Math 214 Fall 2022 Number Theory I

GCD – greatest common divisor

Sankar Sitaraman – nature-lover.net/math

Math Dept, Howard University

9-18-2022

Outline

Definition of GCD

$gcd(a, b)$ is the greatest integer d such that d divides both a and b.

$gcd(a, b) = 1$ means they have no common divisors.
We say a, b are relatively prime to each other.

Finding gcd by factoring

You can find gcd by factoring.

$$a = p_1^{n_1} p_2^{n_2} \ldots . p_k^{n_k}, b = p_1^{m_1} p_2^{m_2} \ldots . p_k^{m_k}$$

$$\implies gcd(a, b) = p_1^{min(n_1, m_1)} p_2^{min(n_2, m_2)} \ldots . p_k^{min(n_k, m_k)}.$$

Euclidean Algorithm

Euclidean Algorithm finds gcd of two integers using repeated division.

First we can divide any integer n by another integer m and say $n = mq + r$ where q is the *quotient* and r is the*remainder.*

We let $r_0 = b, r_{-1} = a$. Assume that $a, b > 0$. If they are negative, same process works, with slight modifications.

Then dividing a by b we get $a = q_1 b + r_1$. Now we replace a, b by $b = r_0 \to a, r_1 \to b$ respectively and repeat the process until $r_i = 0$ for some $i > 0$.

Then the previous remainder r_{i-1} is the gcd.

Why Euclidean Algorithm works

At every stage, notice that the remainder r_i must be *strictly* smaller than the previous remainder r_{i-1}.
Also, the remainders cannot be negative.
So if we start with $r_0 = b$, a finite number, then the sequence $b > r_1 > r_2 \ldots$. must equal 0 at some point.

Suppose r_{i-1} is the smallest nonzero remainder and $r_i = 0$.
Why is this the gcd?
To see this, notice that r_{i-1} divides r_{i-2} because the remainder $r_i = 0$.
Then from $r_{i-3} = q_{i-1} r_{i-2} + r_{i-1}$ we see that it divides r_{i-3} also.
Continuing like this, we get that it divides both a and b.
If another divisor d divides both, working forward from a, b we can show it divides r_{i-1} also.

An algebraic definition of the GCD

The GCD is also defined as the smallest positive value of $ax + by$ where x, y are integers.

Idea of proof:
Every common divisor of a, b will divide $min(ax + by)$. So the gcd would also divide it!

On the other hand, working backward from the Euclidean algorithm, we see that the gcd generated by that algorithm is of the form $ax + by$. It is also the smallest because the gcd divides every number of form $ax + by$.
Basically, $gcd(a, b)$ is the smallest positive integer you can get by repeatedly adding and subtracting a and b.

An algebraic definition of the GCD – all solutions

If $gcd(a, b) = g$ then the equation $ax + by = g$ is a linear equation!

We can figure out ALL the *integer* solutions (x, y) for the equation $ax + by = g$.

Suppose (x_1, y_1) is a solution. Then all the solutions are given by

$$(x_1 + k(b/g), y_1 - k(a/g)),\ k \in \mathbb{Z}.$$

In particular, if $g = 1$, then all solutions are of form $(x_1 + kb, y_1 - ka)$.

Role of Algebra in Number Theory

1. The definition of $gcd(a, b)$ in terms of linear combinations of a and b is quite a useful one, especially as we try to generalize the notion of GCD to other rings.
2. This is just one example of how properties of numbers can be better understood using an abstract framework.
3. In class we saw how the rational points on an elliptic curve form a group. Later we will see how to make a group out of the remainders mod any integer.

contd: Role of Algebra in Number Theory

HW3, problem 5: Show that the rational points on a unit circle form a group as follows: If $P = (\cos(2\pi a), \sin(2\pi a))$ and $Q = (\cos(2\pi b), \sin(2\pi b))$ are two rational points then let $P + Q = (\cos 2\pi(a+b), \sin 2\pi(a+b))$. Show that the set of rational points on the unit circle form a group using the addition law described above. What is the inverse element and what is the identity element? Is it an abelian group? What is the order of an element P if $a = m/n$ written in the reduced form (i.e, with m, n relatively prime) ?