Problem Set 5 – Arithmetic Geometry, Frank Thorne (thorne@math.sc.edu)

Due Monday, April 6, 2020

Choose one. The first problem has an analytic number theory flavor, and the second has an algebraic geometry flavor. It is intended that both be accessible with no special background.

(1) A special case of **Schanuel's Theorem** says that

$$C(\mathbb{P}^N(\mathbb{Q}), B) := \{P \in \mathbb{P}^N(\mathbb{Q}) \ : \ H(P) \leq B\} \sim \frac{2^N}{\zeta(N+1)} B^{N+1}.$$

The following exercise outlines a proof of this theorem.

(a) Prove that the set to be counted is in an exactly 2-to-1 correspondence with $N+1$-tuples of integers $(x_0, x_1, \cdots, x_N)$, where $x_i \in [-B, B]$ for each i, and the x_i do not all share a common factor.

(b) Write $C(N, B)$ for the number of $N+1$-tuples of integers $(x_0, x_1, \cdots, x_N)$, where $x_i \in [-B, B]$ for each i (but with no 'no common factor' condition). Prove that

$$C(N, B) = (2B)^{N+1} + O(B^N).$$

(Be sure to justify that the constant implied by the O-notation is in fact independent of B. It may depend on N however. You might wish to be especially careful and actually compute the constant implied in the error term.)

(c) Let $\mu(d)$ be the *Möbius function*, equal to $(-1)^{\omega(d)}$ if d is squarefree, where $\omega(d)$ denotes the number of prime factors of d, and equal to zero otherwise.

Prove that, for any positive integer n, $\sum_{d|n} \mu(d)$ is equal to 1 if $n = 1$ and zero otherwise.

(Hint: the sum can be rewritten as $\prod_{p|n}(1 + \mu(p))$, where the product is over all primes dividing n. Why is this?)

(d) Write $C(N, B, d)$ for the number of $N+1$-tuples of integers $(x_0, x_1, \cdots, x_N)$, where $x_i \in [-B, B]$ for each i, such that d divides all the x_i. Explain why $C(N, B, d) = C(N, B/d)$ and deduce an estimate for $C(N, B, d)$.

(e) Prove that

$$C(\mathbb{P}^N(\mathbb{Q}), B) = \sum_{d=1}^{B} \mu(d) C(N, B, d)$$

and use your previous estimates to conclude that

$$C(\mathbb{P}^N(\mathbb{Q}), B) = 2^N B^{N+1} \sum_{d=1}^{B} \frac{\mu(d)}{d^{B+1}} + o(B^{N+1}).$$

(f) Prove that

$$\sum_{d=B+1}^{\infty} \frac{\mu(d)}{d^{N+1}} = o(1)$$

and that

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^{N+1}} = \frac{1}{\zeta(B+1)}.$$

Conclude that

$$\sum_{d=1}^{B} \frac{\mu(d)}{d^{N+1}} = \frac{1}{\zeta(N+1)} + o(1).$$

(g) Conclude the statement of Schanuel's theorem.

Note that Schanuel proved his result where $\mathbb{Q}$ is replaced with any number field, where the analysis became more difficult. For definitions of height functions in number fields, see Chapter 8.5 of Silverman.

(2) For an algebraic variety $V \subseteq \mathbb{P}^N$, define

$$C(V, B) := \#\{P \in V(\mathbb{Q}) \ : \ H(P) \leq B\}.$$

For each integer $n \geq 1$, define a morphism $\phi_n : \mathbb{P}^1 \to \mathbb{P}^n$ by

$$\phi_n([x : y]) = [x^n : x^{n-1}y : x^{n-2}y^2 : \cdots : y^n],$$

and let $V_n \subseteq \mathbb{P}^n$ be the image of ϕ_n.

(a) Prove, for each n, that V_n (In other words, find one or more polynomials f_i, such that V_n consists precisely of those $[t_0 : t_1 : \cdots : t_n]$ for which all of the $f_i(t_0, \cdots, t_n)$ vanish.)

(b) Construct a morphism from V_n to $\mathbb{P}^1$ which inverts ϕ_n. This proves that ϕ_n is an isomorphism from $\mathbb{P}^1$ to ϕ_n.

In addition, prove that this isomorphism acts bijectively on the sets of rational points $\mathbb{P}^1(\mathbb{Q})$ and $V_n(\mathbb{Q})$.

(c) If $P \in \mathbb{P}^1(\mathbb{Q})$, prove a relationship between $H(P)$ and $H(\phi_n(P))$.

(d) Using the above, and also the result of the first problem, prove an asymptotic formula for $C(V_n, B)$.

It is not necessary here to have solved the first problem! Just to understand the statement of the result.