Euler's Totient Theorem

Misha Lavrov

ARML Practice 11/11/2012

Example

We want to be able to solve the following type of problem:

Problem (VTRMC 2012/4.)

What are the last two digits of $\underbrace{3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}}_{2012 \text{ times}}$ *?*

Review of modular arithmetic

- We say that $a \equiv b \pmod{m}$ if the difference $a - b$ is divisible by m.
- Also, $a \bmod m$ is defined to be the unique b in the set $\{0, 1, 2, \ldots, m-1\}$ such that $a \equiv b \pmod{m}$.

Review of modular arithmetic

- We say that $a \equiv b \pmod{m}$ if the difference $a - b$ is divisible by m.
- Also, $a \bmod m$ is defined to be the unique b in the set $\{0, 1, 2, \ldots, m-1\}$ such that $a \equiv b \pmod{m}$.
- We are allowed to add, subtract, multiply modular equations just like regular equations.
- However, division does not always work:

$$4 \equiv 14 \pmod{10} \quad \text{but} \quad {}^{4}/_{2} \not\equiv {}^{14}/_{2} \pmod{10}.$$

Review of modular arithmetic

- We say that $a \equiv b \pmod{m}$ if the difference $a - b$ is divisible by m.
- Also, $a \bmod m$ is defined to be the unique b in the set $\{0, 1, 2, \ldots, m-1\}$ such that $a \equiv b \pmod{m}$.
- We are allowed to add, subtract, multiply modular equations just like regular equations.
- However, division does not always work:

$$4 \equiv 14 \pmod{10} \quad \text{but} \quad {}^{4}/_{2} \not\equiv {}^{14}/_{2} \pmod{10}.$$

- Our goal is to find out how to simplify $a^b \bmod m$.

Powers modulo a prime

Problem

What is $3^{2012} \bmod 17$*?*

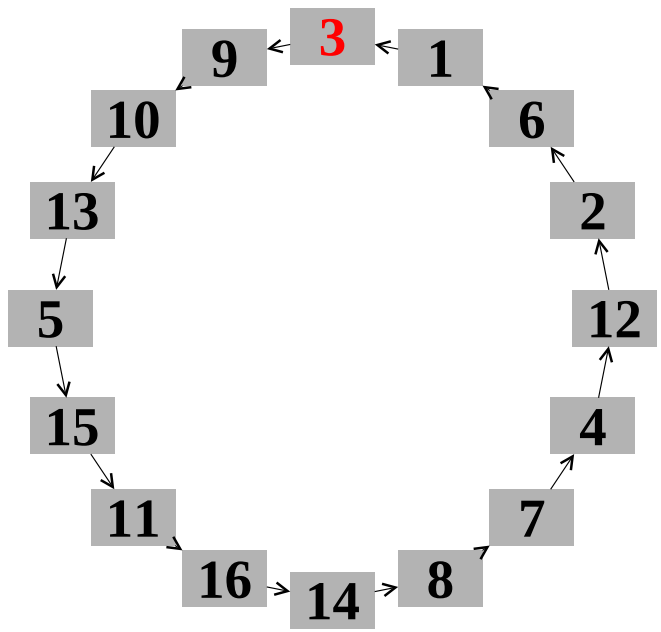
Powers modulo a prime

Problem

What is $3^{2012} \bmod 17$*?*

Solution

The powers of 3 *mod* 17 *go around in a circle like this:*



Since $2012 = 125 \cdot 16 + 12$, $3^{2012} \equiv 3^{12} \equiv 4 \pmod{17}$.

Questions

- How could we have guessed ahead of time that there would be 16 steps around the circle?

Questions

- How could we have guessed ahead of time that there would be 16 steps around the circle?

  Answer: The 16 steps are the remainders $\{1, \ldots, 16\}$. Since 3^k is never divisible by 17, those are all we can get.

Questions

- How could we have guessed ahead of time that there would be 16 steps around the circle?

  Answer: The 16 steps are the remainders $\{1, \ldots, 16\}$. Since 3^k is never divisible by 17, those are all we can get.

- Is it possible that we loop around without hitting all the remainders?

Questions

- How could we have guessed ahead of time that there would be 16 steps around the circle?

  Answer: The 16 steps are the remainders $\{1, \ldots, 16\}$. Since 3^k is never divisible by 17, those are all we can get.

- Is it possible that we loop around without hitting all the remainders?

  Answer: Yes. For example, the values of 2^k mod 17 are $2 \to 4 \to 8 \to 16 \to 15 \to 13 \to 9 \to 1 \to 2$.

Questions

- How could we have guessed ahead of time that there would be 16 steps around the circle?

  Answer: The 16 steps are the remainders $\{1, \ldots, 16\}$. Since 3^k is never divisible by 17, those are all we can get.

- Is it possible that we loop around without hitting all the remainders?

  Answer: Yes. For example, the values of 2^k mod 17 are $2 \to 4 \to 8 \to 16 \to 15 \to 13 \to 9 \to 1 \to 2$.

- Can the loops be of any size less than 16?

Questions

- How could we have guessed ahead of time that there would be 16 steps around the circle?

  Answer: The 16 steps are the remainders $\{1, \ldots, 16\}$. Since 3^k is never divisible by 17, those are all we can get.

- Is it possible that we loop around without hitting all the remainders?

  Answer: Yes. For example, the values of 2^k mod 17 are $2 \to 4 \to 8 \to 16 \to 15 \to 13 \to 9 \to 1 \to 2$.

- Can the loops be of any size less than 16?

  Answer: No. Consider the values of $3 \cdot 2^k$ mod 17: $3 \to 6 \to 12 \to 7 \to 14 \to 11 \to 5 \to 10 \to 3$.

  This loop has the same length, but never meets the other loop. All such loops together must add up to 16, so their length divides 16. In particular, a^{16} mod 17 is always 1.

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

If p is a prime, then for any integer a not divisible by p,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corollary

We can factor a power a^b as some product $a^{p-1} \cdot a^{p-1} \cdots a^{p-1} \cdot a^c$, where c is some small number (in fact, $c = b \bmod (p-1)$).

When we take $a^b \bmod p$, all the powers of a^{p-1} cancel, and we just need to compute $a^c \bmod p$.

Fermat's Little Theorem: Exercises

Problem (1972 AHSME #31)

The number 2^{1000} *is divided by 13. What is the remainder?*

Fermat's Little Theorem: Exercises

Problem (1972 AHSME #31)

The number 2^{1000} *is divided by 13. What is the remainder?*

Solution

We know that $2^{12} \equiv 1 \pmod{13}$. *So we first take out as many factors of* 2^{12} *as possible. We can write* 1000 *as* $83 \cdot 12 + 4$ *(which is another way of saying that* $1000 \equiv 4 \pmod{12}$. *So*

$$2^{1000} = 2^{12 \cdot 83 + 4} = (2^{12})^{83} \cdot 2^4 \equiv 2^4 = 16 \equiv 3 \pmod{13}.$$

What happens when the modulus isn't prime?

- What does the loop for 3^k mod 10 (last digit of 3^k) look like?

What happens when the modulus isn't prime?

- What does the loop for 3^k mod 10 (last digit of 3^k) look like?

$$3 \to 9 \to 7 \to 1 \to 3.$$

This takes 4 steps to loop. In particular, after $10 - 1 = 9$ steps we will *not* be back at 3.

What happens when the modulus isn't prime?

- What does the loop for 3^k mod 10 (last digit of 3^k) look like?

$$3 \to 9 \to 7 \to 1 \to 3.$$

  This takes 4 steps to loop. In particular, after $10 - 1 = 9$ steps we will *not* be back at 3.

- Why does this happen?

What happens when the modulus isn't prime?

- What does the loop for 3^k mod 10 (last digit of 3^k) look like?

$$3 \to 9 \to 7 \to 1 \to 3.$$

This takes 4 steps to loop. In particular, after $10 - 1 = 9$ steps we will *not* be back at 3.

- Why does this happen?

Powers of 3 can never be divisible by 2 and 5. So in addition to excluding the remainder 0, we also exclude 2, 4, 5, 6, and 8. The four remainders above are the only ones left.

Euler's Theorem

Theorem

If a and n have no common divisors, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ is the number of integers in $\{1, 2, \ldots, n\}$ that have no common divisors with n.

So to compute $a^b \bmod n$, first find $\phi(n)$, then calculate $c = b \bmod \phi(n)$. Then all you need to do is compute $a^c \bmod n$.

Wait, but how do we find $\phi(n)$?

- Find $\phi(17)$: the number of integers in $\{1, \ldots, 17\}$ that have no common divisors with 17.
- Find $\phi(81)$.
- Find $\phi(100)$.
- Make a guess for what $\phi(n)$ looks like for as many different kinds of n as you can.

Answers

- $\phi(17) = 16$ because none of the integers in $\{1, \ldots, 17\}$ except 17 itself have any common divisors with 17.

Answers

- $\phi(17) = 16$ because none of the integers in $\{1, \ldots, 17\}$ except 17 itself have any common divisors with 17.
- $\phi(17) = 54$: from the integers $\{1, \ldots, 81\}$ we exclude the ones divisible by 3, of which there are 27.

Answers

- $\phi(17) = 16$ because none of the integers in $\{1, \ldots, 17\}$ except 17 itself have any common divisors with 17.
- $\phi(17) = 54$: from the integers $\{1, \ldots, 81\}$ we exclude the ones divisible by 3, of which there are 27.
- $\phi(100) = 40$. There are two ways to do this:
  - There are 50 numbers in $\{1, \ldots, 100\}$ divisible by 2, which we discard. There are also 20 numbers divisible by 5, which we discard. But 10 numbers were divisible by 10, so we counted them twice. So $\phi(100) = 100 - 50 - 20 + 10 = 40$.
  - Of the numbers in $\{1, \ldots, 100\}$, $1/2$ are not divisible by 2, and $4/5$ are not divisible by 5. So the number that aren't divisible by both is $1/2 \cdot 4/5 \cdot 100 = 40$.

General formula for $\phi(n)$

- First we find a prime factorization of n:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}.$$

General formula for $\phi(n)$

- First we find a prime factorization of n:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}.$$

- For small n, it's easier to do it this way:

$$\phi(n) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) n.$$

General formula for $\phi(n)$

- First we find a prime factorization of n:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}.$$

- For small n, it's easier to do it this way:

$$\phi(n) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) n.$$

- Since $\left(1 - \frac{1}{p_1}\right) p_1^{a_1} = p_1^{a_1 - 1}(p_1 - 1)$, we can write this as

$$\phi(n) = p_1^{a_1 - 1}(p_1 - 1) \cdot p_2^{a_2 - 1}(p_2 - 1) \cdots p_k^{a_k - 1} \cdot (p_k - 1).$$

Euler's Theorem: Exercises

Problem

- *Find the last digit of* 7^{2013}.
- *Find the last two digits of* 2^{2013}. *Note that* 2 *and* 100 *do have a common factor!*

Euler's Theorem: Exercises

Problem

- *Find the last digit of* 7^{2013}.
- *Find the last two digits of* 2^{2013}. *Note that* 2 *and* 100 *do have a common factor!*

Solution

- *Since* $\phi(10) = 4$, *to find* $7^{2013} \bmod 10$ *we find* $2013 \bmod 4 = 1$. *So* $7^{2013} \equiv 7^1 = 7 \pmod{10}$.

Euler's Theorem: Exercises

Problem

- *Find the last digit of* 7^{2013}.
- *Find the last two digits of* 2^{2013}. *Note that* 2 *and* 100 *do have a common factor!*

Solution

- *Since* $\phi(10) = 4$, *to find* $7^{2013} \bmod 10$ *we find* $2013 \bmod 4 = 1$. *So* $7^{2013} \equiv 7^1 = 7 \pmod{10}$.
- *We can find* $2^{2013} \bmod 25$*: since* $\phi(25) = 20$, *this is* $2^{13} \equiv 17$. *This gives us* 4 *possibilities for* $2^{2012} \bmod 100$*: 17, 42, 67, 92. Of these, only* 92 *is possible – the other three aren't divisible by* 4.

The really hard problem

Now let's try to compute $\underbrace{3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}}_{2012 \text{ times}}$ mod 100.

The really hard problem

Now let's try to compute $\underbrace{3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}}_{2012 \text{ times}}$ mod 100.

- We've seen $\phi(100) = 40$. So we need to compute $\underbrace{3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}}_{2011 \text{ times}}$ mod 40, and raise 3 to that power.

The really hard problem

Now let's try to compute $\underbrace{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}_{2012 \text{ times}}$ mod 100.

- We've seen $\phi(100) = 40$. So we need to compute $\underbrace{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}_{2011 \text{ times}}$ mod 40, and raise 3 to that power.
- We recurse to get $\phi(40) = 16$, $\phi(16) = 8$, $\phi(8) = 4$, $\phi(4) = 2$. In particular, $3^k \equiv 3 \pmod 4$ for any k.

The really hard problem

Now let's try to compute $\underbrace{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}_{2012 \text{ times}}$ mod 100.

- We've seen $\phi(100) = 40$. So we need to compute $\underbrace{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}_{2011 \text{ times}}$ mod 40, and raise 3 to that power.
- We recurse to get $\phi(40) = 16$, $\phi(16) = 8$, $\phi(8) = 4$, $\phi(4) = 2$. In particular, $3^k \equiv 3 \pmod 4$ for any k.
- Working backwards, we get that $3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}$ is $3^3 \equiv 3 \bmod 8$, so it's $3^3 \equiv 11 \bmod 16$, so it's $3^{11} \equiv 27 \bmod 40$, so it's $3^{27} \bmod 100$.

The really hard problem

Now let's try to compute $\underbrace{3^{3^{\cdot^{\cdot^{\cdot^3}}}}}_{2012 \text{ times}}$ mod 100.

- We've seen $\phi(100) = 40$. So we need to compute $\underbrace{3^{3^{\cdot^{\cdot^{\cdot^3}}}}}_{2011 \text{ times}}$ mod 40, and raise 3 to that power.
- We recurse to get $\phi(40) = 16$, $\phi(16) = 8$, $\phi(8) = 4$, $\phi(4) = 2$. In particular, $3^k \equiv 3 \pmod 4$ for any k.
- Working backwards, we get that $3^{3^{\cdot^{\cdot^{\cdot^3}}}}$ is $3^3 \equiv 3 \bmod 8$, so it's $3^3 \equiv 11 \bmod 16$, so it's $3^{11} \equiv 27 \bmod 40$, so it's $3^{27} \bmod 100$.
- Handy trick: $3^{27} = 3 \cdot 3^{26} = 3 \cdot (3^{13})^2 = \cdots = 3 \cdot (3 \cdot (27^2)^2)^2$. So we only need to do five multiplications mod 100, and we will end up getting 87.