p_1 + a^{j_1} \leq x,$$

where p_1, p_2 are primes, and j_1, j_2 are non-negative integers, is equal to

$$\sum_{n \leq x} r(n)^2.$$

Romanoff showed that

$$\sum_{n \leq x} r(n)^2 \leq c_2(a)x.$$

By Cauchy's inequality,

$$c_1(a)x \le \sum_{n\le x} r(n) = \sum_{\substack{n\le x\\ r(n)>0}} r(n) \le \Big(\sum_{\substack{n\le x\\ r(n)>0}} r(n)^2\Big)^{1/2}\Big(\sum_{\substack{n\le x\\ r(n)>0}} 1\Big)^{1/2}$$
$$\le \big(c_2(a)x\big)^{1/2}\Big(\sum_{\substack{n\le x\\ r(n)>0}} 1\Big)^{1/2}.$$

We obtain

$$\sum_{\substack{n\le x\\ r(n)>0}} 1 \ge c(a)x.$$

We proved the following result.

Theorem 4 (A. Radomskii)

Let a and d be integers with $a \geq 2$ and $d \geq 1$. Let $f(n) = b_d n^d + \ldots + b_0$ be a polynomial with integer coefficients such that $b_d > 0$ and $f : \mathbb{N} \to \mathbb{N}$. Then there exist positive constants $c_1 = c_1(f, a)$, $c_2 = c_2(f, a)$, and $x_0 = x_0(f, a)$ depending only on f and a such that

$$\frac{c_1 x}{(\ln x)^{1-1/d}} \leq \#\{1 \leq n \leq x : n = p + a^{f(j)} \text{ for some } p \in \mathbb{P} \text{ and } j \in \mathbb{N}\} \leq \frac{c_2 x}{(\ln x)^{1-1/d}}$$

for any real number $x \geq x_0$.

Theorem 5 (A. Radomskii)

Let E be an elliptic curve given by an equation $y^2 = x^3 + Ax + B$, where A and B are integers satisfying $\Delta = 4A^3 + 27B^2 \neq 0$. Suppose that E does not have complex multiplication. For any positive integer n, we put

$$r(n) = \#\{(p, q) \in \mathbb{P}^2 : \ p + \#E(\mathbb{F}_q) = n\}.$$

Then there are constants $x_0 > 0$, $c_1 > 0$, $c_2(E) > 0$, where x_0 and c_1 are absolute constants, $c_2(E)$ is a constant depending only on E, such that

$$\#\left\{1 \leq n \leq x : \ r(n) \geq c_1 \frac{x}{(\ln x)^2}\right\} \geq c_2(E)x$$

for any real number $x \geq x_0$.

Theorem 6 (A. Radomskii)

Let $d \geq 2$ be an integer, and let

$$f(n) = b_d n^d + \ldots + b_0$$

be a polynomial with integer coefficients, $b_d > 0$. For any positive integer n, we put

$$r(n) = \#\{(p, j) \in \mathbb{P} \times \mathbb{N} : \ p + f(j) = n\}.$$

Then there are constants $c_1 > 0$, $c_2 > 0$, $x_0 > 0$ depending only on f such that

$$\# \left\{ 1 \leq n \leq x : \ r(n) \geq c_1 \frac{x^{1/d}}{\ln x} \right\} \geq c_2 x$$

for any real number $x \geq x_0$.

Corollary 1 (A. Radomskii)

Let $d \geq 2$ be an integer. For any positive integer n, we put

$$r(n) = \#\{(p, j) \in \mathbb{P} \times \mathbb{N} : \ p + j^d = n\}.$$

Then there are constants $c_1(d) > 0$ and $c_2(d) > 0$ depending only on d such that

$$\# \left\{ 1 \leq n \leq x : \ r(n) \geq c_1(d) \frac{x^{1/d}}{\ln x} \right\} \geq c_2(d) x$$

for any real number $x \geq 3$.

Corollary 1 extends a result of Romanoff which showed the inequality

$$\#\{1 \leq n \leq x : n = p + j^d \text{ for some } p \in \mathbb{P} \text{ and } j \in \mathbb{N}\} \geq c(d)x.$$

We obtain Theorems 4–6 from the following general result.

Theorem 7 (A. Radomskii)

Let $A = \{a_n\}_{n=1}^{\infty}$ *be a sequence of positive integers (not necessarily distinct) and let*

$$N_A(x) = \#\{j \in \mathbb{N} : \ a_j \leq x\},$$
$$\operatorname{ord}_A(n) = \#\{j \in \mathbb{N} : \ a_j = n\}, \ n \in \mathbb{N},$$
$$\rho_A(x) = \max_{n \leq x} \operatorname{ord}_A(n).$$

Suppose that $\operatorname{ord}_A(n) < +\infty$ *for any positive integer* n.

Theorem (continue)

Suppose also that there are constants $\gamma_1 > 0$, $\gamma_2 > 0$, $\alpha > 0$, $x_0 \geq 10$ *such that*

$$N_A(x) > 0,$$

$$N_A\left(\frac{x}{2}\right) \geq \gamma_1 N_A(x),$$

$$\sum_{\substack{k\in\mathbb{N}:\\ a_k<x}} \sum_{p\leq(\ln x)^\alpha} \frac{\#\{j \in \mathbb{N} : a_k < a_j \leq x \text{ and } a_j \equiv a_k \pmod p\} \ln p}{p}$$

$$\leq \gamma_2 \big(N_A(x)\big)^2$$

for any real number $x \geq x_0$. *Given any positive integer* n, *let*

$$r(n) = \#\{(p, j) \in \mathbb{P} \times \mathbb{N} : \ p + a_j = n\}.$$

Theorem (continue)

Then there are constants $c_1 = c_1(\gamma_1) > 0$ *and* $c_2 = c_2(\gamma_1, \gamma_2, \alpha) > 0$ *depending only on* γ_1 *and* γ_1, γ_2, α, *respectively, such that*

$$\#\left\{1 \le n \le x : \ r(n) \ge c_1 \frac{N_A(x)}{\ln x}\right\} \ge c_2 x \frac{N_A(x)}{N_A(x) + \rho_A(x) \ln x}$$

for any real number $x \ge x_0$. *In particular,*

$$\begin{aligned} &\#\{1 \le n \le x : n = p + a_j \text{ for some } p \in \mathbb{P} \text{ and } j \in \mathbb{N}\} \\ &\qquad \ge c_2 x \frac{N_A(x)}{N_A(x) + \rho_A(x) \ln x}. \end{aligned}$$

Thank you for your attention!