A Friendly Introduction to Number Theory

Chapter1: What is Number Theory?

-Number theory is the study of the set of positive whole numbers (Natural Numbers)

-Relationships between Natural Numbers:

- Odd, even, square, cube, prime, composite, 1(modulo 4), 3 (modulo 4), triangular, perfect, Fibonacci etc.

-**Sum of Squares I** - the sum of two squares be a square? **Yes**. **Pythagorean Triples**.

-**Sum of Squares II** - p is a sum of two squares if it is congruent to 1(modulo 4). In other words, p is a sum of two squares if it leaves a remainder of 1 when divided by 4, and not a sum of two squares if it leaves a remainder of 3. (use prime numbers to see the pattern)

-**Sum of Higher powers**: e.g. sum of nth powers be an nth power? **No. Fermat's Last Theorem.**

-**Infinitude of Primes**: Infinitely many primes? Yes. Infinitely many primes that are 1 modulo 4 numbers? Yes. Infinitely many primes that are 3 modulo 4 numbers? Yes.

-**Number Shapes**:

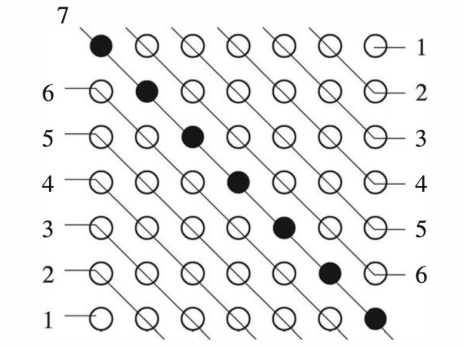
-Triangular numbers: 3, 6, 10, can be arranged in triangles.

-Square numbers: 4, 9, 16, can be arranged in squares.

-a number can be both triangular and square.

-**Geometry Implication of Gauss's formula**: $\frac{n(n+1)}{2}$:

2(1 + 2 + 3 +...+ n) + (n+1) = $(n+1)^2$



Subtract (n+1) from both sides and divided by 2 to get Gauss's formula.

-**Twin Primes:** Consecutive odd numbers are both prime p, p+2. E.g. 3,5,7; 11,13;

-Infinity? No yet known.

-**Primes of the Form** N^2+1 : Infinity? Not yet known.

Steps to study the Theory of Numbers:

1. Accumulate data
2. Find pattern in data
3. Formulate conjectures
4. Test conjectures with additional data
5. Devise a proof

Chapter2: Pythagorean Triples

Primitive Pythagorean Triple (PPT): Triples of numbers that have no common factors and satisfy $a^2 + b^2 = c^2$ with {a odd; b even; a, b, c having no common factors

1. Accumulate Data:
   (3, 4, 5), (5, 12, 13), (8, 15, 17)...
2. Find Pattern & Conjecture & Find more Data & Make Proofs:
   a. One of a and b is odd and the other is even, c is always odd.
      Proof:
      i. (1) Assume a and b both even, c would have to be even, therefore a,b,c would have a common factor of 2, violates the definition of PPT.
      ii. (2) Assume a and b both odd, we can proof by contradiction that c cannot be even.
      iii. (3) Since it can't be both even and both odd, it has to be one even one odd, and from the equation we can easily prove that c is also odd.

Factorization and **Divisibility**:

Assume (a, b, c) is PPT (and assume a to be odd b to be even)

$a^2 = c^2 - b^2 = (c - b)(c + b)$

e.g. $3^2 = 5^4 - 4^2 = (5-4)(5+4) = 1 \cdot 9$ (Find Data)

It seems that $(c-b)$ and $(c+b)$ are always squares (Conjecture 1)

$21^2 = 29^4 - 20^2 = (29-20)(29+20) = 9 \cdot 49$ (Find more data)

It also seems that $(c-b)$ and $(c+b)$ have no common factors (Conjecture 2)

Proof (Conjecture 2): $(c-b)$ and $(c+b)$ have no common factors

Assume d is a common factor between $(c-b)$ and $(c+b)$

→ d divides both $(c-b)$ and $(c+b)$

→ d also divides $(c-b) + (c-b) = 2c$ and $(c+b) - (c-b) = 2b$

→ d divides 2b and 2c

→ since b and c have no common factor, so d must equal 1 or 2

→ But d also divides $(c-b)(c+b) = a^2$, since a is odd, so d must be 1

Conclusion: $(c-b)$ and $(c+b)$ have no common factor.

Proof (Conjecture 1):

Since we have proved in conjecture 2 that $(c-b)$ and $(c+b)$ are positive integers that have no common factor, their product is a square since $(c-b)(c+b) = a^2$, the only way that this can happen is if $(c-b)$ and $(c+b)$ are themselves squares.

→ $(c+b) = s^2$ and $(c-b) = t^2$, where $s > t \geq 1$ are odd integers with no common factors.

→ $c = \frac{s^2+t^2}{2}$ and $b = \frac{s^2-t^2}{2}$

→ $a = \sqrt{(c-b)(c+b)} = st$

Chapter3: Pythagorean Triples and the Unit Circle

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

If we divide this equation by c^2, we obtain $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$

The pair (a/c, b/c), is a solution to the equation $x^2 + y^2 = 1$

Theorem 3.1:

Every point on the circle $x^2 + y^2 = 1$ whose coordinates are rational numbers can be obtained from the formula $(x, y) = (\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2})$, by substituting in rational numbers for m [except for the point (-1,0) which is the limiting value as m → infinity).

If we rewrite the rational number m as a fraction v/u, then our formula becomes

(x, y) = $(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2+v^2})$, clearing the denominator we get

(a, b, c) = $(u^2 - v^2, 2uv, u^2 + v^2)$, which is the Pythagorean triples.

Chapter4: Sums of Higher Powers and Fermat's Last Theorem

$a^n + b^n = c^n$, $where\ n \geq 3$, have no solutions in nonzero integers a, b, c.

Chapter5: Divisibility and the Greatest Common Divisor

Assume m and n are integers with m ≠ 0. If m divides n, m|n, if n does not divide n, m∤n. (e.g. 3|6).

The **greatest common divisor** of two numbers a and b (not both zero) is the largest number that divides both of them, denoted as gcd(a,b). If gcd(a,b) = 1, a and b are **relatively prime**. (e.g. gcd(225, 120) = 15).

Euclidean Algorithm: the most efficient method known for finding the greatest common divisor of two numbers. (Factoring both numbers are not very efficient.)

Example: compute gcd(36, 132).

Step1: divide 132 by 36, gives a quotient of 3 and remainder of 24.
Write it as: 132 = 3 x 36 + 24.

Step2: take 36 and divide it by the remainder 24 from the previous step.
Write it as: 36 = 1 x 24 +12

Step3: Divide 24 by 12, find a remainder of 0.
Write it as 24 = 2 x 12 +0

As soon as you get a remainder of 0, the remainder from the previous step is the greatest common divisor of the original two numbers. So in this case gcd(132, 36) = 12.

General Algorithm: at each step, we divide a number A by number B to get a quotient Q and a remainder R:

A = Q x B + R

At the next step we replace our old A and B with the numbers B and R and continue the process until we get a remainder of 0. The remainder R from previous step is the greatest common divisor of our original two numbers.

$a = q_1 \times b + r_1$

$b = q_2 \times r_1 + r_2$

$r_1 = q_3 \times r_2 + r_3$

…

$r_{n-2} = q_n \times r_{n-1} + r_n$

$r_{n-1} = q_{n+1} r_n + 0$

(r_n *is the gcd*)

$Equation: \quad r_{i-1} = q_{i+1} \times r_i + r_{i+1}$

Side Notes: Method to compute Q and R:

- Divide A by B, get a number with decimals.
- Discard the decimals (e.g. (int)) to get Q.
- To find R, use the formula R = A - B x Q.

Why is the last non-zero remainder r_n a **common divisor** of a and b? (Hint: go through the equations from bottom to top).

Since r_n divides r_{n-1} ,

→ and since r_n also divides both r_{n-1} and r_n when we move up a line…

→ we will eventually reach the top line where r_n will be able to divide a.

Why is the last non-zero remainder r_n the **greatest common divisor** of a and b? (Hint: go through the equations from top to bottom).

Assume d is any common divisor of a and b.

→ if $a = q_1 \times b + r_1$ and d is a common divisor of a and b, d will also be able to divide r_1

→ continuing down line by line, for each $r_{i-1} = q_{i+1} \times r_i + r_{i+1}$, for each stage we will know that d divides the previous two reminders r_{i-1} and r_i .

→ d divides r_n

→ r_n must be the greatest common divisor of a and b.

Theorem 5.1 (**Euclidean Algorithm**): To compute the greatest common divisor of two numbers a and b, let r_{-1} = a, let r_0 = b, and compute successive quotients and remainders

$r_{i-1} = q_{i+1} \times r_i + r_{i+1}$

For $i = 0, 1, 2...$ until some remainder r_{n+1} is 0. The last non-zero remainder r_n is the greatest common divisor of a and b.

Note: The number of steps in the Euclidean algorithm is at most seven times the number of digits in b.