QUESTION

Let p be an odd prime. Let x be a positive integer such that the congruence class $[x]$ is a generator for U_p, the group of units modulo p. If m divides $p-1$ write $\prod(m)$ for the integer

$$\prod(m) = 1 + x^m + x^{2m} + x^{3m} + \ldots + x^{m(((p-1)/m)-1)} = 1 + x^m + \ldots + x^{p-1-m}.$$

(i) Show that

$$\prod(p-1) \equiv 1 \text{modulo} p).$$

(ii) If $1 \leq m < p-1$ show that

$$(x^m - 1)\prod(m) \equiv 0(\text{ modulo } p).$$

(iii) Use (ii) to show that

$$\prod(m) \equiv 0 \text{ modulo } p)$$

if $1 \leq m < p-1$.

(iv) For the rest of the question suppose that $p = p_1 \ldots p_k + 1$ where $p_1, p_2, \ldots, p_k$ are distinct primes. Show that $\sum_{1 \leq j \leq p-1, gcd(j,p-1)} 1^{x^j}$

$$\equiv \prod(1) - \sum_s \prod(p_s) + \sum_{s<t} \prod(p_s p_t) - \sum_{s<t<u} \prod(p_s p_t p_u)$$

$$+ \ldots + (-1)^k \prod(p_1 p_2 \ldots p_k) \ ((modulo)p).$$

(v) Use part (iv) to show that

$$\sum_{1 \leq j \leq p-1, gcd(j,p-1)=1} x^j \equiv (-1)^k \text{ (modulo } p).$$

ANSWER

(i) By definition we have $\prod(p-1) = 1$.

(ii) If $1 \leq m < p-1$ then

$$\begin{aligned} & (x^m - 1)\prod(m) \\ = \; & x^m(1 + x^m + \ldots \overset{p-1-1}{x}) - (1 + x^m + \ldots + x^{p-1-m}) \\ = \; & x^m + x^{2m} + \ldots + x^p + 1 - 1 - x^m - \ldots - x^{p-1-m} \\ = \; & x^{p-1} - 1 \end{aligned}$$

and $x^{p-1} \equiv 1$ (modulo p) by Fermat's little Theorem.

(iii) Since x is a generator for U_p it has multiplicative order $p-1$ modulo p. Therefore, when $1 \leq m < p-1$ the integer $x^m - 1$ is prime to p and so we can find integers a, b sech that $1 = ap + b(x^m - 1)$. Hence $\prod(m) = \prod(m)ap + \prod(m)b(x^m - 1)$ which is divisible by p, by (ii).

(iv) Suppose that $p = p_1 \ldots p_k + 1$ where $p_1, p_2, \ldots .p_k$ are distinct primes. Then the sum $\sum_{1 \leq j \leq p-1, gcd(j,p-1)=1} x^j$ may be written as

$$\sum_{i \leq j \leq p-1} x^j - \sum_{1 \leq j \leq p-1, gcd(j,p-1)>1} x^j = \prod(1) - \sum_{1 \leq j \leq p-1, gcd(j,p-1)>1} x^j$$

Now the integers, j, which satisfy $1 \leq j \leq p-1, gcd(j, p-1) > 1$ are precisely all the multiples of

$$p_1, p_2 \ldots p_k$$

Therefore as a first approximation to the difference of the two sums consider

$$\prod(1) - \sum_s \prod(p_s)$$

In this difference we have subtracted from $\prod(1)$ all the x^{p_s}'s but we have subtracted twice the x^v's where v is a multiple of two of the p_s's. Therefore we should consider

$$\prod(1) - \sum_s \prod(p_s) + \sum_{s<t} \prod(p_s p_t) - \sum_{s<t<w} \prod(p_s p_t p_w) + \ldots + (-1)^k \prod(p_2 p_2 \ldots p_k)$$

as required.

(v) This follows from (i)-(iv) since all the terms in the alternating sum of (iv) are zero modulo p except for the last one, which contributes $(-1)^k$ (modulo p).