3. Prime numbers and the Fundamental Theorem of Arithmetic

(20 slides)

3.1 Def. A natural number greater than 1 and whose only divisors in $\mathbb{N}$ are 1 and itself is called a prime number.

EX: 2, 3, 5, 7, 11, ...

A number which is not prime is called a composite number.

3.2. Theorem. Every integer $n > 1$ is either a prime or a product of primes.

Proof. The proof is by induction on $n \in \mathbb{N}$. The theorem is true for $n = 2$ because 2 is a prime. Assume that it is true for all integers less than n. If n is not a prime

n has a divisor $d \neq 1, d \neq n$ and $n = ed$ for some integer $e \neq 1, e \neq n$. Then, $1 < d, e < n$ and by induction hypothesis, both e and d are products of prime numbers and so so is n. □

3.3) **Theorem 3** (Euclid) There are an infinite number of primes.

Proof (Euclid) Deny. Assume that $p_1, \ldots, p_r$ are the only prime integer. Consider $N = p_1 \cdots p_r + 1$. Then either N is a prime (and so equal to one of the p_i's by hypothesis) or n is product of primes. However $n \neq p_i$ for each $i = 1, \ldots, r$ and no p_i divides N, because otherwise, p_i divides 1 but $p_i > 1$. So, this contradiction implies that, ☒ if N is not a

then there is at least one prime different from $p_1, \ldots, p_r$. □

(3.4) Remarks

(i) Euclid's proof is still considered to be one of the illustration of ~~what~~ a the concept of a proof and the best demonstration of the elegance in Mathematics.

(ii) Many other proofs of the infiniteness of the cardinality of the set $\mathbb{P}$ of primes is known. We see several in this course.

One approach is to construct an infinite sequence $\{n_i\}_{i=1}^{\infty}$ of pairwise coprime integers. Then, since there is at least one prime dividing each n_i and no prime divides more than one n_i, the union of the

Sets S_i, $i=1,2,\cdots$, of prime divisors of n_i is an infinite subset of $\mathbb{P}$. So, $\mathbb{P}$ also is infinite.

Ex: 1) Consider sequence $\{n_i\}_{i=1}^{\infty}$:

$n_1=2$, $n_2=n_1+1$, $n_3=n_1n_2+1$, $\cdots$, $n_k=n_1\cdots n_{k-1}+1$.

Since $n_i>1$, $S_i\neq\phi$. Since $(n_i,n_j)=1$ for $i\neq j$, S_i and S_j are disjoint. So, $S=\bigcup_{i=1}^{\infty}S_i$ is an infinite subset of $\mathbb{P}$. □

Ex.2: (Fermat numbers) Consider the sequence $\{F_n\}_{n=0}^{\infty}$ of Fermat numbers, where $F_n=1+2^{2^n}$.

Thus, $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$, $\cdots$

Claim: For $m,n\in\mathbb{N}$, $(F_m,F_n)=1$ if $m\neq n$.

Proof. Let $d=(F_m,F_n)$. We may assume $m>n$.

$$\frac{F_m-2}{F_n}=\frac{(2^{2^n})^{2^{m-n}}-1}{(2^{2^n}-1)}=\frac{x^k-1}{x-1}=(x^{k-1}+x^{k-2}+\cdots+x+1)$$

where $x = 2^{2^n}$ and $k = 2^{m-n}$. So, $F_n \mid F_m - 2$.
Since $d \mid F_n$, $d \mid F_m - 2$. But, $d \mid F_m$ also. So, $d \mid 2$. But F_n's are all odd. So, $d = 1$. □.
Thus, $\mathbb{P}$ contains an infinite subset.

Two remarks about Fermat numbers.

(a) Fermat conjectured that F_n is a prime number for each integer $n \geq 0$ and verified that F_i, $i = 0, 1, 2, 3, 4$, are all prime. In fact, these are the only primes among F_n's. We do not know if there are any other primes of the type F_n, let alone the infiniteness of the set of Fermat primes.
We show that F_5 is not prime. ($F_5 = 4294967297$)
Let $a = 2^7$ and $b = 5$. Then, $1 + ab = 641$.

$$1 + ab - b^4 = 1 + (a - b^3)b = 1 + 3b = 2^4.$$

Now, $F_5 = 2^{2^5}+1 = 2^{32}+1 = 2^4a^4+1 = (1+ab-b^4)a^4+1$

$= (1+ab)a^4 + (1-a^4b^4)$

$= (1+ab)[a^4+(1+a^2b^2)(1-ab)]$ is not prime!

b) Another reason for the interest in Fermat numbers is that Gauss showed (very early in life!) a regular n-gon in the Euclidean plane can be constructed using only ruler and compass if, and only if, $n = 2^k$ or $n = 2^k p_1 \cdots p_s$, where $k \geq 0$ and $p_1, \ldots, p_r$ are Fermat primes.

Here, 'using only ruler and compass' means one is allowed only draw straight lines joining two points and draw arcs.

- Bisecting a line with given end points is an example of construction using only

ruler and compass we learn in schools.

Construction of regular n-gons for $n = 2^k$, $2^k \times 3$, $2^k \times 5$, $2^k \times 17$ were known since the time of Greek geometers. Before Gauss, no one suspected that a regular 17-gon can be constructed. Gauss was so proud of this achievement that he wanted this to be inscribed on his tomb stone. (It was not, but later inscribed on a side of a monument erected in Brunswick in his honour.).

(3.5) (i) If a prime p does not divide a, $a \in \mathbb{Z}$, then $\gcd(p, a) = 1$.

Pf. Let $d = (p, a)$. Since $d \mid p$ and p is a prime, either $d = 1$ or $d = p$. Since $d \nmid p$, $d = 1$. □

(ii) If $a, b \in \mathbb{Z}$, p a prime, and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. If $p \nmid a$, by (i) $(p, a) = 1$. By Euclid's lemma, there exist integers x, y such that $1 = ax + py$.

So, $b = abx + pby$. Since $p \mid ab$ and $p \mid pby$, $p \mid b$. □

Cor: If a prime p divides the product $a_1 \cdots a_r$, $a_i \in \mathbb{Z}$, then $p \mid a_i$ for some i.

Proof. Easy induction. □

(3.6) The importance of the prime number comes from

Thm: (Fundamental Theorem of Arithmetic)
Each integer $n > 1$ can be expressed as a product of prime numbers. This expression is unique except for the order of the factors. Explicitly, if

$$n = p_1 p_2 \cdots p_r \quad \text{and} \quad n = q_1 \cdots q_s.$$

where $p_1, \cdots, p_r$ are (not necessarily distinct) primes and $q_1, \cdots, q_s$ are also (not necessarily distinct) primes, then

(i) $r \geq s$; (ii) for each t, $1 \leq t \leq r$, there exist t', $1 \leq t' \leq s$ such that $p_t = q_{t'}$ and $|\{ l : p_l = p_t \}| = |\{ l' : q_{l'} = q_{t'} \}|$

Proof. (i) Existance: That n can be written as a product of primes follows by induction on n.

(ii) uniqueness of the factorization is by induction on n:

If n is prime, then there is nothing to prove.

Suppose, n is not a prime and has 2 factorizations

$$n = p_1 \cdots p_r = q_1 \cdots q_s,$$

where p_i's and q_i's are all primes, not necessarily distinct.

Since $p_1 \mid n = q_1 \cdots q_s$, by Cor. to 3.5(ii), $p_1 \mid q_j$ for some j. Rearranging $q_1, \ldots, q_s$ if necessary, we can assume that $j = 1$. Then, since p_1 and q_1 are primes and $p_1 \mid q_1$, $p_1 = q_1$. So,

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s$$

are two prime factorizations of $n/p_1 < n$. (If $\frac{n}{p_1} > 1$, ✓)

by induction hypothesis, $r = s$ and there exists a bijection $\theta : \{2, \ldots, r\} \to \{2, \ldots, s\}$ such that $p_i = q_{\theta(i)}$. (Of course, if $n/p_1 = 1$, $n = p_1$ and the theorem is trivially true.). □

Remark. In view of this theorem, a prime factorization of $n > 1$ can be written as:

$n = p_1^{a_1} \cdots p_t^{a_t}$, p_i's are primes, $p_i \neq p_j$ for $i \neq j$

$p_1 < p_2 < \cdots < p_t$, $a_i \geq 1$ for all i.

(3.7) Let $n = \prod_{i=1}^{r} p_i^{e_i}$ and $m = \prod_{j=1}^{s} q_j^{g_i}$ be prime decompositions of $m, n \in \mathbb{Z}$, $e_i, f_i > 0$, $p_i \neq p_j$ and $q_k \neq q_l$ for $i \neq j$ and $k \neq l$.

~~By introducing~~ If a prime p appears in the factorization of only one of them, we introduce p^0 in the other and rewrite the above factorizations as

$$n = \prod_{i=1}^{t} p_i^{e_i'} \quad \text{and} \quad m = \prod_{i=1}^{t} p_i^{f_i'}$$

where $p_1, \ldots, p_t$ are distinct primes and $e_i' \geq 0$ and $f_i' \geq 0$.

DEF: Recall that the least common multiple $[a,b]$ of $a, b \in \mathbb{Z}$ is an integer $m > 0$ such that: (i) $a|m$, $b|m$; and (ii) $a|n$, $b|n$ for $n \in \mathbb{N} \Rightarrow m|n$.

Thm: (i) $n \mid m \iff e_i' \leq f_i'$ for each $i = 1, \dots, t$;

(ii) $\gcd(n,m) = \prod_{i=1}^{t} p_i^{\min(e_i', f_i')}$;

(iii) $\operatorname{lcm}[n,m] = \prod_{i=1}^{t} p_i^{\max(e_i', f_i')}$.

Proof: Exercise. □

Exc: Show that given any two integers a, b, their least common multiple exists and it is unique. Show that $[a,b] \cdot (a,b) = ab$.

(3.7) ~~[illegible]~~ allows us to read off the gcd and lcm of two integers. The following method due to Euclid gives an easy algorithm to find the gcd of any two integers (and so the lcm by the exercise above).

(3.8) Euclidean Algorithm

This algorithm depends on ~~the~~ repeated use of

(3.8.1) **Theorem** (The division algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then, there exists unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < b.$$

q is called the quotient and r the remainder.

$b)\overline{a}\,(q$
$\quad\;\; r$

Proof: (i) Consider the set

~~Let~~ $S = \{ y \in \mathbb{Z} : y = a - bx, x \in \mathbb{Z}, y \geq 0 \} \subseteq \mathbb{N}$.

Then, S is non empty (?). By the well-ordered principal of natural numbers (Lect. 1, iv) S has a smallest element, say $r = a - bq$.

Then $a = bq + r$, $r \geq 0$. We now show that $r < b$.

Suppose, for a contradiction, that $r \geq b$.

Then, $0 \leq r - b < r$ and $r - b = a - b(q+1) \in S$, a contradiction to the choice of r as the smallest element in S. So, $r < b$. This completes the proof of the existance of q and r.

(ii) Uniqueness of q and r: Suppose that there is another pair of integers q', r' such that

$$a = bq + r = bq' + r', \quad 0 \leq r, r' < b.$$

Then, $b(q - q') = r' - r$. So, $b \mid (r - r')$. Since $0 \leq r, r' < b$, it follows that $r = r'$. Now, since $b \neq 0$ and $b(q - q') = 0$, it follows that $q = q'$. □

Note: The proof not only shows the existance of q and r, but also a method to find q and r: Start from a ($a > 0$) and successively find: a, $a - b$, $a - b - b$, ... , $a - tb$ until one

arrives at the smallest non negative integer which is r. (How do you know that you arrive at a non negative integer?). If $a<0$ and $-a = bq + r$, $0 \le r < b$, $a = b(-q-1) + (b-r)$. ∎

(3.8.2) Lemma. If $a = bq + r$, then $(a,b) = (b,r)$.

Proof. Let $d = (a,b)$. Then, $d|b$ and $d|a-bq = r$. So, d is a common divisor of b and r.

If c is a divisor of b and r, then $c|qb+r = a$ also. So, $c|(a,b)$ by the definition of $\gcd(a,b)$.

So, Thus, $d|c$ and $c|d$. So, $d = c$. □

The following algorithm to find the gcd of two integers is in Euclid's famous book 'Elements'. Perhaps, it was known earlier.

3.8.3 **Theorem** (Euclidean algorithm)

Let a, b be positive integers, $b \nmid a$. Let $r_0 = a$, $r_1 = b$. Applying the division algorithm successively we obtain a set of nonnegative integers $r_2, \cdots, r_n, r_{n+1} = 0$ satisfying the relations:

$$r_0 = r_1 q_1 + r_2 \qquad 0 < r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3 \qquad 0 < r_3 < r_2$$
$$\vdots$$
$$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1} \qquad 0 < r_{n-1} < r_{n-2}$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$$
$$r_{n-1} = r_n q_n + r_{n+1} \qquad r_{n+1} = 0.$$

Then, $r_n = \gcd(r_0, r_1) = \gcd(a, b)$.

Proof. There is a stage at which $r_{n+1} = 0$, because r_i's are decreasing and nonnegative integers. By the previous lemma,

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

□

Note that this is the method taught in elementary schools to find gcd even today!

Example 1: $\gcd(12378, 3054) = 6$

$$\begin{aligned}
12378 &= 8(3054) + 162 \\
3054 &= 18(162) + 138 \\
162 &= 1(138) + 24 \\
138 &= 5(24) + 18 \\
24 &= 1(18) + 6 \\
18 &= 6(3) + 0.
\end{aligned}$$

$$\begin{array}{r|l|l|r}
18 & 3054 & 12378 & 8 \\
 & \cdots & \cdots & \\
 & 138 & 162 & 1 \\
 & & 138 & \\
 & & \cdots & \\
 & 0 & 6 &
\end{array}$$

(3.8.4). We saw earlier that if $a, b \in \mathbb{Z}$ and $d = (a,b)$, then $d = ax + by$ for some integers x and y. The Euclidean algorithm gives a method to find x and y.

From Thm. 3.8.3,

$$(a,b) = r_n = r_{n-2} - r_{n-1} q_{n-1}$$

$$= r_{n-2} - q_{n-1}(r_{n-3} - r_{n-2} q_{n-2})$$

$$= (1 + q_{n-1} q_{n-2}) r_{n-2} + (-q_{n-1}) r_{n-3} = \cdots$$

Continuing in this manner, we get integers x, y such that $(r_n =) \gcd(a,b) = r_0 x + r_1 y = ax + by$. □

Ex. Consider the Example 1:

$$6 = 24 - 18 = 24 - (138 - 5 \times 24) = 6(24) - 138$$

$$= 6(162 - 138) - 138 = 6(162) - 7(138)$$

$$= 6(162) - 7[3054 - 18(162)] = 132(162) - 7(3054)$$

$$= 132[12378 - 8(3054)] - 7(3054).$$

$x =$

$= 132(12378) + (-535)3054.$ □

Ex: Find the gcd of $(42823, 64094) =: d$ and find x, y such that $d = 42823x + 64094y$.

(8.3.4) GCD of $(a_1, \cdots, a_n)$, $a_i \in \mathbb{Z}$

For integers a_1, a_2, a_3,

$(a_1, (a_2, a_3)) = ((a_1, a_2), a_3) = ((a_1, a_3), a_2)$

and $(a_1, a_2) = (a_2, a_1)$.

So, the integer $(a_1, (a_2, a_3))$ does not change if the order in which a_1, a_2, a_3 is interchanged. We call this common number the greatest common divisor of a_1, a_2, a_3 and denote this common number by $\gcd(a_1, a_2, a_3)$ or just (a_1, a_2, a_3).

For $n > 3$, we define the greatest common divisor by induction:

$d = \gcd(a_1, \cdots, a_n) = (a_1, \cdots, a_n) \overset{\text{def}}{=\!=} (a_1, (a_2, \cdots, a_n))$.

We have:

(1) $d \mid a_i$ for each i and, $c \in \mathbb{Z}$ is such that $c \mid a_i$ for each i, then $c \mid d$. Thus, d is the largest among the common divisors of $a_1, \cdots, a_n$.

(ii) There exists integers $x_1, \cdots, x_n$ such that

$$d = a_1 x_1 + \cdots + a_n x_n. \quad \square$$

Pf: Exercise. $\square$