LN II a

§1.3

<u>Definition</u>: p is a prime if it has exactly 2 divisors: 1 and p.

<u>Thm</u> (Fund. Thm. of Arithmetics).

$\forall n \geq 2$ $\exists$ primes $p_1 \leq p_2 \leq \dots \leq p_s$ s.t.

$$n = p_1 p_2 \cdots p_s.$$

The factorization is unique.

We will need two Lemmas to prove this Theorem.

<u>Lemma 1</u>: p prime

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Pf: $(a,p) = 1$ or $(a,p) = p$

If $(a,p)=p \Rightarrow p|a$.

Suppose $(a,p)=1$.

Then $\exists$ s,t. (See Proof. Thm 1.1.2)

$$1 = sa + tp.$$

Multiply by b.

$$\left.\begin{aligned} b &= sab + tpb \\ p|ab \quad & p|pb \end{aligned}\right\} \longrightarrow p|b \qquad \square.$$

<u>Lemma 2</u> p prime

$$p \mid a_1 \cdots a_n \Longrightarrow \exists i \quad p|a_i$$

<u>Proof</u> Induction in n.

$n=2$: OK, Lemma 1.

Suppose the Lemma holds for n and

$$p \mid a_1 a_2 \cdots a_n a_{n+1}$$

Then $p \mid (a_1 a_2 \cdots a_n) a_{n+1}$

<u>lemma 1</u> says

$p \mid a_{n+1}$ done

or

$p \mid a_1 \cdots a_n$

The Induction Hypothesis says $\exists i$

$p \mid a_i$ $\square$

Proof Fund Thm of Arithmetics

<u>Part I</u> Existence

Induction in n.

$n=2$ Done.

Suppose the Theorem holds for $k \leq n$.

If $n+1$ is a prime: Done

Suppose $n+1$ not a prime

$$n+1 = a \cdot b$$

$a, b > 1$.

$a = p_1 \cdots p_s$ $\quad p_k, q_\ell$ prime.

$b = q_1 \cdots q_t$

$n+1 = p_1 \cdots p_s q_1 \cdots q_t$ $\quad$ Done.

- Part II Uniqueness.

- $n = p_1 \cdots p_r$ $\quad p_1 \leq p_2 \leq \cdots \leq p_r$.

Induction

r = 1: $n = p$.

Suppose $n = q_1 \cdots q_s$ $\Big\}$ $p = q_1 \cdots q_s$. p prime.

- So $s = 1$ and $q_1 = p$. $\quad$ Done

- Suppose uniqueness holds for r.

Let $n = p_1 \cdots p_{r+1} = q_1 q_2 \cdots q_s$.

$p_1 | n \Longrightarrow p_1 | q_1 \cdots q_s \xrightarrow{\text{Lemma 2}} p_1 | q_i$

We may assume $p_1 | q_1$.

So $p_1 = q_1$

$p_2 p_3 \cdots p_r = q_2 \cdots q_s$

Ind. Hyp implies $p_i = q_i$ $s = r$.

<u>Thm</u> There are ∞- many primes.

Pf] Suppose not.

$p_1 \; p_2 \; \cdots \; p_n$

are all primes.

Let $N = p_1 p_2 \cdots p_n + 1$.

N has a prime factorization.

So $\exists$ p_i $p_i \mid N$.

However

$$N = \Big(\prod_{j \neq i} p_j\Big) p_i + 1$$

Remainder is 1 : contradiction $\square$

I) Questions II says:

When quotients are larger the algorithm goes faster.
So the slowest cases are when all $q_n = 1$.

$$r_{n-1} = r_n + r_{n+1}$$

This is the same as the definition of Fibonacci numbers.

This allows you to answer Q1, Q3, Q4 ~~and~~ Q5. is similar but there is a detail 202 is not a Fibo number.
Q1, 3, 4, 5 will give a Hint for Q6.

—//—

left is Q2.

Explaination for Q2

Observe $r_n > \tilde{r}_n$ implies that $(b,\tilde{a})$ will be finished earlier than (b,a). When $\tilde{r}_k = 0$ then $r_k > 0$ is still positive.

How to prove Q2.?

Observe.

$$r_{k-1} = q_k r_k + r_{k+1}$$

So

$$r_{k-1} > q_k r_k$$

and

$$r_k < \frac{r_1}{\prod_{j \leq k} q_j}$$

Observe also.

$$r_{k-1} = q_k r_k + r_{k-1} < (q_k + 1) r_k$$

So

$$r_k > \frac{r_{k-1}}{q_k + 1}$$

$$r_k > \frac{r_1}{\prod_{j \le k} q_j + 1}$$

Show $\tilde{r}_1 < r_1$

Put together

$$r_k > \frac{r_1}{\prod_{j \le k} q_j + 1} \ge \frac{\tilde{r}_1}{\prod_{j \le k} \tilde{q}_j} > \tilde{r}_k.$$

$\square$.

§1.4 Congruence Classes

Definition a and b are congruent mod n

$$a \equiv b \mod n$$

iff. $n \mid b-a$

Ex) $-1 \equiv 4 \mod 5$

$19 \equiv 7 \mod 12$

Lemma If $a \equiv b \mod n$. then

$$a+c = b+c \mod n$$

$$a-c = b-c \mod n$$

$$ac = bc \mod n.$$

Congruence class of a mod n.

$$[a]_n = \{b \mid b \equiv a \mod n\}.$$

$$\mathbb{Z}_n = \{[0]_n\ [1]_n, [2]_n, \ldots [n-1]_n\}.$$

Every class has ∞-many "representatives":

$$[1]_5 = [6]_5 = [38]_5 = [-4]_5 = \dots$$

<u>Definition</u>

$$[a]_n + [b]_n = [a+b]_n$$
$$[a]_n \, [b]_n = [ab]_n .$$

<u>Lemma</u>: The sum and product is well-defined.

<u>Pf</u> $\oplus$ $\tilde{a} \in [a]_n$ $\tilde{b} \in [b]_n$ the

$\tilde{a} = a + sn$ $\tilde{b} = b + t \cdot n$

<u>Claim</u> $\tilde{a} + \tilde{b} \equiv a+b \mod n$

Hence $[\tilde{a}+\tilde{b}]_n = [a+b]_n$.

Pf $(\tilde{a}+\tilde{b}) - (a+b) = (s-t)n$ $\square$.

$\otimes$ Similar. $\square$.

Example how to use $\mathbb{Z}_n$:

$$11 \mid 10! + 1$$

We need to show $[10!+1]_{11} = [0]_{11}$

$[4!]_{11} = [24]_{11} = [2]_{11}$

$[5!]_{11} = [2 \cdot 5]_{11} = [10]_{11}$

$[6!]_{11} = [10 \cdot 6]_{11} = [60]_{11} = [5]_{11}$

$[7!]_{11} = [35]_{11} = [2]_{11}$

$[8!]_{11} = [2 \cdot 8] = [16]_{11} = [5]_{11}$

$[9!]_{11} = [5 \cdot 9]_{11} = [1]_{11}$

$[10!]_{11} = [1 \cdot 10]_{11} = [10]_{11}$

$[10!+1]_{11} = [10+1]_{11} = [0]_{11}$ $\square$.

Definition

$[a]_n$ is invertible iff $\exists b$ $[b]_n \neq [0]_n$ s.t. $[a]_n [b]_n = [1]_n$.

$[0]_n \neq [a_n]$ is a zero-divisor iff $\exists b$ $[b]_n \neq [0]_n$ $[a]_n [b]_n = [0]_n$.

Ex) $\mathbb{Z}_4$ multiplication table

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$[1]_4, [3]_4$ invertible $[2]_4$ zero-divisor.

Thm $[a]_n$ is invertible $\Longleftrightarrow (a,n)=1$

Pf) $[a]_n [b]_n = [1]_n \Leftrightarrow [ab]_n = [1]_n$

$ab - 1 = k \cdot n \Longleftrightarrow a \cdot b + n \cdot k = 1.$

$\Longleftrightarrow (a,n) = 1.$ $\square$

Ex) $[8]_{11}$ what is its inverse?

$(8,11) = 1$

$$8 \cdot \underset{\uparrow}{?} + 11 \cdot \underset{\uparrow}{?} = 1$$

7 5

Check: $[8][7] = [56]_{11} = [1]_{11}$

<u>Lemma:</u> $[a]_n \in \mathbb{Z}_n$ either invertible or zero-divisor.

Pf) If $[a]_n$ is invertible. Done.

Suppose $[a]_n$ is not invertible. The

$$(a,n) = d > 1$$

$a = kd \qquad n = td. \qquad t \leq n-1$

$at = k\underbrace{td}_{n}$ is divisible by n.

$[at]_n = [0]_n \qquad [a]_n [t]_n = [0]_n \quad \square.$

<u>Lemma:</u> p prime.

Every non-zero in $\mathbb{Z}_p$ is invertible.