Number theory and geometry were the two branches of mathematics studied by the Greeks. The first is the study of numbers, the second of shapes. My philosophy about number theory (and many disagree with it) is the following. There are two basic operations on numbers: addition and multiplication. Number theory is the study of the strange and beautiful relation between these two operations. Until recently number theory has been called the *queen of mathematics*. G.H. Hardy (1940) explains why:

\[ \ldots \text{both Gauss and lesser mathematicians may be justified in rejoicing that there is one science [number theory] at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.} \]

Since the mid-1970’s, everyone assumes that Hardy is rolling in his grave because that was the time of the marriage of number theory to cryptography. Number theory is now one of the most applied branches of mathematics.

Since cryptography is being offered next year, I will do my best to keep this course distinct. This course will remain true to classical number theory. It will be pure, abstract and theoretical. In the cryptography courses number theory will be presented in a totally applied way with a minimum of theory.

In this course you will turn in homework on Wednesdays and Fridays. Homework will not be due on Mondays so that you have a chance to see me in office hours before homework is due. WHEN DOING HOMEWORK, YOU CAN USE EARLIER HOMEWORK PROBLEMS THAT WERE NOT ASSIGNED. I will drop the lowest two lecture’s worth of homework. Please write your proofs using full sentences.

I will prove most of the theorems I state. You will almost never need these proofs for homework or exams. But I want you to follow the proofs so that you learn how to write one. Writing proofs will be in your homework and on exams.

Office Hours: Monday 1:40 - 2:40, Tuesday 11:15 - 12:15, 1 - 2, Thursday 4 - 5.

Your grade will be 25% homework, 35% midterm, 40% final. The midterm will be Friday, May 8. The final is on Monday, June 8 at 1:30.
Topics covered:

1.2 Inductive reasoning and Fibonacci Sequence
1.4 Mathematical induction
1.5 Well-ordering principle
1.7 Division algorithm
2.1 Divisibility
2.2 Greatest common divisor
2.3 Euclidean algorithm
2.4 Least common multiple
2.5 Fundamental theorem of arithmetic
2.6 Pythagorean triples
3.1 Sieve of Eratosthenes
3.2 Infinitude of primes
3.3 Prime number theorem
3.4 Mersenne, Fermat and perfect numbers
4.1 Congruences
4.2 Special divisibility criteria
4.3 Euler $\phi$ function
5.1 Linear congruences
5.2 Chinese remainder theorem
5.4 Theorems of Lagrange and Wilson
5.6 Quadratic reciprocity

Two weeks on partition functions, not from the text.
People have been fascinated with numbers for thousands of years. Tables have been found from 1700 BC, written by the ancient Babylonians, centuries before the Pythagoreans, listing many Pythagorean triples: (3, 4, 5) (5, 12, 13), etc. Some triples were so large it’s clear they had a systematic way of generating them. They used these tables as primitive trigonometric tables, since all they knew were integers.

Ancient Egyptians had such lists as well. Later, the Pythagoreans (525 BC) proved the Pythagorean theorem and even later Greek geometers wrote down the method of generating all Pythagorean triples, that is integers \( x, y, z \) satisfying \( x^2 + y^2 = z^2 \). We’ll derive this description later.

Euclid (350BC) proved that there are infinitely many prime numbers.

In the 17th century, Fermat suggested that \( x^n + y^n = z^n \) has no positive integer solutions for \( n \geq 3 \) (this is known as Fermat’s Last Theorem - though he did not prove it) and he proved the \( n = 4 \) case. In the 18th/19th century, Gauss/Euler proved the \( n = 3 \) case. In 19th century, Dirichlet/Legendre proved the \( n = 5 \) case. How about the \( n = 6 \) case? Can you prove \( x^6 + y^6 = z^6 \) has no positive integer solutions given what you know now?

Fermat’s Last Theorem was not proven for all \( n \) until 1994 (Wiles and Taylor), using the theory of elliptic curves.

The study of squares wasn’t over with the Pythagoreans. Euler, Legendre and Gauss studied numbers of form \( x^2 + y^2, x^2 + 2y^2, x^2 + 3y^2 \) with \( x, y \) integers. For example they proved that a prime number is of the form \( x^2 + 5y^2 \) if and only if it is of the form \( 20k + 1 \) or \( 20k + 9 \). This study leads to quadratic forms and quadratic reciprocity (we’ll learn latter). Lagrange proved that if \( n \) is a positive integer, then \( n \) is the sum of at most four squares. \( 99 = 81 + 9 + 9 \). Sum of reciprocals of squares \( \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \) was proved by Euler.

The 19th century also gave us the prime number theorem (conjectured by Gauss and proved in 1898 by Hadamard and Poussin) which describes the density of primes over intervals.

Even into the late 20th century and early 21st century, many important results in number theory were proved.

Number theory is known for having many unsolved problems that can explain to a secondary school student. Here are a few:

1) A prime pair is a pair of prime numbers that differ by two, like \( (3, 5), (101, 103), (9857, 9859) \). Conjecture: There are infinitely many prime pairs.

2) Note \( 4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 5 + 5, 12 = 5 + 7, 14 = 7 + 7, 16 = 5 + 11, 18 = 7 + 11, 20 = 3 + 17, 22 = 11 + 11, 24 = 7 + 17, \ldots \). Goldbach’s (19th century) Conjecture: Every even integer \( \geq 4 \) is the sum of two primes.

3) Note some primes are of the form \( n^2 + 1 \) where \( n \) is an integer. Examples: \( 2, 5, 17, 37, 101, \ldots \). Conjecture: There are infinitely many primes of the form \( n^2 + 1 \).
Department and course goals

The course will help you achieve three of the department’s goals:

There will be a lot of proof writing in this course and we will spend a lot of time learning working on how to write proofs well. This will help you toward the goal:

2a) Students must be able to understand and write rigorous arguments (i.e., proofs) for theorems.

We will be learning number theory from an algebraic point of view. In particular, we will use what we have learned in Math 52 about groups to make more sense of number theory. This will help you toward the goal:

2b) Students must show mastery in the three basic areas of mathematics: analysis, algebra, and topology /geometry on a basic level in lower division courses and at an advanced level in upper division courses.

In addition, we will be study algorithms such as the Euclidean algorithm which will help you toward the goal:

3b) Students will acquire a strong facility for developing, analyzing, and applying algorithms.

Specific goals and objectives:

This course will strengthen each student’s

- ability to use theory to solve concrete problems
- write proofs
- understand applications of abstract algebra
- know the theory behind the mathematics used for cryptography
- solve recreational problems, many of which are rooted in number theory.

This course will

- enable students to see the beauty of number theory
- learn the history and basics concepts of number theory
- give students the ability to solve problems in elementary number theory.

Homework for Number Theory, Spring 2009

Due April 1: Read the syllabus.

Due April 3: §1.4: 8, 9. §1.7: 1, 2, 7, 8. Extra: A, C, D.
Due April 8: §2.1: 2, 4, 5. §2.3: 1a, 3 \((a \geq 0)\), 9, 12. Extra: E - H.

Due April 15: §2.4: 1a, 2, 3, 6, 12. Extra: I, J.
§2.5: 1, 3, (read 10, 11), 12 assume \(a_i > 0\). Extra: L, M

Due April 17: §2.5: 5, 7, 9 (last two words should be “an integer”). Extra N, O,

Due April 22: §2.6: 4, 6, 10. Extra P, Q, R.
On 2.6 # 6: Let P be the point where the line including the z-side meets the circle. Let Q be the point where the z-side meets the x-side. Compute the distance from P to Q in two ways. On 2.6 # 10: It should say “positive odd integer greater than or equal to 3 can be the side . . .”

Due April 29: §3.2: 2 (don’t use Dirichlet), 5, 8, 9. §3.4: 1 - 4, 10. Extra T, T.5.

Due May 1: §4.1: 4-6, 8, 11-13, 16, 22.

Due May 6: §4.1: 10, 18 (\(a^{2n}\) not \(a^{2n}\)), 23, 24, 26, 27. §4.2: 1. Extra U, V, W, Y, Z.

Due May 13: §4.3” 7, 8 (should say “arbitrary ODD positive n”), 11, 12, 14, 16, 17, 23. Extra AA, BB, CC.

Due May 15: §5.1: 1 - 4

Due May 20: §5.2: 1 - 3 (on 3 careful, \(\gcd(4,2) \neq 1\)), 5, 8, 10. §5.4: 1 (do for \(n > 1\). Prove that if \((n - 1)! \equiv -1(\text{mod } n)\) and \(n \geq 2\) then \(n\) is prime), 12 - 14. 13 is hard to read. Note that “A only if B” is logically equivalent to “If A then B”. So on 13 prove that “If \(p\) is an odd prime and \(x^2 \equiv -1(\text{mod } p)\) is solvable, then \(p \equiv 1(\text{mod } 4)\)”. On 5.4, don’t use results about the Legendre symbol.
Due May 22: §5.5: 2 - 4. On 3b, 4b, state number of incongruent solutions and just find one each time. Note from Thm 94.5, $3x^2 + 6x + 5 \equiv 0 \pmod{49}$ has at most two solutions). If you have green copy of Long’s text, then the answer in the back to 2b is wrong.

Due May 29: §5.6: 4 (should say primes), 5, 8, 16.

Due June 3: DD, EE, FF, GG, HH.

Due June 5: II, JJ, KK, LL.

Extra problems for number theory, Spring 2009.

A) The sum of two irrational numbers is irrational. Prove or give a counterexample.

B) Find all positive integer solutions to $a^b = b^a$. Prove your answer. Hints: $\ln(a^b) = \ln(b^a)$, $b\ln(a) = a\ln(b)$, $\ln(a) = \ln(b)$. Graph $y = \ln(x)$.

C) Show $p$, $p + 2$ and $p + 4$ are not all prime unless $p = 3$.

D) Find all primes of the form $n^3 - 1$. (We are assuming, as in this class, that primes are positive.) Prove your answer.

E) Prove that any amount greater than 11 cents can be made using only 4- and 5-cent stamps. If $n, m$ are relatively prime positive integers, conjecture a formula for the largest amount that can not be obtained from $n$- and $m$-cent stamps (so for $n = 4, m = 5$ that amount is 11). You need not prove that formula.

F) Let $k, m, n, t \in \mathbb{Z}_{\neq 0}$.
   a) Prove that $k \mid m$ implies $k \mid mn$.
   b) Prove that $k \mid m$ and $k \nmid n$ implies $k \nmid m + n$.

G) a) Compute $(x^{10} - 1) \div (x^2 - 1)$. b) If $a, m, k \in \mathbb{Z}_{> 0}$ and $m \mid k$, show $a^m - 1 \mid a^k - 1$.

H) Recall $0! = 1$, $1! = 1$, for $n > 1$ we have $n! = 1 \cdot 2 \cdot 3 \cdots (n - 1) \cdot n$. Recall the binomial theorem. If $n \geq 0$ then $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$ where $\binom{n}{i} = \frac{n!}{i!(n-i)!}$. (So you can assume that $\binom{n}{i} \in \mathbb{Z}$). (Problem begins:) Let $p$ be a prime number. Let $k \in \mathbb{Z}$ with $1 \leq k \leq p - 1$. Prove $p \mid \binom{p}{k}$.

I) Let $a$ and $b$ be fixed positive integers. Let $g = \gcd(a, b)$. Consider the set $S = \{xa + yb \mid x, y \in \mathbb{Z}\}$ (note that I have not made the restriction that $xa + yb > 0$). i) Prove that if
$v \in S$ then $g | v$. (So now we know that all elements of $S$ are multiples of $g$).

ii) \ Prove that every multiple of $g$ is in $S$. (Now we know that $S$ is equal to the set of all multiples of $g$).

J) \ Give an example of $a_1, a_2, a_3 \in \mathbb{Z}$ such that $\gcd(a_1, \ldots, a_3) = 1$ but no two are pairwise relative prime (so for any $i, j$, we have $\gcd(a_i, a_j) > 1$).

K) \ Let $a, b, c \in \mathbb{Z}$ with $a$ and $b$ not both 0. Assume $a | c$ and $b | c$ and $(a, b) = 1$. Prove $ab | c$.

L) \ Show $3$ and $1 + \sqrt{-6}$ are both irreducible in $\mathbb{Z}[\sqrt{-6}]$.

M) \ Prove that if $x, y \in \mathbb{Z}[\sqrt{-6}]$, then $N(xy) = N(x)N(y)$.

N) \ a) Does $a^3 | b^2$ imply $a | b$? \ Prove or give a counterexample.
   b) Does $a^2 | b^3$ imply $a | b$? \ Prove or give a counterexample.

O) \ Determine all primes $p$ such that $11p + 1$ is a perfect square. \ Prove your answer.

P) \ Prove $\sqrt{2} \notin \mathbb{Q}$ using the Fundamental Theorem of Arithmetic.

Q) \ Find one million consecutive composite integers. (Remember, $n$ is composite if $n \in \mathbb{Z}_{>2}$ and $n$ is not prime).

R) \ Find all primitive Pythagorean triangles where the area and perimeter are the same. Prove you have them all.

S) \ Find a function $f : \mathbb{Z}_{>0} \rightarrow \mathbb{Z}_{>0}$ following the pattern below:
   \begin{align*}
n: & \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad \ldots \\
f(n): & \quad 1 \quad 1 \quad 2 \quad 2 \quad 3 \quad 3 \quad 4 \quad 4 \quad 5 \quad 5 \quad \ldots
\end{align*}

T) \ Show that there are infinitely many primes which end in 54321. (As an example, 7154321 is prime).

T.5) \ Consider the sequence $2^{2^5} + 1, \ 2^{2^6} + 1, \ldots, 2^{2^n} + 1, \ldots$. Those are the 5th, 6th, etc. Fermat numbers. Use the prime number theorem to approximate the expected number which are prime. The expected number is given exactly by the formula $\sum_{n=5}^{\infty} \Pr(2^{2^n} + 1 \text{ is prime})$. The homework problem is finished here.

Notes: Once you finish the problem, you will see that the expected number is much less than 1. For that reason, we conjecture that there are no primes in the sequence of Fermat numbers after $n = 4$. Let me explain why the formula is correct (for those who have taken a course in probability). For $n \in \mathbb{Z}_{\geq 5}$, let $X_n = 1$ if $2^{2^n} + 1$ is prime and $X_n = 0$ if $2^{2^n} + 1$ is composite. We see that $X_n$ is a random variable. The number of Fermat primes $\geq 5$ is given by $X_5 + X_6 + \ldots$. The expected number of Fermat primes $\geq 5$ is given by $E[X_5 + X_6 + \ldots] = E[X_5] + E[X_6] + \ldots$. Note $E[X_n] = 1 \cdot \Pr(2^{2^n} + 1 \text{ is prime}) + 0 \cdot \Pr(2^{2^n} + 1 \text{ is composite}) = \Pr(2^{2^n} + 1 \text{ is prime}).$ So $E[X_5] + E[X_6] + \ldots = \Pr(2^{2^5} + 1 \text{ is prime}) + \Pr(2^{2^6} + 1 \text{ is prime}) + \ldots$. \label{eq:fermat-primes}
U) a) Make a multiplication table for $\mathbb{Z}_{10}$.
   b) Make an addition table for $\mathbb{Z}_6$.

V) Does $a \equiv b \pmod{m}$ imply $a^2 \equiv b^2 \pmod{m^2}$? Prove or give a counterexample.

W) Solve the MU problem. All strings allowed are made up of the letters M,I,U. You start with the string MI. You can apply any of the following 4 rules to change your string.
   1) If last letter of string is I, can add a U at the end (so MI can become MIU).
   2) Suppose you have Mx (where x is any string of M,I,U’s), can change to Mxx. (from MIU can get MIUIU, from MUM can get MUMUM).
   3) If III occurs in a string, can replace with U (from UMIIMU can get UMUMU, but can’t change IIMII with this rule).
   4) If UU occurs in a string you can drop it. Question: Can you get the string MU? (Most of you won’t get this, don’t spend more than 30 minutes on it).

Y) Show that $y^2 = x^3 - x - 1$ has no solutions in integers. Hint: $(\mod 3)$.

Z) Consider the nine functions $f_n(x) = nx$ from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{12}$, for $n = 2, 3, 4, \ldots, 10$. Consider them one at a time; the first is $f_2(x) = 2x$. How many elements are in the range of $f_n$ for these nine $n$’s. Come up with a formula predicting those values based on $n$ and 12.

AA) Prove that if $n \in \mathbb{Z}$ and $n > 2$ then $\phi(n)$ is even.

BB) Find $\phi(7200)$.

CC) Find the last 2 digits of $3^{333}$.

DD) Show that if $p$ is prime and $p \geq 7$ then there are always two consecutive quadratic residues of $p$. Hint: First show that at least one of 2, 5 and 10 is a quadratic residue.

EE) Find $\left( \frac{2607}{20011} \right)$.

   As a check, $p(6) + p(7) + p(8) + p(9) = 78$. You may want to keep a copy of your solutions for the later problem LL.

GG) For $n = 9$, find the partitions into distinct summands and find the partitions into odd summands. There should be the same number. Pair them up using the correspondence given in Example 111 and Theorem 112.

HH) The Fibonacci numbers are $F_1 = 1$, $F_2 = 1$ and for $n \geq 3$ we have $F_n = F_{n-1} + F_{n-2}$. We create the Fibonacci power series $1 + F_1x^1 + F_2x^2 + F_3x^3 + \ldots$. Compute $(1 + F_1x^1 + F_2x^2 + F_3x^3 + \ldots)^{-1}$ up to the $x^9$ term. Do ALL the computations. Don’t just quit once you’ve noticed the pattern and fill in the remaining terms based on your guess. (Problem HH ends here). The pattern you may notice goes on forever. That can be proven by induction, but I am not asking you to do so.

II) Consider the function $f(n) = n + 1$ for $n \in \mathbb{Z}_{\geq 0}$.
i) Write out the generating function for $f(n)$.

ii) This power series is the Taylor series at $x = 0$ of what function? (Hint: Math 11 and 13)

iii) Recall that the function and the Taylor series are equal for $|x| < 1$. So find an exact value for the infinite series $1 + 2(\frac{1}{2}) + 3(\frac{1}{2})^2 + 4(\frac{1}{2})^3 + \ldots$.

JJ) i) The function $d^e(n)$ counts the number of partitions of $n$ into distinct even summands (so the summands themselves are even, not necessarily the number of them, e.g. if $n = 12$ then 6, 4, 2 is such a partition). Write the generating function for $d^e(n)$ as an infinite product (see Example 116).

ii) Look at the second proof of Theorem 112 and find another representation for the generating function for $d^e(n)$ as an infinite product. You may use the fact that we have the proof of Theorem 112; so you don’t need to go through a similar proof all over again for this case. This is a short problem.

iii) Using this new generating function for $d^e(n)$, we see that $d^e(n) = p^S(n)$ for some set $S$ of positive integers. Describe the set $S$. (Problem iii ends here.) So we have found that the number of partitions of $n$ into distinct even summands is the same as the number of partitions of $n$ into summands coming from the set $S$.

iv) Check your answer for part iii) for $n = 12$ by finding the partitions of 12 into distinct even summands and by finding the partitions of 12 into summands from your set $S$. Hope you get the same number of them!

KK) i) Write the generating function for $d^o(n)$ as an infinite product. This is the function counting the number of partitions into distinct odd summands.

ii) Using the second proof of Theorem 112 and your answer to JJ ii), find another representation for the generating function for $d^o(n)$ as an infinite product. (It is OK that you will have terms in the numerator and terms in the denominator.)

LL) Use Theorem 119 to find $p(n)$ for $10 \leq n \leq 16$. (As a check, $p(16) = 231$.) Recall $p(0) = 1, p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5, p(5) = 7, p(6) = 11, p(7) = 15, p(8) = 22, p(9) = 30$.

MM) You have a die (the singular of dice). On each side is a certain number of dots. Those six numbers are all positive integers. For this die, let $f$ be the function from $\mathbb{Z}$ to $\mathbb{Z}$ such that $d(n) = m$ if $n$ dots appear on $m$ sides. Let $g_d$ be the associated generating function. So if your die had 3, 3, 5, 5, 5 and 8 dots then the associated generating function would be $2x^3 + 3x^5 + x^8$.

Let’s say we have two normal die, $d_1, d_2$. Their associated generating functions are $g_{d_1} = g_{d_2} = x + x^2 + x^3 + x^4 + x^5 + x^6$.

If we multiply them together we get $g_{d_1}g_{d_2} = x^2 + 2x^3 + 3x^4 + 4x^5 + 5x^6 + 6x^7 + 5x^8 + 4x^9 + 3x^{10} + 2x^{11} + x^{12}$. If we roll the dice, we can look at the sum of the upper faces. The table below gives the possible outcomes.
We see that the coefficient of \( x^n \) in \( g_{d_1}g_{d_2} \) is the number of ways of getting the sum \( n \).

Cool.

Here is the problem to solve: Find a different pair of dice (the two dice you find need not be the same as each other), where there is a positive integer number of dots on each of the twelve sides and such that we get the same sums in exactly the same number of ways as for a pair of normal dice. I.e. there should be one way of getting the sum 2, two ways of getting the sum 3, \ldots, one way of getting the sum 12.

Hints. Clearly from above, we need to factor \( g_{d_1}g_{d_2} \) into a different pair of polynomials. \( g_{d_1} = x(x + 1)(x^2 - x + 1)(x^2 + x + 1) \). Let the weight of a polynomial be the sum of its coefficients. We have \( w(x) = 1 \), \( w(x + 1) = 2 \), \( w(x^2 - x + 1) = 1 \), \( w(x^2 + x + 1) = 3 \), \( w(g_{d_1}) = 6 \) and \( w(g_{d_1}g_{d_2}) = 36 \). It is always true that \( w(fg) = w(f)w(g) \) (that is obvious by noting that \( w(f) = f(1) \) and we know \( (fg)(1) = f(1)g(1) \)). The weight can help.