

ASSIGNMENT 2: NUMBER THEORY

SEPTEMBER 29, 2024

EUCLID'S ALGORITHM

Consider the following 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 gives way to the Euclid algorithm of finding the greatest common divisor of (a, b) : start with pair (a, b) and replace it by $(b, r = a \bmod b)$; 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 only 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 $ax \equiv 1 \pmod n$) if and only if $\gcd(a, n) = 1$; in this case, numbers a, n are called *relatively prime*.

SIMPLE PROBLEMS

1. Prove that $2222^{5555} + 5555^{2222}$ is divisible by 7
2. How many perfect squares are divisors of the product $1! \cdot 2! \cdot \dots \cdot 9!$?
3. There are 200 lightbulbs in a row, labeled 1 – 200, that all start turned off. A guard comes in and flips all the switches. Then he flips all the switches for the even lightbulbs, then he flips the switches for the multiples of 3. He continues to flip every multiple of k until $k = 200$. Which bulbs will be on at the end?
4. Prove that, given any prime $p > 5$, there is a number of the form $111\dots 1$ which is divisible by p . [Hint: look at remainder upon division by p]
5. Show that for any prime $p > 3$, then $p^2 \equiv 1 \pmod{24}$.
6. In an account with \$400 in it, you can make deposits of exactly \$132 and withdrawals of exactly \$210. What is the maximum amount of cash you can get out of the account? Note that the balance cannot go negative.

HARDER PROBLEMS

6. Show that if p and $p^2 + 2$ are prime, then $p^3 + 2$ is also prime.
7. Let $a_n = 111\dots 1$ (n ones).
Find $\gcd(a_{179}, a_{57})$.
8. What is the largest integer that can not be written in the form $17x + 39y$ with non-negative integer x, y ?
9. 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 intersection with the grid lines?
10. (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?
- 11.** (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!