Oscar, Brayden, Nathan

Math 251, Fri 20-Nov-2020 -- Fri 20-Nov-2020
Discrete Mathematics
Fall 2020

RSA encryption needs
- fast modular exponentiation
- solving modular equations

Friday, November 20th 2020

Wk 12, Fr
Topic:: Euclidean algorithm
Read:: Rosen 4.3
Topic:: Solving congruences
Read:: Rosen 4.4

Arithmetic mod m (need integer $m \geq 2$)

Define $\mathbb{Z}_m$:

both a set of integers $\{0, 1, 2, 3, \ldots, m-1\}$

along with operations

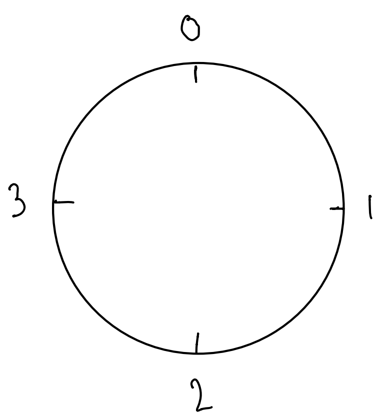
$$a +_m b = a + b \bmod m$$

$$a \cdot_m b = ab \bmod m$$

Ex. Work mod 4 $\quad \mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1



$$27 \cdot_4 (-5) \equiv 3 \cdot_4 (-1) = -3 \bmod 4$$
$$= 1.$$

In $\mathbb{R}$, the solution x to $ax = 1$ is called the multiplicative inverse of a.

In mod 4 arithmetic, 3 is its own multiplicative inverse.

Solving congruence equations

Ex.) Solve $3x + 1 \equiv 2 \pmod 4$

$3x \equiv 1 \pmod 4$ after subtracting 1

Now, since 3 is multiplicative inv. (mod 4) of itself, can multiply both sides by 3

$3 \cdot 3x \equiv 3 \cdot 1 \pmod 4$

$\rightarrow \quad 1x \equiv 3 \pmod 4$

Soln. $x \equiv 3 \pmod 4$

(really means all of these solns:

$\ldots, -5, -1, 3, 7, 11, 15, \ldots$

Hard: Solve

$19x \equiv 51 \pmod{420}$

Underlying question: What is 19's mult. inv. (mod 420)?

Euclidean Algorithm

Our main purpose in learning it: You use it to determine gcd(a, b).

How it works:

Repeatedly do division alg. until remainder of 0.

1. Start with two (usually positive) integers a, b. Call the larger one r_0, the smaller r_1.
2. Iterate the division algorithm:
   - Divide r_0 by r_1—that is, find integers q_1 and r_2 (Note: $0 \leqslant r_2 < r_1$) so that

$$r_0 = q_1 r_1 + r_2$$

   - Shift roles r_1 into the former role of r_0, r_2 into the former role of r_1, and repeat, using the division algorithm to find q_2 and r_3. (Note: $0 \leqslant r_3 < r_2$.)

$$r_1 = q_2 r_2 + r_3$$

We continue to shift roles of the r_j and repeat. This process produces a strictly decreasing sequence

$$r_0,\ r_1,\ r_2,\ \ldots,\ r_n$$

until a remainder, call it r_{n+1}, finally is zero, which is our **stopping criterion**.

Example 1:

Perform the Euclidean algorithm with $a = 276$, $b = 324$, to find gcd(276, 324). ■

Start by labeling larger number r_0, smaller r_1.

$r_0 = 324$, $r_1 = 276$.

$$\overset{r_0}{324} = \overset{r_1}{276} \cdot \overset{q}{\underline{1}} + \underline{48}$$

Notes:

- Call my remainder $r_2 = 48$.
- Any divisor of two-out-of-three in list r_0, r_1, r_2 is a divisor of all three.
- $r_2 < r_1$

See website https://www.extendedeuclideanalgorithm.com/calculator.php.

$$\underset{r_1}{276} = \underset{r_2}{48} \cdot \underline{5} + \underset{r_3}{\underline{36}}$$

Notes:

- Call $r_3 = 36$
- Any divisor of two-out-of-three in list r_1, r_2, r_3 is a divisor of r_0, r_1, r_2 and r_3
- $r_3 < r_2$

$$48 = 36 \cdot \underline{1} + \underline{12}$$

$r_4 = 12$

$$36 = 12 \cdot \underline{3} + \underline{0}$$

gcd = last nonzero remainder

$= 12.$

Example 2:

Perform the Euclidean algorithm with $a = 4312$, $b = 585$. ■

$r_0 = 4312$, $r_1 = 585$

$$4312 = \underline{7}(585) + \underline{217} \quad r_2$$

$$585 = \underline{2}(217) + \underline{151} \quad r_3$$

$$217 = \underline{1}(151) + \underline{66} \quad r_4$$

$$151 = \underline{2}(66) + \underline{19} \quad r_5$$

$$66 = \underline{3}(19) + \underline{9} \quad r_6$$

$$19 = \underline{2}(9) + \underline{1} \quad r_7$$

$$9 = \underline{9}(1) + \underline{0}$$

$\gcd(4312, 585) = 1$, say 4312 and 585 are relatively prime.

Foreshadow: This means 585 has a multiplicative inverse mod 4312.

Extended Euclidean Algorithm

Our main purpose in learning it:

to write gcd(a,b) as a linear combination $ta+sb$

Key theorem based on our Eucl. alg. work

Ex.) Above we found gcd$(324, 276) = 12$

In preparation, solve for remainder

$48 = 36 \cdot 1 + 12 \rightarrow 12 = 48 - 36$

$276 = 48 \cdot 5 + 36 \rightarrow 36 = 276 - (48)(5)$

$324 = 276 \cdot 1 + 48 \rightarrow 48 = 324 - 276$

Now carry out extended Euc. Alg — Writing $12 = t \cdot 324 + s \cdot 276$ w/ $s, t \in \mathbb{Z}$.

$$\begin{aligned} 12 &= 48 - 36 \\ &= 48 - [276 - (48)(5)] \\ &= (48)(6) - 276 \\ &= (324 - 276)(6) - 276 \\ &= (324)6 + (276)(-7) \end{aligned}$$

$a = 324$ $t = 6$ $b = 276$ $s = -7$