Number Theory

What is number theory?

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Summary

1. **Analytic Number Theory**
   - Prime counting
   - Partitions
2. **Geometry of Numbers**
   - Lattice points in convex bodies
3. **Arithmetric algebraic geometry**
   - Pythagorean tripples
4. **Connections to Algebra**
   - In the course!
   - Not in the course
5. **Elementary Number Theory**
   - Elementary?
6. **This course**
   - Literature
   - Lectures

Summary

1. **Analytic Number Theory**
   - Prime counting
   - Partitions
2. **Geometry of Numbers**
   - Lattice points in convex bodies
3. **Arithmetric algebraic geometry**
   - Pythagorean tripples
4. **Connections to Algebra**
   - In the course!
   - Not in the course
5. **Elementary Number Theory**
   - Elementary?
6. **This course**
   - Literature
   - Lectures

1. **Analytic Number Theory**
   - Prime counting
   - Partitions
2. **Geometry of Numbers**
   - Lattice points in convex bodies
3. **Arithmetic algebraic geometry**
   - Pythagorean tripples
4. **Connections to Algebra**
   - In the course!
   - Not in the course
5. **Elementary Number Theory**
   - Elementary?
6. **This course**
   - Literature
   - Lectures

1. **Analytic Number Theory**
   - Prime counting
   - Partitions
2. **Geometry of Numbers**
   - Lattice points in convex bodies
3. **Arithmetic algebraic geometry**
   - Pythagorean tripples
4. **Connections to Algebra**
   - In the course!
   - Not in the course
5. **Elementary Number Theory**
   - Elementary?
6. **This course**
   - Literature
   - Lectures

Summary

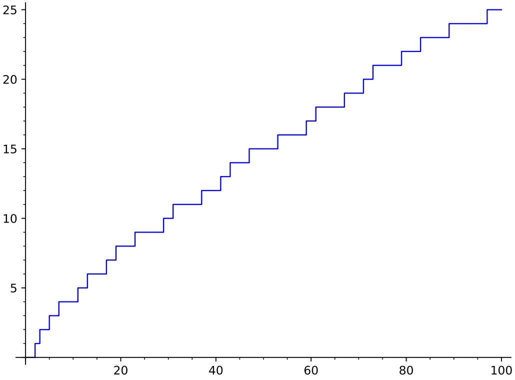
1. **Analytic Number Theory**
   - Prime counting
   - Partitions
2. **Geometry of Numbers**
   - Lattice points in convex bodies
3. **Arithmetic algebraic geometry**
   - Pythagorean tripples
4. **Connections to Algebra**
   - In the course!
   - Not in the course
5. **Elementary Number Theory**
   - Elementary?
6. **This course**
   - Literature
   - Lectures

Summary

1. **Analytic Number Theory**
   - Prime counting
   - Partitions
2. **Geometry of Numbers**
   - Lattice points in convex bodies
3. **Arithmetic algebraic geometry**
   - Pythagorean tripples
4. **Connections to Algebra**
   - In the course!
   - Not in the course
5. **Elementary Number Theory**
   - Elementary?
6. **This course**
   - Literature
   - Lectures

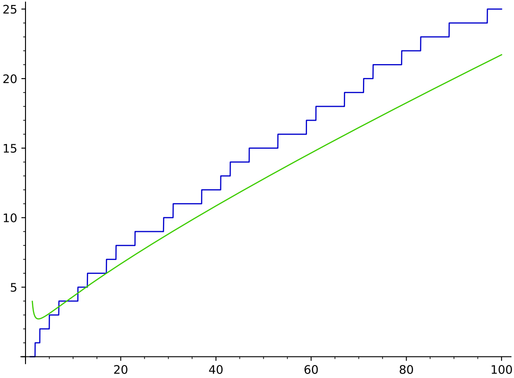
Definition

$\pi(x) = \sum_{k \leq x} \mathrm{IsPrime}(x)$



Theorem (Hadamard, de la Vallée Poussin)

$\pi(x) \sim \frac{x}{\log x}$ *as* $x \to \infty$.



Definition

Prime density function $\mathbf{p}(x) = \pi(x)/x$.

Prime number theorem: $\mathbf{p}(x) \sim 1/\log(x)$.

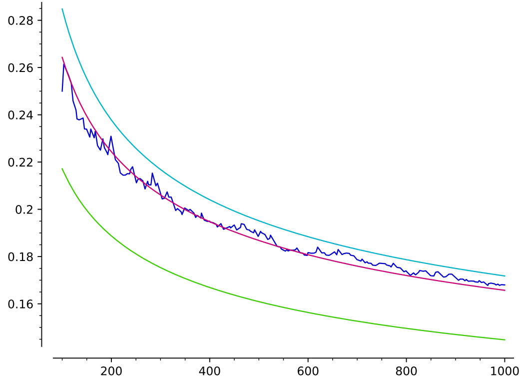
Example

Probability that a positive integer ≤ 1000 is prime is
$\mathbf{p}(1000) \approx \frac{1}{\log(1000)} = 0.145$. Actually 168 primes ≤ 1000.

Theorem

$\mathbf{p}(x) = \sum_{k=1}^{n-1} \frac{(k-1)!}{\log(x)^k} + \mathcal{O}\left(\frac{(n-1)!}{(log(x)^n)}\right)$ *as* $x \to \infty$.

Check the first 3 approximations, from 100 to 1000:



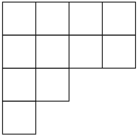
Definition

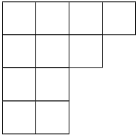
n positive integer. A partition $\lambda \vdash n$ is a non-increasing sequence of positive integers that sum to n.

Example

$\lambda = (3, 3, 2, 1, 1, 1) \vdash 11$. There are 7 partitions of 5, namely

$$[[5], [4, 1], [3, 2], [3, 1, 1], [2, 2, 1], [2, 1, 1, 1], [1, 1, 1, 1, 1]]$$

- The *Young Diagram* of a partition is a pile of boxes, the size of the parts.
- The conjugate of a partition is obtained by turning the diagram around.
- $$\lambda = (4, 4, 2, 1) =$$ 

  $$\lambda^* = (4, 3, 2, 2) =$$ 
- Bijection between partitions with at most k parts and partsizes $\leq k$

- At most 4 parts, or partsize ≤ 4
- c_j counts nr such partitions of j
- $p_4(x) = \sum_{j \geq 0} c_j x^j$ generating function
- $p_4(x) = 1 + 1x + 2x^2 + 3x^3 + 5x^4 + 6x^5 + 9x^6 + \mathcal{O}\left(x^7\right)$
- Easy to see that $p_4(x) = \frac{1}{(x^4-1)(x^3-1)(x^2-1)(x-1)}$
- Partial fractions: $p_4(x) = \frac{x+1}{9\,(x^2+x+1)} + \frac{1}{8\,(x^2+1)} + \frac{1}{8\,(x+1)} - \frac{17}{72\,(x-1)} + \frac{1}{32\,(x+1)^2} + \frac{59}{288\,(x-1)^2} - \frac{1}{8\,(x-1)^3} + \frac{1}{24\,(x-1)^4}$
- Gives asymptotic growth of j'th coefficient

Definition

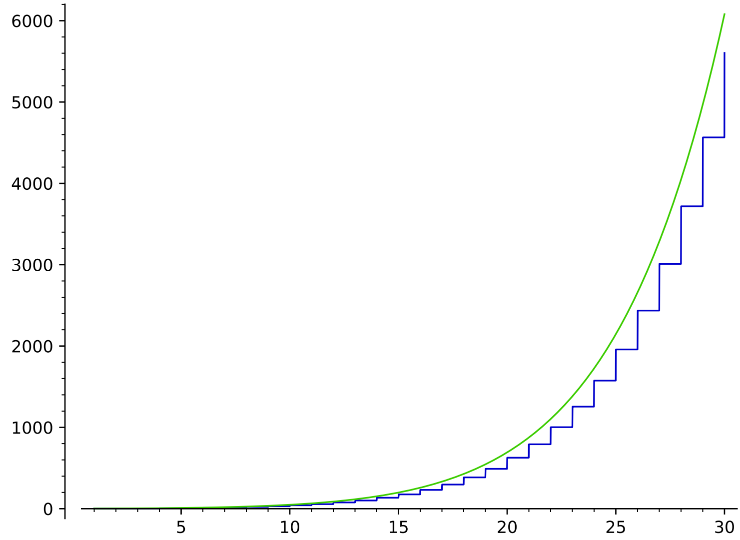
$p(n)$ is the number of partitions of n.

Lemma (Easy)

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}$$

Theorem (Hardy-Ramanujan)

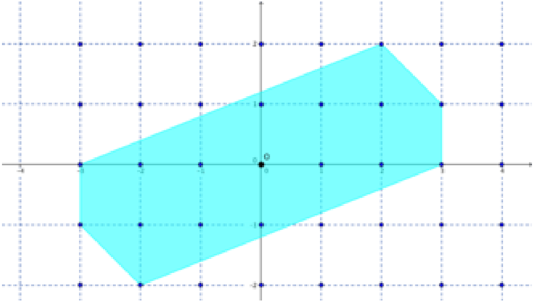
$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$ *as* $n \to \infty$.


6000
5000
4000
3000
2000
1000
0
5
10
15
20
25
30

G. H. Hardy

Theorem (Minkowski)

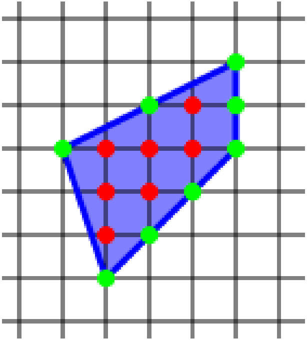
$D \subset \mathbb{R}^n$ convex, volume $> 2^n$, $-D = D$. Then D contains lattice point (other than the origin).



Theorem

A area of triangle, i nr interior lattice points, b nr boundary lattice points. Then

$$A = i + \frac{b}{2} - 1$$



$i = 7, b = 8, A = i + b/2 - 1 = 10$

We'll find the Pythagorean triples!

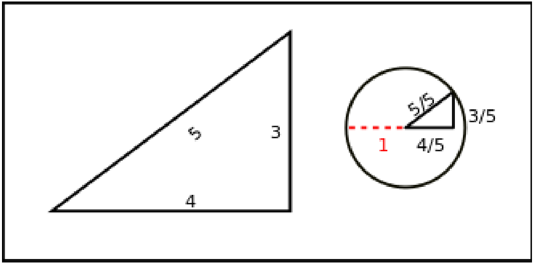
Theorem

The integer solutions to

$$a^2 + b^2 = c^2$$

correspond to rational point $(a/c, b/c)$ *on the unit circle; they can be parametrised by*

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2$$



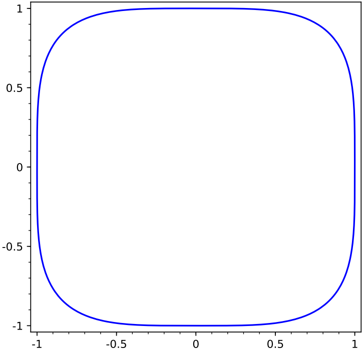
Too hard...

Theorem

For $n \geq 3$, the equation

$$x^n + y^n = z^n$$

has no non-trivial integer solutions.



Algebra-related things that we'll treat

- The group $\mathbb{Z}_n^*$ is cyclic when n a prime power
- $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ iff $\gcd(m, n) = 1$, same for $\mathbb{Z}_{mn}^*$.
- $\mathbb{Z}[i] = \{ a + bi | a, b \in \mathbb{Z} \}$ is a principal ideal domain
- Hensel lifting
- Möbius inversion

Algebra-related things that we'll treat

- The group $\mathbb{Z}_n^*$ is cyclic when n a prime power
- $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ iff $\gcd(m, n) = 1$, same for $\mathbb{Z}_{mn}^*$.
- $\mathbb{Z}[i] = \{ a + bi | a, b \in \mathbb{Z} \}$ is a principal ideal domain
- Hensel lifting
- Möbius inversion

Algebra-related things that we'll treat

- The group $\mathbb{Z}_n^*$ is cyclic when n a prime power
- $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ iff $\gcd(m, n) = 1$, same for $\mathbb{Z}_{mn}^*$.
- $\mathbb{Z}[i] = \{ a + bi | a, b \in \mathbb{Z} \}$ is a principal ideal domain
- Hensel lifting
- Möbius inversion

Algebra-related things that we'll treat

- The group $\mathbb{Z}_n^*$ is cyclic when n a prime power
- $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ iff $\gcd(m, n) = 1$, same for $\mathbb{Z}_{mn}^*$.
- $\mathbb{Z}[i] = \{ a + bi | a, b \in \mathbb{Z} \}$ is a principal ideal domain
- Hensel lifting
- Möbius inversion

Algebra-related things that we'll treat

- The group $\mathbb{Z}_n^*$ is cyclic when n a prime power
- $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ iff $\gcd(m, n) = 1$, same for $\mathbb{Z}_{mn}^*$.
- $\mathbb{Z}[i] = \{ a + bi | a, b \in \mathbb{Z} \}$ is a principal ideal domain
- Hensel lifting
- Möbius inversion

Algebra-related things that we'll skip

- Permutations, cycle type, partitions
- Algebraic number fields, their rings of integers, class number

Algebra-related things that we'll skip

- Permutations, cycle type, partitions
- Algebraic number fields, their rings of integers, class number

Elementary Number Theory

- “Elementary” means no analysis, no advanced algebra, no convalouted combinatoric machinery
- Does not mean that it is easy
- Theory developed “from scratch”
- Need: set theory, induction
- Useful: linear algebra

Elementary Number Theory

- "Elementary" means no analysis, no advanced algebra, no convalouted combinatoric machinery
- Does not mean that it is easy
- Theory developed "from scratch"
- Need: set theory, induction
- Useful: linear algebra

Elementary Number Theory

- “Elementary” means no analysis, no advanced algebra, no convalouted combinatoric machinery
- Does not mean that it is easy
- Theory developed “from scratch”
- Need: set theory, induction
- Useful: linear algebra

Elementary Number Theory

- "Elementary" means no analysis, no advanced algebra, no convalouted combinatoric machinery
- Does not mean that it is easy
- Theory developed "from scratch"
- Need: set theory, induction
- Useful: linear algebra

Elementary Number Theory

- “Elementary” means no analysis, no advanced algebra, no convalouted combinatoric machinery
- Does not mean that it is easy
- Theory developed “from scratch”
- Need: set theory, induction
- Useful: linear algebra

Textbook: Rosen

- "Elementary Number Theory" by Rosen
- Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- That's what the written exam will check
- I won't lecture on everything
- I'll also use "Elementary number Theory" by Stein (parts of)
- Hackman's manuscript good, as well
- Gaussian integers using Conrad's manuscript

Textbook: Rosen

- “Elementary Number Theory” by Rosen
- Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- That’s what the written exam will check
- I won’t lecture on everything
- I’ll also use “Elementary number Theory” by Stein (parts of)
- Hackman’s manuscript good, as well
- Gaussian integers using Conrad’s manuscript

Textbook: Rosen

- “Elementary Number Theory” by Rosen
- Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- That’s what the written exam will check
- I won’t lecture on everything
- I’ll also use “Elementary number Theory” by Stein (parts of)
- Hackman’s manuscript good, as well
- Gaussian integers using Conrad’s manuscript

Textbook: Rosen

- “Elementary Number Theory” by Rosen
- Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- That’s what the written exam will check
- I won’t lecture on everything
- I’ll also use “Elementary number Theory” by Stein (parts of)
- Hackman’s manuscript good, as well
- Gaussian integers using Conrad’s manuscript

Textbook: Rosen

- “Elementary Number Theory” by Rosen
- Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- That’s what the written exam will check
- I won’t lecture on everything
- I’ll also use “Elementary number Theory” by Stein (parts of)
- Hackman’s manuscript good, as well
- Gaussian integers using Conrad’s manuscript

Textbook: Rosen

- “Elementary Number Theory” by Rosen
- Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- That’s what the written exam will check
- I won’t lecture on everything
- I’ll also use “Elementary number Theory” by Stein (parts of)
- Hackman’s manuscript good, as well
- Gaussian integers using Conrad’s manuscript

Textbook: Rosen

- "Elementary Number Theory" by Rosen
- Chapt 1.5, 2.1, 3, 4.1-4, 5.1, 6, 7.1-4, 9, 11.1-4, 12, 13.1-4, 14.
- That's what the written exam will check
- I won't lecture on everything
- I'll also use "Elementary number Theory" by Stein (parts of)
- Hackman's manuscript good, as well
- Gaussian integers using Conrad's manuscript

Lectures, exercises

- 19 sessions
- Maybe discuss the exercises sometimes
- You should do plenty of exercises!
- List of recommended exercises at course home page, `http://courses.mai.liu.se/GU/TATA54/`

Lectures, exercises

- 19 sessions
- Maybe discuss the exercises sometimes
- You should do plenty of exercises!
- List of recommended exercises at course home page, http://courses.mai.liu.se/GU/TATA54/

Lectures, exercises

- 19 sessions
- Maybe discuss the exercises sometimes
- You should do plenty of exercises!
- List of recommended exercises at course home page, `http://courses.mai.liu.se/GU/TATA54/`

Lectures, exercises

- 19 sessions
- Maybe discuss the exercises sometimes
- You should do plenty of exercises!
- List of recommended exercises at course home page, `http://courses.mai.liu.se/GU/TATA54/`

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)

Course outline

1. Integers, divisibility
2. Unique factorization
3. Greatest common divisor, Linear Diophantine equations
4. Congruences, Chinese remainder theorem
5. Multiplicative order, Fermat, Euler
6. Arithmetical functions, Mobius inversion
7. Hensel lifting
8. Lagrange, Primitive roots, Discrete logarithms (2 lectures)
9. Quadratic Reciprocity (2 lectures)
10. Continued fractions (2 lectures)
11. Pell's equation
12. Sum of squares
13. Gaussian integers (2 lectures)