One, Two, Three ... Sorority

Sujith Vijay

Given a set S, let $X = \{x_1, \ldots, x_m\}$ be a subset of S and let $f_i : S \to S$, $1 \le i \le n$ be a collection of functions. Define $\mathcal{C}(f_1, \ldots, f_n; x_1, \ldots, x_m)$ to be the smallest set with the following properties:

- $\forall i$, $1 \le i \le m$,
  $x_i \in \mathcal{C}(f_1, \ldots, f_n; x_1, \ldots, x_m)$
- $\forall j$, $1 \le j \le n$,
  $x \in \mathcal{C}(f_1, \ldots, f_n; x_1, \ldots, x_m) \Rightarrow f_j(x) \in \mathcal{C}(f_1, \ldots, f_n; x_1, \ldots, x_m)$

Example If $S = I\!N = \{0, 1, 2, \ldots\}$, $f_1(n) = 2n$, $f_2(n) = 2n + 1$, we have $\mathcal{C}(f_1, f_2; 0) = I\!N$.

Notation In what follows, $\tau(n)$ shall denote the number of divisors of n and $\phi(n)$ shall denote the order of the multiplicative group of integers modulo n. We shall also use $\Gamma(n)$ instead of $(n-1)!$ with ulterior motives. Further, given a function $f(n)$, the result of k applications of f to n shall be denoted by $f^k(n)$, with $f^0(n) \doteq n$.

Theorem 1 $\mathcal{C}(\tau, \phi, \Gamma; 4) = \mathbb{Z}^+$

Proof For a positive integer n, let $e_2(n)$ denote the unique non-negative integer k such that $n \equiv 2^k (\text{mod } 2^{k+1})$. Equivalently, $n = 2^{e_2(n)} q$, where q is an odd integer.

Let $m \in \mathbb{Z}^+$ and $s = \Gamma^m(4)$. Since $e_2(\Gamma^{k+1}(4)) > e_2(\Gamma^k(4))\, \forall k \ge 1$, it follows that $e_2(s) \ge m$.

Let $e_2(s) = t$, so that $s = 2^t u$, where $u \ge 3$ is odd. Let $\phi(s) = 2^{t-1}\phi(u) = 2^{t'} u'$, where u' is odd. Since $\phi(u)$ is even, $t' \ge t$ and $u' < u$. Thus $\exists\, \ell \in I\!N$, $\phi^\ell(s) = 2^p$, $p \ge m$, $p \in I\!N$.

Since $\phi(2^{k+1}) = 2^k \; \forall\, k \in I\!N$, we have $\phi^{\ell+p-m+1}(s) = 2^{m-1}$. Since m is arbitrary, we have shown that $2^a \in \mathcal{C}(\phi, \Gamma; 4) \,\forall a \in I\!N$. But $\tau(2^{m-1}) = m$, hence $m \in \mathcal{C}(\tau, \phi, \Gamma; 4)$. ∎

Let p_n denote the n^{th} prime, and let $\pi(n)$ denote the number of primes not exceeding n. Thus,

$$\pi(n) = \sup_{m \in I\!N} \{m : p_m \leq n\}$$

As a consequence of the prime number theorem, $p_n \sim n \ln n$. This motivates the following definitions:

$$p'_n \doteq n \ln n$$
$$\pi'(n) \doteq \sup_{m \in I\!N} \{m : p'_m \leq n\}$$

We will show that any positive integer can be obtained by a sequence of applications of π', ϕ and Γ.

Given $m \in I\!N$, $m \geq 3$, define $a_0(m) = m$; $a_{k+1}(m) = p'_{a_k(m)} = a_k(m) \ln a_k(m)$.

Let $b_k(m) = \ln a_k(m)$, so that $b_0(m) = \ln m$; $b_{k+1}(m) = \ln a_{k+1}(m) = \ln a_k(m) + \ln \ln a_k(m) = b_k(m) + \ln b_k(m)$.

Let $c_m = \max(2, b_2(m)/2 \ln 2)$.

Lemma A $\forall c \geq 2, \forall k \geq 2, \ln c + 2 \ln k \leq 1 + c \ln k$

Proof Let $f(c) = \ln c - 1$ and $g(c) = (c-2) \ln 2$. Observe that $f'(c) = 1/c \leq \ln 2 = g'(c) \,\forall c \geq 2$. Further, $f(2) \leq g(2)$. Thus $f(c) \leq g(c) \,\forall c \geq 2$. Hence, $\ln c - 1 = f(c) \leq g(c) = (c-2) \ln 2 \leq (c-2) \ln k$. Rearranging terms, we obtain $\ln c + 2 \ln k \leq 1 + c \ln k$. ∎

Lemma B $b_k(m) \leq c_m \, k \ln k \;\; \forall k \geq 2$.

Proof Observe that $b_2(m) \leq 2\, c_m \ln 2$. Assume $b_k \leq c_m k \ln k$. Now

$$\begin{aligned}
b_{k+1} &= b_k + \ln b_k \leq c_m \, k \ln k + \ln c_m + \ln k + \ln \ln k \\
&\leq c_m k \ln k + \ln c_m + 2 \ln k \leq c_m k \ln k + c_m \ln k + 1 \text{ (Lemma A)} \\
&\leq c_m k \ln k + c_m \ln k + c_m (k+1)/2k \\
&\leq c_m (k+1) \ln k + c_m (k+1) \ln(1 + 1/k) \\
&= c_m (k+1) \ln(k+1)
\end{aligned}$$

where the final inequality follows from the fact that $\ln(1+x) > x/2$ $\forall x \in [0,1]$.

By induction, the proposition is true for $k \geq 2$. ∎

Lemma C Let $r_k(m) = a_k(m+1)/a_k(m)$. Then,

$$\forall m \in \mathbb{N}, \forall M \in \mathbb{R}, \exists k_0 \in \mathbb{N}, \text{such that } r_{k_0}(m) > M$$

Proof We have,

$$\begin{aligned} r_{k+1}(m) &= \frac{a_{k+1}(m+1)}{a_{k+1}(m)} = \frac{a_k(m+1)\ln a_k(m+1)}{a_k(m)\ln a_k(m)} \\ &= r_k(m)\left(1 + \frac{\ln a_k(m+1) - \ln a_k(m)}{\ln a_k(m)}\right) \\ &= r_k(m)\left(1 + \frac{\ln r_k(m)}{b_k(m)}\right) \end{aligned}$$

Telescoping the above relation yields,

$$\begin{aligned} r_{k+1}(m) &= r_0(m)\prod_{j=0}^{k}\left(1 + \frac{\ln r_j(m)}{b_j(m)}\right) \\ &\geq r_0(m)\prod_{j=0}^{k}\left(1 + \frac{\ln r_0(m)}{b_j(m)}\right) \\ &\geq r_0(m)\sum_{j=0}^{k}\frac{\ln r_0(m)}{b_j(m)} \\ &= r_0(m)\ln r_0(m)\sum_{j=0}^{k}\frac{1}{b_j(m)} \\ &\geq \frac{r_0(m)\ln r_0(m)}{c_m}\sum_{j=2}^{k}\frac{1}{j\ln j} \end{aligned}$$

where the final inequality follows from Lemma B.

But $\sum \frac{1}{j\ln j}$ diverges. Thus $\exists k_0$ such that $r_{k_0}(m) > M$. ∎

Theorem 2 $\mathcal{C}(\pi', \phi, \Gamma; 4) = \mathbb{Z}^+$

Proof By Lemma C, $\forall\, m \in \mathbb{N}, \exists\, k \in \mathbb{N}$, such that $a_k(m+1) > 2\, a_k(m)$. Thus $a_k(m) \le 2^\ell < a_k(m+1)$, for some $\ell \in \mathbb{N}$. Since $2^\ell \in \mathcal{C}(\phi, \Gamma; 4)$, and $m = (\pi')^k(2^\ell)$, it follows that $m \in \mathcal{C}(\pi', \phi, \Gamma; 4)$. Hence, $\mathcal{C}(\pi', \phi, \Gamma; 4) = \mathbb{N}$, as claimed. ∎

This raises a natural question.

Conjecture $\mathcal{C}(\pi, \phi, \Gamma; 4) = \mathbb{Z}^+$

Margins will not be blamed.

Acknowledgements

Carl Pomerance and Thomas Robinson are thanked for useful discussions and several helpful suggestions. Thanks are also due to the founders of the Tau Phi Gamma sorority.