**Homework 1.1.:** Known: $a=2$ is fine. Why is $n$ prime? Suppose not:

$n = i \cdot j$. We have been told that $a^n - 1$ is prime, so if we show $a^n-1$ is composite we have a contradiction.

$$a^{i \cdot j} - 1 =$$

$$a^{2\cdot 3} - 1 = a^6 - 1 = (a-1)\cdot(a^5+a^4+a^3+a^2+a+1)$$

$$\begin{array}{l|l}
a^6 - 1 & a-1 \\ \hline
\underline{a^6 - a^5} & a^5+a^4+a^3+a^2+a+1 \\
\quad a^5 - 1 & \\
\quad \underline{a^5 - a^4} & \\
\qquad a^4 - 1 & \\
\qquad \underline{a^4 - a^3} & \\
\qquad\quad a^3 - 1 & \\
\qquad\quad \underline{a^3 - a^2} & \\
\qquad\qquad a^2 - 1 & \\
\qquad\qquad \underline{a^2 - a} & \\
\qquad\qquad\quad a - 1 & \\
\qquad\qquad\quad \underline{a - 1} & \\
\qquad\qquad\qquad 0 &
\end{array}
\qquad
\begin{array}{l|l}
a^6 - 1 & a^2-1 \\ \hline
\underline{a^6 - a^4} & a^4+a^2+1 \\
\quad a^4 - 1 & \\
\quad \underline{a^4 - a^2} & \\
\qquad a^2 - 1 & \\
\qquad \underline{a^2 - 1} & \\
\qquad\quad 0 &
\end{array}$$

$$a^{3\cdot 2} - 1 = (a^2-1)\cdot(a^4+a^2+1)$$

$$a^{i\cdot j} - 1 = (a^i - 1)\cdot(a^{i\cdot(j-1)} + a^{i\cdot(j-2)} + \dots + a^i + 1)$$

**Homework 1.3.:** $n = p_1^{e_1} \cdots p_r^{e_r}$ $\quad b$ must divide $a \cdot e_i$ for all $i$.

**Attempt:** $$\underbrace{n^{\frac{a}{b}}}_{\text{suppose it is rational}} = p_1^{\frac{a e_1}{b}} \cdots p_r^{\frac{a e_r}{b}} = P \cdot \underbrace{p_{i_1}^{\frac{a e_{i_1}}{b}} \cdots p_{i_j}^{\frac{a \cdot e_{i_j}}{b}}}_{\underline{\text{not}} \text{ rational}}$$

$$p_{i_1}^{\frac{a \cdot e_{i_1}}{b}} \cdots p_{i_j}^{\frac{a \cdot e_{i_j}}{b}} = \frac{n^{\frac{a}{b}}}{p} \quad \text{is also rational.}$$

Let $n^{\frac{a}{b}} = \frac{x}{y}$, $x, y \in \mathbb{Z}$. Now: $\underbrace{n^a}_{\text{integer}} = (n^{\frac{a}{b}})^b = \left(\frac{x}{y}\right)^b = \frac{x^b}{y^b}$

$y \nmid x$. Does $y^b \mid x^b$? No!

If $n = p_1^{e_1} \cdots p_r^{e_r}$ and $b$ divides $a \cdot e_i$ for all $i$, then $n^{\frac{a}{b}}$ is an integer.

If $n^{\frac{a}{b}}$ is rational, then it is an integer.

$n^{\frac{a}{b}} = m$ so $n^a = m^b$ so $(p_1^{e_1} \cdots p_r^{e_r})^a = (q_1^{f_1} \cdots q_s^{f_s})^b$

Key step: Fundamental Theorem of Arithmetic.

$$p_1^{a \cdot e_1} \cdots p_r^{a \cdot e_r} = q_1^{b \cdot f_1} \cdots q_s^{b \cdot f_s}$$

$p_i = q_i$ and $a \cdot e_i = b \cdot f_i$.

## Homework 1.4.:

1. All sets are finite.

2. One set is infinite countable.

3. More than one set is infinite countable.

1. Idea: $A, B$ are finite then $A \times B$ is finite. $|A \times B| = |A| \cdot |B|$.

$f: A \times B \longrightarrow S$, $S$ with $|A| \cdot |B|$ elements.

Scale this to $A_1 \times \cdots \times A_n$ by induction.

2. Idea: $A$ finite and $B$ countable, then $A \times B$ is in bijection with $B$.

$$B = \mathbb{N}, \quad A = \{1, \dots, n\}$$

<u>Remark:</u> The segment $(0,1)$ is <u>not</u> countable.

$$\begin{array}{ll} 1. & 0.a_{11}a_{12}a_{13}\cdots \\ 2. & 0.a_{21}a_{22}a_{23}\cdots \\ 3. & 0.a_{31}a_{32}a_{33}\cdots \\ \vdots & \vdots \end{array}$$

construct $0.b_1b_2b_3\cdots$ where $b_i \neq a_{ii} \ \forall i$.

Now $0.b_1b_2b_3\cdots$ is in $(0,1)$ but it is <u>not</u> on the list.

3. Idea: $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|$. Scale this by induction.

<u>Note:</u> $|A \times B| = |A| \cdot |B|$ is only true for $|A|$ and $|B|$ finite.

| $\mathbb{Z} \backslash \mathbb{Z}$ | 0 | 1 | -1 | 2 | -2 | $\cdots$ |
|---|---|---|---|---|---|---|
| 0 | (0,0) | (0,1) | | | | |
| 1 | (1,0) | (1,1) | | | | |
| -1 | | | $\ddots$ | | | |
| $\vdots$ | | | | | | |

exactly the elements of $\mathbb{Z} \times \mathbb{Z}$.

<u>Definition:</u> Two sets have the same cardinality if there is a bijection between them.

$$f: \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$$
$$0 \longmapsto (0,0)$$
$$1 \longmapsto (0,1)$$

$$-1 \longmapsto (1,0)$$

$$2 \longmapsto (-1,0)$$

$$-2 \longmapsto (1,1)$$

$$\vdots$$

**Homework 1.5.:**

$x_s$ $\qquad$ $x_s \longrightarrow y_s$

$y_s$

$$x \longmapsto \frac{x - x_{min}}{x_{max} - x_{min}} \cdot (y_{max} - y_{min}) + y_{min}$$

**Homework 1.9.:** Want: $p_{n+1} \leq 2^{2^{n+1}}$. We know this holds for $n=0$.

Suppose it is true for $n$, prove $n+1$.

$$p_n \cdot 2^{2^n} \leq 2^{2^{n+1}} \rightsquigarrow p_n \leq 2^{2^{n+1}} \cdot \frac{1}{2^{2^n}} = 2^{2^{n+1} - 2^n} = 2^{2^n}$$

$$p_{n+1} \leq p_n^n + 1 \rightsquigarrow p_n^n \geq p_{n+1} - 1$$

$$p_{n+1} - 1 \leq p_n^n \leq \left(2^{2^n}\right)^n = 2^{n \cdot 2^n}$$

We know:

$$p_{n+1} \underset{\text{Euclid's idea.}}{\leq} p_1 \cdots p_n + 1 \underset{p_i \leq 2^{2^i}}{\leq} 2^{2^1} \cdots 2^{2^n} + 1 = 2^{\sum_{i=1}^{n} 2^i} + 1 = 2^{2^{n+1} - 2} + 1 = 2^{2^{n+1}} \cdot 2^{-2} + 1 \leq 2^{2^{n+1}}$$

$$\sum_{i=1}^{n} 2^i = 2^{n+1} - 2 \quad \text{geometric series}$$

$$\sum_{i=1}^{n} a^i = a^{n+1} - a.$$

$$p_{n+1} \leq p_n^n + 1 \leq 2^{2^n} \cdots 2^{2^n} + 1 = 2^{n \cdot 2^n} + 1 \leq 2^{2^{n+1}}.$$

?

$n \leq 2^n$ and more.