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
  $$a^{p-1} \equiv 1 \pmod{p}$$
  $2^6 \equiv 1 \mod 7$ $\quad$ $5^{10} \equiv 1 \mod 11$
- Why? Because the multiples of a are all the numbers in mod p.
  multiples of 2: 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, ...
  mod 7: 2, 4, 6, 1, 3, 5, 0, 2, 4, 6, ...
- This is also true if $\gcd(a, n) = 1$: then multiples of a mod n are also all the numbers in mod n.
  Ex. $a = 3$, $n = 10$
  3, 6, 9, 12, 15, 18, 21, 24, 27, 30
  mod 10: 3, 6, 9, 2, 5, 8, 1, 4, 7, 0 ✓

Adapting the proof

- What goes wrong with this attempted proof?

Claim: $3^9 \equiv 1 \mod 10$

proof. $3 \equiv \frac{3}{1} \equiv \frac{6}{2} \equiv \frac{9}{3} \equiv \cdots \equiv \frac{27}{9}$ (A) ←

$\Rightarrow 3^9 \equiv \frac{3}{1} \cdot \frac{6}{2} \cdot \frac{9}{3} \cdot \cdots \cdot \frac{27}{9}$ (B)

$\Rightarrow 3^9 \equiv \frac{3}{1} \cdot \frac{6}{2} \cdot \frac{9}{3} \cdot \frac{2}{4} \cdot \frac{5}{5} \cdot \frac{8}{6} \cdot \frac{1}{7} \cdot \frac{4}{8} \cdot \frac{7}{9}$ (C)

$\Rightarrow 3^9 \equiv 1$ by cancelling out terms. (D) ←

(E) The proof is right

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.

$\frac{1}{3}$ mod 8 exists. But $\frac{1}{2}$ mod 8 doesn't

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

$\frac{3}{1} \cdot \frac{6}{2}$ → need to divide by 2

- What numbers can we divide by in mod n?

Answer in chat

Using relative primes

1, 3, 7, 9

Claim: $3^4 \equiv 1 \mod 10$

proof: $3 \equiv \frac{3}{1} \equiv \frac{6}{2} \equiv \frac{9}{3} \equiv \frac{12}{4} \equiv \frac{15}{5} \equiv \frac{18}{6} \equiv \frac{21}{7} \equiv \frac{24}{8} \equiv \frac{27}{9}$

Thus $3^4 \equiv \frac{3}{1} \cdot \frac{9}{3} \cdot \frac{21}{7} \cdot \frac{27}{9}$

$3^4 \equiv \frac{3}{1} \cdot \frac{9}{3} \cdot \frac{1}{7} \cdot \frac{7}{9}$ ↺ same set of numbers

$\Rightarrow 3^4 \equiv 1 \mod 10$ by canceling terms.

□

Multiplying relative primes

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

answer in chat

proof. Look at prime factorizations of a, b, and n.

Clearly, a & n have no primes in common.

b & n have no primes in common.

So, ab has not primes in common with n.

$\Rightarrow \gcd(ab, n) = 1$.

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 $b \equiv c \pmod{n}$.

proof. Because $\gcd(a,n) = 1$, we can divide by a, ☒

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

Ex. If a_1, a_2, a_3, a_4 are relatively primes to n.

Then a_1^2, $a_1 a_2$, $a_1 a_3$, $a_1 a_4$ are all different numbers mod n.

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

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

E: None of the above

Euler's totient function $\phi(n)$

Euler's Theorem

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

$a^6 \equiv 1 \mod 7$

- 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.

$\phi(10) \equiv 10 \cdot \left(\frac{1}{2}\right) \cdot \left(\frac{4}{5}\right) = 4$

$a^4 \equiv 1 \mod 10$

Powers mod 8 $\phi(8)=4$								
	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 $\phi(10)=4$								
	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 $\phi(14)=6$								
	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 $\phi(15)=8$								
	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
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 $\phi(18)=6$								
	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
  $$a^{\phi(n)} \equiv 1 \pmod{n}$$

proof. Let $a_1, \ldots, a_{\phi(n)}$ be all the relative primes, starting from $a = a_1$.

Then $a \equiv \frac{a a_1}{a_1} \equiv \frac{a a_2}{a_2} \equiv \frac{a a_3}{a_3} \equiv \cdots \equiv \frac{a\, a^{\phi(n)}}{a^{\phi(n)}}$ ($a a_1 = a_1^2$)

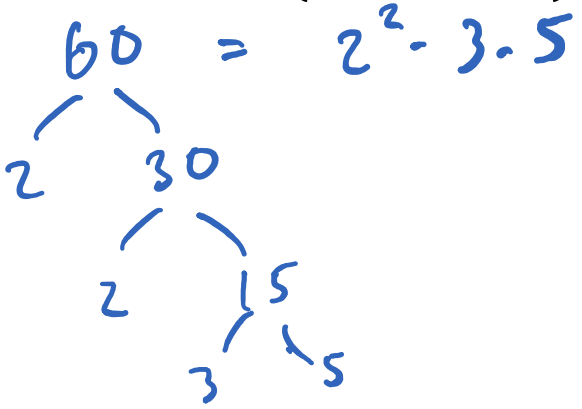
then $a^{\phi(n)} \equiv \frac{a a_1 \cdot a a_2 \cdot a a_3 \cdots a\, a^{\phi(n)}}{a_1 \cdot a_2 \cdot a_3 \cdots a_{\phi(n)}}$ (all diff. relative primes)

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

∎

Application

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



$\phi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$

$\phi(60) = 16$

Also, $\gcd(11, 60) = 1$.

Thus, by Euler's thm,

$11^{16} \equiv 1 \mod 60$.

Application

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

$57 = 3 \cdot 19$ so $\phi(57) = 57 \cdot \frac{2}{3} \cdot \frac{18}{19} = 36$

$\Rightarrow a^{36} \equiv 1 \mod 57$ if $\gcd(a, 57) = 1$

Note $\gcd(2, 57) = 1 \Rightarrow 2^{36} \equiv 1$

$36 \overline{)75}$ 2 r 3

$\frac{72}{3}$

$\Rightarrow 2^{75} \equiv 2^{36 \cdot 2 + 3}$

$\equiv 2^{36 \cdot 2} \cdot 2^3$

$\equiv 2^3 \equiv 8 \mod 57$

If p is prime, $\phi(p) = p\left(1 - \frac{1}{p}\right) = p \cdot \frac{p-1}{p}$

$= p - 1$

Try it out

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

$55 = 5 \cdot 11$ $\quad \phi(55) = 55 \cdot \frac{4}{5} \cdot \frac{10}{11} = 40$

Also, $\gcd(3, 55) = 1$

Thus, $3^{40} \equiv 1 \mod 55$

$\Rightarrow 3^{84} \equiv 3^{40 \cdot 2} \cdot 3^4 \equiv 3^4 \mod 55$

$\equiv 81 \equiv 26 \mod 55$

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

Try it out

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

gcd [6, 27) = 3, so can't use Euler's Thm

Incorrect: $\phi(27) = 27 \cdot \frac{2}{3} = 18$

$6^{18} \equiv 1$

$6^{55} \equiv 6^{18 \cdot 3 + 1} \equiv 6 \mod 27$

WRONG

$6 \equiv 6$

$6^2 = 36 \equiv 9$

$6^4 = 81 \equiv 0$

$6^{55} \equiv 6^4 \cdot 6^{51} \equiv 0 \cdot 6^{51} \equiv 0$

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