1999

p197
PR

Discrete Mathematics

Long question 1

Define Euler's totient function $\varphi(n)$. [2 marks]

Prove the Fermat-Euler Theorem that $a^{\varphi(n)} \equiv 1 \pmod{n}$ for appropriate a. [8 marks]

Deduce a theorem of Fermat about $a^{p-1} - 1$ for a prime number p. [2 marks]

Given a prime, p, with $p \neq 2$ and $p \neq 5$, show that there are infinitely many natural numbers, each of which has 9s as all its digits and which is divisible by p. [8 marks]

Answer

$\varphi(n) = |\{ x \in \mathbb{N} \mid 1 \leq x < n \text{ and } (x, n) = 1 \}|$ where (x, n) denotes the highest common factor of x and n.

Suppose $n > 1$ and $(n, a) = 1$. Let $U_n = \{ x \in \mathbb{N} \mid 1 \leq x < n \text{ and } (x, n) = 1 \}$ be the set of units modulo n. Say $U_n = \{u_1, u_2, \ldots, u_f\}$ where $f = \varphi(n)$. Observe $a \in U_n$ so $a.u_1, a.u_2, \ldots, a.u_f$ are all in U_n. Moreover, they are distinct because $a.u_i = a.u_j \Rightarrow n \mid a.(u_i - u_j)$, so $u_i = u_j$. Hence $\{a.u_1, a.u_2, \ldots, a.u_f\} = U_n = \{u_1, u_2, \ldots, u_f\}$. Consider the products of the elements in the two sets: $a^f u_1u_2 \ldots u_f = u_1u_2 \ldots u_f$. Units have multiplicative inverses modulo n and so can be divided away leaving $a^f \equiv 1 \pmod{n}$

Given a prime p, $\varphi(p) = p-1$, and $a < p$ means that $(p, a) = 1$. Hence p divides $a^{p-1}-1$.

Let $a = 10$ so $(p, a) = 1$ and $p \mid 10^p-1$. Consider $10^{kp}-1$ for $k = 1, 2, \ldots$. Each has 9s as all its digits and is divisible by 10^p-1, and so is divisible by p.