Oscar, Nathan, Germaine

Math 251, Wed 17-Nov-2021 -- Wed 17-Nov-2021
Discrete Mathematics
Fall 2021

Wednesday, November 17th 2021

Wk 12, Fr
Topic:: Fast modular exponentiation
Read:: Rosen 4.2
~~HW(([illegible] due Sat.~~

Modular congruence
- definition $\qquad a \equiv b \pmod{m} \longleftrightarrow m \mid a-b$
- equivalence classes
- Z_m
    - as a set
    - equipped with addition and multiplication
    - lack of a "cancellation rule"

Note that

$$40 \equiv 5 \pmod{7}$$
$$47 \equiv 5 \pmod{7}$$
$$54 \equiv 5 \pmod{7}$$
$$-2 \equiv 5 \pmod{7}$$

In fact

represents the list

$$\ldots, -16, -9, -2, 5, 12, 19, 26, \ldots \quad \text{are all congruent mod } 7.$$

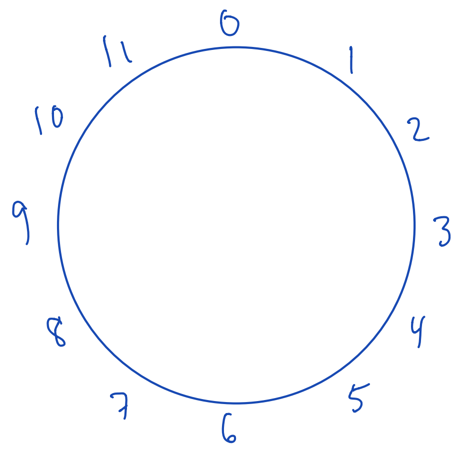
equivalence classes mod 7

$$\left\{\begin{array}{l}
\ldots, -16, -9, -2, 5, 12, 19, 26, \ldots \\
\ldots, -17, -10, -3, 4, 11, 18, 25, \ldots \\
\ldots, -18, -11, -4, 3, 10, 17, 24, \ldots \\
\ldots, -19, -12, -5, 2, 9, 16, \ldots \\
\ldots, -20, -13, -6, 1, 8, 15, \ldots \\
\ldots, -21, -14, -7, 0, 7, 14, \ldots \\
\ldots, -22, -15, -8, -1, 6, 13, \ldots
\end{array}\right.$$

Define $\mathbb{Z}_7$ to be the collection of representatives $\{0, 1, 2, \ldots, 6\}$

w/ $+, \cdot$ operations carried out mod 7.

Have been working in $\mathbb{Z}_{12}$ most of your life.



Solve equations?

$3x + 4 \equiv 2 \pmod{5}$, find x

$x \equiv 1 \pmod{5}$

Test intuition:

1. If $a \equiv b \pmod{m}$, $c \in \mathbb{Z}$

   Does it follow that $ac \equiv bc \pmod{m}$? Answer: Yes

   Assume $a \equiv b \pmod{m} \longrightarrow m \mid a - b$

   Ask $ac \equiv bc \pmod{m}$, by checking $m \mid ac - bc = (a-b)c$

2. If $ac \equiv bc \pmod{m}$,

   does it follow that $a \equiv b \pmod{m}$? Ans: No

   Counterexample:

   $3 \cdot 2 \equiv 3 \cdot 4 \pmod{6}$ but $2 \not\equiv 4 \pmod{6}$

   Modular arithmetic does not support a cancellation law, generally, only works when the modulus is prime.

Fast Modular Exponentiation is based on these three ideas:

Idea #1: Every positive integer can be written as sums of powers of 2.

Some of the powers of two are

$$\begin{array}{lll} 2^0 = 1 & 2^4 = 16 & 2^8 = 256 \\ 2^1 = 2 & 2^4 = 32 & 2^9 = 512 \\ 2^2 = 4 & 2^4 = 64 & 2^{10} = 1024 \\ 2^3 = 8 & 2^4 = 128 & 2^{11} = 2048 \end{array}$$

and so on. We can write the integers as sums of these powers

$$\begin{array}{rcl} 1 &=& 2^0 \\ 2 &=& 2^1 \\ 3 &=& 1+2 = 2^0 + 2^1 \\ 4 &=& 2^2 \\ 5 &=& 4+1 = 2^2 + 2^0 \\ 6 &=& 4+2 = 2^2 + 2^1 \\ 7 &=& 4+2+1 = 2^2 + 2^1 + 2^0 \\ 8 &=& 2^3 \\ &\vdots& \end{array} \qquad \begin{array}{rcl} 63 &=& 32+16+8+4+2+1 = 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 \\ 64 &=& 2^6 \\ 65 &=& 64+1 = 2^6 + 2^0 \\ &\vdots& \\ 254 &=& 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 \\ 255 &=& 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 \\ 256 &=& 2^8 \\ 257 &=& 256+1 = 2^8 + 2^0 \\ \vdots && \end{array}$$

Idea #2: Arithmetic operations in mod n allow you to "mod" along the way.

$$\begin{aligned} &(27)(33) \bmod 8 \quad \text{is the same as} \quad (27 \bmod 8)(33 \bmod 8) \bmod 8 = (3)(1) \bmod 8 = 3. \\ &(27+33) \bmod 8 \quad \text{is the same as} \quad ((27 \bmod 8) + (33 \bmod 8)) \bmod 8 = (3+1) \bmod 8 = 4. \\ &10^{15} \bmod 13 \quad \text{is the same as} \\ &\quad (5 \cdot 2)^{15} \bmod 13 = (5^{14})(5)(2^{12})(2^3) \bmod 13 = (5^2)^7(5)(2^6)^2(2^3) \bmod 13 \\ &\qquad\qquad\qquad = (-1)^7(5)(-1)^2(2^3) \bmod 13 = (-1)(40) \bmod 13 \\ &\qquad\qquad\qquad = (-1)(40 \bmod 13) \bmod 13 = (-1) \bmod 13 = 12. \end{aligned}$$

Idea #3: Combined squaring

We have

$$\begin{aligned} &(7^2)(5^2) \bmod 11 = (7 \cdot 5)^2 \bmod 11 = 2^2 \bmod 11 = 4, \text{ and} \\ &(31^8)(7^2) \bmod 55 = [(31^2)^2]^2(7^2) \bmod 55 = [(31^2)^2 \cdot 7]^2 \bmod 55 \\ &\qquad\qquad = [(31^2 \bmod 55)^2 \cdot 7]^2 \bmod 55 = [(26)^2 \cdot 7]^2 \bmod 55 \\ &\qquad\qquad = [(26^2 \bmod 55) \cdot 7]^2 \bmod 55 = (16 \cdot 7)^2 \bmod 55 = 2. \end{aligned}$$

Fast modular exponentiation is the result of combining Ideas #1–#3.

Examples:

1. Calculate [redacted] $37^{55} \bmod 89$

$$55 = 32 + 23 = 2^5 + 16 + 7 = 2^5 + 2^4 + 2^2 + 2^1 + 2^0$$

$$\begin{aligned}
37^{55} \bmod 89 &= 37^{32+16+4+2+1} \bmod 89 \\
&= 37^{32} \cdot 37^{16} \cdot 37^{4} \cdot 37^{2} \cdot 37 \bmod 89 \\
&= \left(\left(37^{16} \cdot 37^{8} \cdot 37^{2}\right) \cdot 37\right)^2 \cdot 37 \bmod 89 \\
&= \left(\left(\left(37^{8} \cdot 37^{4}\right) \cdot 37\right)^2 \cdot 37\right)^2 \cdot 37 \bmod 89 \\
&= \left(\left(\left(\left(37^{4} \cdot 37^{2}\right)\right)^2 \cdot 37\right)^2 \cdot 37\right)^2 \cdot 37 \bmod 89 \\
&= \left(\left(\left(\left(37^{2} \cdot 37\right)^2\right)^2 \cdot 37\right)^2 \cdot 37\right)^2 \cdot 37 \bmod 89
\end{aligned}$$

$$= \left(\left(\left(\left(37^2 \bmod 89 \cdot 37 \bmod 89\right)^2 \bmod 89\right)^2 \bmod 89 \cdot 37 \bmod 89\right)^2 \bmod 89 \cdot 37 \bmod 89\right)^2 \bmod 89 \cdot 37 \bmod 89$$

2. Calculate $37^{109} \bmod 4501$,
   We can first use Idea #1 to write the *exponent*

$$109 \;=\; 64+32+8+4+1 \;=\; 2^6+2^5+2^3+2^2+2^0.$$

Thus,

$$\begin{aligned}
87^{109} \bmod 4501 &= 87^{64+32+8+4+1} \bmod 4501 \qquad \text{(Idea \#1)}\\
&= (87)^{64}(87)^{32}(87)^{8}(87)^{4}(87) \bmod 4501 \qquad \text{(algebra)}\\
&= (((((87^2)^2)^2)^2)^2)^2((((87^2)^2)^2)^2)^2((87^2)^2)^2(87^2)^2(87) \bmod 4501 \qquad \text{(algebra)}\\
&= [((((87^2)^2)^2)^2)^2 \cdot (((87^2)^2)^2)^2 \cdot (87^2)^2 \cdot 87^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)}\\
&= [[(((87^2)^2)^2)^2 \cdot ((87^2)^2)^2 \cdot 87^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)}\\
&= [[[((87^2)^2)^2 \cdot (87^2)^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)}\\
&= [[[[(87^2)^2 \cdot 87^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)}\\
&= [[[[[87^2 \cdot 87]^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#3)}\\
&= [[[[[(87^2 \bmod 4501) \cdot 87]^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= [[[[[3068 \cdot 87]^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 87^2 \bmod 4501 = 3068)\\
&= [[[[[3068 \cdot 87 \bmod 4501]^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= [[[[1357^2]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 3068 \cdot 87 \bmod 4501 = 1357)\\
&= [[[[1357^2 \bmod 4501]^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= [[[540^2 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 1357^2 \bmod 4501 = 540)\\
&= [[[(540^2 \bmod 4501) \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= [[[3536 \cdot 87]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 540^2 \bmod 4501 = 3536)\\
&= [[[3536 \cdot 87 \bmod 4501]^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= [[1564^2 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 3536 \cdot 87 \bmod 4501 = 1564)\\
&= [[(1564^2 \bmod 4501) \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= [[2053 \cdot 87]^2]^2(87) \bmod 4501 \qquad \text{(since } 1564^2 \bmod 4501 = 2053)\\
&= [[2053 \cdot 87 \bmod 4501]^2]^2(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= [3072^2]^2(87) \bmod 4501 \qquad \text{(since } 2053 \cdot 87 \bmod 4501 = 3072)\\
&= [3072^2 \bmod 4501]^2(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= 3088^2(87) \bmod 4501 \qquad \text{(since } 3072^2 \bmod 4501 = 3088)\\
&= (3088^2 \bmod 4501)(87) \bmod 4501 \qquad \text{(Idea \#2)}\\
&= (2626)(87) \bmod 4501 \qquad \text{(since } 3088^2 \bmod 4501 = 2626)\\
&= 3412.
\end{aligned}$$

3. See also content at website https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/fast-modular-exponentiation