Euler's Theorem
Lecture 10c: 2022-03-23

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Adapting Fermat's Little Theorem

- Fermat's Little Theorem:
  For prime p, if $a \not\equiv 0 \pmod{p}$, then
  $$a^{p-1} \equiv 1 \pmod{p}$$

- Why? Because the multiples of a are all the numbers in mod p.

- This is also true if $\gcd(a, n) = 1$: then multiples of a mod n are also all the numbers in mod n.

Adapting the proof

- What goes wrong with this attempted proof?

Problems with division

- If $\gcd(a, n) = 1$, then the multiples of a are all numbers in mod n arithmetic.

- Also, if $\gcd(a, n) = 1$, then the reciprocal $\frac{1}{a}$ exists and is unique in mod n arithmetic, so we can always divide by a.

- But, we tried dividing by all non-zero numbers in the previous proof.

- What numbers can we divide by in mod n?

Answer in chat

Using relative primes

Multiplying relative primes

- Claim: if $\gcd(a, n) = 1$, and $\gcd(b\,, n) = 1$, then $\gcd(ab, n) = 1$.

More multiplying relative primes

- Claim: Let $\gcd(a, n) = 1$, $\gcd(b\,, n) = 1$, and $\gcd(c\,, n) = 1$. Then if $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

- This means that each time we multiply by a different relative prime in mod n, we don't get the same thing.

Recall

- Which of the following methods tells you how many numbers smaller than n are relatively prime to n?

A: The Euclidean Algorithm

B: Using the prime factorization $n = 2^{a_2}3^{a_3}5^{a_5}7^{a_7}11^{a_{11}}\cdots$ and then multiplying together to get the product $a_2a_3a_5a_7a_{11}\cdots$

C: Using the prime factorization $n = 2^{a_2}3^{a_3}5^{a_5}7^{a_7}11^{a_{11}}\cdots$ and then multiplying together to get the product

$$(a_2+1)(a_3+1)(a_5+1)(a_7+1)(a_{11}+1)\cdots$$

D: Using the prime factorization of n, and for all the primes $p_1, \ldots, p_k$ that appear in the prime factorization, compute

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

E: None of the above

Euler's Theorem

- Fermat's Little Theorem:
  For prime p, if $a \not\equiv 0 \pmod{p}$, then
  $$a^{p-1} \equiv 1 \pmod{p}$$

- Euler's Theorem:
  For any number n, if $\gcd(a, n) = 1$, then
  $$a^{\phi(n)} \equiv 1 \pmod{n}$$
  where $\phi(n)$ is Euler's totient function counting the number of relative primes smaller than n.

Powers mod 8								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
3	3	1	3	1	3	1	3	1
5	5	1	5	1	5	1	5	1
7	7	1	7	1	7	1	7	1

Powers mod 10								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
3	3	9	7	1	3	9	7	1
7	7	9	3	1	7	9	3	1
9	9	1	9	1	9	1	9	1

Powers mod 14								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
3	3	9	13	11	5	1	3	9
5	5	11	13	9	3	1	5	11
9	9	11	1	9	11	1	9	11
11	11	9	1	11	9	1	11	9
13	13	1	13	1	13	1	13	1

Powers mod 15								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1
4	4	1	4	1	4	1	4	1
7	7	4	13	1	7	4	13	1
8	8	4	2	1	8	4	2	1
11	11	1	11	1	11	1	11	1
13	13	4	7	1	13	4	7	1
14	14	1	14	1	14	1	14	1

Powers mod 18								
	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	1	1	1	1	1	1	1
5	5	7	17	13	11	1	5	7
7	7	13	1	7	13	1	7	13
11	11	13	17	7	5	1	11	13
13	13	7	1	13	7	1	13	7
17	17	1	17	1	17	1	17	1

Proof of Euler's Theorem

- Euler's Theorem:
  For any number n, if $\gcd(a, n) = 1$, then
  $$a^{\phi(n)} \equiv 1 \pmod{n}$$

Application

- $11^{16} \equiv 1 \pmod{60}$

Application

- Compute $2^{75} \pmod{57}$

Try it out

- Compute $3^{84} \pmod{55}$

A: 0
B: 6
C: 25
D: 26
E: None of the above

Try it out

- Compute $6^{55} \pmod{27}$

A: 0
B: 6
C: 25
D: 26
E: None of the above