

Jacob Malone
9/12/21

Math 437

(1) Chinese Remainder Theorem

Def: If a, b are integers, then

$$[a, b] := \{n \in \mathbb{Z} \mid a \leq n \leq b\}$$

Theorem: If m_1 and m_2 are relatively prime ($\gcd(m_1, m_2) = 1$) then the mappings

$$f: [0, m_1 m_2 - 1] \rightarrow [0, m_1 - 1] \times [0, m_2 - 1],$$

defined by: $f(x) := (x \pmod{m_1}, x \pmod{m_2})$ is one-to-one (a bijection)

Proof: If $f(x) = (a, b)$, then x is divisible by m_1 and m_2 . Since m_1 and m_2 are relatively prime, it is a multiple of $m_1 m_2$ and since $0 \leq x < m_1 m_2$, $x = 0$.

So if $f(x_1) = f(x_2)$, then $f(x_1 - x_2) = (0, 0)$ and hence $x_1 - x_2 = 0$, so $x_1 = x_2$. So we have a bijective mapping.

Because $[0, m_1 m_2 - 1]$ has the same cardinality as $[0, m_1 - 1] \times [0, m_2 - 1]$ it is one-to-one it must be onto by the pigeonhole principle.

(2) $\frac{1}{2} + \frac{1}{3} + \frac{1}{5}$ into a usual fraction.

$$2 \cdot 3 \cdot 5 = 30 \left[\frac{15}{30} + \frac{10}{30} + \frac{6}{30} \right] = \frac{31}{30}$$

(Greedy Algorithm)

$$\frac{1}{30} \text{ reciprocal} = \frac{30}{1}, \text{ceil}(30) = 30, \text{floor}(1 - \frac{1}{30}) = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{30} + \frac{1}{30}$$

Dividing pieces is easier with the Egyptian fraction $\frac{1}{2} + \frac{1}{3} + \frac{1}{5}$ because it is faster (computations) to merge.

(3) Find the smallest integers such that:

x leaves remainder 2 when divided by 3

x leaves remainder 6 when divided by 7

$$a = x \pmod{m} \rightarrow \begin{cases} x = 3k + 2 \\ x = 7l + 6 \end{cases} \text{ as } b \pmod{n} \rightarrow \begin{cases} 2 = x \pmod{3} \\ 6 = x \pmod{7} \end{cases}, f(x) = (x \pmod{3}, x \pmod{7})$$

$$x = 20, 41 \text{ have this property. } \begin{cases} 20 = 3 \cdot 5 + 2, & 20 = 7 \cdot 2 + 6 \\ 41 = 3 \cdot 13 + 2, & 41 = 7 \cdot 5 + 6 \end{cases}$$

(5) leaves r when divided by 3, $\frac{x}{3} = k + r \rightarrow x \pmod{3} = r$

leaves s when divided by 7, $\frac{x}{7} = k + s \rightarrow x \pmod{7} = s$

9/12/21

$$\left. \begin{array}{l} x \pmod{3} = 2 \\ x \pmod{7} = 4 \end{array} \right\} f(x) := (x \pmod{3}, x \pmod{7})$$

$$\begin{aligned} f(0) &= (0, 0), f(1) = (1, 1), f(2) = (2, 2), f(3) = (0, 4), f(4) = (1, 3) \\ f(5) &= (2, 5), f(6) = (0, 6), f(7) = (1, 0), f(8) = (2, 1), f(9) = (0, 2), f(10) = (1, 3) \\ \dots & f(11) = (2, 4) \dots f(18) = (2, 3) \dots f(25) = (0, 4) \dots f(32) = (2, 4) \end{aligned}$$

81

79

$$x = 11, 32$$

(C) leaves remainder 0 when divided by 3, $\frac{x}{3} = 10$, $f(x) := (x \pmod{3}, x \pmod{7})$
leaves remainder 2 when divided by 7, $\frac{x}{7} = 12$,

$$\left. \begin{array}{l} f(0) = (0, 0), f(1) = (1, 1) \\ f(9) = (0, 2) \\ f(16) = (1, 2) \end{array} \right\} x = 9, 30$$