Dirichlet theorem

Mentor: : Avraham Aizenbud
Position: Ph.D. student
Age: 22 Gender: Male
Spoken languages: Hebrew, Russian, English
E-mail: aizenr@yahoo.com
Supervisor: : Prof. J.Bernstein & Prof. V.Berkovich

Abstract

Our aim is to prove Dirichlet theorem: "Any arithmetic sequence $\{an+b\}$ has infinitely many primes in it (if a,b are coprime)". The thing that makes this thorem so interesting is its proof rather than its formulation. It involves most of the subjects of 19th centuary number theory. Also it historically gave raise to a half of 20th century number theory and some other parts of mathematics such as representation theory and commutative algebra. Another benefit of this guided research will be acquaintance with some concepts of modern algebra. On our way to prove this theorem we will prove the following famous theorems from number theory:

1. Euclid theorem: "there exist infinitely many primes".
2. The main theorem of arithmetic: "any integer can be uniquely decomposed into a product of primes".
3. Euler theorem: "$\sum_{p-prime} \frac{1}{p} = \infty$".
4. The small Fermat theorem: "$a^p \equiv a \, mod \; p$".
5. Euler Theorem: "$a^{\varphi(n)} \equiv 1 mod \, n$ for $gcd(a,n) = 1$".
6. Quadratic reciprocity: "$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$ for primes $p,q \neq 2$".
7. Classification of sums of two integral squares: "a number can be represented as a sum of two integral squares if and only if all the odd primes that occur in its decomposition in odd degree are of the form $4n+1$."

If we shall have time we may also prove:

8. The main theorem of Algebra: “any polynomial with complex coefficients has at least one complex root.”
9. Varing theorem: “any integer number can be represented as a sum of four integral squares.”

I’ll try to divide these topics into small enough problems, such that the students will be able to solve them by themselves. The work will be similar to a guided research rather than a theoretical study.

No preliminary knowledge is required except school material. However some acquaintance with basic concepts of linear algebra, group theory, number theory and calculus can be helpful.

Explanations on notation

- $a^p \equiv a \bmod p$ means that $a = b + nk$ for some integer k;
- $gcd(a,b)$ is the greatest common divisor of a and b;
- $\varphi(n)$ is the number of integers $0 < k < n$ such that $gcd(n,k) = 1$;
- $\left(\dfrac{n}{p}\right) = \begin{cases} 0, n \equiv 0 \bmod p \\ 1, n \equiv k^2 \bmod p \\ -1, otherwise \end{cases}$.

Background Bibliography

1. *H. Davenport*. “The Higher Arithmetic.” Chapters: Introduction, 1.1, 1.2, 1.3, 1.6, 1.7, 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 3.3, 5.1, 5.2.

Advanced Reading

1. *H. Davenport.* “The Higher Arithmetic.” The rest of chapters 1, 2, 3, 5.
2. *Harvey Cohn.* “Advanced number theory.” Chapter 8.

Specifications of the Work

☐ Work with organisms. Species:

☐ Work with computers

☐ Work with laser

☐ Work with advanced instrumentation

☐ Wet-lab

☒ Theoretical work

☐ Other. Specify:

Essential requested experience

☐ Programming languages. Specify:

☐ None

☒ Some acquaintance with basic concepts of linear algebra, group theory, number theory and calculus can be helpful.

Timetable

Day 1: Euclid theorem, the main theorem of arithmetic, rings, domains, Euclidian domains, Euclid algorithm, principal domains, unique factorization domains, prime and maximal ideals.

Day 2: Geometric series, Riemann Zeta function, Euler product formula, Linear approximation, Euler theorem, Dirichlet characters, Dirichlet L-function.

Day 3: Congruence, the small Fermat theorem, Abelian groups, Lagrange theorem, Euler thorem.

Day 4: Complex numbers, De-Moiver formula, Euler formula, roots of unity, Bezout theorem, the main theorem of algebra, Viette theorem.

Day 5: Harmonic analyses on finite Abelian groups (Discrete Fourier Transform).

Day 6: Deducing Dirichlet theorem from $L(1,\chi) \neq 0$ for quadratic χ.

Day 7: Chinese remainder theorem, primitive roots.

Day 8: Quadratic characters, Legendre symbol, quadratic reciprocity, Gauss sum, finite fields, Frobenius automorphism, proof of quadratic reciprocity.

Day 9: Gauss numbers, classification of sums of two integral squares, quaternions, sums of 4 integral squares.

Day 10: Dedekind Zeta function for UFD, proof of Dirichlet theorem for UFD case, Pell equation.

Day 11: Algebraic integers, quadratic Dedekind domains, unique factorisation into prime idiales, Dedekind Zeta function.

Day 12: Norms of idiales, Dedekind Zeta function, proof of Dirichlet theorem.

Day 13: Writing report