Number Theory I

Discrete Algebraic Structures

Thomas J. Friese

December 12, 2024

Pigeonhole principle (again)

For $|A| > k|B|$ and $f : A \to B$:
There exist $k+1$ distinct elements $x_1, x_2, \ldots, x_k$ such that

$$f(x_1) = f(x_2) = \cdots = f(x_{k+1})$$

Pigeonhole principle (again) $\to$ proof of Exercise 6.5

For $|X| = k \cdot |Y| + 1$ and $f : X \to Y$:
There exists y such that $|f^{-1}(\{y\})| \geq k + 1$.

Proof by contradiction.

$\square$

Pigeonhole principle (again) $\rightarrow$ proof of Exercise 6.5

For $|X| = k \cdot |Y| + 1$ and $f : X \rightarrow Y$:
There exists y such that $|f^{-1}(\{y\})| \geq k + 1$.

Proof by contradiction.

- ◇ Assume that for all $y \in Y$, $|f^{-1}(\{y\})| \leq k$.

□

Pigeonhole principle (again) $\rightarrow$ proof of Exercise 6.5

For $|X| = k \cdot |Y| + 1$ and $f : X \to Y$:
There exists y such that $|f^{-1}(\{y\})| \geq k + 1$.

Proof by contradiction.

- Assume that for all $y \in Y$, $|f^{-1}(\{y\})| \leq k$.
- We find that $\bigcup_{y \in Y} f^{-1}(\{y\}) = X$ and $f^{-1}(\{y\}) \cap f^{-1}(\{y'\}) = \emptyset$ for $y \neq y'$, since f is a function.

$\square$

Pigeonhole principle (again) $\rightarrow$ proof of Exercise 6.5

For $|X| = k \cdot |Y| + 1$ and $f : X \to Y$:
There exists y such that $|f^{-1}(\{y\})| \geq k + 1$.

Proof by contradiction.

- Assume that for all $y \in Y$, $|f^{-1}(\{y\})| \leq k$.
- We find that $\bigcup_{y \in Y} f^{-1}(\{y\}) = X$ and $f^{-1}(\{y\}) \cap f^{-1}(\{y'\}) = \emptyset$ for $y \neq y'$, since f is a function.
- Thus $|X| = \sum_{y \in Y} |f^{-1}(\{y\})| \leq k \cdot |Y|$ by the union rule.

□

Euclid's algorithm and Bezout's coefficients

$$
\begin{aligned}
r_0 &= q_1 \cdot r_1 + r_2 \\
r_1 &= q_2 \cdot r_2 + r_3 \\
&\vdots \\
r_{k-2} &= q_{k-1} \cdot r_{k-1} + r_k \\
r_{k-1} &= q_k \cdot r_k + 0 \\
&\to r_k = \gcd(r_0, r_1)
\end{aligned}
$$

Euclid's algorithm and Bezout's coefficients

$\rightarrow$ find coefficients u, v such that $u \cdot r_0 + v \cdot r_1 = \gcd(r_0, r_1)$

$$r_{k-1} = q_k \cdot r_k + 0$$

$$r_{k-2} = q_{k-1} \cdot r_{k-1} + r_k \quad \rightarrow \quad r_k = r_{k-2} - q_{k-1} \cdot r_{k-1}$$

$$r_{k-3} = q_{k-2} \cdot r_{k-2} + r_{k-1} \quad \rightarrow \quad r_k = r_{k-2} - q_{k-1} \cdot (r_{k-3} - q_{k-2} \cdot r_{k-2})$$

$$\vdots$$

$$r_1 = q_2 \cdot r_2 + r_3$$

$$r_0 = q_1 \cdot r_1 + r_2$$

Base decomposition

- To write n in base b, find exponent k such that $b^k \leq n < b^{k+1}$.
- Write $n = q \cdot b^k + r$, $r < b^k$.
- Repeat with r.

Alternative tricks:

- Repeated division by b (rounding down) – sequence of remainders are the final number in reversed order
- Basis 2 $\leftrightarrow$ 16: $2^4 = 16$, so can just convert 4 bits to one digit and vice versa.

$\mathcal{O}$ notation

$f \in \mathcal{O}(g) \iff \exists C \in \mathbb{R}^+, N_0 \in \mathbb{N}$ such that $\forall n \geq N_0$: $f(n) \leq C \cdot g(n)$ (grows slower)

$f \in o(g) \iff \forall C \in \mathbb{R}^+, \exists N_0 \in \mathbb{N}$ such that $\forall n \geq N_0$: $f(n) \leq C \cdot g(n)$ (grows strictly slower)

$f \in \Theta(g) \iff f \in \mathcal{O}(g)$ and $g \in \mathcal{O}(f)$ (grows as fast as)