ASSIGNMENT 14: NUMBER THEORY

MARCH 17, 2024

Simple problems

1. Find the remainder upon the division of 17^{2022} by 7.

2. In how many zeroes does the number 100! end?

3. Prove that $2222^{5555} + 5555^{2222}$ is divisible by 7

4. How many perfect squares are divisors of of the product $1! \cdot 2! \cdots 9!$?

5. Prove that, given any prime $p > 5$, there is a number of the form $111\dots1$ which is divisible by p. [Hint: look at remainder upon division by p]

Euclid's algorithm revisited

Recall the following simple statement.
If a, b are positive integers, with $a \geq b$, then

- Pairs (a, b) and $(a - b, b)$ have same common divisors (i.e., d is a common divisor of (a, b) if and only if it is a common divisor of $(a - b, b)$)
- Let r be the remainder upon division of a by b: $a = bq + r$. Then pairs (a, b) and (b, r) have the same common divisors.

This implies the Euclid algorithm of finding the greatest common divisor of (a, b): start with pair (a, b) and replace it by $(b, r = a \mod b)$; repeat until you have pair $(d, 0)$. The gcd doesn't change during this, so $\gcd(a, b) = \gcd(d, 0) = d$.

This also implies more useful corollaries.

1. A number n is a common divisor of (a, b) if and only if n is a divisor of $d = \gcd(a, b)$.

2. A number c can be written as a combination of a, b (i.e. in the form $ax + by$, with x, y integer) if and ony if c is a multiple of $d = \gcd(a, b)$.

3. A number a is invertible mod n (i.e. there exists an integer x such that $ax \equiv 1 \mod n$) if and only if $\gcd(a, n) = 1$); in this case, numbers a, n are called *relatively prime*.

Harder problems

6. Let $a_n = 111\dots1$ (n ones).
Find $\gcd(a_{179}, a_{57})$.

7. What is the largest integer that can not be written in the form $17x + 39y$ with non-negative integer x, y?

8. Sasha has drawn an $n \times n$ rectangle on a square ruled paper and then drawn a diagonal of that rectangle.

(a) How many nodes will this diagonal contain? [A node is a point where the grid lines intersect.]

(b) Into how many segments will this diagonal be divided by its intersectiosn with the grid lines?

9. (a) Let $a > b$ be positive integers. Show that then

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^{a-b} - 1, 2^b - 1)$$

(b) Show that

$$\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1.$$

(c) Does the same work if we replace 2 by other numbers?

10. (a) Show that $2^{3k} + 1$ is divisible by $2^k + 1$

(b) Show that the same is true if we replace 3 by any odd integer: e.g., $2^{5k} + 1$ is also divisible by $2^k + 1$

(c) Show that if a number $2^m + 1$ is a prime, then m itself is a power of 2.

(d) Find as many prime numbers of the form $2^m + 1$ as you can. Whoever gets most, gets a special prize!