ELEMENTARY NUMBER THEORY

CIPRIAN MANOLESCU

1. A few results

An integer m is **divisible** by n if $\frac{m}{n}$ is an integer. Then m is called a **multiple** of n and n is called a divisor of m. We write $m|n$.

An integer $p > 1$ is called **prime** if its only positive divisors are 1 and p.

Theorem 1.1 (Euclid)**.** *There exist infinitely many primes.*

Theorem 1.2 (The Fundamental Theorem of Arithmetic)**.** *Any integer $n > 1$ has a unique representation (up to reordering of factors) as a product of primes:*

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}.$$

Given positive integers m and n, we denote their **greatest common divisor** by $\gcd(m, n)$ and their **least common multiple** by $\mathrm{lcm}(m, n)$. The numbers m and n are called **relatively prime** if $\gcd(m, n) = 1$.

Theorem 1.3 (Bézout)**.** *If $\gcd(m, n) = d$, there exist integers x and y such that $mx + ny = d$.*

If m divides $a - b$, we write

$$a \equiv b \pmod{m}$$

and say that a and b are **congruent** modulo m. Congruence modulo m is an equivalence relation, in that it splits $\mathbb{Z}$ into equivalence classes

$$\hat{0}, \hat{1}, \dots, \widehat{m-1}$$

where

$$\hat{k} = \{a \in \mathbb{Z} \mid a \equiv k \pmod{m}\}.$$

The equivalence classes are called **residue classes**, and form a set

$$\mathbb{Z}/m = \{\hat{0}, \hat{1}, \dots, \widehat{m-1}\}.$$

We can add and multiply equivalence classes as usual. We say that $\mathbb{Z}/m$ is a **ring**.

When $m = p$ is prime, every nonzero residue has an inverse. That is, given $\hat{a} \in \mathbb{Z}/p$, there exists $\hat{b} = \hat{a}^{-1} \in \mathbb{Z}/p$ such that $\hat{a} \cdot \hat{b} = \hat{1}$, i.e.,

$$ab \equiv 1 \pmod{p}.$$

We say that $\mathbb{Z}/p$ (for p prime) is a **field**.

More generally, we have:

Theorem 1.4 (The Chinese Remainder Theorem)**.** *Let $n_1, \dots, n_k$ be pairwise relatively prime integers, and $a_1, \dots, a_k$ arbitrary integers. Then there exists an integer x such that*

$$x \equiv a_i \pmod{m_i}$$

for all $i = 1, \dots, k$.

2. Problems

1. If m and n are positive integers, show that

$$\gcd(m,n) \cdot \mathrm{lcm}(m,n) = mn.$$

2. (a) Show that $\sqrt{3}$ is irrational. (b) Show that $\sqrt{3}+\sqrt{5}$ is irrational.

3. Show that $2^{2x+1}+1$ is divisible by 3, for any x.

4. Show that $4^{3x+1}+2^{3x+1}+1$ is divisible by 7.

5. Find a formula for all possible pairs of integers (x,y) such that $25x-10y=5$.

6. What are the last two digits of 3^{1234}?

7. Prove that if $2n+1$ and $3n+1$ are both perfect squares, then n is divisible by 40.

8. Prove that the difference of the squares of any two odd numbers is divisible by 8.

9. Find 20 consecutive composite numbers.

10. Prove that the number $1,000,003$ cannot be written as a sum of two perfect squares.

11. (a) Find the inverse of each nonzero residue class modulo 11. (b) Find $\hat{x} \in \mathbb{Z}/11$ such that $\hat{x} \cdot \hat{5} = \hat{2}$.

12. Which residue classes modulo 9 admit inverses? Find those inverses.

13. Find the smallest positive integer n such that $n/2$ is a perfect square, $n/3$ is a perfect cube, and $n/5$ is a perfect fifth power.

14. Prove that if ab, ac and bc are perfect cubes for some positive integers a, b, c, then a, b and c must also be perfect cubes.

15. Do there exist a million of consecutive integers, each of which contains a repeated prime factor? (*Hint:* Use the Chinese Remainder Theorem.)

16. Find all integers x such that $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod 6$.

17. Show that there exist infinitely many primes of the form $4k-1$. (*Hint:* Suppose there are only finitely many, say $p_1, \dots, p_k$. Consider the number $(p_1 \dots p_k)^2 - 1$.)

18. (a) Find the highest power of 3 in $100! = 1 \cdot 2 \cdot \dots \cdot 100$. (b) Find the number of zeros at the end of the decimal representation of 100!.

19. What is the largest positive integer n for which n^3+100 is divisible by $n+100$?

20. Let d be a positive integer not equal to $2, 5$, or 13. Show that one can find distinct a, b in the set $\{2, 5, 13, d\}$ such that $ab-1$ is not a perfect square.