MATH240 – Lecture 12

Enlai Li

February 10, 2023

1 Last lecture

1.1 Euclid's algorithm

$$a, b \in \mathbb{Z} \to gcd(a, b) = d$$

1.2 Bezout's theorem

$$d = gcd(a, b) \to d = sa + tb$$

1.3 Corollary

If $c|a$ and $c|b$, then $c|gcd(a, b)$

1.4 Proof

$$c|a \text{ and } c|b$$
$$\Rightarrow a = kc \text{ and } b = nc$$

Then

$$\begin{aligned} d &= gcd(a, b) \\ &= sa + tb, \text{ where } s, t \in \mathbb{Z} \\ &= sac + tbc \\ &= c(sk + tn) \Rightarrow c|d \end{aligned}$$

2 Coprime

two integers a,b are coprime if gcd(a,b) = 1 ex:

- 42 and 515 are coprime
- a = 7, n = not a multiple of 7
  $\Rightarrow gcd(7, 9) = 1$

That's because the only divisions of 7 are 1 (only possibility left) and 7 (not a divisor of n)

This works for any other prime number

Theorem a and b are coprime $\iff 1 = sa + tb$
proof Bezout when d=1

$$\begin{gathered} 1 = sa + tb \\ \text{Let } d = gcd(a, b) \\ \text{Goal: prove } d = 1 \\ d|a \text{ and } d|b \\ \Rightarrow d|sa + tb \text{ (elementary property of 1)} \\ \Rightarrow d|1 \\ \Rightarrow d = 1 \end{gathered}$$

3 prime numbers

p is prime $\iff p > 1$ and its only positive divisors are 1 and p
ex:

$$2, 3, 5, 7, 11, 13, \ldots$$

A number that is not a prime is called composite ex:

$$42 = 6 \times 7$$

n is composite $\iff n = ab$, where $a, b > 1$

Prime numbers are interesting in number theory because they are easy to understand, yet they easily lead to very difficult problems

3.1 Goldbach's conjecture (open since 1742)

Every even number $n > 2$ is the sum of two primes
ex:

$$\begin{gathered} 42 = 19 + 23 \\ 20 = 13 + 7 \end{gathered}$$

It's been tested by computers to work up to very large numbers (400 trillions), no one has proved it

3.2 Fundamental Theorem of Arithmetic (FTA)

primes are a fundamental role in number theory as the building blocks of all integers
ex: we can write 42 as product of primes

$$\begin{aligned} 42 &= 6 \times 7 \\ &= 2 \times 3 \times 7 \end{aligned}$$

We can always decompose a number as a product of primes, in a unique way. We need the following lemma to prove this:
Lemma if p is prime and $p|ab$ then $p|a$ or $p|b$
ex:

We really need p to be prime for this to work

$$3|42 = 6 \times 7 \text{ and indeed } 3|6$$
$$\text{Counter-example } 14|42 = 6 \times 7 \text{ but } 14\not|6 \text{ and } 14\not|7$$

Proof

$$\text{Assume } p|ab, p \text{ is prime } \Rightarrow ab = px$$
$$\text{Goal: } p|a \text{ or } p|b$$
$$\text{Assume } p\not|a, \text{ New goal} p|b$$
$$\text{Since } p\not|a \text{ then p and a are coprime}$$

$$\begin{aligned} \Rightarrow 1 &= sp + ta \\ b &= spb + tab \\ &= spb + tpx \\ &= p(sb + tx) \\ &\Rightarrow p|b \end{aligned}$$

□

Let $n \geq 2$ be an integer, the we can find prime numbers

$$p_1 \leq p_2 \leq p_3 \cdots \leq p_k$$

such that $n = p_1 \leq p_2 \leq p_3 \cdots \leq p_k$ moreover this list of prime is unique
Proof We must prove existence and uniqueness of the prime factorization of n. We do both in a single proof by strong induction!
Base case: n = 2

- Existence: n = 2 (prime)
- Uniqueness: $2 = p_1 p_2 p_3 \ldots p_k$, where $p_1 = 2$ and $p_2 p_3 \ldots p_k = 1$

Induction step Asuume the FTA true for all integers $< b$. We want to prove it for n. 2 cases:
n is prime: same as base case (replace 2 by n)
n is composite:

- Existence: $n = ab, n > a, b \geq \mathbb{Z}$, by induction hypothesis we can write

$$a = p_1 p_2 p_3 \cdots \leq p_k$$
$$b = q_1 q_2 q_3 \cdots \leq q_l$$
$$\Rightarrow n = p_1 p_2 \ldots p_k q_1 q_2 q_l$$

  This is a product of primes! rearrange them in increasing order and we have a solution

- Uniqueness: Assume the two prime decompositions of n

$$
\begin{gathered}
n = p_1 p_2 p_3 \dots p_k \text{, where } p_1 \leq \dots \leq p_k \\
n = q_1 q_2 q_3 \dots q_l \text{, where } q_1 \leq \dots \leq q_l \\
p_1 | n \Rightarrow p_1 | q_1 q_2 \dots q_l \\
\text{By the lemma} \\
p_1 | q_1 \text{ or } p_1 | q_2 \text{ or } \dots \text{ or } p_1 | q_l \\
\Rightarrow p_1 = q_1 \text{ or } p_1 = q_2 \text{ or } \dots \text{ or } p_1 = q_l \\
\Rightarrow p_1 = q_1 \text{, for some } i
\end{gathered}
$$

  Now we consider the number $\frac{n}{p_1} < n$ by the induction hypothesis, all primes $p_2 p_3 \dots p_k$ are the same as the primes $q_1 q_2 q_3 \dots q_l$. All primes $p_1 p_2 p_3 \dots p_k$ are the same as $q_1 q_2 q_3 \dots q_l$

$$
k = l \text{ and } p_1 = q_1 \text{ and } \dots \text{ and } p_k = p_l
$$

□

We can regroup repeated factors and write the prime decomposition with exponents (canonical form)

$$
n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k} \text{, where } p_1 < \dots < p_k \text{ and } \alpha_1 > \dots > \alpha_k > 0
$$

ex:

$$
\begin{aligned}
72 &= 2 \times 36 \\
&= 2 \times 2 \times 2 \times 3 \times 3 \\
&= 2^3 \times 3^2
\end{aligned}
$$

We could in fact allow 0 in the exponents but we could lose uniqueness of the list of primes
Lemma

$$
\begin{gathered}
\text{With all exponents } \leq 0 \text{, let} \\
a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k} \\
b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_k^{\beta_k} \\
\text{Then} \\
a | b \iff \alpha_i \leq \beta_i \text{, for all } i
\end{gathered}
$$

Ex:

$$
\begin{gathered}
72 = 3^2 2^3 \\
36 = 3^2 2^2
\end{gathered}
$$

Proof Suppose $a|b$ then $b = ac$
Let $c = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$, Then $c = ac$

$$p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_k^{\beta_k} = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k} \times p_1^{q_1} p_2^{q_2} p_3^{q_3} \dots p_k^{q_k}$$

Exponents are unique (by FTA)

$$\beta_1 = \alpha + q_1 \geq \alpha_1$$
$$\beta_2 = \alpha + q_2 \geq \alpha_2$$
$$\beta_k = \alpha + q_k \geq \alpha_k$$

Assume $\alpha_i \leq \beta_i, \forall i$ Let

$$p_i = \beta - \alpha_i, \forall i \geq 0$$

Let $c = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_k$ Then $b = acRaa|b$