# Fermat's Little Theorem Solutions

Joseph Zoller

September 27, 2015

## Solutions

1. Find $3^{31}$ mod 7.

   [Solution: $3^{31} \equiv 3 \bmod 7$]

   By Fermat's Little Theorem, $3^6 \equiv 1 \bmod 7$. Thus, $3^{31} \equiv 3^1 \equiv 3 \bmod 7$.

2. Find $2^{35}$ mod 7.

   [Solution: $2^{35} \equiv 4 \bmod 7$]

   By Fermat's Little Theorem, $2^6 \equiv 1 \bmod 7$. Thus, $2^{35} \equiv 2^5 \equiv 32 \equiv 4 \bmod 7$.

3. Find $128^{129}$ mod 17.

   [Solution: $128^{129} \equiv 9 \bmod 17$]

   By Fermat's Little Theorem, $128^{16} \equiv 9^{16} \equiv 1 \bmod 17$. Thus, $128^{129} \equiv 9^1 \equiv 9 \bmod 17$.

4. (1972 AHSME 31) The number $2^{1000}$ is divided by 13. What is the remainder?

   [Solution: $2^{1000} \equiv 3 \bmod 13$]

   By Fermat's Little Theorem, $2^{12} \equiv 1 \bmod 13$. Thus, $2^{1000} \equiv 2^{400} \equiv 2^{40} \equiv 2^4 \equiv 16 \equiv 3 \bmod 13$.

5. Find $29^{25}$ mod 11.

   [Solution: $29^{25} \equiv 10 \bmod 11$]

   By Fermat's Little Theorem, $29^{10} \equiv 7^{10} \equiv 1 \bmod 11$. Thus, $29^{25} \equiv 7^5 \equiv 7(-4)^4 \equiv 7 \cdot 256 \equiv 7 \cdot 3 \equiv 21 \equiv 10 \bmod 11$.

6. Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ mod 7.

   [Solution: $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 0 \bmod 7$]

   By Fermat's Little Theorem, $2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \bmod 7$. Thus, $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 2^2 + 3^0 + 4^4 + 5^2 + 6^0 \equiv 4 + 1 + 2^8 + 25 + 1 \equiv 4 + 1 + 4 + 4 + 1 \equiv 14 \equiv 0 \bmod 7$.

7. Let

   $$a_1 = 4 \ , \ a_n = 4^{a_{n-1}} \ , \ n > 1$$

   Find $a_{100}$ mod 7.

   [Solution: $a_{100} \equiv 4 \bmod 7$]

   By Fermat's Little Theorem, $4^6 \equiv 1 \bmod 7$. Now, $4^a \equiv 4 \bmod 6$ for all positive $a$. Thus, $4^{a_k} \equiv 4 \bmod 6$ for all positive $k$, which also means that $a_{k+1} \equiv 4 \bmod 6$ for all positive $k$. Let $a_{99} = 4 + 6t$ for some integer $t$. Then,

$$a_{100} \equiv 4^{a_{99}} \equiv 4^{4+6t} \equiv 4^4(4^6)^t \equiv 256 \equiv 46 \equiv 4 \bmod 7$$

(Actually $a_n \equiv 4 \bmod 7$ for all $n \geq 1$.)

8. Solve the congruence

$$x^{103} \equiv 4 \bmod 11.$$

[Solution: $x \equiv 5 \bmod 11$]

By Fermat's Little Theorem, $x^{10} \equiv 1 \bmod 11$. Thus, $x^{103} \equiv x^3 \bmod 11$. So, we only need to solve $x^3 \equiv 4 \bmod 11$. If we try all the values from $x = 1$ through $x = 10$, we find that $5^3 \equiv 4 \bmod 11$. Thus, $x \equiv 5 \bmod 11$.

9. Find all integers $x$ such that $x^{86} \equiv 6 \bmod 29$.

[Solution: $x \equiv 8, 21 \bmod 29$]

By Fermat's Little Theorem, $x^{28} \equiv 1 \bmod 29$. Thus, $x^{86} \equiv x^2 \bmod 29$. So, we only need to solve $x^2 \equiv 6 \bmod 29$. This is the same as $x^2 \equiv 64 \bmod 29$, which means that $x^2 - 64 \equiv (x-8)(x+8) \equiv 0 \bmod 29$. Thus, $x \equiv 8, 21 \bmod 29$.

10. What are the possible periods of the sequence $x, x^2, x^3, ...$ in mod 13 for different values of $x$? Find values of $x$ that achieve these periods.

[Solution: $1, 2, 3, 4, 6, 12$]

By Fermat's Little Theorem, $x^{12} \equiv 1 \pmod{13}$. Thus, every cyclic length has to be a factor of 12, because after 12 iterations, every cyclic should be back where it started. Thus, the possible cycle lengths are: $1, 2, 3, 4, 6, 12$.

$$\text{Cycle length} = 1 : x = 1\ (1)$$
$$\text{Cycle length} = 12 : x = 2\ (1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7)$$

Since 2 has a maximum side length, we can take powers of 2 to get the other cycle lengths:

$$\text{Cycle length} = 2 : x = 2^{12/2} = 2^6 = 64 \implies x = 12\ (1, 12)$$
$$\text{Cycle length} = 3 : x = 2^{12/3} = 2^4 = 16 \implies x = 3\ (1, 3, 9)$$
$$\text{Cycle length} = 4 : x = 2^{12/4} = 2^3 = 8 \implies x = 8\ (1, 8, 12, 5)$$
$$\text{Cycle length} = 6 : x = 2^{12/6} = 2^2 = 4 \implies x = 4\ (1, 4, 3, 12, 9, 10)$$

11. If a googolplex is $10^{10^{100}}$, what day of the week will it be a googolplex days from now? (Today is Sunday)

[Solution: Thursday (4 days from today)]

By Fermat's Little Theorem, $10^6 \equiv 1 \pmod 7$. Thus, we want to find out what $10^{100}$ is in mod 6. Notice that

$$10^2 = 100 \equiv 4 \equiv 10 \pmod 6$$

Thus, by induction it is true that $10^k \equiv$ '$10 \equiv 4 \pmod 6 \implies 10^{100} \equiv 4 \pmod 6$.
Therefore, I can say that $10^{100} = 6c + 4$ for some positive integer $c$. By substituting, we get that

$$10^{10^{100}} = 10^{6c+4} = (10^6)^c 10^4 \implies 10^{10^{100}} \equiv (1)^c 100^2 \equiv 100^2 \equiv 2^2 \equiv 4 \pmod 7$$

This means that googolplex is 4 more than a multiple of 7, which means the day of the week will increase by 4. Therefore, in googolplex days it will be a Thursday.

12. Suppose that $p$ and $q$ are distinct primes, $a^p \equiv a \pmod q$, and $a^q \equiv a \pmod p$. Prove that $a^{pq} \equiv a \pmod{pq}$.

    [Proof:]

    By Fermat's Little Theorem, we know that $a^p \equiv a \pmod p$ and $a^q \equiv a \pmod q$ no matter what integer $a$ is. Combining with what is given, we have that

$$\begin{aligned} a^p \equiv a \pmod p &\implies (a^p)^q \equiv a^q \equiv a \pmod p \implies a^{pq} \equiv a \pmod p \\ a^q \equiv a \pmod q &\implies (a^q)^p \equiv a^p \equiv a \pmod q \implies a^{pq} \equiv a \pmod q \end{aligned}$$

    This means that $a^{pq} = px + a = qy + a$ for some integers $x$ and $y$. However, this then implies that $px = qy \implies x = qk, y = pk$ for some integer $k$, because $p$ and $q$ are both prime. Thus, $a^{pq} = p(qk) + a = q(pk) + a = (pq)k + a \implies a^{pq} \equiv a \pmod{pq}$. □

13. Find all positive integers $x$ such that $2^{2^x+1} + 2$ is divisible by 17.

    [Solution: $x = 2$]

    First, we need find when $2^a + 2$ is divisible by 17, where $a$ is some positive integer. This is exactly when

$$2^a + 2 \equiv 0 \pmod{17} \iff 2^a \equiv -2 \equiv 15 \equiv 32 \pmod{17}$$

    Thus, $a = 5$ is smallest solution.
    By Fermat's Little Theorem, we know that $2^{16} \equiv 1 \pmod{17}$. Thus, the cycle created by 2 has to have a length divisible by 16. Notice that $2^4 \equiv 16 \equiv -1 \pmod{17} \implies 2^8 \equiv (-1)^2 \equiv 1 \pmod{17}$, so the cycle has a length of 8 because this is the smallest power possible. Thus, $2^a + 2 \equiv 0 \pmod{17}$ exactly when $a \equiv 5 \pmod 8$.

    Next, we need to find all $x$ such that $2^x + 1 \equiv 5 \pmod 8$. Simplify to get

$$2^x + 1 \equiv 5 \pmod 8 \iff 2^x \equiv 4 \pmod 8$$

    This is only true when $x = 2$, because for all greater powers, $2^x$ is divisible by 8, so the congruency will never be true again.

    Thus, $2^{2^x+1} + 2$ is divisible by 17 $\iff x = 2$.

14. An alternative proof of Fermat's Little Theorem, in two steps:

    (a) Show that $(x+1)^p \equiv x^p + 1 \pmod p$ for every integer $x$, by showing that the coefficient of $x^k$ is the same on both sides for every $k = 0, ..., p$.

    [Proof:]

    $(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k = 1 + x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k \equiv 1 + x^p + \sum_{k=1}^{p-1} 0x^k \pmod p = 1 + x^p \pmod p$

    because $\binom{p}{k}$ has a factor of $p$ in it when $0 < k < p$. □

    (b) Show that $x^p \equiv x \pmod p$ by induction over $x$.

    [Proof:]

    First, we must show the base case is true for $x = 0$: $0^p \equiv 0 \pmod p$. ✓

    Second, we must prove the inductive case. Assume that $x^p \equiv x \pmod p$. Then, from part (a) we know that:

$$(x+1)^p \equiv x^p + 1 \pmod p \equiv (x) + 1 \pmod p \equiv (x+1) \pmod p$$

Thus, by induction, we have shown that $x^p \equiv x \pmod p$ for every integer $x$

15. Let $p$ be an odd prime. Expand $(x-y)^{p-1}$, reducing the coefficients mod $p$.

[Solution: $(x-y)^{p-1} \equiv \displaystyle\sum_{k=0}^{p-1} x^{p-1-k} y^k \pmod p$]

First of all, we know that

$$(x-y)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} x^{p-1-k}(-y)^k = \sum_{k=0}^{p-1} \frac{(p-1)!}{k!(p-1-k)!}(-1)^k x^{p-1-k} y^k$$

By Wilson's Theorem, we know that $(p-1)! \equiv -1 \pmod p$.
Also, we can examine $k!$:

$$\begin{aligned}
k! = (k)(k-1)...(1) &\equiv (k-p)(k-1-p)...(1-p) \pmod p \\
&\equiv (p-k)(p-k+1)...(p-1)(-1)^k \pmod p \\
&\equiv (-1)^k (p-1)...(p-(k-1))(p-k) \pmod p \\
\implies k!(p-1-k)! &\equiv (-1)^k (p-1)...(p-(k-1))(p-k)(p-1-k)! \pmod p \\
&\equiv (-1)^k (p-1)! \pmod p \\
\implies k!(p-1-k)! &\equiv (-1)^k (p-1)! \pmod p \\
\implies 1 &\equiv \frac{(p-1)!}{k!(p-1-k)!}(-1)^k \pmod p
\end{aligned}$$

because $k!$ and $(p-1-k)!$ are relatively prime to $p$, since $p$ is prime and they have no factors of $p$. Thus, by substituting, we get that

$$(x-y)^{p-1} = \sum_{k=0}^{p-1} \frac{(p-1)!}{k!(p-1-k)!}(-1)^k x^{p-1-k} y^k \equiv \sum_{k=0}^{p-1} x^{p-1-k} y^k \pmod p$$

so every coefficient is reduced to 1 in mod $p$.