Fermat's Theorem

THEOREM: (FERMAT'S THEOREM) LET p BE A PRIME AND SUPPOSE THAT $p \nmid a$. THEN $a^{p-1} \equiv_p 1$.

COROLLARY: IF p IS A PRIME THEN $a^p \equiv_p a$ FOR ANY INTEGER a.

EXERCISE 1: USE FERMAT'S THEOREM TO VERIFY THAT 17 DIVIDES $11^{104}+1$.

SOLUTION: SINCE $17 \nmid 11$ THEN BY FERMAT'S THEOREM, $11^{16} \equiv_{17} 1$. NOTICE THAT $104 = 16.6+8$ AND $121 = 11^2 = 17.7+2$. THEREFORE,

$$11^{104} \equiv_{17} 11^{16.6+8} \equiv_{17} (11^6)^{16} . 11^8 \equiv_{17} 1^{16} . 11^8 \equiv_{17} 11^8 \equiv_{17} (11^2)^4 \equiv_{17} 2^4 \equiv_{17} 16 \equiv_{17} -1.$$

WE THUS HAVE $11^{104} \equiv_{17} -1$ WHICH SHOWS 17 DIVIDES $11^{104}+1$.

EXERCISE 2: IF $\gcd(a,35)=1$ SHOW THAT $a^{12} \equiv_{35} 1$.

SOLUTION: SUPPOSE THAT $\gcd(a,35)=1$. THEN $\gcd(a,5) \in \{a,5\}$. IF $\gcd(a,5)=5$ THEN $5 \mid a$ AND $5 \mid 35$ IMPLY THAT $5 \mid \gcd(a,5)=1$. THIS SHOWS $\gcd(a,5)=1$. SIMILARLY, $\gcd(a,7)=1$. WE THEN OBSERVE $5 \nmid a$, $7 \nmid a$ AND SINCE 5, 7 ARE PRIMES, BY FERMAT'S THEOREM, $a^6 \equiv_7 1$ AND $a^4 \equiv_5 1$. WE THUS HAVE

$$a^{12} \equiv_7 a^{6.2} \equiv_7 (a^6)^2 \equiv_7 1^2 \equiv_7 1 \quad \text{AND} \quad a^{12} \equiv_5 a^{4.3} \equiv_5 (a^4)^3 \equiv_5 1^3 \equiv_5 1.$$

THIS SHOWS THAT $7 \mid a^{12}-1$ AND $5 \mid a^{12}-1$. SINCE $\gcd(7,5)=1$ WE THEREFORE HAVE $7.5 \mid a^{12}-1$. THIS SHOWS $a^{12} \equiv_{35} 1$.

EXERCISE 3: IF $\gcd(a,133) = \gcd(b,133) = 1$ SHOW THAT $133 \mid a^{18} - b^{18}$.

SOLUTION: WE FIRST OBSERVE THAT $133 = 7.19$. SINCE $\gcd(a,133) = 1$ THEN $\gcd(a,7) = \gcd(a,19) = 1$. SIMILARLY, AS $\gcd(b,133) = 1$ WE GET $\gcd(b,7) = \gcd(b,19) = 1$. THEN, SINCE 7 DOES NOT DIVIDE a NOR b, BY FERMAT'S THEOREM, $a^6 \equiv_7 1$ AND $b^6 \equiv_7 1$. THIS SHOWS $a^6 - b^6 \equiv_7 0$ AND SO $7 \mid a^6 - b^6$. SIMILARLY, SINCE $19 \nmid a$ NOR $19 \nmid b$ WE HAVE $a^{18} \equiv_{19} 1 \equiv_{19} b^{18}$ WHICH IMPLIES $19 \mid a^{18} - b^{18}$. SINCE $\gcd(7,19) = 1$, WE THUS HAVE $7.19 \mid a^{18} - b^{18}$. THE RESULT FOLLOWS.

EXERCISE 4: FROM FERMAT'S THEOREM DEDUCE THAT 13 DIVIDES $11^{12m+6} + 1$ FOR ANY INTEGER $m \geq 0$.

SOLUTION: SINCE $13 \nmid 11$ WE HAVE $11^{12} \equiv_{13} 1$ BY FERMAT'S THEOREM. THEN $11^{12m} \equiv_{13} (11^{12})^m \equiv_{13} 1^m \equiv_{13} 1$. WE ALSO OBSERVE THAT $121 = 13.9 + 4$ AND $64 = 13.5 - 1$. WE THEREFORE HAVE $11^6 \equiv_{13} (11^2)^3 \equiv_{13} 121^3 \equiv_{13} 4^3 \equiv_{13} 64 \equiv_{13} 13.5 - 1 \equiv_{13} -1$. THIS IMPLIES THAT $11^{12m+6} \equiv_{13} 11^{12m} . 11^6 \equiv_{13} 1.(-1) \equiv_{13} -1$. HENCE, $13 \mid 11^{12m+6} + 1$.

EXERCISE 5: DERIVE EACH OF THE FOLLOWING CONGRUENCES:

(i) $a^{21} \equiv_{15} a$ FOR ALL a, (ii) $a^9 \equiv_{30} a$ FOR ALL a.

SOLUTION:

(i) BY FERMAT'S THEOREM, $a^5 \equiv_5 a$ AND $a^3 \equiv_3 a$. THIS SHOWS THAT

$$a^{21} \equiv_5 a . a^{20} \equiv_5 a . (a^5)^4 \equiv_5 a . a^4 \equiv_5 a^5 \equiv_5 a,$$

$$a^{21} \equiv_3 (a^3)^7 \equiv_3 a^7 \equiv_3 a . a^6 \equiv_3 a . (a^3)^2 \equiv_3 a . a^2 \equiv_3 a^3 \equiv_3 a.$$

THEN, $5 \mid a^{21} - a$ AND $3 \mid a^{21} - a$. AS $\gcd(3,5) = 1$, WE GET $3.5 \mid a^{21} - a$. THIS SHOWS THAT $a^{21} \equiv_{15} a$.

(ii) BY FERMAT'S THEOREM, $a^5 \equiv_5 a$, $a^3 \equiv_3 a$ AND $a^2 \equiv_2 a$. THEN,

$$a^9 \equiv_5 a^5 \cdot a^4 \equiv_5 a \cdot a^4 \equiv_5 a^5 \equiv_5 a,$$

$$a^9 \equiv_3 (a^3)^3 \equiv_3 a^3 \equiv_3 a,$$

$$a^9 \equiv_2 (a^2)^4 \cdot a \equiv_2 a^4 \cdot a \equiv_2 (a^2)^2 \cdot a \equiv_2 a^2 a \equiv_2 a \cdot a \equiv_2 a^2 \equiv_2 a.$$

THIS SHOWS THAT $5 \mid a^9 - a$, $3 \mid a^9 - a$ AND $2 \mid a^9 - a$. NOTE THAT $30 = 5 \cdot 3 \cdot 2$ AND THAT $\gcd(5,3,2) = 1$. WE THEREFORE HAVE $30 \mid a^9 - a$ WHICH MEANS $a^9 \equiv_{30} a$.

EXERCISE 6: IF $7 \nmid a$ PROVE THAT EITHER a^3+1 OR a^3-1 IS DIVISIBLE BY 7.

SOLUTION: BY FERMAT'S THEOREM WE HAVE $a^6 \equiv_7 1$. THEN, $7 \mid a^6 - 1$. WE ALSO OBSERVE $a^6 - 1 = (a^3+1) \cdot (a^3-1)$. IF $7 \mid a^3+1$ WE ARE DONE. SUPPOSE NEXT $7 \nmid a^3+1$. THEN, $\gcd(7, a^3+1) = 1$. WE THUS HAVE THAT $7 \mid a^3 - 1$.

EXERCISE 7: LET p BE A PRIME AND $\gcd(a,p) = 1$. USE FERMAT'S THEOREM TO VERIFY THAT $x \equiv_p a^{p-2} b$ IS A SOLUTION OF $ax \equiv_p b$. SOLVE $6x \equiv_{11} 5$.

SOLUTION: BY FERMAT'S THEOREM $a^{p-1} \equiv_p 1$. SUPPOSE $ax \equiv_p b$. THEN, $a^{p-2} \cdot ax \equiv_p a^{p-2} b$. BUT $a^{p-2} \cdot a x \equiv_p a^{p-1} x \equiv_p 1 \cdot x \equiv_p x$. THEN, $x \equiv_p a^{p-2} b$.

WE NOW USE WHAT WE PROVE TO SOLVE $6x \equiv_{11} 5$. IT FOLLOWS THAT $x \equiv_{11} 6^9 \cdot 5$.

SO, $x \equiv_{11} 6^9 \cdot 5 \equiv_{11} (6^2)^4 \cdot 6 \cdot 5 \equiv_{11} 3^4 \cdot (-3) \equiv_{11} 4 \cdot (-3) \equiv_{11} -12 \equiv_{11} -1 \equiv_{11} 10$. HENCE, $x \equiv_{11} 10$.

EXERCISE 8: ASSUMING THAT a AND b ARE INTEGERS NOT DIVISIBLE BY THE PRIME p, PROVE:

(i) IF $a^p \equiv_p b^p$ THEN $a \equiv_p b$.

(ii) IF $a^p \equiv_p b^p$ THEN $a^p \equiv_{p^2} b^p$.

SOLUTION: ASSUME $p \nmid a$, $p \nmid b$. THEN $a^p \equiv_p a$ AND $b^p \equiv_p b$.

(i) WE OBSERVE $a \equiv_p a^p \equiv_p b^p \equiv_p b$ WHICH IMPLIES $a \equiv_p b$.

(ii) BY (i), $a \equiv_p b$. SO, $p \mid b-a$. THEN, $b = pk + a$ FOR SOME $k \in \mathbb{Z}$.

THEN, $a^p - b^p = a^p - (pk+a)^p = a^p - \sum_{j=0}^{p} \binom{p}{j} \cdot (pk)^j \cdot a^{p-j} = -\sum_{j=1}^{p} \binom{p}{j} \cdot (pk)^j \cdot a^{p-j}$

$$= -p^2 \cdot k \cdot a^{p-1} - \sum_{j=2}^{p} \binom{p}{j} p^j k^j a^{p-j}$$

$$= p^2 \cdot \left(-k a^{p-1} - \sum_{j=2}^{p} \binom{p}{j} p^{j-2} k^j a^{p-j} \right)$$

THUS, $p^2 \mid a^p - b^p$ WHICH IMPLIES $a^p \equiv_{p^2} b^p$.

EXERCISE 9: EMPLOY FERMAT'S THEOREM TO PROVE THAT, IF p IS AN ODD PRIME, THEN $1^{p-1} + 2^{p-1} + 3^{p-1} + \dots + (p-1)^{p-1} \equiv_p -1$.

SOLUTION: SUPPOSE THAT p IS AN ODD INTEGER. THEN $p \geq 3$. IF $a < p$ THEN $p \nmid a$ AND SO, $a^{p-1} \equiv_p 1$ BY FERMAT'S THEOREM. THEN,

$$\sum_{a=1}^{p-1} a^{p-1} \equiv_p \sum_{a=1}^{p-1} 1 \equiv_p p-1 \equiv_p -1.$$

WE OBSERVE THE RESULT HOLDS EVEN FOR $p=2$ SINCE $1 = (p-1)^{p-1}$ AND $1 \equiv_2 -1$.

EXERCISE 10: EMPLOY FERMAT'S THEOREM TO PROVE THAT, IF p IS AN ODD PRIME, THEN $1^p + 2^p + 3^p + \dots + (p-1)^p \equiv_p 0$.

SOLUTION: BY FERMAT'S THEOREM, $a^p \equiv_p a$. THEN,

$$\sum_{a=1}^{p-1} a^p \equiv_p \sum_{a=1}^{p-1} a \equiv_p \frac{p \cdot (p-1)}{2} \equiv_p \frac{p \cdot 2k}{2} \equiv_p pk \equiv_p 0$$ SINCE $p-1$ IS EVEN AS p IS odd.

EXERCISE 11: PROVE THAT IF p IS AN ODD PRIME AND k IS AN INTEGER SATISFYING $1 \leq k \leq p-1$ THEN $\binom{p-1}{k} \equiv_p (-1)^k$.

SOLUTION: IF $P=2$, IT TRIVIALLY HOLDS. ASSUME $P \geq 3$. WE NOTE

$$k! \binom{P-1}{k} = \frac{(P-1)!}{(P-k-1)!} = \prod_{j=1}^{k} (P-j).$$ SINCE $P-j \equiv_P -j$,

$$k! \binom{P-1}{k} \equiv_P \prod_{j=1}^{k} (P-j) \equiv_P \prod_{j=1}^{k} -j \equiv_P (-1)^k \cdot k!$$. THIS SHOWS THAT

$P \mid k! \left[\binom{P-1}{k} - (-1)^k \right]$. SINCE $1 \leq k \leq P-1$ WE HAVE $P \nmid k!$. HENCE,

P DIVIDES $\binom{P-1}{k} - (-1)^k$ WHICH SHOWS $\binom{P-1}{k} \equiv_P (-1)^k$.

EXERCISE 13: ASSUME THAT P AND q ARE DISTINCT ODD PRIMES SUCH THAT $P-1 \mid q-1$. IF $\gcd(a, Pq) = 1$ SHOW THAT $a^{q-1} \equiv_{Pq} 1$.

SOLUTION: SINCE P, q ARE DISTINCT PRIMES AND $\gcd(a, Pq) = 1$, WE HAVE $\gcd(a, P) = \gcd(a, q) = 1$. THEN, BY FERMAT'S THEOREM, $a^{P-1} \equiv_P 1$ AND $a^{q-1} \equiv_q 1$. SINCE $P-1 \mid q-1$ WE HAVE $q-1 = k(P-1)$ FOR SOME $k \in \mathbb{Z}$. SO,

$a^{q-1} \equiv_P a^{(P-1)k} \equiv_P (a^{P-1})^k \equiv_P 1^k \equiv_P 1$. THEN, $P \mid a^{q-1} - 1$. SINCE WE ALSO HAVE $q \mid a^{q-1} - 1$ AND $\gcd(P, q) = 1$, $Pq \mid a^{q-1} - 1$. HENCE $a^{q-1} \equiv_{Pq} 1$.