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 rational number, 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

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 22, 25</td>
<td>Primes, factorizing, fundamental theorem of arithmetic</td>
</tr>
<tr>
<td>Jan/Feb 29, 1</td>
<td>gcd, lcm, congruences</td>
</tr>
<tr>
<td>Feb 5, 8</td>
<td>Fermat-Euler theorem, Chinese remainder theorem</td>
</tr>
<tr>
<td>Feb 12, 15</td>
<td>Higher congruences, quadratic residues</td>
</tr>
<tr>
<td>Feb 19, 22</td>
<td>Primes of the form 4k+1, Midterm</td>
</tr>
<tr>
<td>Feb/Mar 26, 1</td>
<td>Legendre symbol, Gauss’ lemma</td>
</tr>
<tr>
<td>Mar 5, 8</td>
<td>Quadratic reciprocity law, sums of squares</td>
</tr>
<tr>
<td>Mar 12, 15</td>
<td>Fractions and irrationals</td>
</tr>
<tr>
<td>Mar 19, 22</td>
<td>Spring break</td>
</tr>
<tr>
<td>Mar 26, 29</td>
<td>Continued fractions</td>
</tr>
<tr>
<td>Apr 2, 5</td>
<td>Midterm week</td>
</tr>
<tr>
<td>Apr 9, 12</td>
<td>Diophantine approximation</td>
</tr>
<tr>
<td>Apr 16, 19</td>
<td>Some Diophantine equations</td>
</tr>
<tr>
<td>Apr 23, 26</td>
<td>Computers: primality and factoring, cryptography</td>
</tr>
<tr>
<td>Apr/May 30, 3</td>
<td>Erasthotenes’ sieve and a theorem of Brun on twin primes</td>
</tr>
</tbody>
</table>

### 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 $n \in \mathbb{N}$. 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 $n \in \mathbb{N}$ is not a perfect square, show that $\sqrt{n}$ is irrational.
2. Show that for each $n \in \mathbb{N}$, $(n, n + 1) = 1$. How is this used in Euclid’s proof that there are infinitely many primes?
3. Let $a, b, c \in \mathbb{N}$. 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 $a \equiv b \mod p$ for every prime $p$. 
(5) Let \( p \) be a prime. Show that \((a + b)^p \equiv a^p + b^p \pmod{p}\).

*Hint: Binomial expansion.*

(6) Show that if the *alternating* sum of the digits of \( n \in \mathbb{N} \) 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 \( p \equiv 1 \pmod{4} \).

**Homework 3, due Feb 15**

(1) Let \( p \) be a prime. Show that \((p - 2)! \equiv 1 \pmod{p}\).

(2) Let \( n \neq 4 \) be composite. Prove that \((n - 1)! \equiv 0 \pmod{n}\).

(3) Solve the system of equations

\[
\begin{align*}
x &\equiv 3 \pmod{9} \\
x &\equiv 5 \pmod{10} \\
x &\equiv 7 \pmod{11}
\end{align*}
\]

(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 \( m, n \in \mathbb{N} \) such that \( m + n = 504 \) and \((m, n) = 24\).

(5) Let \( m > n > 0 \), and \( a \geq 2 \). Show that if \( m \equiv r \pmod{n} \) 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 
\[
\left(\frac{16}{17}\right), \quad \left(\frac{14}{17}\right), \quad \left(\frac{-3}{17}\right).
\]

(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 \( \mathbb{Z}_p = \{0, 1, \ldots, p - 1\} \) be the complete set of residues mod \( p \). Choose \( a \in \mathbb{Z}_p \) 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 \( \mathbb{Z}_p \). In other words, multiplication by \( a \) induces a permutation of the residues mod \( p \).

**Homework 7, due Mar 15**

(1) Compute the Legendre symbols 
\[
\left(\frac{-26}{73}\right), \quad \left(\frac{19}{73}\right), \quad \left(\frac{33}{73}\right).
\]

(2) Are the following congruences soluble:
\[
x^2 \equiv 125 \pmod{1016}, \quad 41x^2 \equiv 43 \pmod{79}.
\]

(3) Find all primes for which \( 7 \) is a quadratic residue.

(4) Show that if \( n \in \mathbb{N} \) is of the form \( n = 2^e d^2 p_1 \cdots p_k \), where \( e \in \{0, 1\}, \ d \in \mathbb{N}, \ p_1, \ldots, p_k \) are distinct primes each congruent to \( 1 \pmod{4} \), 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.