Mathematical Foundations of Computer Science

Project 10

Log Creative

Student ID:

June 25, 2021

Warmups

8 The residue number system $(x \bmod 3, x \bmod 5)$ considered in the text has the curious property that 13 corresponds to (1, 3), which looks almost the same. Explain how to find all instances of such a coincidence, without calculating all fifteen pairs of residues. In other words, find all solutions to the congruences

$$10x + y \equiv x \pmod 3, \quad 10x + y \equiv y \pmod 5.$$

Hint: Use the facts that $10u + 6v \equiv u \pmod 3$ and $10u + 6v \equiv v \pmod 5$

Solution. $10u + 6v$ is a number that satisfies the congruences within the range of 0 to 15:

$$10u + 6v \equiv u \pmod 3, \quad 10u + 6v \equiv 6v \equiv v \pmod 5$$

Then, it suffices to find the solution to

$$10x + 6y \equiv 10x + y \pmod{15}$$

In other word,

$$5y \equiv 0 \pmod{15}$$

Thus,

$$y \equiv 0 \pmod 3 \text{ and } y \leq 3$$

All pairs satisfies

$$\begin{cases} x = 0 \text{ or } 1 \\ y = 0 \text{ or } 3 \end{cases}$$

The full list of them: 0, 3, 10, 13. □

9 Show that $(3^{77} - 1)/2$ is odd and composite. Hint: What is $3^{77} \bmod 4$?

Proof.

$$\begin{aligned} 3^{77} - 1 &\equiv (-1)^{77} - 1 \pmod 4 \\ &\equiv -1 - 1 \pmod 4 \\ &\equiv 2 \pmod 4 \end{aligned}$$

Thus $3^{77}-1$ could be interpreted as $4k+2 (k \in \mathbb{Z})$. And $\frac{3^{77}-1}{2} = 2k+1 (k \in \mathbb{Z})$, which is an odd number.

Because $3^{77}-1 = (3^7)^{11} - 1 = (3^7 - 1)\left(\sum_{i=0}^{10} (3^7)^i\right)$,

$$3^7 - 1 | 3^{77} - 1$$

$$\frac{3^7-1}{2} \left| \frac{3^{77}-1}{2} \right.$$

Then, $(3^{77}-1)/2$ is composite. □

10 Compute $\varphi(999)$.

Solution.

$$999 = 3^3 \times 37$$

According to Euler's theorem,

$$\varphi(999) = 999 \times \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{37}\right) = 648$$

□

11 Find a function $\sigma(n)$ with the property that

$$g(n) = \sum_{0 \le k \le n} f(k) \Leftrightarrow f(n) = \sum_{0 \le k \le n} \sigma(k) g(n-k).$$

(This is analogous to the Möbius function; see (4.56).)

Solution. $\sigma(n)$ is defined by the formula:

$$\sigma(n) = \begin{cases} 1, & n = 0 \\ -1, & n = 1 \\ 0, & n > 1 \end{cases}$$

$\Rightarrow$: If $g(n) = \sum_{0 \le k \le n} f(k)$,

$$\begin{aligned} \sum_{0 \le k \le n} \sigma(k) g(n-k) &= \sum_{0 \le k \le n} \sigma(k) \sum_{0 \le j \le n-k} f(j) \\ &= \sum_{0 \le k \le n} \sigma(k) \sum_{k \le j \le n} f(n-j) \\ &= \sum_{0 \le j \le n} f(n-j) - \sum_{1 \le j \le n} f(n-j) \\ &= f(n) \end{aligned}$$

$\Leftarrow$: If $f(n) = \sum_{0 \le k \le n} \sigma(k) g(n-k) = g(n) - g(n-1)$,

$$\sum_{0 \le k \le n} f(k) = g(n) - g(0) + f(0) = g(n)$$

where the last equation is followed by

$$f(0) = \sigma(0) g(0) = g(0)$$

□

12 Simplify the formula $\sum_{d|m}\sum_{k|d}\mu(k)g(d/k)$.

Solution.

$$\begin{aligned}
\sum_{d|m}\sum_{k|d}\mu(k)g\left(\frac{d}{k}\right) &= \sum_{d|m}\left(\sum_{k|d}\mu\left(\frac{d}{k}\right)g(k)\right) && \text{(Inversion)}\\
&= \sum_{k|m}\sum_{l|(m/k)}\mu\left(\frac{kl}{k}\right)g(k) && \text{(Interchange)}\\
&= \sum_{k|m}\left(\sum_{l|(m/k)}\mu(l)g(k)\right) && \text{(associative)}\\
&= \sum_{k|m}g(k)\sum_{l|(m/k)}\mu(l) && \text{(distributive)}\\
&= \sum_{k|m}g(k)\left[\frac{m}{k}=1\right] && \text{(defination)}\\
&= g(m) && \text{(only } m=k\text{)}
\end{aligned}$$

□

13 A positive integer n is called *squarefree* if it is not divisible by m^2 for any $m > 1$. Find a necessary and sufficient condition that n is squarefree,

a in terms of the prime-exponent representation (4.11) of n;

Solution. For the prime-exponent representation of n:

$$n = \prod_{i=1}^{k} p_i^{n_i}$$

to be squarefree, due to every prime could only be divided by 1 and itself,

$$0 \le n_i < 2, \quad \forall i = 1, \cdots, k$$

□

b in terms of $\mu(n)$.

Solution.

$$m \text{ is squarefree } \Leftrightarrow \mu(m) = 0$$

which is followed by

$$\mu(m) = \begin{cases} (-1)^k, & \text{if } m = p_1 p_2 \cdots p_k \text{distinct primes,} \\ 0, & \text{if } p^2 | m \text{ for some prime } p \end{cases}$$

□

Basics

16 What is the sum of the reciprocals of the first n Euclid numbers?

Solution. By calculating some first terms,

i	1	2	3	4	$\cdots$
e_i	2	3	7	43	$\cdots$
$\frac{1}{e_i}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{7}$	$\frac{1}{43}$	$\cdots$
$\sum_{k=1}^{i} \frac{1}{e_k}$	$\frac{1}{2}$	$\frac{5}{6}$	$\frac{41}{42}$	$\cdots$	$\cdots$

The following hypothesis could be formed:

$$\sum_{i=1}^{n} \frac{1}{e_i} = 1 - \frac{1}{e_{n+1} - 1} \tag{1}$$

Prove by mathematical induction. The basic steps have be validated by the previous context. And assuming Equation (1) is true, then

$$\sum_{i=1}^{n+1} \frac{1}{e_i} = \sum_{i=1}^{n} \frac{1}{e_i} + \frac{1}{e_{n+1}} = 1 - \frac{1}{e_{n+1} - 1} + \frac{1}{e_{n+1}} = 1 - \frac{1}{(e_{n+1} - 1)e_{n+1}}$$

Due to

$$e_{n+2} = (e_{n+1} - 1)e_{n+1} + 1$$

Thus,

$$\sum_{i=1}^{n+1} \frac{1}{e_i} = 1 - \frac{1}{e_{n+2} - 1}$$

As a result, Equation (1) is true for $\forall n \in \mathbb{N}_+$. □

17 Let f_n be the "Fermat number" $2^{2^n} + 1$. Prove that $f_m \perp f_n$ if $m < n$.

Proof. Consider

$$\begin{aligned} f_n = 2^{2^n} + 1 = 2^{2^m \times 2^{n-m}} + 1 = (2^{2^m})^{2^{n-m}} + 1 &\equiv (-1)^{2^{n-m}} + 1 \pmod{f_m} \\ &\equiv 1 + 1 = 2 \pmod{f_m} \end{aligned}$$

Then, by Euclid's algorithm,

$$\gcd(f_n, f_m) = \gcd(f_m, 2) = 1$$

The last equation holds for f_m is an odd number. And this follows:

$$f_m \perp f_n, \quad \text{if } m < n$$

□

18 Show that if $2^n + 1$ is prime then n is a power of 2.

Proof. Prove by contradiction. If n is not a power of 2, then assuming that

$$n = qm$$

where $q > 1$ is an odd number. Then,

$$2^n + 1 = 2^{qm} + 1 = (2^m)^q + 1 = (2^m + 1)\left(2^{(q-1)m} - 2^{(q-2)m} + \cdots - 2^m + 1\right)$$

Thus, $2^m + 1 | 2^n + 1$ and $2^m + 1 < 2^n + 1$ followed by $q > 1$, indicates that $2^n + 1$ is not prime. A contradiction follows that n is a power of 2. □