Lecture 4

Henry Kim BA 6250 R 2–3pm
Yuan yuan Zheng SS 622 M 2:45–3:45 pm
Ann Dranovski F 12–1pm

Chap. 7 Fundamental Thm of Arithmetic

Every integer n can be factorized into a product of primes in a unique way (up to permutation):

$12 = 2\times2\times3 = 2\times3\times2$ $\qquad n = p_1 p_2 \cdots p_r$, p_i not necessarily distinct primes

Claim: Let p be a prime and $p \mid ab$. Then $p \mid a$ or $p \mid b$.
Proof: If $p \mid a$ true. done
If $p \nmid a$. $\gcd(p,a) = 1$ [$\gcd(p,a) \mid p$, so $\gcd(p,a) = p$, but $\gcd(p,a) \mid a$, so $\gcd(p,a) = 1$]
There exists x, y s.t. $px + ay = 1$
$pbx + aby = b$, so $p \mid (pbx + aby)$, $\Rightarrow p \mid b$

Claim: p prime and $p \mid (a_1 \cdots a_r)$, then $p \mid a_i$ for some i. (Prime Divisibility Property)

e.g. E-zone = even number world
$\mathbb{E} = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\}$
m E-divides n if $n = mk$ for some $k \in \mathbb{E}$
say 6 E-divides 12: $12 = 6\times2$
6 not E-divides 18: $18 = 6\times3$, but $3 \notin \mathbb{E}$
E-prime
p is E-prime if it is not divisible by any number.
Remark: In E-zone, a number is not divisible by 1 or itself.
So E-primes are $\cdots, 2, 6, 10, 14, \cdots$

In the E-zone, prime divisibility does not hold.
$p = 6$, E-prime $\quad$ 6 E-divides $10\times18 = 180 = 6\times30$, but 6 E-divides neither 10 nor 18 neither of these E-divisible as well.
In E-zone, every # can be factorized as a product of E-primes, but unique factorization fails.

Remark: $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{-5}, a, b \in \mathbb{Z}\}$ unique factorization fails
$6 = 2\times3 = (1+\sqrt{-5})(1-\sqrt{-5})$, $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ all primes

Hence need to show:
① n can be factorized into a product of primes in some way (we use induction)
② The factorization is unique to permutation (use prime divisibility property)

Induction
Proof: $P(n)$: Statement for $n \geq a$
1st kind: true for $n = a$ $(a=1)$
Assume $P(n-1)$ induction hypothesis
then show $P(n)$
2nd kind: true for all $k < n$ and then show $P(n)$ is true

e.g. $f_1 = 1, f_2 = 1, f_3 = 2, \cdots$ Fibonacci Sequence, find formula for n-th term
$f_n = f_{n-1} + f_{n-2}$, $n \geq 3$

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \quad \forall n$$

use 2nd induction.

Assume true $\forall$ integer $< n$

prove n $\qquad f_n = f_{n-1} + f_{n-2}$

$$= \frac{1}{\sqrt{5}}(\alpha^{n-1} - \beta^{n-1}) + \frac{1}{\sqrt{5}}(\alpha^{n-2} - \beta^{n-2})$$

$$= \frac{1}{\sqrt{5}}\left[\alpha^{n-2}(1+\alpha) - \beta^{n-2}(1+\beta)\right]$$

$$= \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$$

Back to where we start.

Assume it's true for all $n \leq N$.

i.e. we need to prove it is true for $N+1$.

Two possibilities: $N+1$ is a prime (Then we are done)

$N+1$ is not a prime

$N+1 = n_1 n_2$, $n_1, n_2 \leq N$

By our assumption, n_1 & n_2 can be written as a product of primes,

$$\left.\begin{aligned} n_1 &= p_1 \cdots p_r \\ n_2 &= q_1 \cdots q_s \end{aligned}\right\} \; p_i, q_j \text{ are primes.}$$

so $N+1 = n_1 n_2 = p_1 \cdots p_r q_1 \cdots q_s$, done.