ABOUT A PROBLEM FROM NUMBER THEORY

BY

K. I. Tsishchanka

Definition: A prime number is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Definition: A prime number is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example: In the sequence

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20$$

the red numbers are primes and the black ones are not.

Definition: A **prime number** is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example: In the sequence

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20$$

the red numbers are primes and the black ones are not.

Euclid

Theorem: There are infinitely many prime numbers.

Definition: A **prime number** is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example: In the sequence

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20$$

the red numbers are primes and the black ones are not.

Pierre Fermat

Theorem: If p is a prime number and a a positive integer, then $a^p - a$ is divisible by p.

Definition: A prime number is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example: In the sequence

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20$$

the red numbers are primes and the black ones are not.

Leonard Euler

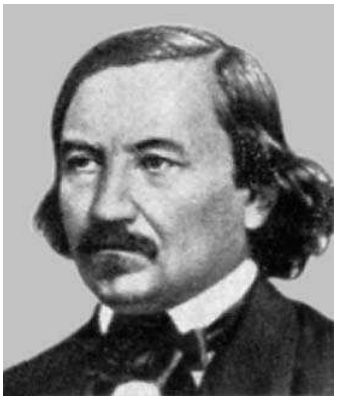
Theorem: If p is a prime number and a a positive integer, then $a^p - a$ is divisible by p.

Definition: A **prime number** is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example: In the sequence

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20$$

the red numbers are primes and the black ones are not.



Joseph Bertrand

Conjecture: There is at least one prime between n and $2n-2$ for every $n > 3$.

Definition: A **prime number** is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example: In the sequence

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20$$

the red numbers are primes and the black ones are not.

Pafnuty Chebyshev

Theorem: There is at least one prime between n and $2n-2$ for every $n > 3$.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Edward Waring

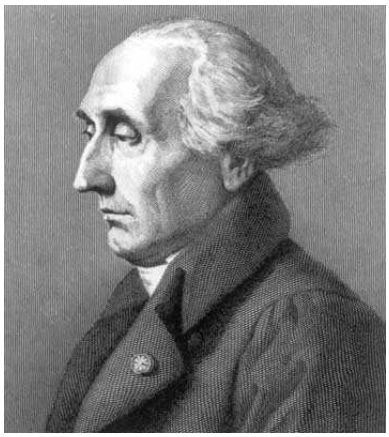
The theorem was proposed by John Wilson and published by Waring (1770).

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Gottfried Leibniz

The theorem was proposed by John Wilson and published by Waring (1770), although it was previously known to Leibniz.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.



Joseph-Louis Lagrange

The theorem was proposed by John Wilson and published by Waring (1770), although it was previously known to Leibniz. It was proved by Lagrange in 1773.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Notation: $n! = 1 \cdot 2 \cdot 3 \ldots n$.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Notation: $n! = 1 \cdot 2 \cdot 3 \ldots n$.

Example: $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$.

Theorem: **Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.**

$$(2-1)!+1 = 2$$
$$(3-1)!+1 = 3$$
$$(4-1)!+1 = 7$$
$$(5-1)!+1 = 5^2$$
$$(6-1)!+1 = 11^2$$
$$(7-1)!+1 = 7 \cdot 103$$
$$(8-1)!+1 = 71^2$$
$$(9-1)!+1 = 61 \cdot 661$$
$$(10-1)!+1 = 19 \cdot 71 \cdot 269$$
$$(11-1)!+1 = 11 \cdot 329891$$
$$(12-1)!+1 = 39916801$$
$$(13-1)!+1 = 13^2 \cdot 2834329$$
$$(14-1)!+1 = 83 \cdot 75024347$$
$$(15-1)!+1 = 23 \cdot 3790360487$$
$$(16-1)!+1 = 59 \cdot 479 \cdot 46271341$$
$$(17-1)!+1 = 17 \cdot 61 \cdot 137 \cdot 139 \cdot 1059511$$

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

$$(2-1)!+1 = 2$$
$$(3-1)!+1 = 3$$
$$(4-1)!+1 = 7$$
$$(5-1)!+1 = 5^2$$
$$(6-1)!+1 = 11^2$$
$$(7-1)!+1 = 7 \cdot 103$$
$$(8-1)!+1 = 71^2$$
$$(9-1)!+1 = 61 \cdot 661$$
$$(10-1)!+1 = 19 \cdot 71 \cdot 269$$
$$(11-1)!+1 = 11 \cdot 329891$$
$$(12-1)!+1 = 39916801$$
$$(13-1)!+1 = 13^2 \cdot 2834329$$
$$(14-1)!+1 = 83 \cdot 75024347$$
$$(15-1)!+1 = 23 \cdot 3790360487$$
$$(16-1)!+1 = 59 \cdot 479 \cdot 46271341$$
$$(17-1)!+1 = 17 \cdot 61 \cdot 137 \cdot 139 \cdot 1059511$$

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

$(2-1)!+1 = 2$

$(3-1)!+1 = 3$

$(5-1)!+1 = 5^2$

$(7-1)!+1 = 7 \cdot 103$

$(11-1)!+1 = 11 \cdot 329891$

$(13-1)!+1 = 13^2 \cdot 2834329$

$(17-1)!+1 = 17 \cdot 61 \cdot 137 \cdot 139 \cdot 1059511$

$(19-1)!+1 = 19 \cdot 23 \cdot 29 \cdot 61 \cdot 67 \cdot 123610951$

$(23-1)!+1 = 23 \cdot 521 \cdot 93799610095769647$

$(29-1)!+1 = 29 \cdot 10513391193507374500051862069$

$(31-1)!+1 = 31 \cdot 12421 \cdot 82561 \cdot 1080941 \cdot 7719068319927551$

$(37-1)!+1 = 37 \cdot 83 \cdot 739 \cdot 1483 \cdot 165202043 \cdot 669043459524628666916941$

$(41-1)!+1 = 41 \cdot 59 \cdot 277 \cdot 217823 \cdot 16558103 \cdot 142410167827 \cdot 2370686450613664429$

$(43-1)!+1 = 43 \cdot 70552493296669 \cdot 463124113000222170026612414799459103$

$(47-1)!+1 = 47 \cdot 268662306503771535067 \cdot 435777793891607546778854755077304349$

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Problem: Show that if p is a prime with $p > 5$, then $(p-1)!+1$ has at least two different prime divisors.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Problem: Show that if p is a prime with $p \geq 7$, then $(p-1)!+1$ has at least two different prime divisors.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Problem: Show that if p is a prime with $p \geq 7$, then $(p-1)!+1$ has at least two different prime divisors.

Problem′: Show that if p is a prime with $p \geq 7$, then

$$(p-1)!+1 \neq p^k$$

for any integer $k \geq 1$.

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Problem: Show that if p is a prime with $p \geq 7$, then $(p-1)!+1$ has at least two different prime divisors.

Problem′: Show that if p is a prime with $p \geq 7$, then

$$(p-1)!+1 \neq p^k$$

for any integer $k \geq 1$.

Proof:

Theorem: Let p be a positive integer. Then $(p-1)!+1$ is divisible by p if and only if p is prime.

Problem: Show that if p is a prime with $p \geq 7$, then $(p-1)!+1$ has at least two different prime divisors.

Problem′: Show that if p is a prime with $p \geq 7$, then

$$(p-1)!+1 \neq p^k$$

for any integer $k \geq 1$.

Proof: Assume to the contrary that

$$(p-1)!+1 = p^k$$

for some integer $k \geq 1$.

Then

$$(p-1)!+1=p^k$$

Then

$$(p-1)! + 1 = p^k$$

$$(p-1)! = p^k - 1$$

Then

$$(p-1)! + 1 = p^k$$

$$(p-1)! = p^k - 1$$

$$(p-1)! = (p-1)(p^{k-1} + p^{k-2} + \ldots + p + 1)$$

Then

$$(p-1)! + 1 = p^k$$

$$(p-1)! = p^k - 1$$

$$(p-1)! = (p-1)(p^{k-1} + p^{k-2} + \ldots + p + 1)$$

$$1 \cdot 2 \cdot 3 \ldots (p-2)(p-1) = (p-1)(p^{k-1} + p^{k-2} + \ldots + p + 1)$$

Then

$$(p-1)! + 1 = p^k$$

$$(p-1)! = p^k - 1$$

$$(p-1)! = (p-1)(p^{k-1} + p^{k-2} + \ldots + p + 1)$$

$$1 \cdot 2 \cdot 3 \ldots (p-2)(p-1) = (p-1)(p^{k-1} + p^{k-2} + \ldots + p + 1)$$

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^{k-1} + p^{k-2} + \ldots + p + 1$$

Then

$$(p-1)!+1=p^4$$

$$(p-1)!=p^4-1$$

$$(p-1)!=(p-1)(p^3+p^2+p+1)$$

$$1\cdot 2\cdot 3\ldots(p-2)(p-1)=(p-1)(p^3+p^2+p+1)$$

$$1\cdot 2\cdot 3\ldots(p-2)=p^3+p^2+p+1$$

Then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^3 + p^2 + p + 1$$

$$= p^3 - 2p^2 + 3p^2 - 6p + 7p - 14 + 15$$

Then

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^3 + p^2 + p + 1 \\ &= p^3 - 2p^2 + 3p^2 - 6p + 7p - 14 + 15 \\ &= p^2(p-2) + 3p(p-2) + 7(p-2) + 15 \end{aligned}$$

Then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^3 + p^2 + p + 1$$

$$= p^3 - 2p^2 + 3p^2 - 6p + 7p - 14 + 15$$

$$= p^2(p-2) + 3p(p-2) + 7(p-2) + 15$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^4$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^3 + p^2 + p + 1.$$

From this it follows that 15 is divisible by $p-2$.

Then

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^4 + p^3 + p^2 + p + 1 \\ &= p^4 - 2p^3 + 3p^3 - 6p^2 + \ldots + 31 \\ &= p^3(p-2) + 3p^2(p-2) + \ldots + 31 \end{aligned}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^5$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 31 is divisible by $p - 2$.

Then

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^5 + p^4 + p^3 + p^2 + p + 1 \\ &= p^5 - 2p^4 + 3p^4 - 6p^3 + \ldots + 63 \\ &= p^4(p-2) + 3p^3(p-2) + \ldots + 63 \end{aligned}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^6$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^5 + p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 63 is divisible by $p - 2$.

Then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^6 + p^5 + p^4 + p^3 + p^2 + p + 1$$

$$= p^6 - 2p^5 + 3p^5 - 6p^4 + \ldots + 127$$

$$= p^5(p-2) + 3p^4(p-2) + \ldots + 127$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^7$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^6 + p^5 + p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 127 is divisible by $p - 2$.

Then

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^7 + p^6 + p^5 + p^4 + p^3 + p^2 + p + 1 \\ &= p^7 - 2p^6 + 3p^6 - 6p^5 + \ldots + 255 \\ &= p^6(p-2) + 3p^5(p-2) + \ldots + 255 \end{aligned}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^8$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^7 + p^6 + p^5 + p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 255 is divisible by $p - 2$.

Then

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^7 + p^6 + p^5 + p^4 + p^3 + p^2 + p + 1 \\ &= p^7 - 2p^6 + 3p^6 - 6p^5 + \ldots + 255 \\ &= p^6(p-2) + 3p^5(p-2) + \ldots + 255 \end{aligned}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^8$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^7 + p^6 + p^5 + p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 255 is divisible by $p - 2$.

$$31,\ 63,\ 127,\ 255, \ldots$$

Then

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^7 + p^6 + p^5 + p^4 + p^3 + p^2 + p + 1 \\ &= p^7 - 2p^6 + 3p^6 - 6p^5 + \ldots + 255 \\ &= p^6(p-2) + 3p^5(p-2) + \ldots + 255 \end{aligned}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^8$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^7 + p^6 + p^5 + p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 255 is divisible by $p - 2$.

$$31,\ 63,\ 127,\ 255, \ldots, 2^k - 1$$

Then

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^{k-1} + p^{k-2} + \ldots + p + 1 \\ &= p^{k-1} - 2p^{k-2} + 3p^{k-2} - \ldots + 2^k - 1 \\ &= p^{k-2}(p-2) + \ldots + 2^k - 1 \end{aligned}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^k$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^{k-1} + p^{k-2} + \ldots + p + 1.$$

From this it follows that $2^k - 1$ is divisible by $p - 2$.

We have

$$\mathbf{1 \cdot 2 \cdot 3 \ldots (p-2) = p^3 + p^2 + p + 1}$$

We have

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^3 + p^2 + p + 1$$

$$= p^3 - 3p^2 + 4p^2 - 12p + 13p - 39 + 40$$

We have

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^3 + p^2 + p + 1$$

$$= p^3 - 3p^2 + 4p^2 - 12p + 13p - 39 + 40$$

$$= p^2(p-3) + 4p(p-3) + 13(p-3) + 40$$

We have

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^3 + p^2 + p + 1$$

$$= p^3 - 3p^2 + 4p^2 - 12p + 13p - 39 + 40$$

$$= p^2(p-3) + 4p(p-3) + 13(p-3) + 40$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^4$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^3 + p^2 + p + 1.$$

From this it follows that 40 is divisible by $p-2$.

We have

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^4 + p^3 + p^2 + p + 1 \\ &= p^4 - 3p^3 + \ldots + 121 \\ &= p^3(p-3) + \ldots + 121 \end{aligned}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^5$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 121 is divisible by $p - 3$.

We have

$$\begin{aligned} 1 \cdot 2 \cdot 3 \ldots (p-2) &= p^5 + p^4 + p^3 + p^2 + p + 1 \\ &= p^5 - 3p^4 + \ldots + 364 \\ &= p^4(p-3) + \ldots + 364 \end{aligned}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^6$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^5 + p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 364 is divisible by $p - 3$.

We have

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^5 + p^4 + p^3 + p^2 + p + 1$$

$$= p^5 - 3p^4 + \ldots + 364$$

$$= p^4(p-3) + \ldots + 364$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^6$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^5 + p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 364 is divisible by $p - 3$.

$$40,\ 121,\ 364,\ \ldots$$

We have

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^5 + p^4 + p^3 + p^2 + p + 1$$

$$= p^5 - 3p^4 + \ldots + 364$$

$$= p^4(p-3) + \ldots + 364$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^6$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^5 + p^4 + p^3 + p^2 + p + 1.$$

From this it follows that 364 is divisible by $p - 3$.

$$40,\ 121,\ 364,\ \ldots, \frac{3^k - 1}{2}$$

Then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^{k-1} + p^{k-2} + \ldots + p + 1$$

$$= p^{k-1} - 3p^{k-2} + 4p^{k-2} - \ldots + \frac{3^k - 1}{2}$$

$$= p^{k-2}(p-3) + \ldots + \frac{3^k - 1}{2}$$

<u>CONCLUSION:</u> If $(p-1)! + 1 = p^k$, then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^{k-1} + p^{k-2} + \ldots + p + 1.$$

From this it follows that $\frac{3^k - 1}{2}$ is divisible by $p - 3$.

Then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^{k-1} + p^{k-2} + \ldots + p + 1$$

$$= p^{k-1} - 3p^{k-2} + 4p^{k-2} - \ldots + \frac{3^k - 1}{2}$$

$$= p^{k-2}(p-3) + \ldots + \frac{3^k - 1}{2}$$

<u>CONCLUSION:</u> If $(p-1)!+1 = p^k$, then $\frac{3^k - 1}{2}$ is divisible by $p - 3$.

Then

$$1 \cdot 2 \cdot 3 \ldots (p-2) = p^{k-1} + p^{k-2} + \ldots + p + 1$$

$$= p^{k-1} - 3p^{k-2} + 4p^{k-2} - \ldots + \frac{3^k - 1}{2}$$

$$= p^{k-2}(p-3) + \ldots + \frac{3^k - 1}{2}$$

<u>CONCLUSION:</u> If $(p-1)!+1 = p^k$, then $\frac{3^k - 1}{2}$ is divisible by $p - 3$.

<u>CONCLUSION:</u> If $(p-1)!+1 = p^k$, then $2^k - 1$ is divisible by $p - 2$.

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

PROOF: Rewrite $(p-1)!+1=p^k$, as $(p-1!)=p^k-1$, then

$$(p-1)!=(p-1)(p^{k-1}+p^{k-2}+\ldots+p+1),$$

therefore

$$(p-2)!=p^{k-1}+p^{k-2}+\ldots+p+1.$$

For any natural $m > 1$ we have

$$p^{k-1} + p^{k-2} + \ldots + p + 1$$

$$= p^{k-1} - mp^{k-2} + (m+1)p^{k-2}$$

$$-\frac{m(m^2-1)}{m-1}p^{k-3} + \left(\frac{m(m^2-1)}{m-1} + 1\right)p^{k-3}$$

$$-\frac{m(m^3-1)}{m-1}p^{k-4} + \ldots$$

$$+\left(\frac{m(m^{k-2}-1)}{m-1} + 1\right)p - \frac{m(m^{k-1}-1)}{m-1}$$

$$+\frac{m(m^{k-1}-1)}{m-1} + 1$$

$$= p^{k-2}(p-m) + p^{k-3}(m+1)(p-m)$$

$$+p^{k-4}\left(\frac{m(m^2-1)}{m-1}+1\right)(p-m)$$

$$+\ldots+$$

$$+p\left(\frac{m(m^{k-2}-1)}{m-1}+1\right)(p-m)$$

$$+\frac{m^k-1}{m-1}.$$

$$p^{k-1}+p^{k-2}+\ldots+p+1$$

$$=p^{k-2}(p-m)+p^{k-3}(m+1)(p-m)$$

$$+p^{k-4}\left(\frac{m(m^2-1)}{m-1}+1\right)(p-m)$$

$$+\ldots+$$

$$+p\left(\frac{m(m^{k-2}-1)}{m-1}+1\right)(p-m)$$

$$+\frac{m^k-1}{m-1}.$$

$$p^{k-1}+p^{k-2}+\ldots+p+1$$

$$=p^{k-2}(p-m)+p^{k-3}(m+1)(p-m)$$

$$+p^{k-4}\left(\frac{m(m^2-1)}{m-1}+1\right)(p-m)$$

$$+\ldots+$$

$$+p\left(\frac{m(m^{k-2}-1)}{m-1}+1\right)(p-m)$$

$$+\frac{m^k-1}{m-1}.$$

$$(p-2)!=p^{k-1}+p^{k-2}+\ldots+p+1.$$

$$(p-2)!$$

$$= p^{k-2}(p-m) + p^{k-3}(m+1)(p-m)$$

$$+p^{k-4}\left(\frac{m(m^2-1)}{m-1}+1\right)(p-m)$$

$$+\ldots+$$

$$+p\left(\frac{m(m^{k-2}-1)}{m-1}+1\right)(p-m)$$

$$+\frac{m^k-1}{m-1}.$$

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

PROOF:

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

PROOF: Rewrite $(p-1)! + 1 = p^k$ as

$$(p-2)! = p^{k-1} + p^{k-2} + \ldots + p + 1.$$

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

PROOF: Rewrite $(p-1)!+1=p^k$ as

$$(p-2)!=p^{k-1}+p^{k-2}+\ldots+p+1.$$

From this it follows that

$$p^{k-1}+p^{k-2}+\ldots+p+1 \quad \text{is divisible by} \quad p-m$$

for any natural $2 \le m \le p-1$.

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

PROOF: Rewrite $(p-1)!+1=p^k$ as

$$(p-2)!=p^{k-1}+p^{k-2}+\ldots+p+1.$$

From this it follows that

$$p^{k-1}+p^{k-2}+\ldots+p+1 \quad \text{is divisible by} \quad p-m$$

for any natural $2\le m\le p-1$. On the other hand,

$$p^{k-1}+p^{k-2}+\ldots+p+1-(m^{k-1}+m^{k-2}+\ldots+m+1)$$

is divisible by $p-m$.

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

PROOF: Rewrite $(p-1)!+1=p^k$ as

$$(p-2)!=p^{k-1}+p^{k-2}+\ldots+p+1.$$

From this it follows that

$$p^{k-1}+p^{k-2}+\ldots+p+1 \quad \text{is divisible by} \quad p-m$$

for any natural $2\le m\le p-1$. On the other hand,

$$p^{k-1}+p^{k-2}+\ldots+p+1-(m^{k-1}+m^{k-2}+\ldots+m+1)$$

is divisible by $p-m$. Therefore

$$m^{k-1}+m^{k-2}+\ldots+m+1 \quad \text{is divisible by} \quad p-m.$$

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

PROOF: Rewrite $(p-1)!+1=p^k$ as

$$(p-2)!=p^{k-1}+p^{k-2}+\ldots+p+1.$$

From this it follows that

$$p^{k-1}+p^{k-2}+\ldots+p+1 \quad \text{is divisible by} \quad p-m$$

for any natural $2\le m\le p-1$. On the other hand,

$$p^{k-1}+p^{k-2}+\ldots+p+1-(m^{k-1}+m^{k-2}+\ldots+m+1)$$

is divisible by $p-m$. Therefore

$$m^{k-1}+m^{k-2}+\ldots+m+1 \quad \text{is divisible by} \quad p-m. \blacksquare$$

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

Problem: Show that if p is a prime with $p \geq 7$, then

$$(p-1)! + 1 \neq p^k$$

for any integer $k \geq 1$.

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

Put $m = \dfrac{p+1}{2}$ and $d = m - 1$.

LEMMA: If $(p-1)! + 1 = p^k$, then

$$\frac{m^k - 1}{m - 1} \quad \text{is divisible by} \quad p - m$$

for any $m = 2, 3, \ldots, p-2$.

Put $m = \dfrac{p+1}{2}$ and $d = m - 1$. Then

$$\frac{(d+1)^k - 1}{d} \quad \text{is divisible by } d.$$

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

Put $m=\dfrac{p+1}{2}$ and $d=m-1$. Then

$$\frac{(d+1)^k-1}{d} \quad \text{is divisible by } d.$$

It follows that

$$d^{k-1}+kd^{k-2}+\ldots+\binom{k}{2}d+k \quad \text{is divisible by } d.$$

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

Put $m=\dfrac{p+1}{2}$ and $d=m-1$. Then

$$\frac{(d+1)^k-1}{d} \quad \text{is divisible by } d.$$

It follows that

$$d^{k-1}+kd^{k-2}+\ldots+\binom{k}{2}d+k \quad \text{is divisible by } d.$$

Hence k is divisible by d.

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

Put $m=\dfrac{p+1}{2}$ and $d=m-1$. Then

$$\frac{(d+1)^k-1}{d} \quad \text{is divisible by } d.$$

It follows that

$$d^{k-1}+kd^{k-2}+\ldots+\binom{k}{2}d+k \quad \text{is divisible by } d.$$

Hence k is divisible by $\dfrac{p-1}{2}$.

LEMMA: If $(p-1)!+1=p^k$, then

$$\frac{m^k-1}{m-1} \quad \text{is divisible by} \quad p-m$$

for any $m=2,3,\ldots,p-2$.

Put $m=\dfrac{p+1}{2}$ and $d=m-1$. Then

$$\frac{(d+1)^k-1}{d} \quad \text{is divisible by } d.$$

It follows that

$$d^{k-1}+kd^{k-2}+\ldots+\binom{k}{2}d+k \quad \text{is divisible by } d.$$

Hence k is divisible by $\dfrac{p-1}{2}$. Therefore

$$k=\frac{p-1}{2} \quad \text{or} \quad 2\frac{p-1}{2}, \quad \text{or} \quad 3\frac{p-1}{2},\ldots$$

LEMMA: If $(p-1)! + 1 = p^k$, then

$$k = \frac{p-1}{2} \quad \text{or} \quad 2\frac{p-1}{2}, \quad \text{or} \quad 3\frac{p-1}{2}, \ldots$$

LEMMA: If $(p-1)! + 1 = p^k$, then

$$k = \frac{p-1}{2} \quad \text{or} \quad 2\frac{p-1}{2}, \quad \text{or} \quad 3\frac{p-1}{2}, \ldots$$

In other words, if $(p-1)! + 1 = p^k$, then either

$$k = \frac{p-1}{2} \quad \text{or} \quad k \geq p-1.$$

LEMMA: If $(p-1)! + 1 = p^k$, then

$$k = \frac{p-1}{2} \quad \text{or} \quad 2\frac{p-1}{2}, \quad \text{or} \quad 3\frac{p-1}{2}, \ldots$$

In other words, if $(p-1)! + 1 = p^k$, then either

$$k = \frac{p-1}{2} \quad \text{or} \quad k \geq p-1.$$

This is a contradiction, since $(p-1)! + 1 = p^k$ implies

$$\frac{p-1}{2} < k < p-1.$$

LEMMA: If $(p-1)! + 1 = p^k$, then

$$k = \frac{p-1}{2} \quad \text{or} \quad 2\frac{p-1}{2}, \quad \text{or} \quad 3\frac{p-1}{2}, \ldots$$

In other words, if $(p-1)! + 1 = p^k$, then either

$$k = \frac{p-1}{2} \quad \text{or} \quad k \geq p-1.$$

This is a contradiction, since $(p-1)! + 1 = p^k$ implies

$$\frac{p-1}{2} < k < p-1. \blacksquare$$

LEMMA: If $(p-1)! + 1 = p^k$, then

$$k = \frac{p-1}{2} \quad \text{or} \quad 2\frac{p-1}{2}, \quad \text{or} \quad 3\frac{p-1}{2}, \ldots$$

In other words, if $(p-1)! + 1 = p^k$, then either

$$k = \frac{p-1}{2} \quad \text{or} \quad k \geq p-1.$$

This is a contradiction, since $(p-1)! + 1 = p^k$ implies

$$\frac{p-1}{2} < k < p-1. \blacksquare$$

Problem: Show that if p is a prime with $p \geq 7$, then

$$(p-1)! + 1 \neq p^k$$

for any integer $k \geq 1$.

Assume to the contrary that there is a natural number $k > 1$ such that

$$(p-1)! + 1 = p^k.$$

This can be rewritten as

$$(p-2)! = p^{k-1} + p^{k-2} + \ldots + p + 1$$

which implies that

$$p^{k-1} + p^{k-2} + \ldots + p + 1 \quad \text{is divisible by } (p-m) \tag{1}$$

for any natural m with $1 < m < p$. On the other hand, we have

$$p^{k-1} + p^{k-2} + \ldots + p + 1 - (m^{k-1} + m^{k-2} + \ldots + m + 1) \quad \text{is divisible by } (p-m). \tag{2}$$

From (1) and (2) it follows that

$$m^{k-1} + m^{k-2} + \ldots + m + 1 \text{ is divisible by } (p-m),$$

so

$$\frac{m^k - 1}{m-1} \text{ is divisible by } (p-m).$$

Put $m = \dfrac{p+1}{2}$ and $d = m - 1$. Then $\dfrac{(d+1)^k - 1}{d}$ is divisible by d. It follows that

$$d^{k-1} + kd^{k-2} + \ldots + \binom{k}{2} d + k \text{ is divisible by } d.$$

Hence k is divisible by $\dfrac{p-1}{2}$. Therefore $k = \dfrac{p-1}{2}$ or $2\dfrac{p-1}{2}$, or $3\dfrac{p-1}{2}, \ldots$ In other words, either $k = \dfrac{p-1}{2}$ or $k \geq p - 1$. This is a contradiction, since $(p-1)! + 1 = p^k$ implies

$$\frac{p-1}{2} < k < p - 1. \blacksquare$$

Assume to the contrary that there is a natural number $k > 1$ such that

$$p^k = (p-1)! + 1. \qquad (*)$$

Assume to the contrary that there is a natural number $k > 1$ such that

$$p^k = (p-1)! + 1. \qquad (*)$$

This can be rewritten as

$$p^{k-1} + p^{k-2} + \ldots + p + 1 = (p-2)!$$

Assume to the contrary that there is a natural number $k > 1$ such that

$$p^k = (p-1)! + 1. \qquad (*)$$

This can be rewritten as

$$p^{k-1} + p^{k-2} + \ldots + p + 1 = (p-2)!$$

which implies

$$p^{k-1} + p^{k-2} + \ldots + p + 1 \text{ is divisible by } \frac{p-1}{2}.$$

Assume to the contrary that there is a natural number $k > 1$ such that

$$p^k = (p-1)! + 1. \qquad (*)$$

This can be rewritten as

$$p^{k-1} + p^{k-2} + \ldots + p + 1 = (p-2)!$$

which implies

$$p^{k-1} + p^{k-2} + \ldots + p + 1 \text{ is divisible by } \frac{p-1}{2}.$$

Since $p = 2\,\dfrac{p-1}{2} + 1$,

Assume to the contrary that there is a natural number $k > 1$ such that

$$p^k = (p-1)! + 1. \qquad (*)$$

This can be rewritten as

$$p^{k-1} + p^{k-2} + \ldots + p + 1 = (p-2)!$$

which implies

$$p^{k-1} + p^{k-2} + \ldots + p + 1 \text{ is divisible by } \frac{p-1}{2}.$$

Since $p = 2\,\dfrac{p-1}{2} + 1$, **we have**

$$\left(2\,\frac{p-1}{2} + 1\right)^{k-1} + \left(2\,\frac{p-1}{2} + 1\right)^{k-2} + \ldots + \left(2\,\frac{p-1}{2} + 1\right) + 1$$

is divisible by $\dfrac{p-1}{2}$.

Assume to the contrary that there is a natural number $k > 1$ such that

$$p^k = (p-1)! + 1. \qquad (*)$$

This can be rewritten as

$$p^{k-1} + p^{k-2} + \ldots + p + 1 = (p-2)!$$

which implies

$$p^{k-1} + p^{k-2} + \ldots + p + 1 \text{ is divisible by } \frac{p-1}{2}.$$

Since $p = 2\,\dfrac{p-1}{2} + 1$, we have

$$\left(2\,\frac{p-1}{2} + 1\right)^{k-1} + \left(2\,\frac{p-1}{2} + 1\right)^{k-2} + \ldots + \left(2\,\frac{p-1}{2} + 1\right) + 1$$

is divisible by $\dfrac{p-1}{2}$. If we expand the parentheses here, we get

$$k \text{ is divisible by } \frac{p-1}{2}$$

Assume to the contrary that there is a natural number $k > 1$ such that

$$p^k = (p-1)! + 1. \qquad (*)$$

This can be rewritten as

$$p^{k-1} + p^{k-2} + \ldots + p + 1 = (p-2)!$$

which implies

$$p^{k-1} + p^{k-2} + \ldots + p + 1 \text{ is divisible by } \frac{p-1}{2}.$$

Since $p = 2\,\dfrac{p-1}{2} + 1$, we have

$$\left(2\,\frac{p-1}{2} + 1\right)^{k-1} + \left(2\,\frac{p-1}{2} + 1\right)^{k-2} + \ldots + \left(2\,\frac{p-1}{2} + 1\right) + 1$$

is divisible by $\dfrac{p-1}{2}$. If we expand the parentheses here, we get

$$k \text{ is divisible by } \frac{p-1}{2}$$

which is impossible.

Assume to the contrary that there is a natural number $k > 1$ such that

$$p^k = (p-1)! + 1. \qquad (*)$$

This can be rewritten as

$$p^{k-1} + p^{k-2} + \ldots + p + 1 = (p-2)!$$

which implies

$$p^{k-1} + p^{k-2} + \ldots + p + 1 \text{ is divisible by } \frac{p-1}{2}.$$

Since $p = 2\,\dfrac{p-1}{2} + 1$, we have

$$\left(2\,\frac{p-1}{2} + 1\right)^{k-1} + \left(2\,\frac{p-1}{2} + 1\right)^{k-2} + \ldots + \left(2\,\frac{p-1}{2} + 1\right) + 1$$

is divisible by $\dfrac{p-1}{2}$. If we expand the parentheses here, we get

$$k \text{ is divisible by } \frac{p-1}{2}$$

which is impossible. ■

$$(2-1)!+1=2$$

$$(3-1)!+1=3$$

$$(5-1)!+1=5^2$$

$$(7-1)!+1=7\cdot 103$$

$$(11-1)!+1=11\cdot 329891$$

$$(13-1)!+1=13^2\cdot 2834329$$

$$(17-1)!+1=17\cdot 61\cdot 137\cdot 139\cdot 1059511$$

$$(19-1)!+1=19\cdot 23\cdot 29\cdot 61\cdot 67\cdot 123610951$$

$$(23-1)!+1=23\cdot 521\cdot 93799610095769647$$

$$(29-1)!+1=29\cdot 10513391193507374500051862069$$

$$(31-1)!+1=31\cdot 12421\cdot 82561\cdot 1080941\cdot 7719068319927551$$

$$(37-1)!+1=37\cdot 83\cdot 739\cdot 1483\cdot 165202043\cdot 669043459524628666916941$$

$$(41-1)!+1=41\cdot 59\cdot 277\cdot 217823\cdot 16558103\cdot 142410167827\cdot 2370686450613664429$$

$$(43-1)!+1=43\cdot 70552493296669\cdot 463124113000222170026612414799459103$$

$$(47-1)!+1=47\cdot 268662306503771535067\cdot 435777793891607546778854755077304349$$

Problem: Show that if p is a prime with $p \geq 17$, then

$$(p-1)! + 1$$

has at least three different prime divisors.

Problem: **Show that if p is a prime with $p \geq 17$, then**

$$(p-1)! + 1$$

has at least three different prime divisors.

Problem: **Show that if p is a prime with $p \geq 17$, then**

$$(p-1)! + 1 \neq p^k q^\ell$$

for all integers $k,\ \ell \geq 1$.