Wilson's Theorem

THEOREM: (WILSON) IF P IS A PRIME THEN $(P-1)! \equiv_P -1$.

EXERCISE 1: FIND THE REMINDER WHEN $2(26!)$ IS DIVIDED BY 29.

SOLUTION: SINCE 29 IS PRIME, BY WILSON'S THEOREM $28! \equiv_{29} -1$. WE NOW OBSERVE $28.27 = 29.26+2$ WHICH MEANS $28.27 \equiv_{29} 2$. THIS SHOWS THAT $2.26! \equiv_{29} 28.27.26! \equiv_{29} 28! \equiv_{29} -1 \equiv_{29} 28$. WE THUS HAVE $2.(26!)$ HAS REMAINDER 28 IN THE DIVISION BY 29.

EXERCISE 2: FIND THE REMAINDER WHEN $15!$ IS DIVIDED BY 17.

SOLUTION: SINCE 17 IS PRIME, BY WILSON'S THEOREM WE HAVE $16! \equiv_{17} -1$. WE NOW NOTICE THAT $(-1).15! \equiv_{17} 16.15! \equiv_{17} 16! \equiv_{17} -1$. THIS SHOWS THAT $(-1).(-1).15! \equiv_{17} (-1).(-1)$. HENCE, $15! \equiv_{17} 1$ AND THE REMAINDER OF $15!$ IN THE DIVISION BY 17 IS 1.

EXERCISE 3: SHOW THAT $18! \equiv_{437} -1$.

SOLUTION: WE FIRST NOTE $437 = 19.23$. NOTE ALSO THAT $19, 23$ ARE PRIME. THEN, BY WILSON'S THEOREM, $18! \equiv_{19} -1$ AND $22! \equiv_{23} -1$. WE NOW OBSERVE $22! \equiv_{23} 22.21.20.19.18! \equiv_{23} (-1).(-2).(-3).(-4).18! \equiv_{23} 24.18! \equiv_{23} 1.18! \equiv_{23} 18!$. THEN $18! \equiv_{23} -1$. WE THEREFORE HAVE $23 \mid 18!+1$ AND $19 \mid 18!+1$. SINCE $\gcd(19,23)=1$ WE HAVE $19.23 \mid 18!+1$. HENCE $18! \equiv_{19.23} -1$.

THE CONVERSE OF WILSON'S THEOREM IS ALSO TRUE. IF $(m-1)! \equiv_m -1$ THEN m MUST BE PRIME. TO SEE THIS, SUPPOSE THAT m IS NOT A PRIME. THEN, m HAS A DIVISOR d WITH $1 < d < m$. NOTE THAT $d \leq m-1$. SO d IS ONE FACTOR OF $(m-1)!$. THIS SHOWS $d \mid (m-1)!$. SINCE $d \mid m$

AND $m \mid (m-1)!+1$ WE HAVE $d \mid (m-1)!+1$. THIS IMPLIES $d \mid 1$ AS $1 = (m-1)!+1-(m-1)!$, WHICH IS A CONTRADICTION.

THEOREM: AN INTEGER $m>1$ IS PRIME IFF $(m-1)! \equiv_m -1$.

EXERCISE 4: PROVE THAT AN INTEGER $m>1$ IS PRIME IFF $(m-2)! \equiv_m 1$.

SOLUTION: SINCE $m \cdot 1 + (m-1)\cdot(-1) = m - m + 1 = 1$ WE HAVE $(m-1)\cdot(-1) \equiv_m 1$. THIS SHOWS THAT $(m-1) \equiv_m -1$. WE NOW OBSERVE $(m-1)! \equiv_m -1$ IFF $(m-2)! \equiv_m 1$. IF $(m-2)! \equiv_m 1$ THEN $(m-1)(m-2)! \equiv_m (-1)\cdot 1$ AND SO $(m-1)! \equiv_m -1$. CONVERSELY, ASSUME $(m-1)! \equiv_m -1$. THEN $(m-1)! \equiv_m (m-1)(m-2)! \equiv_m (-1)\cdot(m-2)! \equiv_m -1$. THIS SHOWS $(m-2)! \equiv_m 1$. WE THEREFORE HAVE

$$m \text{ IS PRIME IFF } (m-1)! \equiv_m -1 \text{ IFF } (m-2)! \equiv_m 1.$$

EXERCISE 5: IF m IS COMPOSITE SHOW THAT $(m-1)! \equiv_m 0$ EXCEPT WHEN $m=4$.

SOLUTION: FOR $m=4$ WE HAVE $(4-1)! = 3! = 6 \equiv_4 2$. ASSUME THAT $m>4$. SINCE m IS COMPOSITE THEN $m = r \cdot s$ FOR SOME INTEGERS $1<r,s<m$. THEN r AND s ARE FACTORS OF $(m-1)!$. IF $r \neq s$ THEN r AND s ARE DIFFERENT FACTORS IN $(m-1)!$. SO, $rs \mid (m-1)!$. THEN $(m-1)! \equiv_m 0$. ASSUME NOW THAT $r=s$. THEN $m = r^2$. IF $r \geq \frac{m}{2}$ THEN $m = r^2 \geq \left(\frac{m}{2}\right)^2 = \frac{m^2}{4}$ AND $4m \geq m^2$. THIS SHOWS $m(m-4) \leq 0$ WHICH IMPLIES THAT $m \leq 4$, A CONTRADICTION. THEN $r < \frac{m}{2}$ AND $2r<m$. THEREFORE, $2r \leq m-1$. NOW, NOTE r AND $2r$ ARE BOTH DIFFERENT FACTORS OF $(m-1)!$ AND SO $r\cdot(2r) \mid (m-1)!$. THEN $r^2 \mid (m-1)!$ WHICH IMPLIES $(m-1)! \equiv_m 0$.

EXERCISE 6: GIVEN A PRIME NUMBER p, ESTABLISH THE CONGRUENCE

$$(p-1)! \equiv_{1+2+3+\cdots+(p-1)} p-1$$

SOLUTION: SINCE P IS PRIME, BY WILSON'S THEOREM $(P-1)! \equiv_P -1 \equiv_P P-1$.

NOTE THAT $1+2+\ldots+(P-1) = \frac{P.(P-1)}{2}$. IF $P=2$ THEN THIS IS TRIVIALLY TRUE.

ASSUME THAT $P \geqslant 3$. THEN $P-1$ IS EVEN AND $\frac{P-1}{2} \in \mathbb{Z}$. NOTE $\frac{P-1}{2} < P-1$

AND SO $\frac{P-1}{2}$ IS A FACTOR OF $(P-1)!$ WHICH SHOWS $(P-1)! \equiv_{\frac{P-1}{2}} 0$. NOTE

ALSO THAT $\frac{P-1}{2}$ DIVIDES $P-1$ AND SO $\frac{(P-1)}{2} \mid (P-1)! - (P-1)$. WE ALSO

HAVE $P-1 \mid (P-1)! - (P-1)$. SINCE P IS PRIME WE HAVE $\gcd\left(\frac{P-1}{2}, P\right) = 1$.

THIS SHOWS $\frac{(P-1)}{2}.P$ DIVIDES $(P-1)! - (P-1)$. THEN $(P-1)! \equiv_{\frac{P-1}{2}.P} P-1$.

THIS SHOWS $(P-1)! \equiv P-1 \left(\bmod\ 1+2+3+\ldots+(P-1)\right)$.