THEORY OF NUMBERS
SPRING 2019

Time and place: TF2 10:20–11:40am, Hill 009, Busch Campus
Instructor: Claire Burrin, claire.burrin@rutgers.edu, Hill Center 232
Office hour: Fridays, 2–3pm, Hill 232 (starting Feb 1)
Prerequisite: Math 300 – you are expected to be comfortable with mathematical proofs, the course will be fast-paced, and might be very hard if you enter it ill-prepared.
Final: May 15, 8:00–11:00 AM, Hill 009

Number theory studies the natural numbers, their indivisible atoms, a.k.a. the primes, and their fractions, the rational numbers. We will revisit (with proofs !) basic properties of numbers you encountered in school (a number is a multiple of 3 if the sum of its digits is a multiple of 3, $\sqrt{2}$ is not a fraction, every number decomposes uniquely as a product of primes, ...), and explore new fields of expression (modular arithmetic, continued fractions, quadratic forms) through the tools and tricks developed by the early modern number theorists Fermat (1607–1665), Euler (1707–1783), Lagrange (1736–1813), Legendre (1752–1833), Gauss (1777–1855)... Gauss said "Mathematics is the queen of the sciences, and number theory is the queen of mathematics." G.H. Hardy (*A Mathematician's Apology*) adamantly insisted on the "purity" of number theory, the intrinsic beauty of its fascinating questions bared from purposeful applications. (Hardy was an anti-war activist.) Contrarily to his belief, the advent of computers and advances in cryptology turned out to be a very fertile ground for number theory. Later on in the semester, we will learn applications of number theory in this context. (For more, take 348 Cryptography !) Given time, we will also address some interactions between of number theory and geometry (ruler and compass constructions, lattices, geodesics) and discuss some famous open problems (Goldbach's conjecture, the twin primes conjecture, Riemann hypothesis).

Textbook:
We will follow the organization of H. Davenport's *The Higher Arithmetic* (Cambridge University Press, 8th ed.) and present its results in class with full proofs and a more rigorous layout. Davenport's book is a great read, but is not written in the style of the usual college textbook. You should use it as a complementary lecture to the material presented in class, rather than the other way around. Note that it is your responsibility to stay informed of any announcement, syllabus or policy adjustment made during class.

Evaluation:
The grade make-up is 20% Homework, 20% each midterm, 40% the final. There will be no quizzes. Anyone absent from an exam without medical proof will receive a zero score. Exceptional circumstances will require a letter from a Dean. Students are expected to behave in accordance with the Code of Academic Integrity http://academicintegrity.rutgers.edu/academic-integrity-policy. Cases of cheating will be reported.

Tentative syllabus

Week	Topics
Jan 22, 25	Primes and factorization
Jan/Feb 29, 1	gcd, lcm, congruences
Feb 5, 8	Fermat–Euler theorem, Chinese remainder theorem
Feb 12, 15	Higher congruences, quadratic residues
Feb 19, 22	Primes of the form 4k+1, Midterm
Feb/Mar 26, 1	Legendre symbol, Gauss' lemma
Mar 5, 8	Quadratic reciprocity law
Mar 12, 15	Farey fractions, continued fractions
Mar 19, 22	Spring break
Mar 26, 29	Irrationals and continued fractions
Apr 2, 5	Midterm week
Apr 9, 12	Pell's equation, sums of squares
Apr 16, 19	Diophantine approximation
Apr 23, 26	Billiards, public-key cryptography
Apr/May 30, 3	PNT, RH, Gaussian integers

Homework assignments: Homework solutions are due on Fridays during the class. Late hand-ins will not be accepted. Remember that your solutions are to be read – and graded! – by someone. Therefore, you should make sure to explain your reasoning as clearly as possible, and to write neatly – this is also considered in the grading. Your homework solutions are expected to show some original effort; solutions that are directly copied from the internet will be sanctioned.

Homework 1, due Feb 1

(1) Show that if $a|b$ and $c|d$, then $ac|bd$.
(2) The Fibonacci sequence (F_n) is defined recursively by $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Prove by induction that
$$F_n = \frac{\gamma^n - \bar{\gamma}^n}{\sqrt{5}}$$
where $\gamma = \frac{1}{2}(1 + \sqrt{5})$, $\bar{\gamma} = \frac{1}{2}(1 - \sqrt{5})$.
(3) Find the prime factorization of 1729, 65536, and 22! (factorial).
(4) Factor 2501 using Fermat's difference of squares method.
(5) Let $n \in \mathbf{N}$. Show that if $2^n - 1$ is prime, then n is prime. Is the converse true ? Justify your answer with a proof or a counter-example.
(6) Show that there exist infinitely many primes of the form $6k - 1$.

Homework 2, due Feb 8

(1) If $n \in \mathbf{N}$ is not a perfect square, show that $\sqrt{n}$ is irrational.
(2) Show that for each $n \in \mathbf{N}$, $(n, n + 1) = 1$. How is this used in Euclid's proof that there are infinitely many primes ?
(3) Let $a, b, c \in \mathbf{N}$. Prove that $(ca, cb) = c(a, b)$.
Hint: To prove this identity, show that $(ca, cb)|c(a, b)$ *and* $c(a, b)|(ca, cb)$.
(4) Show that $a = b$ if and only if if $a \equiv b \bmod p$ for every prime p.

(5) Let p be a prime. Show that $(a+b)^p \equiv a^p + b^p \ (p)$.
Hint: Binomial expansion.
(6) Show that if the *alternating* sum of the digits of $n \in \mathbf{N}$ is a multiple of 11, then n is a multiple of 11.
(7) Show that if a prime $p \geq 3$ can be written as a sum of two squares, then $p \equiv 1 \ (4)$.

Homework 3, due Feb 15

(1) Let p be a prime. Show that $(p-2)! \equiv 1 \mod p$.
(2) Let $n \neq 4$ be composite. Prove that $(n-1)! \equiv 0 \mod n$.
(3) Solve the system of equations

$$\begin{aligned} x &\equiv 3 \mod 9 \\ x &\equiv 5 \mod 10 \\ x &\equiv 7 \mod 11 \end{aligned}$$

(4) What are the last two digits of 9^9 ?
(5) Show that

$$\varphi(2n) = \begin{cases} \varphi(n) & \text{if } n \text{ is odd} \\ 2\varphi(n) & \text{if } n \text{ is even.} \end{cases}$$

(6) Consider the gcd $d = (a, b)$. Show that $\varphi(d)\varphi(ab) = d\varphi(a)\varphi(b)$.

Homework 4, due Feb 22

(1) Solve $97x \equiv 13 \pmod{105}$.
(2) Find all solutions to $35x + 23y = 423$.
(3) Solve $x^2 \equiv -1 \pmod{n}$ for (a) $n = 5$, (b) $n = 25$.
(4) Fix $n \geq 2$. Show that if $a^{n-1} \equiv 1 \pmod{n}$ for each $a = 1, \ldots, n-1$, then n is prime.
Hint: Show that $(a, n) = 1$. Why does this imply that n is prime ?
(5) Let p be an odd prime. Prove that if $(a, p) = 1$, solving the congruence equation $ax^2+bx+c \equiv 0 \pmod{p}$ can be reduced to solving a congruence equation of the form $x^2 \equiv q \pmod{p}$.
Hint: Multiply both sides of the equation by $4a$.
(6) Exhibit a sequence of 14 consecutive composite numbers.

Homework 5, due Mar 1

(1) Compute the greatest common divisor of 390, 720 and 450.
(2) Compute $2^{600} \pmod{60}$.
(3) Solve

$$\begin{cases} x \equiv 1 \pmod{117} \\ x \equiv 10 \pmod{72} \end{cases}$$

(4) Find all $m, n \in \mathbf{N}$ such that $m + n = 504$ and $(m, n) = 24$.
(5) Let $m > n > 0$, and $a \geq 2$. Show that if $m \equiv r \pmod{\text{n}}$ then $a^m - 1 \equiv a^r - 1 \pmod{a^n - 1}$.
(6) Prove that there are infinitely many primes using Fermat numbers.

Homework 6, due Mar 8

(1) List all quadratic residues mod 23.

(2) Compute the Legendre symbols

$$\left(\frac{16}{17}\right), \qquad \left(\frac{14}{17}\right), \qquad \left(\frac{-3}{17}\right).$$

(3) Find all odd primes p for which -2 is a quadratic residue.
(4) Prove, using Gauss's lemma, that 5 is a quadratic residue mod p if $p \equiv \pm 1$ (10) and a quadratic non-residue if $p \equiv \pm 3$ (10).
(5) Let $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ be the complete set of residues mod p. Choose $a \in \mathbf{Z}_p$ such that $a \neq 0$. Show that $\{0, a \pmod p, 2a \pmod p, 3a \pmod p, \ldots, (p-1)a \pmod p\}$ is in one-to-one correspondence with $\mathbf{Z}_p$. In other words, multiplication by a induces a permutation of the residues mod p.

Homework 7, due Mar 15

(1) Compute the Legendre symbols

$$\left(\frac{-26}{73}\right), \qquad \left(\frac{19}{73}\right), \qquad \left(\frac{33}{73}\right).$$

(2) Are the following congruences soluble:

$$x^2 \equiv 125 \ (1016), \quad 41x^2 \equiv 43 \ (79).$$

(3) Find all primes for which 7 is a quadratic residue.
(4) Show that if $n \in \mathbf{N}$ is of the form $n = 2^\varepsilon d^2 p_1 \cdots p_k$, where $\varepsilon \in \{0, 1\}$, $d \in \mathbf{N}$, $p_1, \ldots, p_k$ are distinct primes each congruent to 1 (mod 4), then n can be written as a sum of two squares. *Remark: The converse is also true!*
(5) Find all two-digits numbers that occur as the last two digits of a perfect square.

Homework 8, due Mar 29

(1) Determine the Farey sequence $\mathcal{F}_7$.
(2) Let $n \geq 2$. Show that if $\frac{a}{b} < \frac{c}{d}$ are Farey neighbors in $\mathcal{F}_n$, then at least one of them belongs to $\mathcal{F}_{n-1}$.
(3) Express $\frac{105}{143}$ and $\frac{112}{153}$ as continued fractions.
(4) Determine the fraction given by $[3, 1, 4, 1, 6]$ and $[6, 1, 4, 1, 3]$.
(5) Find the convergents of $[1, 1, 1, 1, 1, 1, 1]$ and $[1, 1, 2, 1, 2, 1, 2]$.
(6) Show that the convergents $\frac{p_k}{q_k}$, $k = 1, \ldots, n$, of the continued fraction expansion $[a_0, \ldots, a_n]$ are given by the following matrix multiplication:

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}$$

(7) Express $\sqrt{3}$, $\sqrt{50}$ as continued fractions.

Homework 9, due Apr ~~12~~ 16

(1) Let $n \in \mathbf{N}^*$ and suppose it is not a perfect square. Show that the continued fraction expansion of $\sqrt{n}$ is of the form $[a_0, \overline{a_1, \ldots, a_k, 2a_0}]$.
(2) Show that $\mathbf{Q}$ is ε-dense in $\mathbf{R}$. More precisely, show that for any $\alpha \in \mathbf{R}$ and any $\varepsilon > 0$, there exists $\frac{a}{b} \in \mathbf{Q}$ such that

$$\left|\alpha - \frac{a}{b}\right| < \varepsilon.$$

Hint: approximate α by its convergents.
(3) Compute the first 10 partial quotient of the continued fraction expansion of π.

(4) There is no distinguishable pattern among the partial quotients of the (simple) continued fraction of π. However if we allow for more general forms of continued fraction expansions, there are beautiful formulas that lend some impression of symmetry to π, for instance

$$\frac{4}{\pi} = 1 + \cfrac{1}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \cfrac{9^2}{\ddots}}}}}. \tag{1}$$

Let

$$I_n = \int_0^1 \frac{x^{2n}}{1+x^2} dx.$$

Show that

(a) $I_0 = \pi/4$ and $I_{n+1} + I_n = 1/(2n+1)$.

(b) Let $\alpha_n = I_{n+1}/I_n$. Use

$$\frac{I_{n+1} + I_n}{I_{n+2} + I_{n+1}} = \frac{2n+3}{2n+1}$$

to show that

$$\alpha_n = \frac{2n+1}{2 + (2n+3)\alpha_{n+1}}.$$

(c) Show that

$$\alpha_0 = \cfrac{1}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{\cdots + \cfrac{(2n-1)^2}{2 + (2n+1)\alpha_n}}}}.$$

(d) Deduce (1).

Homework 10, due Apr 23

(1) Let $n \geq 1$. Show that the continued fraction expansion of $\sqrt{n^2+1}$ is $[n, \overline{2n}]$.

(2) Write 293 as a sum of two squares.

(3) Find all solutions to the Pell equations $x^2 - 2y^2 = 1$ and $x^2 - 2y^2 = -1$.

(4) A number N is said to be square if $N = m^2$ and triangular if $N = \frac{n(n+1)}{2}$. Determine all numbers that are both square and triangular.
Hint: Note that $8m^2 = (2n+1)^2 - 1$. *Then use the previous exercise.*

(5) Use Dirichlet's pigeonhole principle to show that if seven distinct numbers are arbitrarily chosen from the set $\{1, 2, \ldots, 11\}$, then two of these seven numbers add up to 12. Is 7 the optimal value for this problem ?

Homework 11, due Apr 30

(1) Fibonacci's sequence is defined by $F_{-2} = 0$, $F_{-1} = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 0$. Show that the convergents $\frac{p_n}{q_n}$ to the golden mean $\varphi = \frac{1+\sqrt{5}}{2}$ are given by

$$\frac{p_n}{q_n} = \frac{F_n}{F_{n-1}}$$

for $n \geq 0$.

(2) The golden mean is $\varphi \approx 1.618$. This is fairly close to the conversion rate 1 mile = 1.609 km. Use the previous exercise to motivate the following miles/h to km/h conversion table:

m/h	km/h
89	144
55	89
34	55
21	34

Check using the conversion rate 1 mile=1.609 km how accurate this conversion table is.

(3) Consider the set of Ford circles

$$\mathcal{C} = \left\{ C(\tfrac{a}{b}) : 0 < \tfrac{a}{b} \leq 1,\ (a,b) = 1 \right\}.$$

Show that the total area of $\mathcal{C}$, that is the sum of the areas of each Ford circle in $\mathcal{C}$, is exactly

$$\text{area}(\mathcal{C}) = \frac{\pi}{4} \sum_{n \geq 1} \frac{\varphi(n)}{n^4},$$

where here $\varphi(\cdot)$ denotes Euler's totient function. Deduce from this that the sum

$$\sum_{n \geq 1} \frac{\varphi(n)}{n^4}$$

converges.

(4) Suppose that Alice's public key is (n, e) with $n = 583$, $e = 3$, and Bob wants to send Alice the message 'MONDAY'. Bob encodes this message by associated to each letter its rank in the alphabet, $M = 13$, ..., $A = 01$, $Y = 25$, then groups these numbers by blocs of 3.

(a) His message is thus

$$a_1 = \ldots, \quad a_2 = \ldots, \quad a_3 = \ldots, \quad a_4 = 125.$$

(b) What is Bob's message once he has encrypted each bloc, using Alice's public key? That is, find $b_i \equiv a_i^e \pmod{n}$

(c) Compute Alice's private key.

Homework 12

(1) Goldbach's (strong) conjecture states that every even number $n > 2$ can be written as a sum of two primes. Goldbach's (weak) conjecture (settled by Helfgott (2013)) states that every odd number $n > 5$ can be written as a sum of three primes. Show that the strong conjecture implies the weak one.

(2) Let p_n denote the n-th prime number in $\mathbf{N}$. Use the PNT to show that $p_n \sim n \log(n)$ as $n \to \infty$. How do you interpret this result?
Hint: Show first that if $y = x/\log(x)$ then $\log y \sim \log x$ as $x \to \infty$. Then use that $\pi(p_n) = n$.

(3) Use the norm of Gaussian integers to prove that the product of sums of two squares is itself a sum of two squares.

(4) Which of the following Gaussian integers are Gaussian primes: 1+3i, 3+4i, 14-5i ?

(5) Let $d > 0$ be a square-free integer. Consider

$$\mathbf{Z}[\sqrt{-d}] = \{a + \sqrt{-d}b : a, b \in \mathbf{Z}\}.$$

For $d = 1$, this is exactly the ring $\mathbf{Z}[i]$ of Gaussian integers. Show that the proof of the Division Theorem (Thm 44 in the notes) works for $\mathbf{Z}[\sqrt{-2}]$ but fails for $\mathbf{Z}[\sqrt{-3}]$.
Remark: As a result, we don't have unique factorization in $\mathbf{Z}[\sqrt{-3}]$.