Clarification / Correction: In the previous lecture, we said

$$p^{\alpha} \| a \;,\; p^{\beta} \| b \Rightarrow p^{\alpha-\beta} \| \frac{a}{b}.$$

This is true for every a and b, but you may want to have $b|a$ as well because we didn't precisely define what does $p^e \| x$ mean for a rational number x.
For example, $5^2 \| \frac{75}{7}$ while $5^{-3} \| \frac{3}{125}$. Try figuring out the definition for the general case.

How can we check if a given integer n is prime?

- We can check the divisibility by $2, 3, 4, \dots, n-1$.

If n is not divisible by any of them, then it is a prime. We can actually do better.

Lemma: If n is composite, then it must have a prime divisor $p \leq \sqrt{n}$.

Proof: n composite $\Rightarrow n = ab$ for some $1 < a, b < n$.
We have $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ because otherwise
$a > \sqrt{n}\,,\; b > \sqrt{n} \Rightarrow ab > \sqrt{n} \cdot \sqrt{n} = n$.
Say $a \leq \sqrt{n}$ and p be a prime divisor of a, then
$p \leq a \leq \sqrt{n}$ and $p|a$ and $a|n \Rightarrow p|n$.

Thus, we only need to check the divisibility by primes $p \leq \sqrt{n}$.

e.g. 101 prime because it is not divisible by 2, 3, 5, 7.

<u>Sieve of Eratosthenes</u> : Find all primes less than or equal to 50. ($\sqrt{50} < 8$)

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	2
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	3
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	5
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	7
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~	

How can we check the divisibility by 2, 3, 4, 5, 8, 9?

Let $n = \overline{a_k a_{k-1} \cdots a_0}$ (decimal representation)

$$\Rightarrow n = a_0 + 10 a_1 + 10^2 \cdot a_2 + 10^3 \cdot a_3 + \dots + 10^k \cdot a_k. \quad \left(\text{base } 10 \text{ expansion}\right)$$

- Divisibility by 2: $n = a_0 + \underbrace{(10 a_1 + 10^2 a_2 + \dots + 10^k a_k)}_{\text{already divisible by } 2}$

So, $2 \mid n \iff 2 \mid a_0$.

• Divisibility by 4: $n = a_0 + 10a_1 + (10^2 a_2 + 10^3 a_3 + \dots + 10^k a_k)$

So, $4 | n \iff 4 \,|\, \underbrace{a_0 + 10a_1}_{= \overline{a_1 a_0}}$

can generalize to divisibility by 2^m

• Divisibility by 3:

$$n = a_0 + a_1 + a_2 + \dots + a_k + (\underbrace{9a_1 + 99a_2 + 999a_3 + \dots + (10^k - 1)a_k}_{\text{already divisible by } 3})$$

So, $3 | n \iff 3 \,|\, a_0 + a_1 + \dots + a_k$.

• Divisibility by 11:

− observe that $10+1$, $10^2 - 1$, $10^3 + 1$, $10^4 - 1$, $10^5 + 1$ are divisible by 11.

$$n = a_0 - a_1 + a_2 - \dots + (-1)^k a_k + (\underbrace{(10^1 + 1)a_1 + (10^2 - 1)a_2 + \dots + (10^k - (-1)^k)a_k}_{\text{divisible by } 11})$$

So, $11 | n \iff 11 \,|\, a_0 - a_1 + a_2 - \dots + (-1)^k a_k$.

Next, we'll consider the primes of the form $2^m \pm 1$, but first recall:

- $x^a - 1 = (x-1)\cdot(x^{a-1} + x^{a-2} + x^{a-3} + \dots + x^1 + 1)$
- $x^{2a+1} + 1 = (x+1)\cdot(x^{2a} - x^{2a-1} + x^{2a-2} - \dots - x^1 + 1)$.

$x^3 - 1 = (x-1)(x^2 + x + 1)$ $\quad$ $x^3 + 1 = (x+1)\cdot(x^2 - x + 1)$.

Question: Suppose $2^m + 1$. What can we say about m?

- m cannot be odd, because otherwise $2^m + 1 = (2+1)(\dots\dots)$ cannot be prime.

- m is not divisible by any odd number, except 1.

If $m = \underbrace{(2a+1)}_{\text{odd divisor}} \cdot k$, then

$2^m + 1 = (2^k)^{2a+1} + 1 = (2^k + 1)(\dots\dots)$

$\Rightarrow 2^k + 1$ divides $2^m + 1$.

For $2^m + 1$ to be prime, $2^k + 1 = 2^m + 1$

$\Rightarrow k = m \Rightarrow (2a+1) = 1$.

- no odd number > 1 divides $m \Rightarrow m = 2^n$ for some n.