Fall 2018

Number Theory

Wednesday, November 28th, 2018

Mihaela Ifrim

Known results:

Fermat's Little Theorem. For every prime p and any integer a which is not divisible by p, we have

$$a^{p-1} \equiv 1 \text{ (mod p) }.$$

Euler's Theorem. Let $\phi(n)$ denote the number of positive integers in $\{1, 2, 3, \dots n\}$ which are relatively prime to n. Then, for any integer a which is relatively prime to n,

$$a^{\phi(n)} \equiv 1 \text{ (mod n)}$$

Wilson's Theorem. A positive integer n is a prime if and only if $(n-1)! \equiv -1$ (mod n) .

Dirichlet's Theorem. For any two positive integers a and d which are relatevely prime, the arithmetic progression $a, a+d, a+2d, \dots$ contains infinitely many primes .

Quadraric rezidues. Let p be a prime. There are exactly $(p+1)/2$ residues r such that there rxists solutions to

$$x^2 \equiv r \text{ (mod p)}.$$

Fermats Infinite Descent Principle. Fermats infinite descent principle states that there are no strictly decreasing infinite sequences of positive integers. Alternatively, any decreasing sequence of positive integers becomes stationary. This is a corollary of the fundamental property of the set of positive integers that every subset has a smallest element.

Example: Prove that there is no infinite arithmetic progression whose terms are all perfect squares.

The greates integer function. The greatest integer function associates to a number x the greatest integer less than or equal to x. The standard notation is $[x]$.

Example. For a positive integer n and a real number x, prove the identity

$$[x] + \left[x + \frac{1}{n}\right] + \cdots + \left[x + \frac{n-1}{n}\right] = [nx]\,.$$

Factorization and Divizibility. An integer d divides another integer n if there is an integer d' such that $n = dd'$. In this case d is called a divisor of n. We denote by

$gcd(a,b)$ the greatest common divisor of a and b. For any positive integers a and b, Euclids algorithm yields integers x and y such that

$$ax - by = gcd(a,b).$$

Two numbers are called coprime, or relatively prime, if their greatest common divisor is 1. The fact that for coprime numbers a and b there exist integers x and y such that

$$ax - by = 1$$

is called the fundamental theorem of arithmetic.

Example. Prove that thers is no polynomial with integer coefficients $P(x)$ with the property that $P(7) = 5$ and $P(15) = 9$.

Euclid's theorem There are infinitely many prime numbers.

A positive integer is called prime if it has no other divisors than 1 and the number itself. Equivalently, a number is prime if whenever it divides a product it divides one of the factors. Any positive integer can be written as a product of primes in a unique way up to a permutation of the factors.

Modular Arithmetic. A positive integer n partitions of the set of integers $\mathbb{Z}$ into n equivalence classes by the remeinders obtained on fividing by n. The remainders are called residues modulo n. We denote by $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ the set of equivalence classes, indexed by their residues. Two numbers a and b are said to be congruent modulo n, which is written $a \equiv b \pmod{\text{n}}$, if they have the same remainder when divided by n, that is, if $a - b$ is divisible by n.

Example. The number 2^{29} has 9 distinct digits. Without using a calculator, tell which digit is missing.
The Chinese Remainder Theorem. Let $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers greater than 1. Then for any integers $a_1, a_2, \ldots, a_k$, the system of congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, x \equiv a_k \pmod{m_k},$$

has solutions, and any two such solutions are congrient modulo $m = m_1 m_2 \cdots m_k$.
Sylvester's Theorem. Let a and b be coprime positive integers. Then $ab - a - b$ is the largest positive integer c for which the equation

$$ax + by = c$$

is not solvable in nonegative integers.
Please read on your own Section 5.3 from Putnam and Beyind book!

Problems:

1. Prove that there are infinitely many prime numbers of the form $4m + 3$, where $m \geq 0$ is an integer.

2. Show that each positive integer can be written as the difference of two positive integers having the same number of prime factors.

3. Is it possible to place 1995 different positive integers around a circle so that for any two adjacent numbers, the ratio of the greater to the smaller is a prime?

4. Prove that $n!$ is not divisible by 2^n for any positive integer n.

5. Define the sequence $(a_n)_n$ recursevely by $a_1 = 2$, $a_2 = 5$, and
$$a_{n+1} = (2 - n^2)a_n + (2 + n^2)a_{n-1} \text{ for } n \geq 2.$$
Do there exist indices p, q, r such that $a_p \cdot a_q = a_r$?

6. Prove that if n is a positive integer that is divisible by at least two primes, then there exists an n-gon with all angles equal and with side lengths the numbers $1, 2, 3, \ldots, n$ in some order.

7. Prove that the equation $x^2 = y^3 + 7$ has no integer solutions.

8. For each positive integer n, find the gratest common divisor of $n! + 1$ and $(n+1)!$.

9. Let p be an odd prime number. Show that the equation $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

10. If the distinct prime factors of n are $p_1, p_2, \ldots, p_k$ then
$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) n\left(1 - \frac{1}{p_2}\right) \ldots n\left(1 - \frac{1}{p_k}\right).$$

11. Let n be an even positive integer. Prove that $n^2 - 1$ divides $2^{n!} - 1$.

12. Prove that for every n, there exist n consecutive integers each of which is divisible by two different primes.

13. Let a and b be two positive integers such that for any posotive integer n, $a^n + n$ divides $b^n + n$. Prove that $a = b$.

14. Given a piece of paper, we can cut it into 8 or 12 pieces. Any of these pieces can be cut into 8 or 12, and so on. Show that we can obtain any number of pieces greater than 60. Can we obtain exactly 60 pieces?

15. Prove that the d-dimensional cube can be dissected into n d-dimensional cubes for all sufficiently large values of n.