Recall the continued fraction algorithm for $\alpha \in \mathbb{R}$.

(1) Let $a_0 = \lfloor \alpha \rfloor$, $\beta_0 = \alpha - a_0$, $i = 0$.
(2) While $\beta_i \neq 0$ do $a_{i+1} = \lfloor 1/\beta_i \rfloor$, $\beta_{i+1} = 1/\beta_i - a_{i+1}$.

Note that $\alpha = [a_0; a_1, \ldots, a_m + \beta_m]$.
Recall that $[a_0; a_1, \ldots, a_m] = h_m/k_m$.

Theorem 21.1. $\alpha \in \mathbb{Q}$ if and only if the continued fraction of α is finite.

For the rest of the lecture we assume $\alpha \notin \mathbb{Q}$.
The goal of this lecture is to show that h_m/k_m is a very close approximation to α and hence that $\lim_{m\to\infty} h_m/k_m = \alpha$.

Lemma 21.2. With notation as above

$$\alpha = \frac{(1/\beta_m)h_m + h_{m-1}}{(1/\beta_m)k_m + k_{m-1}}.$$

Theorem 21.3.

$$\alpha - h_m/k_m = \frac{(-1)^m}{k_m((1/\beta_m)k_m + k_{m-1})}.$$

Lemma 21.4. $k_m \geq 1$ for $m \geq 0$ and $k_{m+1} > k_m$ for $m \geq 1$.

Corollary 21.5. $|\alpha - h_m/k_m| < 1/(k_m k_{m+1})$.

Corollary 21.6. $\lim_{m\to\infty} h_m/k_m = \alpha$.

Example 21.7. Recall the convergents of $\sqrt{2}$ are h_m/k_m in the below table.

m	0	1	2	3	4
h_m/k_m	1	3/2	7/5	17/12	41/29
$\lvert\sqrt{2} - h_m/k_m\rvert$	0.41...	0.085...	0.0142...	0.0024...	0.00042...
$1/(k_m k_{m+1})$	0.5	0.1	0.0166...	0.0028...	0.00049...

Example 21.8. The continued fraction expansion of π is

$$\pi = [3; 7, 15, 1, 292, 1, \ldots].$$

The convergents are $3, 22/7, 333/106, 355/113, \ldots$.
The approximation $22/7$ is good precisely because $k_2 = 106$ is so large: $|\pi - h_1/k_2| < 1/(k_1 k_2) < 1/(7 \cdot 106) = 1/742$.

Theorem 21.9. Let $\alpha \notin \mathbb{Q}$. Let $a, b \in \mathbb{Z}$ be such that $|\alpha - a/b| < 1/(2b^2)$, then $a/b = h_m/k_m$ for some $m \geq 0$.

Application: Wiener attack on small private exponent RSA.