2019-12-14 Class Summary: Chinese Remainder Theorem

Kalvis Apsītis, kalvis.apsitis@gmail.com
Riga Business School (RBS), University of Latvia (LU)

This document lists the key results from the December 14, 2019 class in Number Theory. This training for competition math is aimed at 16–18 year olds (typically, Grades 10–12).

Keywords: Chinese remainder theorem, Bezout's identity, Modular arithmetic.

Examples

These are **not** the homework problems; it is just a supplementary study material with examples taken from the lecture; most of them were analyzed during the lecture. In case you have forgotten something, hints for these examples are given at the end of this document. Full notes and solutions in Latvian: http://linen-tracer-682.appspot.com/numtheory-tales/tale-numtheory-jun03-crt/content.html#/section

Example 2.1: Find integers x, y such that $18x + 42y = 6$. (Here we have chosen $6 = gcd(18, 42)$.)

Example 2.2: Prove that the sequence $1, 11, 111, \ldots$ contains an infinite subsequence such that any two members of that subsequence are mutually prime.

Blankinship Algorithm: Blankinship Algorithm can be used to find solutions for the Bezout's identity: the integers x, y such that $ax + by = d$. It is explained here: http://mathworld.wolfram.com/BlankinshipAlgorithm.html. It applies Gaussian row operations to a 2×3 matrix: you should know how to subtract one row from another.

Inverse Congruence Class: For a congruence class a that is mutually prime with modulo m, denote by a^{-1} a congruence class such that $a^{-1} \cdot a \equiv 1$ modulo m. (In other words: Given a number $a < m$, find some number b such that $a \cdot b$ gives remainder 1 when divided by m.)

Example 2.3: Find inverses 1^{-1}, 3^{-1}, 5^{-1}, 7^{-1}, 9^{-1}, 11^{-1}, 13^{-1}, 15^{-1} (all modulo 16).

Chinese Remainder Theorem: For multiple mutually prime modulos $m_1, m_2, \ldots, m_k$ one can find x that is congruent to any numbers $a_1, a_2, \ldots, a_k$ with respect to those modulos.

Example 2.4: Find a natural number x that is a solution to this system of congruences:

$$\begin{cases} x \equiv 1 \ (mod\, 3) \\ x \equiv 2 \ (mod\, 5) \\ x \equiv 3 \ (mod\, 7) \end{cases}$$

Example 2.5: Assume that you want to find number x that satisfies both congruences:

$$\begin{cases} x \equiv 4 \ (mod\, 5) \\ x \equiv 6 \ (mod\, 11) \end{cases}$$

You can solve this "graphically" - build a 5×11 table representing all possible pairs of remainders, when you divide numbers by 5 and by 11. Fill in this table by choosing $x = 1, 2, 3, \ldots$ until you find the necessary combination of remainders $(4; 6)$.

Example 2.6: Find the smallest positive integer n, such that numbers $\sqrt[5]{5n}$, $\sqrt[6]{6n}$, $\sqrt[7]{7n}$ are all positive integers.
(From *Vilniaus universiteto Matematikos ir informatikos fakulteto olimpiadas* - a Lithuanian olympiad for high school students by Vilnius university; 2016, Grade 10, P3.)

Example 2.7: Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1, \ldots, k_n$, all strictly greater than 1, such that $k_0 k_1 \ldots k_n - 1$ is the product of two consecutive integers.

Example 2.8: Prove that for every positive integer n, there exist integers a and b such that $4a^2 + 9b^2 - 1$ is divisible by n.
(*Math Prize for Girls Olympiad, 2010, P2*).

Example 2.9: Are there infinitely many Fibonacci numbers that give the following remainders when divided by 1001:
(a) remainder 0; **(b)** remainder 900; **(c)** remainder 1000.

Example 2.10: Prove or disprove the following hypotheses.
(a) For all $k \geq 2$, each sequence of k consecutive positive integers contains a number that is not divisible by any prime number less than k.
(a) For all $k \geq 2$, each sequence of k consecutive positive integers contains a number that is relatively prime to all other members of the sequence.
(*Baltic Way, 2016, P2*).

Hints for Some Examples

Hint 2.1: You can find this by trial and error for small numbers. Or you can run Euclidean Algorithm to find the GCD (greatest common divisor) of numbers 18 and 42. It will tell you, how many times you should add or subtract 18 and 42 to get number 6. (Blaninship's method is essentially the same thing.)

Hint 2.2: If you build the following sequence of mutual primes: $2, 3, 7, 43, \ldots$ (every next number equals the product of all the previous ones plus 1), then the corresponding numbers 11, 111, 1111111, and so on will give remainder 1 every time you divide them one by another.

Hint 2.3: In order to find, say, 9^{-1} (modulo 16), you can try out all the odd remainders $(1, 3, \ldots, 13, 15)$. Or you can solve the Bezout's identity $9x - 16y = 1$. Blankinship's algorithm again.

Hint 2.4: One can build such a number step by step - first write all the numbers congruent to 1 (modulo 3): $1, 4, 7, \ldots$ until you find one that gives remainder 2 when divided by 5, and so on. (Since $3, 5, 7$ are mutually prime, Chinese remainder theorem promises that you will succeed.)

Hint 2.5: Solution is shown in the table: https://bit.ly/2MCzMmf. Try to locate numbers $0, 1, 2, 3, \ldots$ in this table and see the sequence how they fill up the table. Similar ideas are used by problems that ask you to "Measure exactly 4 liters of water, given two jugs with volumes $5L$ and $11L$ respectively".

Hint 2.6: Search for n in the form $n = 2^a 3^b 5^c 7^d$. Then write the necessary conditions (as modular congruences) for all the unknown powers a, b, c, d.

Hint 2.7: Look at the polynomial $F(t) = t^2 + t + 1$ (it is a product of two consecutive numbers t and $t + 1$ plus 1).
Note that all the remainders it gives, when divided by 2, by 3, etc. are periodic. And if $F(t)$ sometimes is divisible by a prime p_1 and sometimes by a prime p_2, then eventually $F(t)$ (for some special arguments t) will be divisible by them both: $p_1 \cdot p_2$.
Now, all you need to show that there are infinitely many primes that sometimes divide the values of $F(t)$. At this point remember the proof that there are infinitely many primes. Assume that this is not true - i.e. $F(t)$ is divisible by only finitely many primes. Then plug into $F(t) = t^2 + t + 1$ the number $t = p_1 \cdot p_2 \ldots \cdot p_k + 1$ their product plus 1.

Hint 2.8: Use Chinese remainder theorem to avoid looking at *all* possible n. Just look at the prime powers p^k (and all the remaining n can be obtained by combining the solutions for p^k in a certain way).
Next, consider two separate cases: $n = 2^k$ (you can now pick b so that it is inverse of 3 modulo 2^k - so that the term $9b^2 - 1$ is congruent to 0). On the other hand, if $n = p^k$ for some other $p \neq 2$, then pick a equal to inverse of 2 modulo p^k for similar reasons.

Hint 2.9: The remainders of Fibonacci numbers when divided by any fixed d are periodic (because the pairs of neighboring remainders eventually start to repeat). What is more interesting: All the remainders of Fibonacci sequence are "clean periodic" (not just "eventually periodic") - every remainder belongs to the period. If $F_0 = 0$ (divisible by any d), then it means that infinitely often F_n will be divisible by that d.
(a) is simple - since F_0 is divisible by 1001, then the remainder 0 is clearly in the period (modulo 1001).
For **(b)** and **(c)** you need to factorize 1001 as a product of three prime factors and search for the combinations of remainders (as per Chinese remainder theorem).

Hint 2.10: Statement **(a)** is clearly false. Just start from 2 and you will find a sequence, where every member is divisible by some small prime.
For **(b)** you need to express some segment of k subsequent numbers as an overlap of several arithmetic progressions with prime differences $d < k$ (so that every progression contains at least two members among these k subsequent numbers and all the k numbers are covered at least by one sequence).
This is doable when $k = 17$. See https://bit.ly/2Q2XASA. Finally - use Chinese remainder theorem to find an actual value N such that the numbers from N to $N + 16$ (inclusive) give the remainders you need.